

# 含無標籤CTL的CUCM混合模式

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[從非安全模式到混合模式 \(無標籤CTL\)](#)

[從硬體eTokens到無令牌解決方案](#)

[從無標籤解決方案到硬體eTokens](#)

[無令牌的CTL解決方案的證書再生](#)

---

## 簡介

本檔案介紹使用/不使用硬體USB eTokens時Cisco Unified Communications Manager(CUCM)安全性之間的差異。

## 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：

- CUCM版本11.5.1SU3及更高版本的許可證伺服器必須是Cisco Prime License Manager(PLM)11.5.1SU2或更高版本。

這是因為CUCM版本11.5.1SU3需要加密許可證來啟用混合模式，而PLM在11.5.1SU2之前不支援加密許可證。

有關詳細資訊，請參閱[Cisco Prime License Manager版本11.5\(1\)SU2的發行說明](#)。

- 您對CUCM發佈器節點的命令列介面(CLI)具有管理訪問許可權。
- 您可以訪問硬體USB eTokens，並且您的PC上已安裝CTL客戶端外掛，用於要求您遷移回使用硬體eTokens的場景。

為了更清楚的瞭解，此要求僅在您在任何時候都有一個需要USB eToken的場景時才適用。大多數人都需要USB eToken的可能性很小。

- 群集中的所有CUCM節點之間具有完全連線。這一點非常重要，因為CTL檔案通過SSH檔案傳輸協定(SFTP)複製到群集中的所有節點。
- 群集中的資料庫(DB)複製工作正常，伺服器可以即時複製資料。
- 預設情況下，部署中的裝置支援安全(TVS)。

您可以使用Cisco Unified Reporting網頁(https://<CUCM IP或FQDN>/cucreports/)中的Unified CM電話功能清單，確定預設情況下支援安全的裝置。

 注意：預設情況下，Cisco Jabber和許多Cisco TelePresence或Cisco 7940/7960系列IP電話目前不支援安全功能。如果在預設情況下使用不支援安全性的裝置部署無令牌的CTL，則對您的系統進行任何更改發佈伺服器上的CallManager證書的更新都會阻止這些裝置的正常功能，直到手動刪除CTL。預設情況下，支援Security的裝置（例如7945和7965電話或更新版本）能夠在發佈器上的CallManager證書更新時安裝CTL檔案，因為它們可以使用信任驗證服務(TVS)。

## 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10.5.1.10000-7（由兩個節點組成的群集）
- Cisco 7975系列IP電話通過韌體版本SCCP75.9-3-1SR4-1S的瘦客戶端控制協定(SCCP)註冊
- 兩個思科安全令牌，用於使用CTL客戶端軟體將群集設定為混合模式

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。


## 背景資訊

本檔案將說明使用硬體USB電子令牌與不使用硬體USB電子令牌時思科整合通訊管理器(CUCM)安全性之間的差異。

本檔案還介紹涉及無標籤憑證信任清單(CTL)的基本實作案例，以及用來確保系統於變更後正常運作的程式。

無令牌的CTL是CUCM 10.0(1)及更高版本中的一項新功能，允許對IP電話的呼叫信令和媒體進行加密，而無需使用硬體USB eTokens和CTL客戶端外掛，這是以前的CUCM版本中的要求。

使用CLI命令將群集置於混合模式時，CTL檔案使用發佈伺服器節點的CCM+TFTP（伺服器）證書進行簽名，並且CTL檔案中沒有eToken證書。

 注意：在發佈伺服器上重新生成CallManager(CCM+TFTP)證書時，會更改檔案的簽名者。預設情況下不支援安全性的電話和裝置也不接受新的CTL檔案，除非從每台裝置上手動刪除CTL檔案。有關詳細資訊，請參閱本文檔的[要求](#)部分中列出的最後一個要求。


## 從非安全模式到混合模式（無標籤CTL）

本節介紹通過CLI將CUCM集群安全性移至Mixed模式所使用的過程。

在此場景之前，CUCM處於非安全模式，這意味著任何節點上都不存在CTL檔案，並且註冊的IP電話僅安裝身份信任清單(ITL)檔案，如以下輸出所示：

```
<#root>
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.
admin:
```

---

 註：如果在群集未處於混合模式時，在伺服器上找到一個CTL檔案，這意味著群集曾處於混合模式，然後移回非混合模式，並且未從群集中刪除CTL檔案。

命令file delete activelog cm/tftpdata/CTLFile.tlv從CUCM群集中的節點刪除CTL檔案；但是，需要在每個節點上輸入該命令。要清除，僅當伺服器具有CTL檔案且群集未處於混合模式時，才使用此命令。

確認集群是否處於混合模式的簡單方法是使用run sql select paramname , paramvalue from processconfig where paramname='ClusterSecurityMode'命令。如果引數值為0，則集群不處於混合模式。

---

```
run sql select paramname,paramvalue from processconfig where paramname='ClusterSecurityMode'
paramname          paramvalue
=====
ClusterSecurityMode 0
```



為了使用新的無令牌的CTL功能將CUCM群集安全移到混合模式，請完成以下步驟：

1. 獲取對CUCM發佈器節點CLI的管理訪問許可權。
2. 在CLI中輸入utils ctl set-cluster mixed-mode命令：

```
<#root>
```

```
admin:
```

```
utils ctl set-cluster mixed-mode
```

```
This operation sets the cluster to Mixed mode. Do you want to continue? (y/n):y
```

```
Moving Cluster to Mixed Mode
```

```
Cluster set to Mixed Mode
```

```
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster  
that run these services
```

```
admin:
```

3. 導航到CUCM Admin Page > System > Enterprise Parameters，並驗證群集是否已設定為Mixed mode(值1表示Mixed mode):

Security Parameters	
<a href="#">Cluster Security Mode</a> *	1
<a href="#">LBM Security Mode</a> *	Insecure ▼
<a href="#">CAPF Phone Port</a> *	3804
<a href="#">CAPF Operation Expires in (days)</a> *	10
<a href="#">Enable Caching</a> *	True ▼

4. 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。
5. 重新啟動所有IP電話，以便它們可以從CUCM TFTP服務獲取CTL檔案。
6. 若要驗證CTL檔案的內容，請在CLI中輸入show ctl命令。
7. 在CTL檔案中，可以看到CUCM發佈伺服器節點的CCM+TFTP ( 伺服器 ) 證書用於對CTL檔案進行簽名 ( 該檔案在群集中的所有伺服器上都是相同的 )。以下是輸出範例：

```
<#root>
```

```
admin:
```

```
show ctl
```

```
The checksum value of the CTL file:
```

```
0c05655de63fe2a042cf252d96c6d609(MD5)
```

```
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)
```

```
Length of CTL file: 4947
```

```
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015
```

```
[...]
```

```

          CTL Record #:1
          -----
BYTEPOS TAG          LENGTH  VALUE
----- --
1      RECORDLENGTH  2      1156
2      DNSNAME       16     cucm-1051-a-pub
3      SUBJECTNAME   62     CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
          ST=Małopołska;C=PL
4      FUNCTION      2      System Administrator Security Token
5      ISSUENAME     62     CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
          ST=Małopołska;C=PL
6      SERIALNUMBER  16
70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7      PUBLICKEY     140

```

```

8      SIGNATURE      128
9      CERTIFICATE    694      E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
                                     A5 A3 8C 9C (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      1156
2      DNSNAME       16     cucm-1051-a-pub
3      SUBJECTNAME   62     CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                     ST=Małopolska;C=PL
4      FUNCTION      2

```

CCM+TFTP

```

5      ISSUENAME     62     CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
                                     ST=Małopolska;C=PL
6      SERIALNUMBER  16

```

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB

```

7      PUBLICKEY     140
8      SIGNATURE     128
9      CERTIFICATE    694     E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
                                     A5 A3 8C 9C (SHA1 Hash HEX)
10     IPADDRESS      4

```

[...]

The CTL file was verified successfully.

- 在IP電話端，您可以驗證服務重新啟動後，它是否下載了TFTP伺服器上目前存在的CTL檔案（與CUCM的輸出相比，MD5校驗和匹配）：



註：驗證電話上的校驗和時，您會看到MD5或SHA1，具體取決於電話型別。



## 從硬體eTokens到無令牌解決方案

本節介紹如何將CUCM群集安全從硬體eTokens遷移到使用新的無令牌解決方案。

在某些情況下，已使用CTL客戶端在CUCM上配置混合模式，並且IP電話使用包含硬體USB eTokens證書的CTL檔案。

在此場景中，CTL檔案由來自其中一個USB eTokens的證書簽名並安裝在IP電話上。以下提供範例：

```
<#root>
```

```
admin:
```

```
show ctl
```

The checksum value of the CTL file:

```
256a661f4630cd86ef460db5aad4e91c(MD5)
```

```
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
```

The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]

CTL Record #:5

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	ISSUENAME	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 used to sign the CTL file.

The CTL file was verified successfully.





完成以下步驟，以便將CUCM集群安全性移至使用無令牌的CTL:

1. 獲取對CUCM發佈器節點CLI的管理訪問許可權。
2. 輸入utils ctl update CTLFile CLI命令：

```
<#root>
```

```
admin:
```

```
utils ctl update CTLFile
```

```
This operation updates the CTLFile. Do you want to continue? (y/n):y
```

```
Updating CTL file
```

```
CTL file Updated
```

```
Please Restart the TFTP and Cisco CallManager services on all nodes in  
the cluster that run these services
```

3. 在運行這些服務的群集中的所有節點上重新啟動TFTP和CallManager服務。
4. 重新啟動所有IP電話，以便它們可以從CUCM TFTP服務獲取CTL檔案。

5. 在CLI中輸入show ctl命令，以驗證CTL檔案的內容。在CTL檔案中，您可以看到CUCM發佈伺服器節點的CCM+TFTP（伺服器）證書用於對CTL檔案進行簽名，而不是對硬體USB eTokens中的證書進行簽名。
6. 在此案例中，另一個重要的區別是，所有硬體USB eTokens的證書都從CTL檔案中刪除。以下是輸出範例：

```
<#root>
```

```
admin:
```

```
show ctl
```

```
The checksum value of the CTL file:
```

```
1d97d9089dd558a062cccfcb1dc4c57f(MD5)
```

```
3b452f9ec9d6543df80e50f8b850cddc92fcf847(SHA1)
```

```
Length of CTL file: 4947
```

```
The CTL File was last modified on Fri Mar 06 21:56:07 CET 2015
```

```
[...]
```

```
CTL Record #:1
```

```
----
```

```
BYTEPOS TAG          LENGTH  VALUE
```

```
-----
```

BYTEPOS	TAG	LENGTH	VALUE
1	RECORDLENGTH	2	1156
2	DNSNAME	16	cucm-1051-a-pub
3	SUBJECTNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Malopolska;C=PL
4	FUNCTION	2	

```
System Administrator Security Token
```

5	ISSUENAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Malopolska;C=PL
6	SERIALNUMBER	16	

```
70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
```

7	PUBLICKEY	140	
8	SIGNATURE	128	
9	CERTIFICATE	694	E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21 A5 A3 8C 9C (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	1156
2	DNSNAME	16	cucm-1051-a-pub
3	SUBJECTNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopolska;C=PL
4	FUNCTION	2	
<b>CCM+TFTP</b>			
5	ISSUERNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopolska;C=PL
6	SERIALNUMBER	16	
<b>70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB</b>			
7	PUBLICKEY	140	
8	SIGNATURE	128	
9	CERTIFICATE	694	E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21 A5 A3 8C 9C (SHA1 Hash HEX)
10	IPADDRESS	4	
[...]			

The CTL file was verified successfully.



注意：在上述輸出中，如果CUCM發佈伺服器的CCM+TFTP（伺服器）證書未簽署者，請移回基於硬體令牌的群集安全模式，然後再次為無令牌解決方案重複更改。

- 在IP電話端，您可以驗證IP電話重新啟動後，它們下載了更新的CTL檔案版本（與CUCM的輸出相比，MD5校驗和匹配）：



## 從無標籤解決方案到硬體eTokens

本節介紹如何將CUCM群集安全從新的無令牌解決方案遷移回硬體eTokens。

如果使用CLI命令將CUCM群集安全設定為「混合」模式，並且使用CUCM Publisher節點的CCM+TFTP（伺服器）證書對CTL檔案進行簽名，則CTL檔案中不存在來自硬體USB eTokens的證書。

因此，當您運行CTL客戶端以更新CTL檔案（返回使用硬體eTokens）時，將顯示以下錯誤消息：

```
The Security Token you have inserted does not exist in the CTL File  
Please remove any Security Tokens already inserted and insert another  
Security Token. Click Ok when done.
```

在包括將系統降級（當版本切換回）到不包括utils ctl命令的10.x之前版本的情況中，這一點尤其重要。

先前的CTL檔案在刷新或Linux到Linux(L2)的升級過程中被遷移（其內容沒有更改），並且它不包含前面提到的eToken證書。以下是輸出範例：

<#root>

admin:

show ctl

The checksum value of the CTL file:

1d97d9089dd558a062cccfcb1dc4c57f(MD5)

3b452f9ec9d6543df80e50f8b850cddc92fcf847(SHA1)

Length of CTL file: 4947

The CTL File was last modified on Fri Mar 06 21:56:07 CET 2015

Parse CTL File

-----  
Version: 1.2  
HeaderLength: 336 (BYTES)

BYTEPOS	TAG	LENGTH	VALUE
-----	---	-----	-----
3	SIGNERID	2	149
4	SIGNERNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Malopolska;C=PL
5	SERIALNUMBER	16	70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
6	CANAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Malopolska;C=PL
7	SIGNATUREINFO	2	15
8	DIGESTALGORTITHM	1	1
9	SIGNATUREALGOINFO	2	8
10	SIGNATUREALGORTITHM	1	1
11	SIGNATUREMODULUS	1	1
12	SIGNATURE	128	
65	ba 26 b4 ba de 2b 13		
b8	18 2 4a 2b 6c 2d 20		
7d	e7 2f bd 6d b3 84 c5		
bf	5 f2 74 cb f2 59 bc		
b5	c1 9f cd 4d 97 3a dd		
6e	7c 75 19 a2 59 66 49		
b7	64 e8 9a 25 7f 5a c8		
56	bb ed 6f 96 95 c3 b3		
72	7 91 10 6b f1 12 f4		
d5	72 e 8f 30 21 fa 80		
bc	5d f6 c5 fb 6a 82 ec		
f1	6d 40 17 1b 7d 63 7b		
52	f7 7a 39 67 e1 1d 45		
b6	fe 82 0 62 e3 db 57		
8c	31 2 56 66 c8 91 c8		
d8	10 cb 5e c3 1f ef a		
14	FILENAME	12	
15	TIMESTAMP	4	

CTL Record #:1

-----

BYTEPOS	TAG	LENGTH	VALUE
-----	---	-----	-----
1	RECORDLENGTH	2	1156
2	DNSNAME	16	cucm-1051-a-pub
3	SUBJECTNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Malopolska;C=PL

4	FUNCTION	2	System Administrator Security Token
5	ISSUERNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;C=PL
6	SERIALNUMBER	16	

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB

7	PUBLICKEY	140	
8	SIGNATURE	128	
9	CERTIFICATE	694	E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21 A5 A3 8C 9C (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	1156
2	DNSNAME	16	cucm-1051-a-pub
3	SUBJECTNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;C=PL
4	FUNCTION	2	

CCM+TFTP

5	ISSUERNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;C=PL
6	SERIALNUMBER	16	

70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB

7	PUBLICKEY	140	
8	SIGNATURE	128	
9	CERTIFICATE	694	E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21 A5 A3 8C 9C (SHA1 Hash HEX)
10	IPADDRESS	4	

CTL Record #:3

----

BYTEPOS	TAG	LENGTH	VALUE
-----	---	-----	-----
1	RECORDLENGTH	2	1138
2	DNSNAME	16	cucm-1051-a-pub
3	SUBJECTNAME	60	CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;C=PL
4	FUNCTION	2	CAPF
5	ISSUERNAME	60	CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;C=PL
6	SERIALNUMBER	16	74:4B:49:99:77:04:96:E7:99:E9:1E:81:D3:C8:10:9B
7	PUBLICKEY	140	
8	SIGNATURE	128	
9	CERTIFICATE	680	46 EE 5A 97 24 65 B0 17 7E 5F 7E 44 F7 6C 0A F3 63 35 4F A7 (SHA1 Hash HEX)
10	IPADDRESS	4	

CTL Record #:4

----

BYTEPOS	TAG	LENGTH	VALUE
1	RECORDLENGTH	2	1161
2	DNSNAME	17	cucm-1051-a-sub1
3	SUBJECTNAME	63	CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow; ST=Małopolska;C=PL
4	FUNCTION	2	CCM+TFTP
5	ISSUERNAME	63	CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow; ST=Małopolska;C=PL
6	SERIALNUMBER	16	6B:EB:FD:CD:CD:8C:A2:77:CB:2F:D1:D1:83:A6:0E:72
7	PUBLICKEY	140	
8	SIGNATURE	128	
9	CERTIFICATE	696	21 7F 23 DE AF FF 04 85 76 72 70 BF B1 BA 44 DB 5E 90 ED 66 (SHA1 Hash HEX)
10	IPADDRESS	4	

The CTL file was verified successfully.

admin:

在此場景中，完成以下步驟即可安全地更新CTL檔案，而無需使用丟失eTokens的過程（最後從所有IP電話上手動刪除CTL檔案）：

1. 獲取對CUCM發佈器節點CLI的管理訪問許可權。
2. 在發佈器節點CLI中輸入file delete tftp CTLFile.tlv命令以刪除CTL檔案：

```
<#root>
```

```
admin:
```

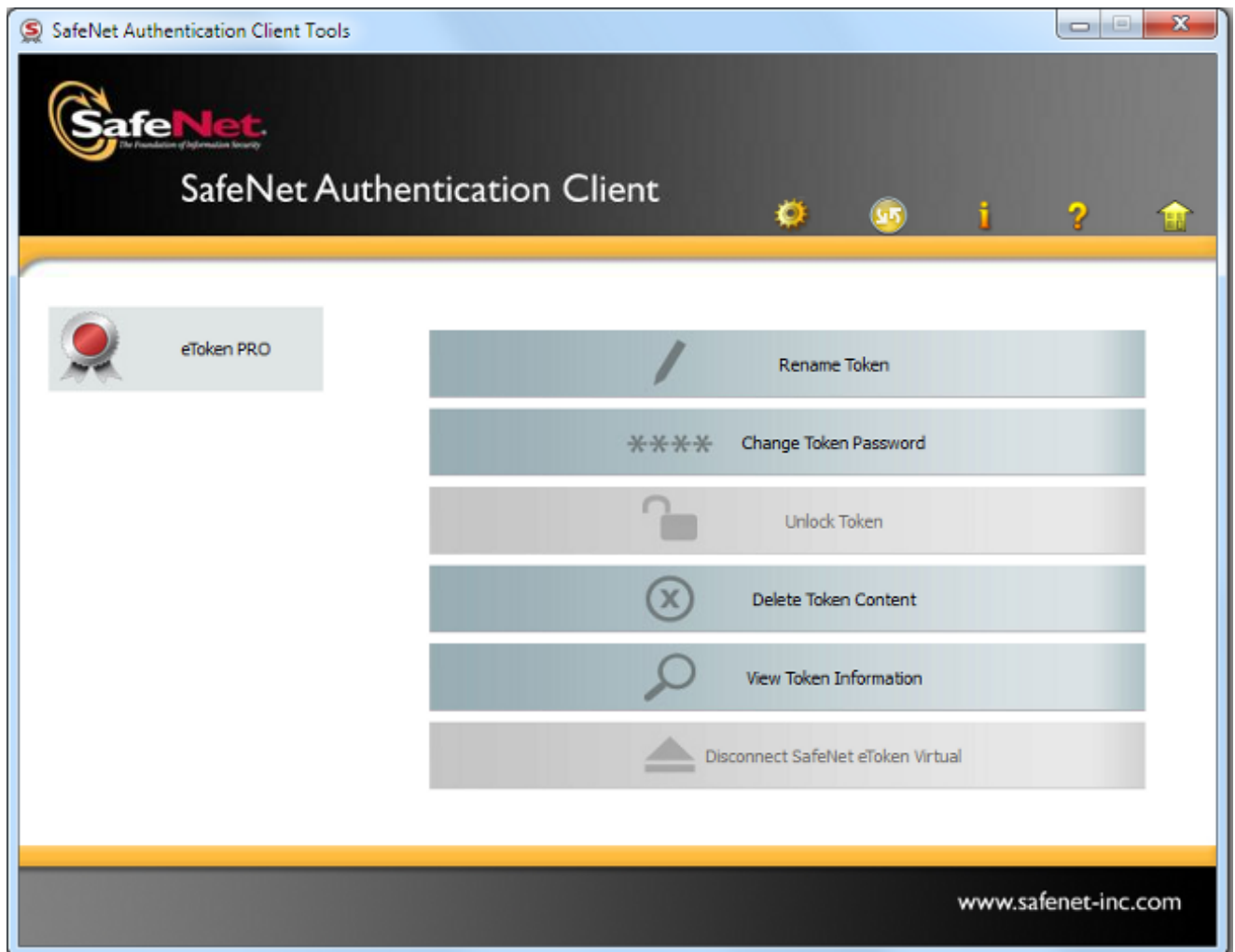
```
file delete tftp CTLFile.tlv
```

```
Delete the File CTLFile.tlv?
```

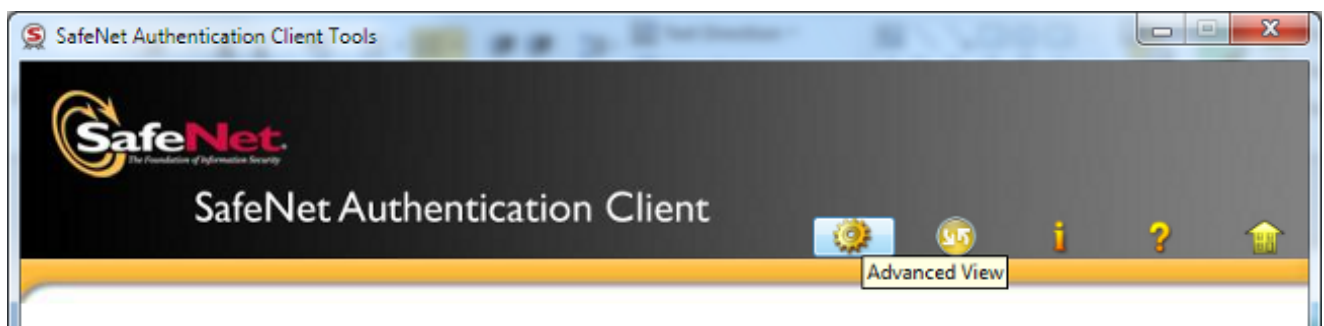
```
Enter "y" followed by return to continue: y
```

```
files: found = 1, deleted = 1
```

3. 在安裝了CTL客戶端的Microsoft Windows電腦上開啟SafeNet身份驗證客戶端（它隨CTL客戶端自動安裝）：



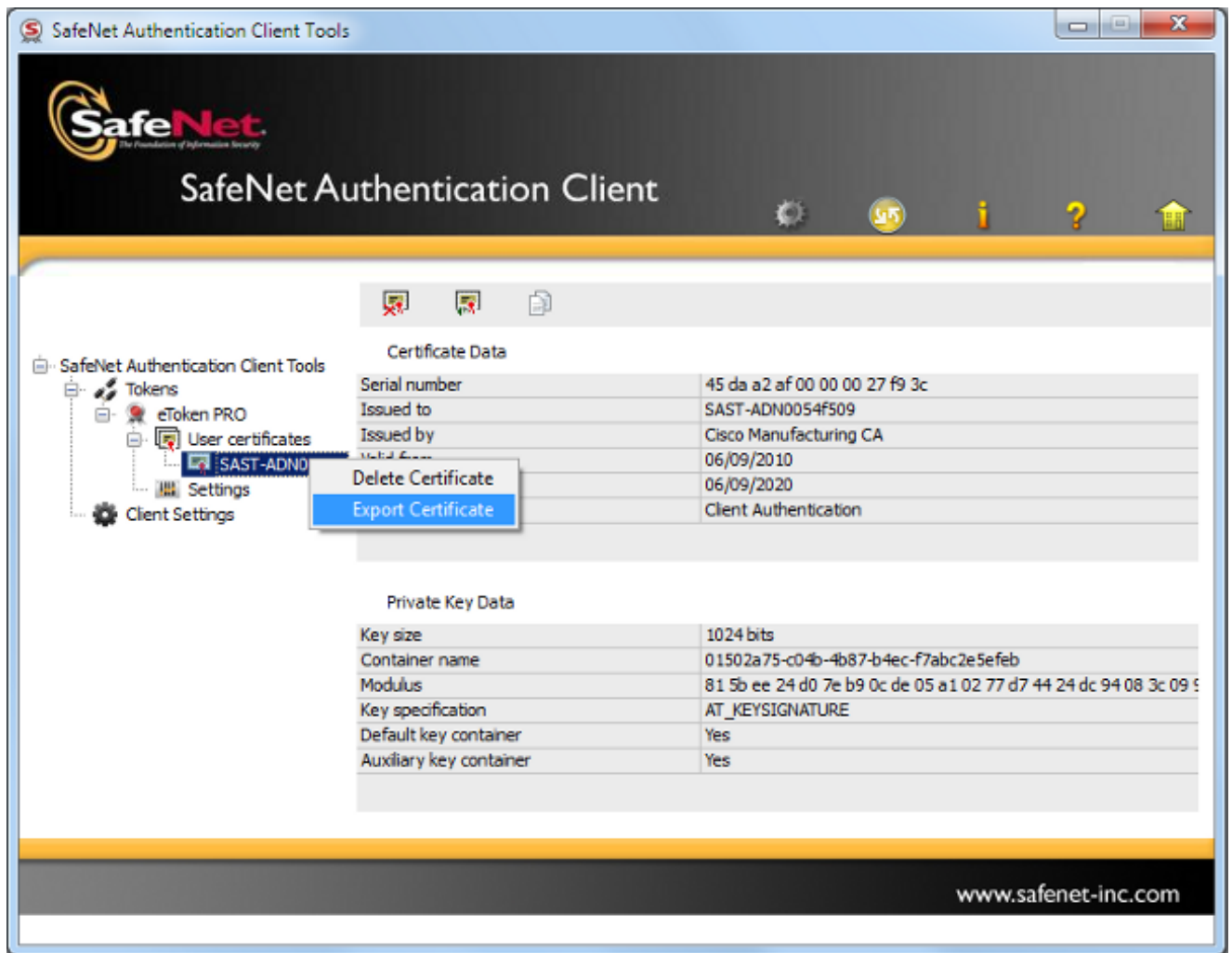
4. 在SafeNet身份驗證客戶端中，導航到高級檢視：



5. 插入第一個硬體USB eToken。

6. 在User certificates資料夾下選擇證書，並將其匯出到PC上的資料夾。當系統提示輸入密碼時，請使用預設密碼Cisco123:

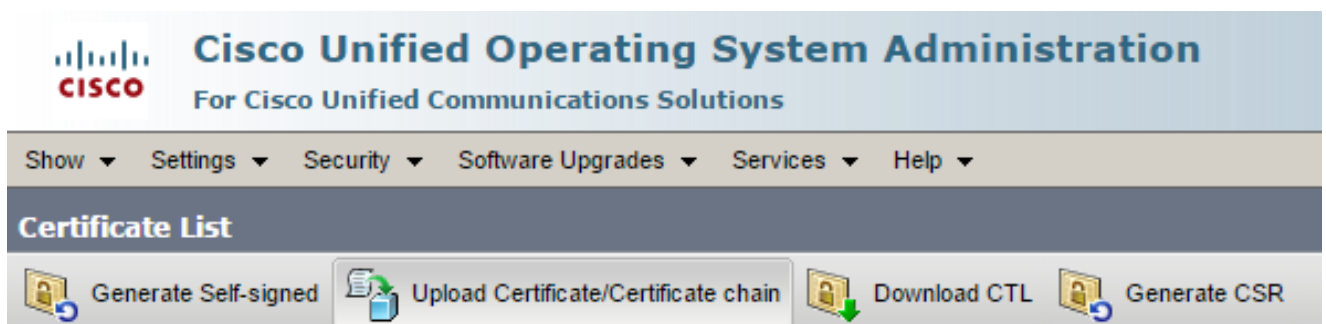




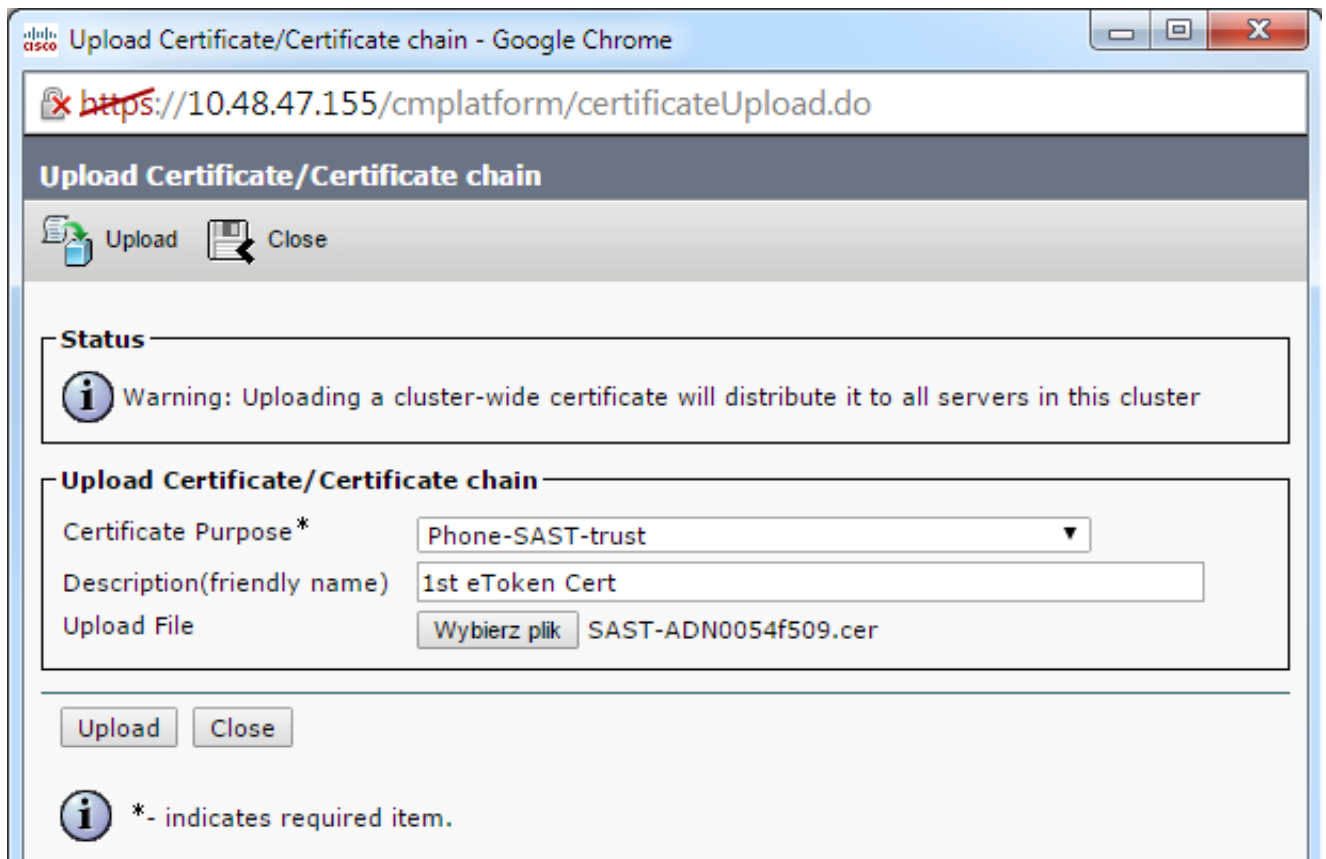
7. 對第二個硬體USB eToken重複以下步驟，以便兩個證書都匯出到PC:

Name	Date modified	Type	Size
SAST-ADN0054f509	06-03-2015 22:32	Security Certificate	1 KB
SAST-ADN008580ef	06-03-2015 22:33	Security Certificate	1 KB

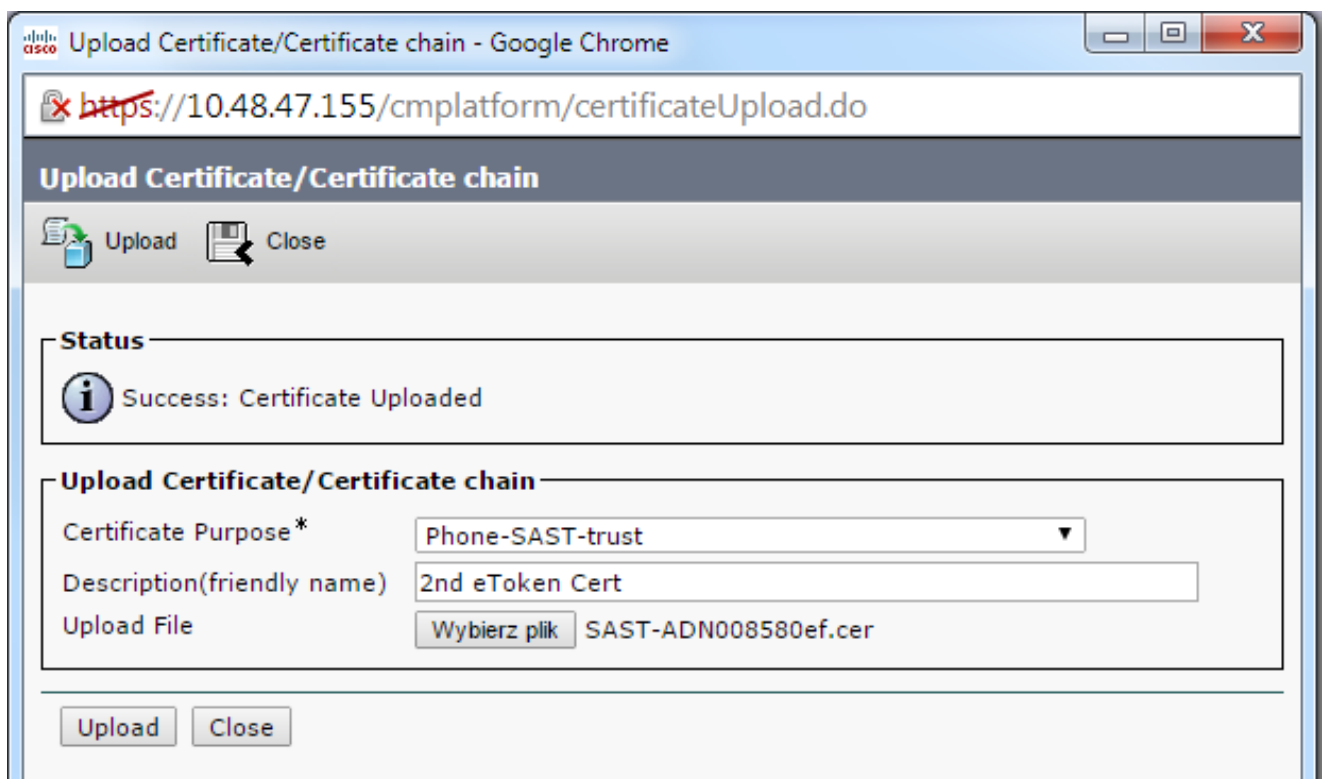
8. 登入思科整合作業系統(OS)管理，然後導覽至安全>憑證管理>上傳憑證:



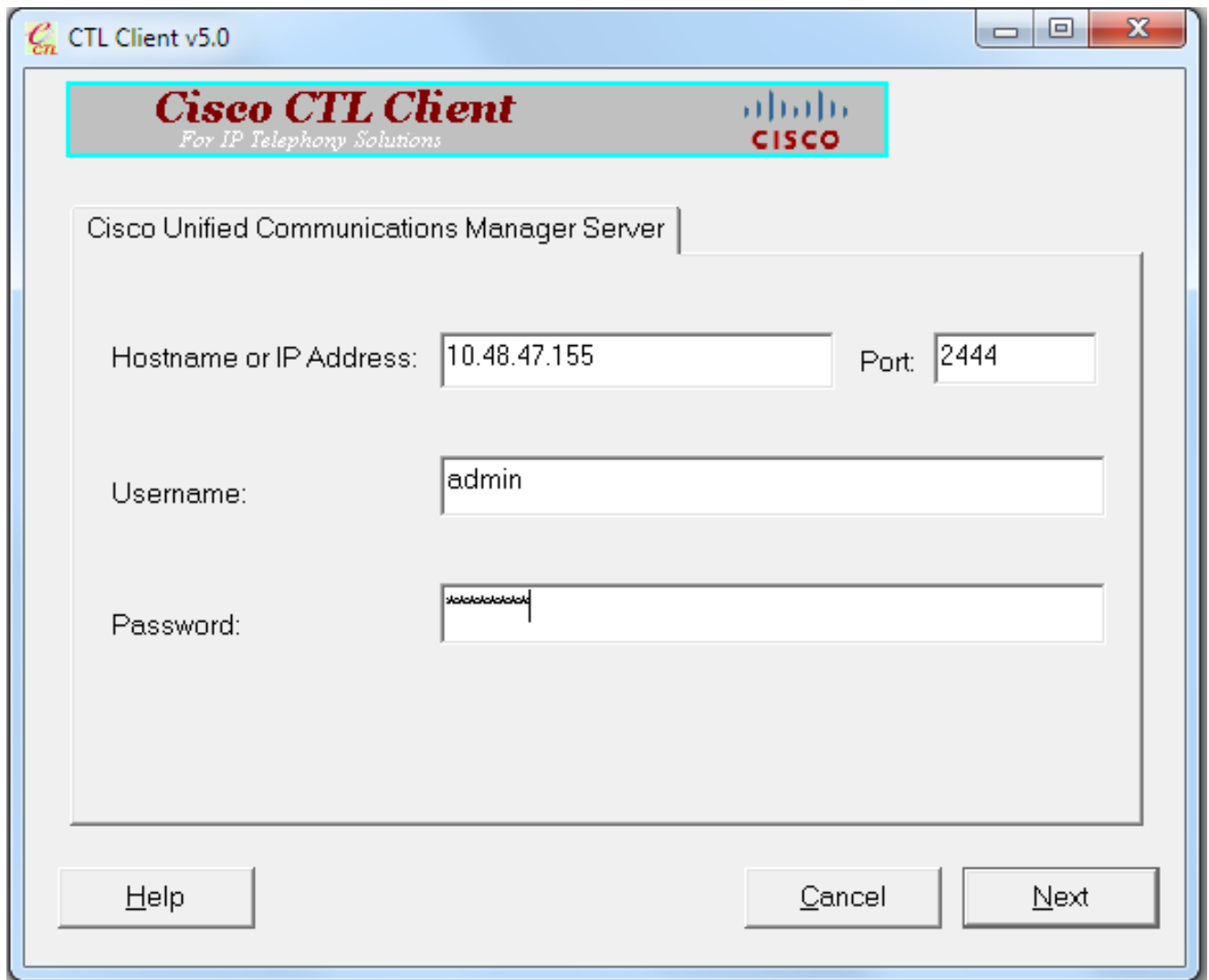
9. 系統將顯示Upload Certificate頁面。從Certificate Purpose下拉選單中選擇Phone-SAST-trust，並選擇您從第一個電子令牌中匯出的證書：



10. 完成前面的步驟，上傳從第二個eToken匯出的證書：



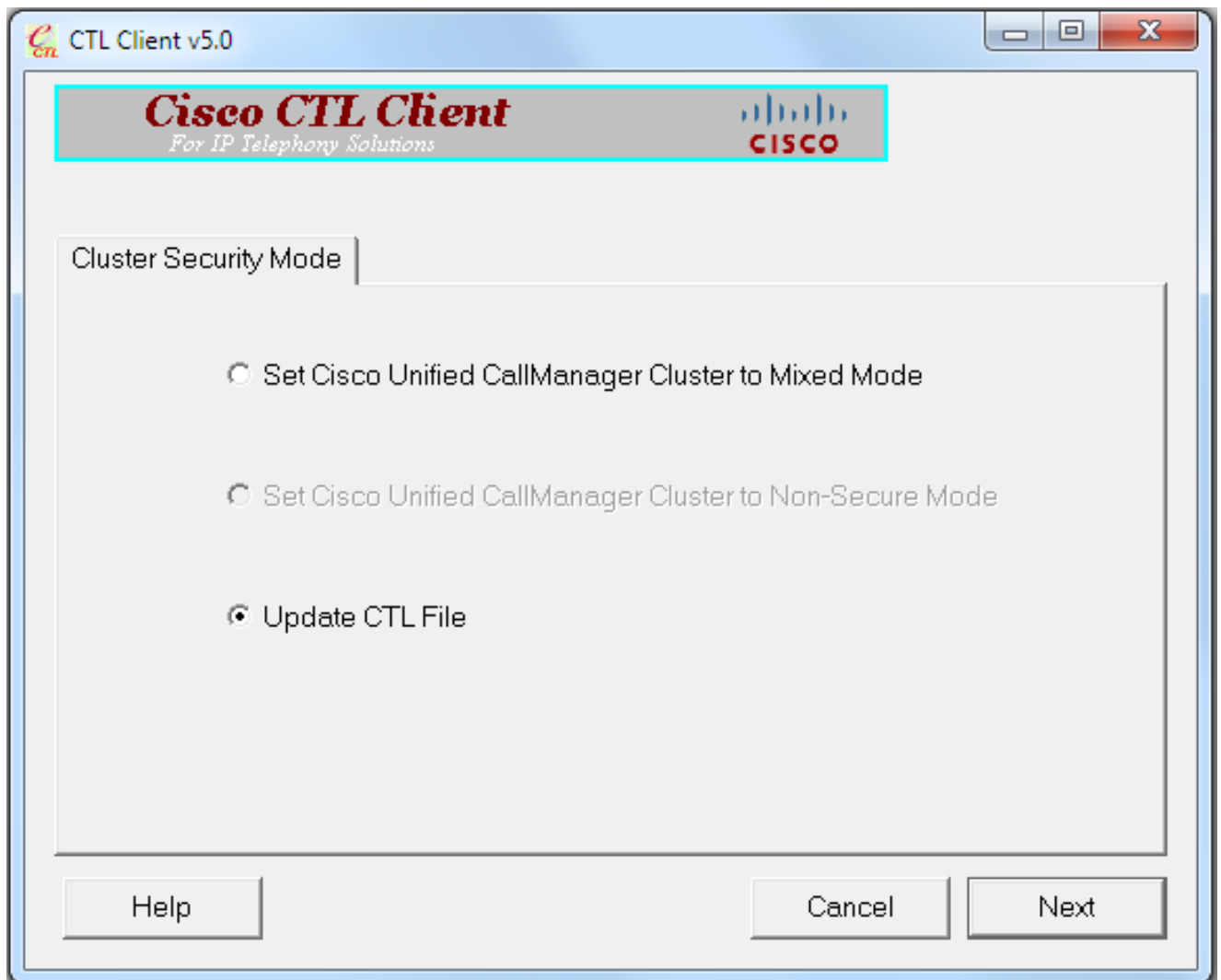
11. 運行CTL客戶端，提供CUCM發佈伺服器節點的IP地址/主機名，並輸入CCM管理員憑據：



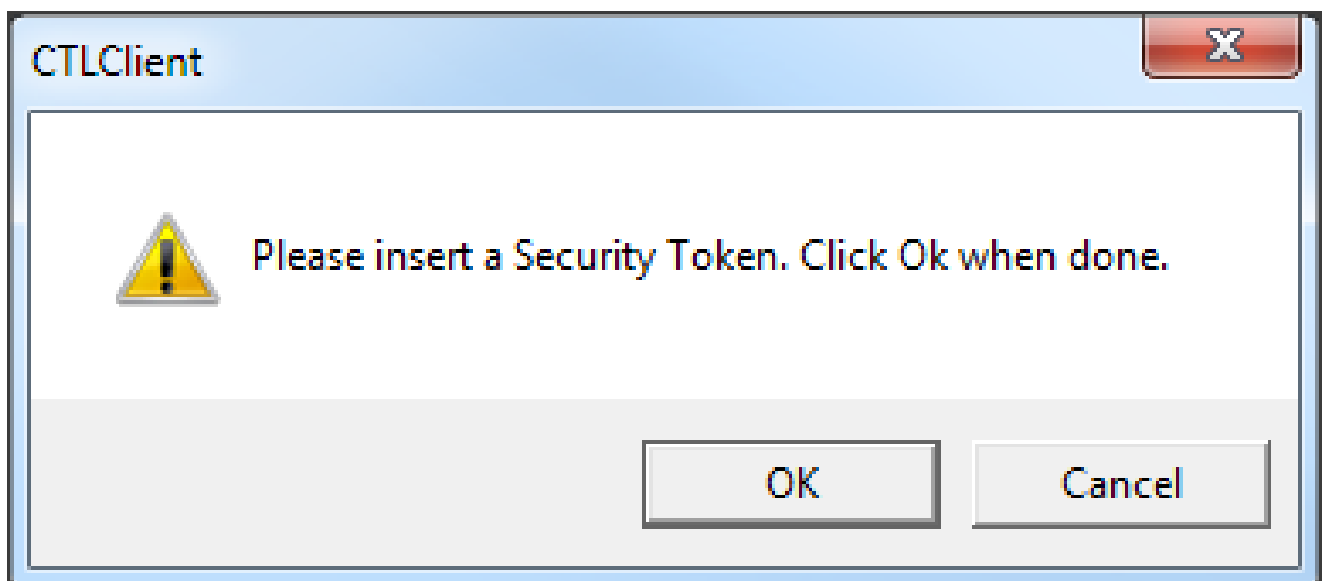
12. 由於群集已經處於混合模式，但發佈器節點上不存在CTL檔案，因此將顯示以下警告消息(按一下OK以忽略它):

No CTL File exists on the server but the Call Manager Cluster Security Mode is in Secure Mode.  
For the system to function, you must create the CTL File and set Call Manager Cluster the Secure Mode.

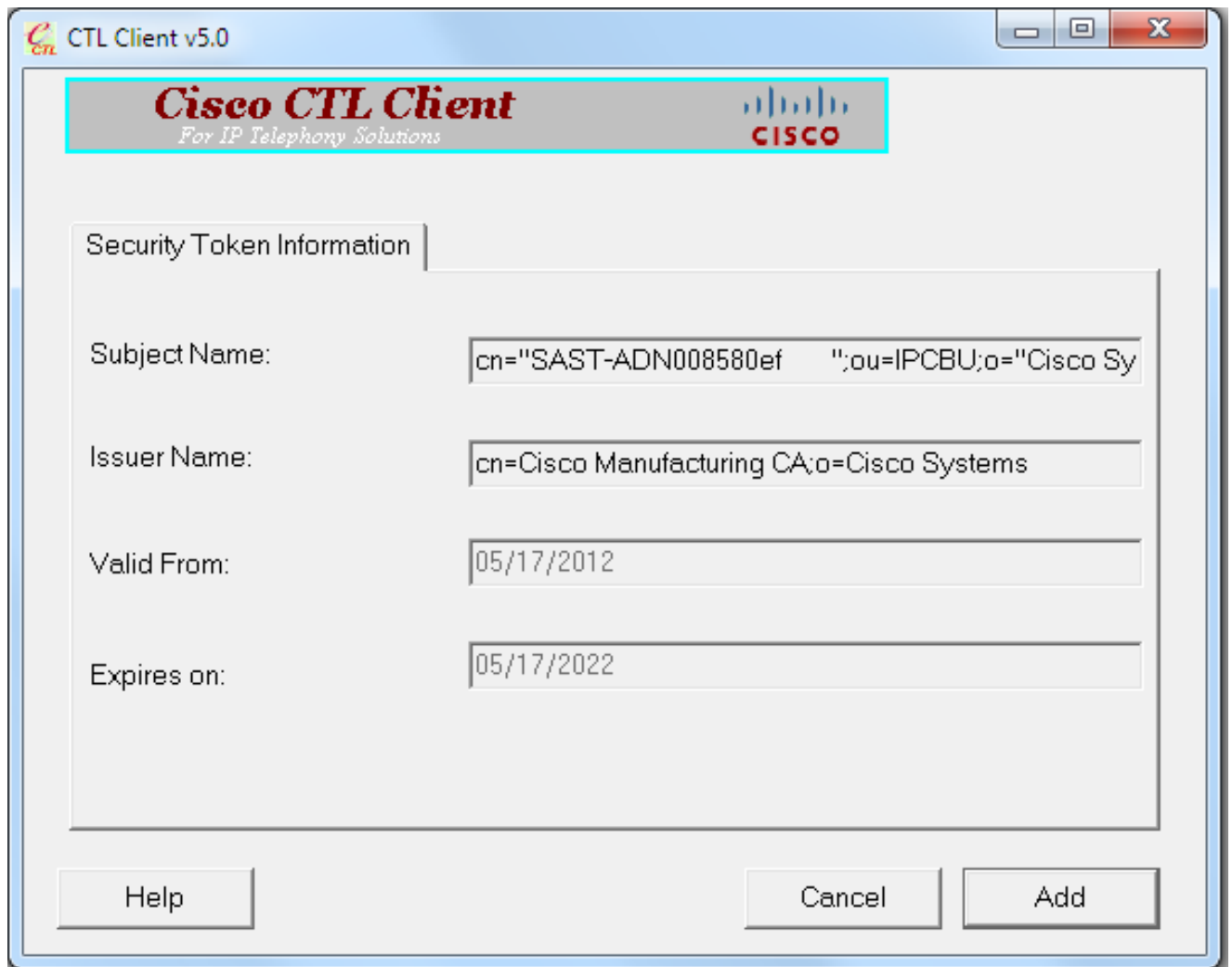
13. 在CTL客戶端中，按一下Update CTL File單選按鈕，然後按一下Next:



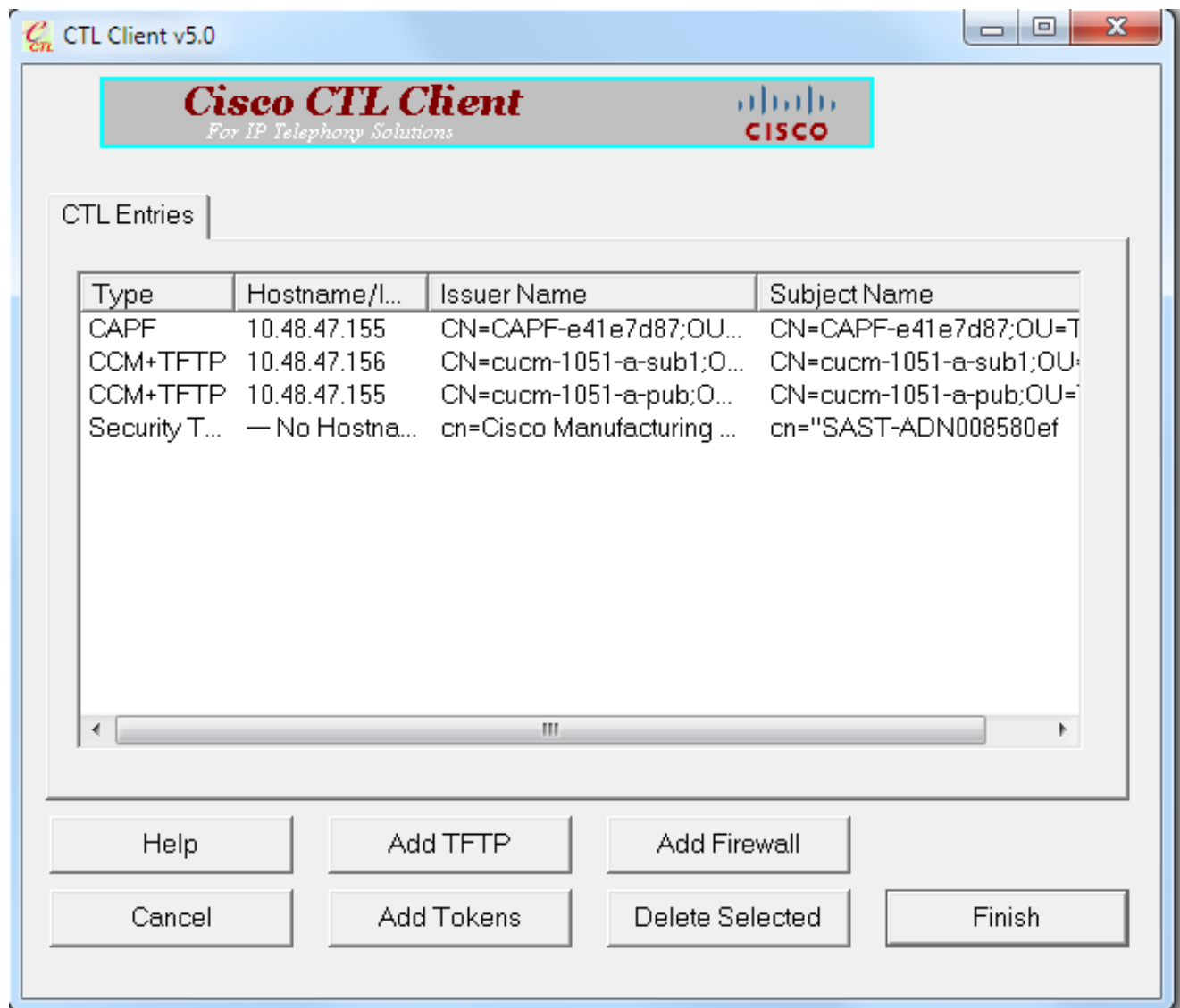
14. 插入第一個安全令牌，然後按一下OK:



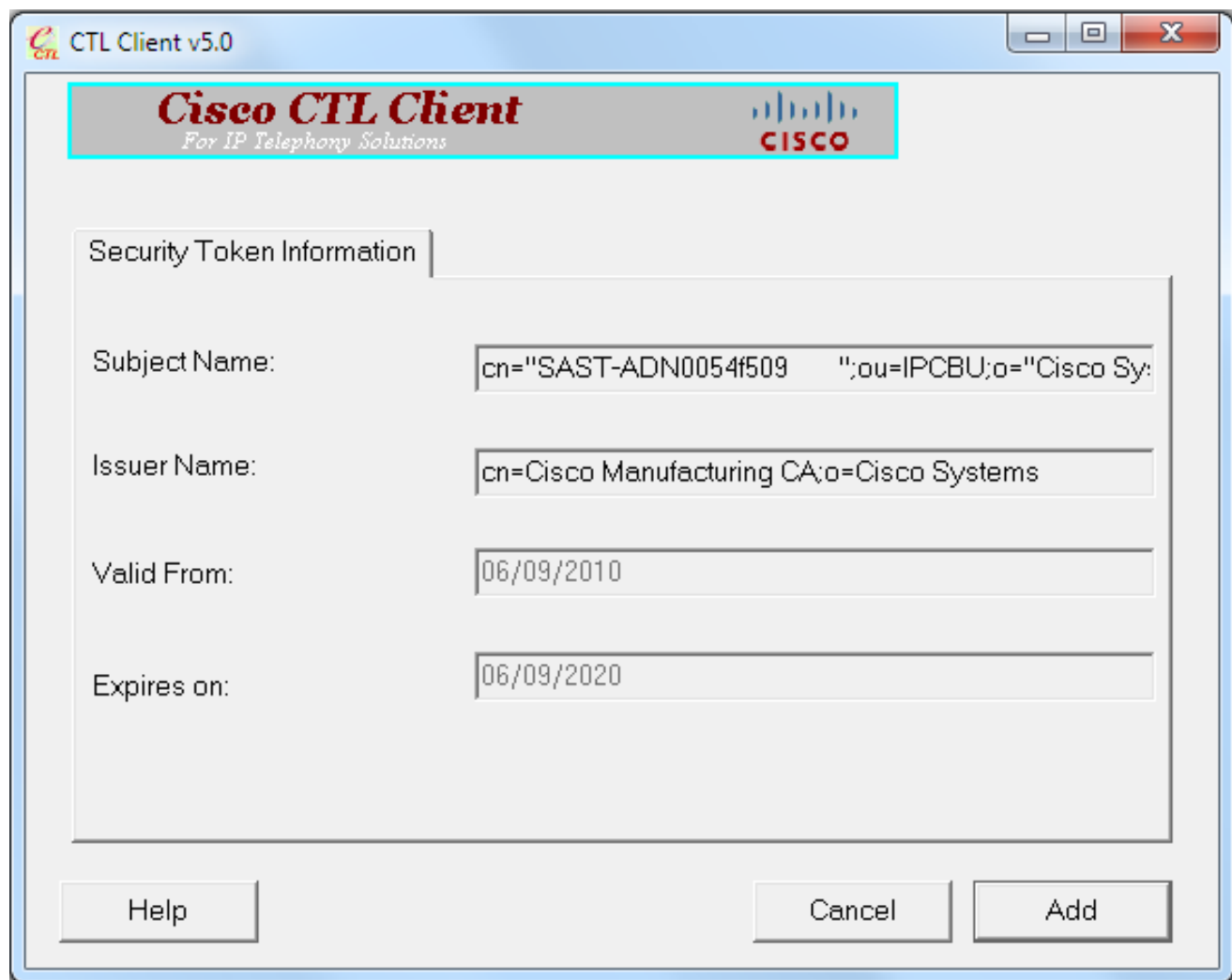
15. 顯示安全令牌詳細資訊後，按一下Add:



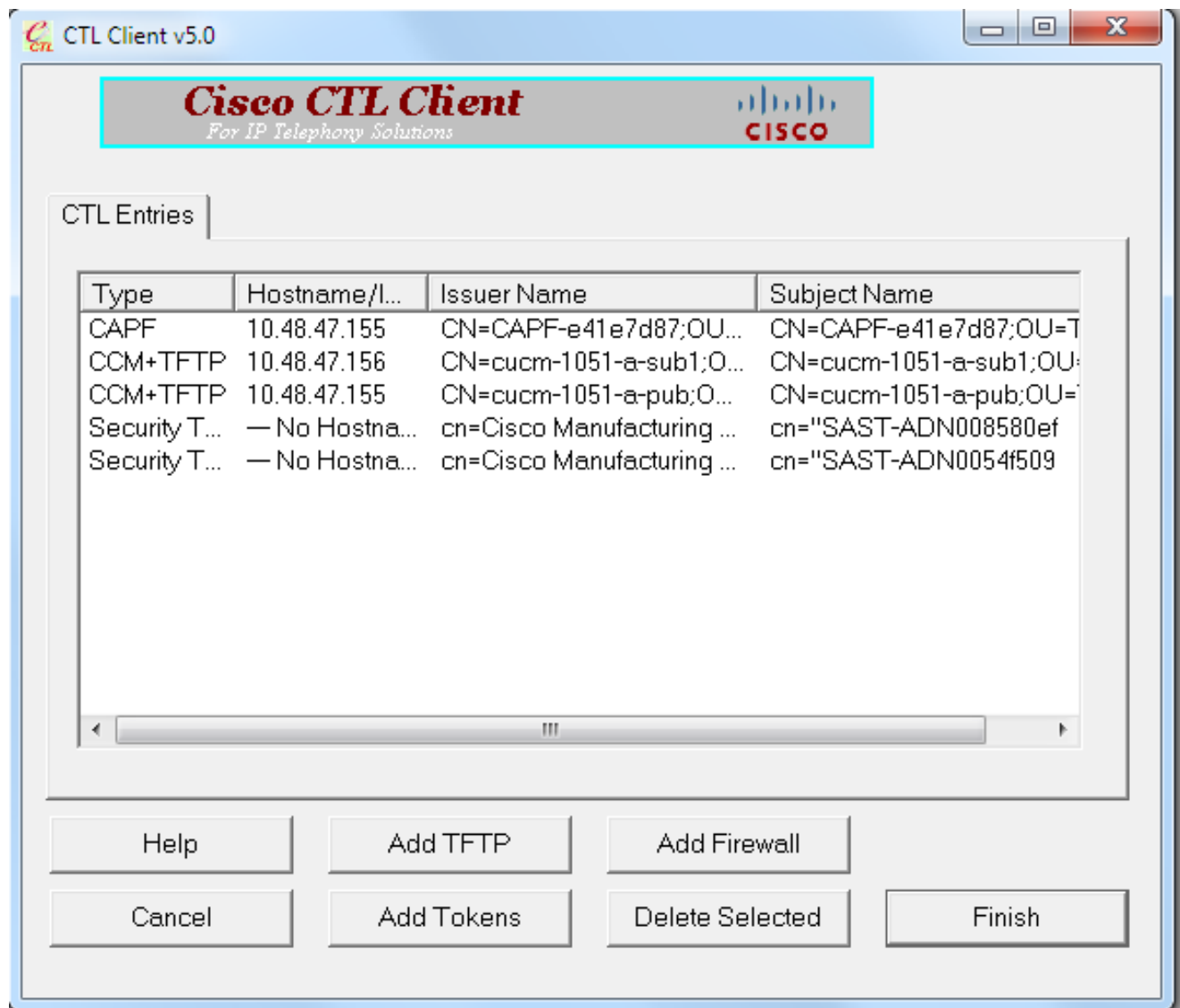
16. 顯示CTL檔案的內容後，按一下Add Tokens以新增第二個USB eToken:



17. 顯示安全令牌詳細資訊後，按一下Add:

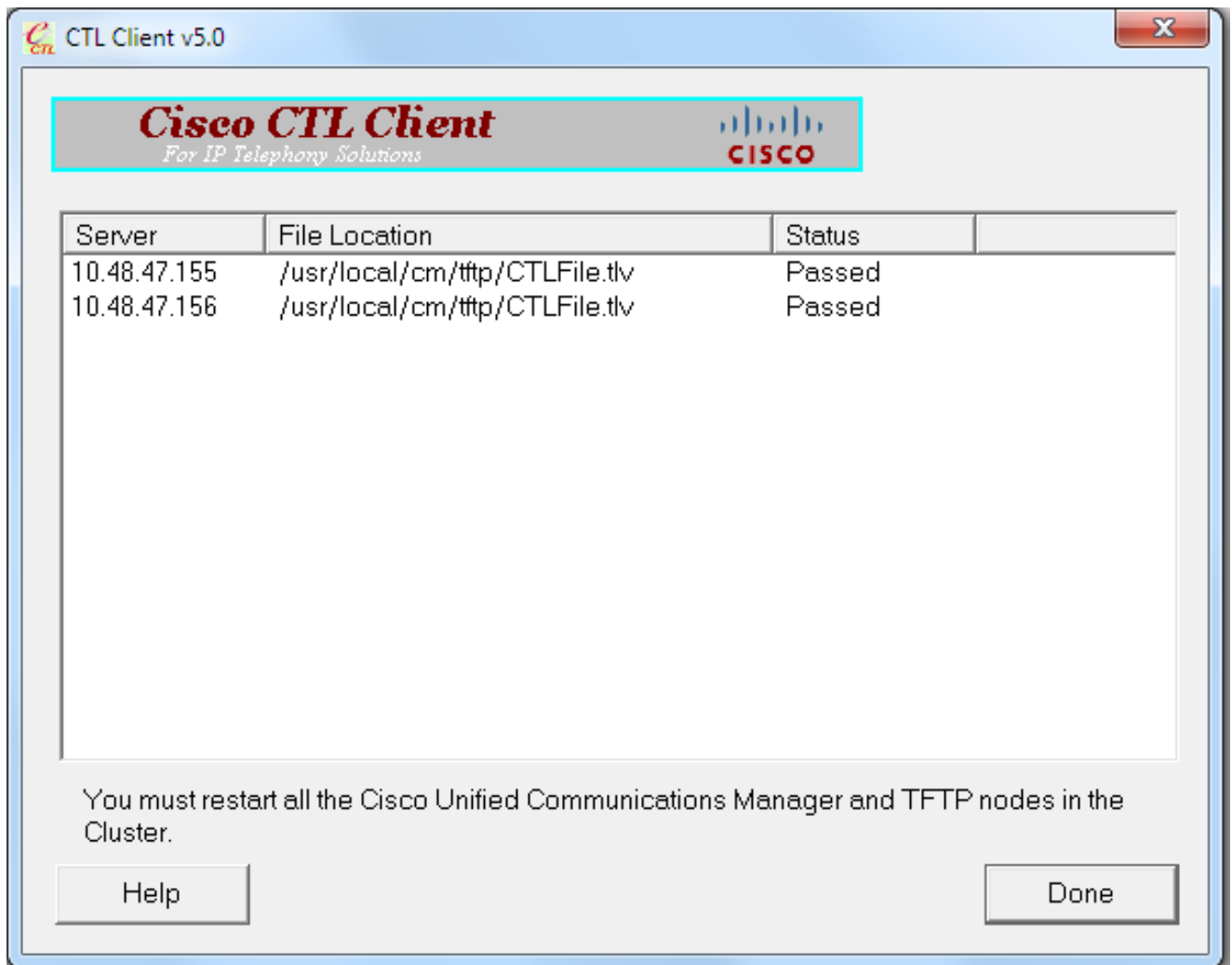


18. 顯示CTL檔案的內容後，按一下Finish。當系統提示輸入密碼時，請輸入Cisco123:



19. 出現CTL檔案所在的CUCM伺服器清單時，按一下Done:





20. 在運行這些服務的群集中的所有節點上重新啟動TFTP和CallManager服務。
21. 重新啟動所有IP電話，以便它們可以從CUCM TFTP服務獲取新版本的CTL檔案。
22. 若要驗證CTL檔案的內容，請在CLI中輸入show ctl命令。在CTL檔案中，您可以看到來自兩個USB eTokens的證書（其中一個用於對CTL檔案進行簽名）。以下是輸出範例：

```
<#root>
```

```
admin:
```

```
show ctl
```

```
The checksum value of the CTL file:
```

```
2e7a6113eadbdae67ffa918d81376902(MD5)
```

```
d0f3511f10eef775cc91cce3fa6840c2640f11b8(SHA1)
```

```
Length of CTL file: 5728
```

```
The CTL File was last modified on Fri Mar 06 22:53:33 CET 2015
```

```
[...]
```

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 not used to sign the CTL file.

[...]

CTL Record #:5

----

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 used to sign the CTL file.

The CTL file was verified successfully.

23. 在IP電話端，您可以驗證IP電話重新啟動後，它們下載了更新的CTL檔案版本（與CUCM的輸出相比，MD5校驗和匹配）：



此更改是可能的，因為您之前已經將eToken證書匯出並上傳到CUCM證書信任庫，並且IP電話能夠驗證此未知證書，該證書用於根據在CUCM上運行的信任驗證服務(TVS)對CTL檔案進行簽名。

此日誌片段說明IP電話如何聯絡CUCM TVS，請求驗證未知的eToken證書，該證書以Phone-SAST-trust方式上傳，並且受信任：

```
<#root>
```

```
//
```

```
In the Phone Console Logs we can see a request sent to TVS server to verify unknown certificate
```

```
8074: NOT 23:00:22.335499 SECD: setupSocketToTvsProxy: Connected to TVS proxy server
8075: NOT 23:00:22.336918 SECD: tvsReqFlushTvsCertCache: Sent Request to TVS proxy,
len: 3708
```

```
//
```

```
In the TVS logs on CUCM we can see the request coming from an IP Phone which is being successfully verified
```

```
23:00:22.052 | debug tvsHandleQueryCertReq
23:00:22.052 | debug tvsHandleQueryCertReq : Subject Name is: cn="SAST-ADN008580ef";ou=IPCBU;o="Cisco Systems"
23:00:22.052 | debug tvsHandleQueryCertReq : Issuer Name is: cn=Cisco Manufacturing
```

```
CA;o=Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq :subjectName and issuerName matches for
eToken certificate
23:00:22.052 | debug tvsHandleQueryCertReq : SAST Issuer Name is: cn=Cisco
Manufacturing CA;o=Cisco Systems
23:00:22.052 | debug tvsHandleQueryCertReq : This is SAST eToken cert
23:00:22.052 | debug tvsHandleQueryCertReq : Serial Number is: 83E908000005545AF31
23:00:22.052 | debug CertificateDBCACHE::getCertificateInformation - Looking up the
certificate cache using Unique MAP ID : 83E908000005545AF31cn=Cisco Manufacturing
CA;o=Cisco Systems
23:00:22.052 | debug ERROR:CertificateDBCACHE::getCertificateInformation - Cannot find
the certificate in the cache
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - Looking up the
certificate cache using Unique MAP ID : 83E908000005545AF31cn=Cisco Manufacturing
CA;o=Cisco Systems, len : 61
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - Found entry
{rolecount : 1}
23:00:22.052 | debug CertificateCTLCache::getCertificateInformation - {role : 0}
23:00:22.052 | debug convertX509ToDER -x509cert : 0xa3ea6f8
23:00:22.053 | debug tvsHandleQueryCertReq: Timer started from tvsHandleNewPhConnection

//
```

In the Phone Console Logs we can see reply from TVS server to trust the new certificate (eToken Certificate which was used to sign the CTL file)

```
8089: NOT 23:00:22.601218 SECD: clpTvsInit: Client message received on TVS proxy socket
8090: NOT 23:00:22.602785 SECD: processTvsClntReq: Success reading the client TVS
request, len : 3708
8091: NOT 23:00:22.603901 SECD: processTvsClntReq: TVS Certificate cache flush
request received
8092: NOT 23:00:22.605720 SECD: tvsFlushCertCache: Completed TVS Certificate cache
flush request
```

## 無令牌的CTL解決方案的證書再生

本節介紹在使用無令牌的CTL解決方案時，如何重新生成CUCM群集安全證書。


在CUCM維護過程中，有時會更改CUCM發佈器節點CallManager證書。

發生這種情況的情況包括更改主機名、更改域，或僅僅重新生成證書（由於關閉證書到期日期）。

更新CTL檔案後，使用與IP電話上安裝的CTL檔案中存在的證書不同的證書進行簽名。

通常，這個新的CTL檔案不被接受；但是，當IP電話發現用於對CTL檔案進行簽名的未知證書後，它會聯絡CUCM上的TVS服務。

---

 注意：TVS伺服器清單位於IP電話配置檔案中，並且從IP電話裝置池> CallManager組對映到CUCM伺服器。

---

成功對TVS伺服器進行驗證後，IP電話會使用新版本更新其CTL檔案。以下情況會發生以下事件：

1. CTL檔案存在於CUCM和IP電話上。CUCM發佈伺服器節點的CCM+TFT（伺服器）證書用於

對CTL檔案進行簽名：

<#root>

admin:

show ctl

The checksum value of the CTL file:

7b7c10c4a7fa6de651d9b694b74db25f(MD5)

819841c6e767a59ecf2f87649064d8e073b0fe87(SHA1)

Length of CTL file: 4947

The CTL File was last modified on Mon Mar 09 16:59:43 CET 2015

[...]

```
          CTL Record #:1
          ----
BYTEPOS TAG          LENGTH  VALUE
----- ---          -
1      RECORDLENGTH  2      1156
2      DNSNAME       16
cucm-1051-a-pub

3      SUBJECTNAME   62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
          ST=Małopolska;C=PL
4      FUNCTION       2
System Administrator Security Token

5      ISSUENAME     62      CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
          ST=Małopolska;C=PL
6      SERIALNUMBER  16
70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB

7      PUBLICKEY     140
8      SIGNATURE     128
9      CERTIFICATE   694      E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D
          21 A5 A3 8C 9C (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      1156
```

2	DNSNAME	16	
	<b>cucm-1051-a-pub</b>		
3	SUBJECTNAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;C=PL
4	FUNCTION	2	
	<b>CCM+TFTP</b>		
5	ISSUENAME	62	CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow; ST=Małopołska;C=PL
6	SERIALNUMBER	16	
	<b>70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB</b>		
7	PUBLICKEY	140	
8	SIGNATURE	128	
9	CERTIFICATE	694	E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21 A5 A3 8C 9C (SHA1 Hash HEX)
10	IPADDRESS	4	

[...]

The CTL file was verified successfully.

## Certificate Details for cucm-1051-a-pub, CallManager



Regenerate



Generate CSR



Download .PEM File



Download .DER File

### Status



Status: Ready

### Certificate Settings





File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

### Certificate File Data

```
[
Version: V3
Serial Number: 70CAF64E090751B9DF22F49F754FC5BB
SignatureAlgorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Validity From: Thu Jun 05 18:31:39 CEST 2014
To: Tue Jun 04 18:31:38 CEST 2019
Subject Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Key: RSA (1.2.840.113549.1.1.1)
Key value:
30818902818100950c9f8791e7677c5bf1a48f1a933549f73ef58d7c0c871b5b77d23a842aa14f5b293
90e586e5945060b109bdf859b4c983cdf21699e3e4abdb0a47ba6f3c04cd7d4f59eff4a60f6cf3c5db
2ec32988605ae4352e77d647da25fae619dedf9ebb0e0bdd98f8ce70307ba106507a8919df8b8fd9f9
03068a52640a6a84487a90203010001
Extensions: 3 present
```


2. 將重新生成CallManager.pem檔案 ( CCM+TFTP證書 ) , 您可以看到證書的序列號會更改 :

### Certificate Details for cucm-1051-a-pub, CallManager

 Regenerate
  Generate CSR
  Download .PEM File
  Download .DER File

---

**Status**

 Status: Ready

---

**Certificate Settings**

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

---

**Certificate File Data**

```
[
Version: V3
Serial Number: 6B1D357B6841740B078FEE4A1813D5D6
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Validity From: Mon Mar 09 17:06:37 CET 2015
To: Sat Mar 07 17:06:36 CET 2020
Subject Name: L=Krakow, ST=Malopolska, CN=cucm-1051-a-pub, OU=TAC, O=Cisco, C=PL
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100c363617e37830eaf5312f4eb3fe68c74e7a037453d26a0514e52476e56d02f78
c19e83623952934279b8dee9b3944a2a43c21714502db749c4141edc4666358974f2248e001e58928
8a608e9a1bc8ef74267e413e03d5d53e61f0705fb564a1dd2744a53840f579a183cd29e9b3e0d5d689
e067b6426c8c8c49078c5c4cc1b6cb6fec83d31ee86661517bf560ef0c01f5ec056db0dcc9746402af2a
b3ed4d66521f6d0b795ac48f78deaafb324dc30962ffa9e96c8615cce6e1a68247f217c83bf324fb3d5c
```

3. 在CLI中輸入了utils ctl update CTLFile命令以更新CTL檔案：

```
<#root>
```

```
admin:
```

```
utils ctl update CTLFile
```

```
This operation updates the CTLFile. Do you want to continue? (y/n):y
```

```
Updating CTL file
```

```
CTL file Updated
```

```
Please Restart the TFTP and Cisco CallManager services on all nodes in
the cluster that run these services
```

```
admin:
```

4. TVS服務使用新的CTL檔案詳細資訊更新其證書快取：

```
<#root>
```



```

17:10:35.825 | debug CertificateCache::localCTLCacheMonitor -
CTLFile.tlv has been
  modified

. Recaching CTL Certificate Cache
17:10:35.826 | debug updateLocalCTLCache :
Refreshing the local CTL certificate cache

17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::

6B1D357B6841740B078FEE4A1813D5D6

CN=
cucm-1051-a-pub

;OU=TAC;O=Cisco;L=Krakow;
  ST=Malopolska;C=PL, length : 93
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::

6B1D357B6841740B078FEE4A1813D5D6

CN=
cucm-1051-a-pub

;OU=TAC;O=Cisco;L=Krakow;
  ST=Malopolska;C=PL, length : 93
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
744B5199770516E799E91E81D3C8109BCN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
  ST=Malopolska;C=PL, length : 91
17:10:35.827 | debug tvs_sql_get_all_CTL_certificate - Unique Key used for Caching ::
6BEBFDCDCD8CA277CB2FD1D183A60E72CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
  ST=Malopolska;C=PL, length : 94

```

5. 檢視CTL檔案內容時，可以看到該檔案已使用發佈伺服器節點的新CallManager伺服器證書簽名：

```

<#root>
admin:
show ctl

The checksum value of the CTL file:
ebc649598280a4477bb3e453345c8c9d(MD5)

ef5c006b6182cad66197fac6e6530f15d009319d(SHA1)

Length of CTL file: 6113
The CTL File was last modified on Mon Mar 09 17:07:52 CET 2015

[...]
```



[...]

The CTL file was verified successfully.

6. 從Unified Serviceability頁面，TFTP和Cisco CallManager服務將在運行這些服務的集群中的所有節點上重新啟動。
7. IP電話將重新啟動，它們會與TVS伺服器聯絡，以驗證現在用於對新版本的CTL檔案進行簽名的未知證書：

```
<#root>
```

```
//
```

```
In the Phone Console Logs we can see a request sent to TVS server to verify
unknown certificate
```

```
2782: NOT 17:21:51.794615 SECD: setupSocketToTvsProxy: Connected to TVS proxy server
2783: NOT 17:21:51.796021 SECD: tvsReqFlushTvsCertCache: Sent Request to TVS
proxy, len: 3708
```

```
//
```

```
In the TVS logs on CUCM we can see the request coming from an IP Phone which is
being successfully verified
```

```
17:21:51.831 | debug tvsHandleQueryCertReq
17:21:51.832 | debug tvsHandleQueryCertReq : Subject Name is: CN=cucm-1051-a-pub;
OU=TAC;O=Cisco;L=Krakow;ST=Malopolska
17:21:51.832 | debug tvsHandleQueryCertReq : Issuer Name is: CN=cucm-1051-a-pub;
OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;
17:21:51.832 | debug tvsHandleQueryCertReq : Serial Number is:
6B1D357B6841740B078FEE4A1813D5D6
17:21:51.832 | debug CertificateDBCACHE::getCertificateInformation - Looking up the
certificate cache using Unique MAPco;L=Krakow;ST=Malopolska;C=PL
17:21:51.832 | debug CertificateDBCACHE::getCertificateInformation - Found entry
{rolecount : 2}
17:21:51.832 | debug CertificateDBCACHE::getCertificateInformation - {role : 0}
17:21:51.832 | debug CertificateDBCACHE::getCertificateInformation - {role : 2}
17:21:51.832 | debug convertX509ToDER -x509cert : 0xf6099df8
17:21:51.832 | debug tvsHandleQueryCertReq: Timer started from
tvsHandleNewPhConnection
```

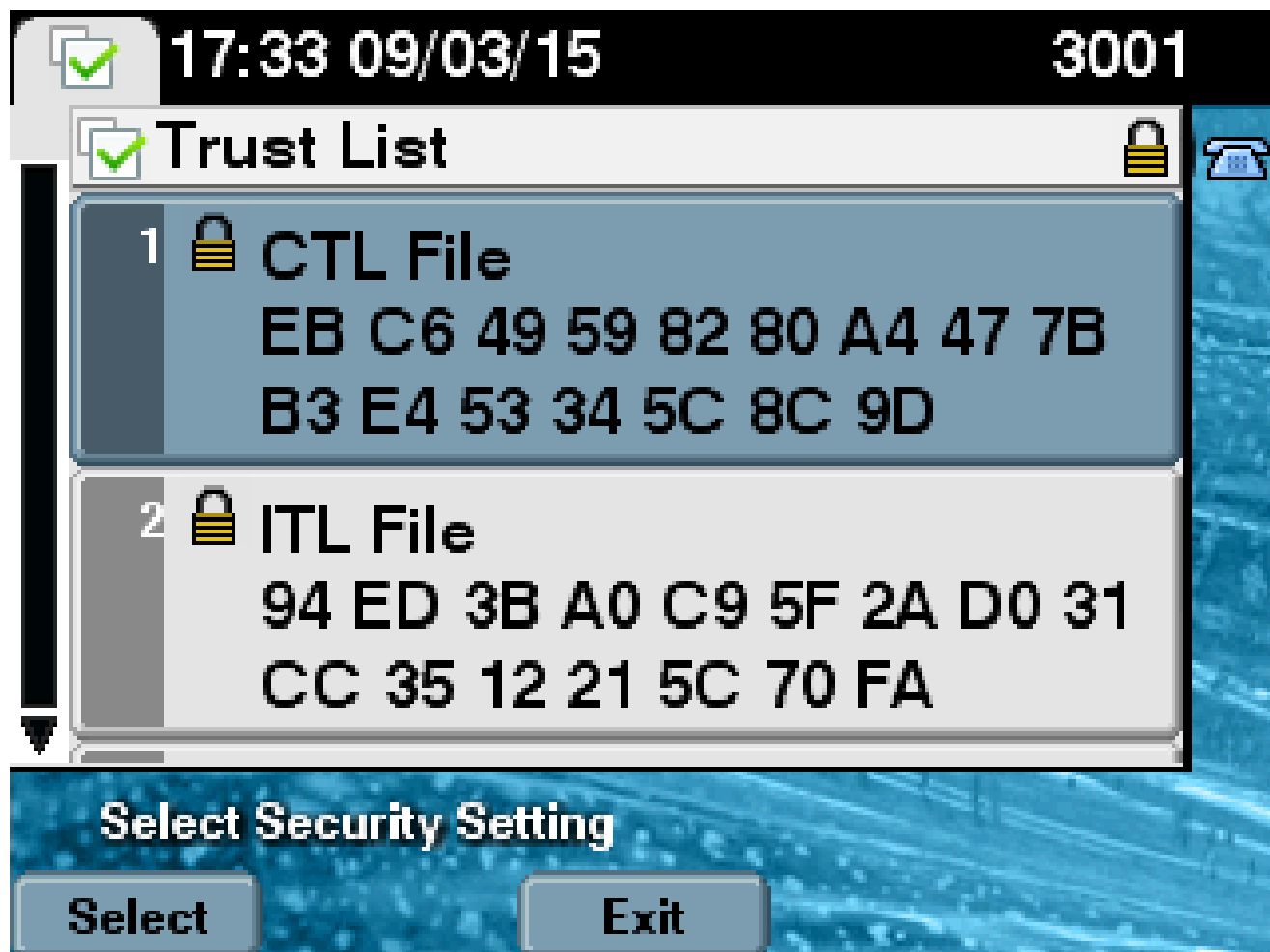
```
//
```

```
In the Phone Console Logs we can see reply from TVS server to trust the new
certificate (new CCM Server Certificate which was used to sign the CTL file)
```

```
2797: NOT 17:21:52.057442 SECD: clpTvsInit: Client message received on TVS
proxy socket
2798: NOT 17:21:52.058874 SECD: processTvsClntReq: Success reading the client TVS
```

```
request, len : 3708
2799: NOT 17:21:52.059987 SECD: processTvsClntReq: TVS Certificate cache flush
request received
2800: NOT 17:21:52.062873 SECD: tvsFlushCertCache: Completed TVS Certificate
cache flush request
```

8. 最後，在IP電話上，您可以驗證CTL檔案是否使用新版本進行更新，以及新CTL檔案的MD5校驗和是否與CUCM的校驗和相匹配：



## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。