

Modalità CUCM mista con CTL senza token

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Dalla modalità non protetta alla modalità mista \(CTL senza token\)](#)

[Da eToken hardware a soluzione senza token](#)

[Dalla soluzione senza token ai eToken hardware](#)

[Rigenerazione certificati per soluzione CTL senza token](#)

Introduzione

In questo documento vengono descritte le differenze tra la protezione di Cisco Unified Communications Manager (CUCM) e l'utilizzo/meno di eToken USB hardware.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di CUCM versione 10.0(1) o successive. Inoltre, assicurarsi che:

- Il server licenze per CUCM versione 11.5.1SU3 e successive deve essere Cisco Prime License Manager (PLM) 11.5.1SU2 o successiva.

Infatti, per abilitare la modalità mista, CUCM versione 11.5.1SU3 richiede una licenza di crittografia e PLM non supporta tale licenza fino alla versione 11.5.1SU2.


Per ulteriori informazioni, consultare le [note di rilascio per Cisco Prime License Manager, versione 11.5\(1\)SU2](#).

- Si dispone dell'accesso amministrativo all'interfaccia della riga di comando (CLI) del nodo di CUCM Publisher.
- È possibile accedere agli eToken USB hardware e verificare che il plug-in client CTL sia installato nel PC per gli scenari che richiedono la migrazione all'utilizzo degli eToken hardware.

Per maggiore chiarezza, questo requisito è valido solo se, in qualsiasi momento, si ha uno scenario in cui sono necessari gli eToken USB. Le probabilità sono molto piccole che USB eToken sono necessari per la maggior parte delle persone.

- Esiste una connettività completa tra tutti i nodi CUCM nel cluster. Questa operazione è molto importante perché il file CTL viene copiato in tutti i nodi del cluster tramite il protocollo SFTP (SSH File Transfer Protocol).
- La replica di database (DB) nel cluster funziona correttamente e i server replicano i dati in tempo reale.
- I dispositivi della distribuzione supportano la protezione per impostazione predefinita (TVS).

È possibile utilizzare Unified CM Phone Feature List dalla pagina Web di Cisco Unified Reporting (<https://<CUCM IP or FQDN>/cucreports/>) per determinare i dispositivi che supportano la sicurezza per impostazione predefinita.

 Nota: Cisco Jabber e molti telefoni IP Cisco TelePresence o Cisco serie 7940/7960 attualmente non supportano la sicurezza per impostazione predefinita. Se si distribuisce un elenco di certificati attendibili (CTL) senza token con dispositivi che non supportano la sicurezza per impostazione predefinita, qualsiasi aggiornamento del sistema che modifichi il certificato di CallManager nel server di pubblicazione impedirà la normale funzionalità di tali dispositivi finché l'elenco di certificati attendibili non viene eliminato manualmente. I dispositivi che supportano la sicurezza per impostazione predefinita, ad esempio telefoni 7945 e 7965 o successivi, possono installare i file CTL quando il certificato CallManager nell'editore viene aggiornato in quanto possono utilizzare il servizio di verifica dell'attendibilità (TVS).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM versione 10.5.1.10000-7 (cluster di due nodi)
- Cisco serie 7975 IP Phone registrati tramite SCCP (Skinny Client Control Protocol) con versione firmware SCCP75.9-3-1SR4-1S
- Due token di sicurezza Cisco utilizzati per impostare il cluster in modalità mista con l'utilizzo del software client CTL

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse


In questo documento viene descritta la differenza tra la protezione di Cisco Unified Communications Manager (CUCM) con e senza l'utilizzo di USB eToken hardware.

Questo documento descrive anche gli scenari di implementazione di base che coinvolgono

l'elenco di certificati attendibili (CTL) senza token e il processo utilizzato per garantire il corretto funzionamento del sistema dopo le modifiche.

Tokenless CTL è una nuova funzionalità di CUCM versione 10.0(1) e successive che consente la crittografia della segnalazione delle chiamate e dei supporti per i telefoni IP senza la necessità di utilizzare hardware USB eToken e il plugin del client CTL, come richiesto nelle precedenti versioni di CUCM.

Quando il cluster viene impostato in modalità mista con l'utilizzo del comando CLI, il file CTL viene firmato con il certificato CCM+TFTP (server) del nodo Publisher e nel file CTL non sono presenti certificati eToken.


 Nota: quando si rigenera il certificato CallManager (CCM+TFTP) nel server di pubblicazione, viene modificato il firmatario del file. Anche i telefoni e i dispositivi che non supportano la protezione per impostazione predefinita non accettano il nuovo file CTL a meno che i file CTL non vengano eliminati manualmente da ogni dispositivo. Per ulteriori informazioni, fare riferimento all'ultimo requisito elencato nella sezione [Requisiti](#) di questo documento.

Dalla modalità non protetta alla modalità mista (CTL senza token)


In questa sezione viene descritto il processo utilizzato per spostare la protezione del cluster CUCM in modalità mista tramite la CLI.

Prima di questo scenario, il CUCM era in modalità non protetta, il che significa che non era presente alcun file CTL su nessuno dei nodi e che i telefoni IP registrati avevano solo un file ITL (Identity Trust List) installato, come mostrato in questi output:

```
<#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:
```

 Nota: se nel server è stato trovato un file CTL mentre il cluster non è in modalità mista, significa che il cluster è stato in modalità mista e quindi è stato nuovamente spostato in modalità non mista e che il file CTL non è stato eliminato dal cluster.

Il file di comando `delete activelog cm/tftpdata/CTLFile.tlv` elimina il file CTL dai nodi nel

 cluster CUCM; tuttavia, il comando deve essere immesso su ogni nodo. Per chiarezza, utilizzare questo comando solo se i server dispongono di un file CTL e il cluster non è in modalità mista.

Un modo semplice per verificare se un cluster è in modalità mista consiste nell'utilizzare il comando `run sql select paramname,paramvalue from processconfig where paramname='ClusterSecurityMode'`. Se il valore del parametro è 0, il cluster non è in modalità mista.

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



Per spostare la protezione del cluster CUCM in modalità mista con l'utilizzo della nuova funzionalità CTL senza token, attenersi alla seguente procedura:

1. Ottenere l'accesso amministrativo alla CLI del nodo di CUCM Publisher.

2. Immettere il comando `utils ctl set-cluster-mixed-mode` nella CLI:

```
<#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. Passare alla pagina Amministratore CUCM > Sistema > Parametri enterprise e verificare se il cluster è stato impostato in modalità mista (il valore 1 indica la modalità mista):

Security Parameters	
Cluster Security Mode *	1
LBM Security Mode *	Insecure ▼
CAPF Phone Port *	3804
CAPF Operation Expires in (days) *	10
Enable Caching *	True ▼

4. Riavviare i servizi TFTP e Cisco CallManager su tutti i nodi del cluster che eseguono questi servizi.

5. Riavviare tutti i telefoni IP in modo che possano ottenere il file CTL dal servizio CUCM TFTP.

6. Per verificare il contenuto del file CTL, immettere il comando `show ctl` nella CLI.

7. Nel file CTL è possibile vedere che il certificato CCM+TFTP (server) per il nodo di CUCM Publisher viene utilizzato per firmare il file CTL (questo file è lo stesso in tutti i server del cluster). Di seguito è riportato un esempio di output:

```
<#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      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
```

[...]

The CTL file was verified successfully.

8. Sul lato IP Phone, è possibile verificare che dopo il riavvio del servizio, scarichi il file CTL, che è ora presente sul server TFTP (il checksum MD5 corrisponde se confrontato con l'output del CUCM):

 Nota: quando si verifica il checksum sul telefono, viene visualizzato MD5 o SHA1, a seconda del tipo di telefono.



Da eToken hardware a soluzione senza token

In questa sezione viene descritto come eseguire la migrazione della protezione del cluster CUCM da eToken hardware all'utilizzo della nuova soluzione senza token.

In alcune situazioni, la modalità mista è già configurata sul CUCM con l'uso del client CTL, e i telefoni IP usano i file CTL che contengono i certificati dei token USB hardware.

In questo scenario, il file CTL è firmato da un certificato da uno degli eToken USB e viene installato sui telefoni IP. Di seguito è riportato un esempio:

<#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	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.



Completare questi passaggi per spostare la protezione del cluster CUCM nell'utilizzo di CTL senza token:

1. Ottenere l'accesso amministrativo alla CLI del nodo di CUCM Publisher.
2. Immettere il comando `utils ctl update CTLFile` CLI:

```
<#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. Riavviare i servizi TFTP e CallManager in tutti i nodi del cluster che eseguono questi servizi.

4. Riavviare tutti i telefoni IP in modo che possano ottenere il file CTL dal servizio CUCM TFTP.
5. Immettere il comando show ctl nella CLI per verificare il contenuto del file CTL. Nel file CTL, è possibile vedere che il certificato CCM+TFTP (server) del nodo CUCM Publisher viene utilizzato per firmare il file CTL anziché il certificato dei eToken USB hardware.
6. Un'altra importante differenza in questo caso è che i certificati di tutti gli eToken USB hardware vengono rimossi dal file CTL. Di seguito è riportato un esempio di output:

```
<#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
-----	---	-----	-----
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	ISSUERNAME	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     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.



Nota: nell'output precedente, se il certificato CCM+TFTP (server) dell'editore CUCM non è firmatario, tornare alla modalità di protezione cluster basata su token hardware e ripetere le modifiche per la soluzione senza token.

7. Dal lato dell'IP Phone, è possibile verificare che dopo il riavvio, i telefoni IP abbiano scaricato la versione aggiornata del file CTL (il checksum MD5 corrisponde all'output del CUCM):



Dalla soluzione senza token ai eToken hardware

In questa sezione viene descritto come eseguire la migrazione della protezione del cluster CUCM dalla nuova soluzione senza token e tornare all'utilizzo di eToken hardware.

Quando la protezione del cluster CUCM è impostata sulla modalità mista con l'uso dei comandi CLI e il file CTL è firmato con il certificato CCM+TFTP (server) per il nodo di CUCM Publisher, non vi sono certificati provenienti dagli eToken USB hardware presenti nel file CTL.

Per questo motivo, quando si esegue il client CTL per aggiornare il file CTL (tornare all'uso di eToken hardware), viene visualizzato questo messaggio di errore:

```
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.
```

Ciò è particolarmente importante negli scenari che includono un downgrade (quando la versione viene ripristinata) del sistema a una versione precedente alla 10.x che non include i comandi utils ctl.

Il file CTL precedente viene migrato (senza modifiche del relativo contenuto) nel processo di aggiornamento o di aggiornamento da Linux a Linux (L2) e non contiene i certificati eToken, come indicato in precedenza. Di seguito è riportato un esempio di output:

<#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	
9	SIGNATUREALGOINFO	2	8
10	SIGNATUREALGORTITHM	1	
11	SIGNATUREMODULUS	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=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=Malopolska;C=PL
4      FUNCTION       2

```

CCM+TFTP

```

5      ISSUERNAME    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

```

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=Malopolska;C=PL
4      FUNCTION       2      CAPF
5      ISSUERNAME    60     CN=CAPF-e41e7d87;OU=TAC;O=Cisco;L=Krakow;
      ST=Malopolska;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=Malopolska;C=PL
4      FUNCTION        2      CCM+TFTP
5      ISSUENAME       63     CN=cucm-1051-a-sub1;OU=TAC;O=Cisco;L=Krakow;
      ST=Malopolska;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:

In questo scenario, completare i seguenti passaggi per aggiornare in modo sicuro i file CTL senza dover utilizzare la procedura per gli eToken persi, che si conclude con l'eliminazione manuale del file CTL da tutti i telefoni IP:

1. Ottenere l'accesso amministrativo alla CLI del nodo di CUCM Publisher.
2. Immettere il comando `file delete tftp CTLFile.tlv` nella CLI del nodo di Publisher per eliminare il file CTL:

<#root>

admin:

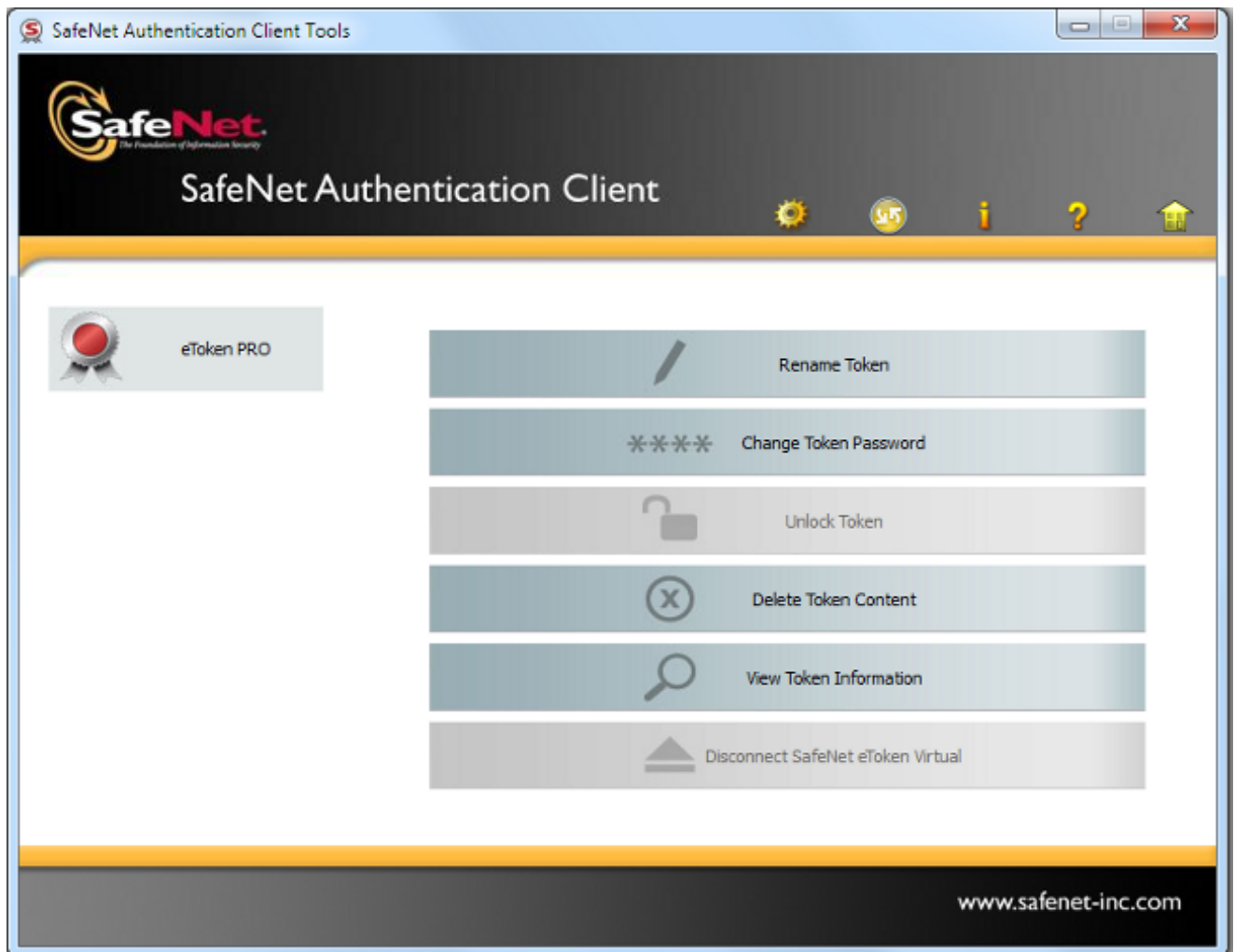
```
file delete tftp CTLFile.tlv
```

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

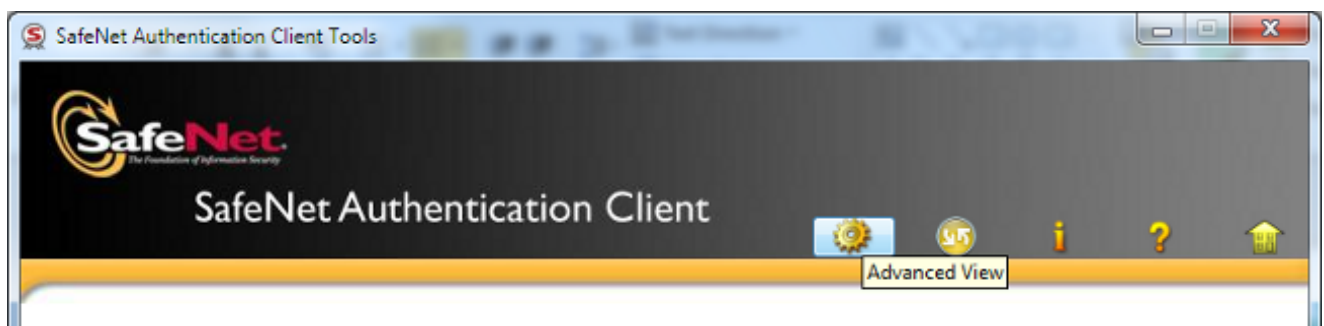
```
Enter "y" followed by return to continue: y
```

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

3. Aprire il client di autenticazione SafeNet sul computer Microsoft Windows in cui è installato il client CTL (viene installato automaticamente con il client CTL):

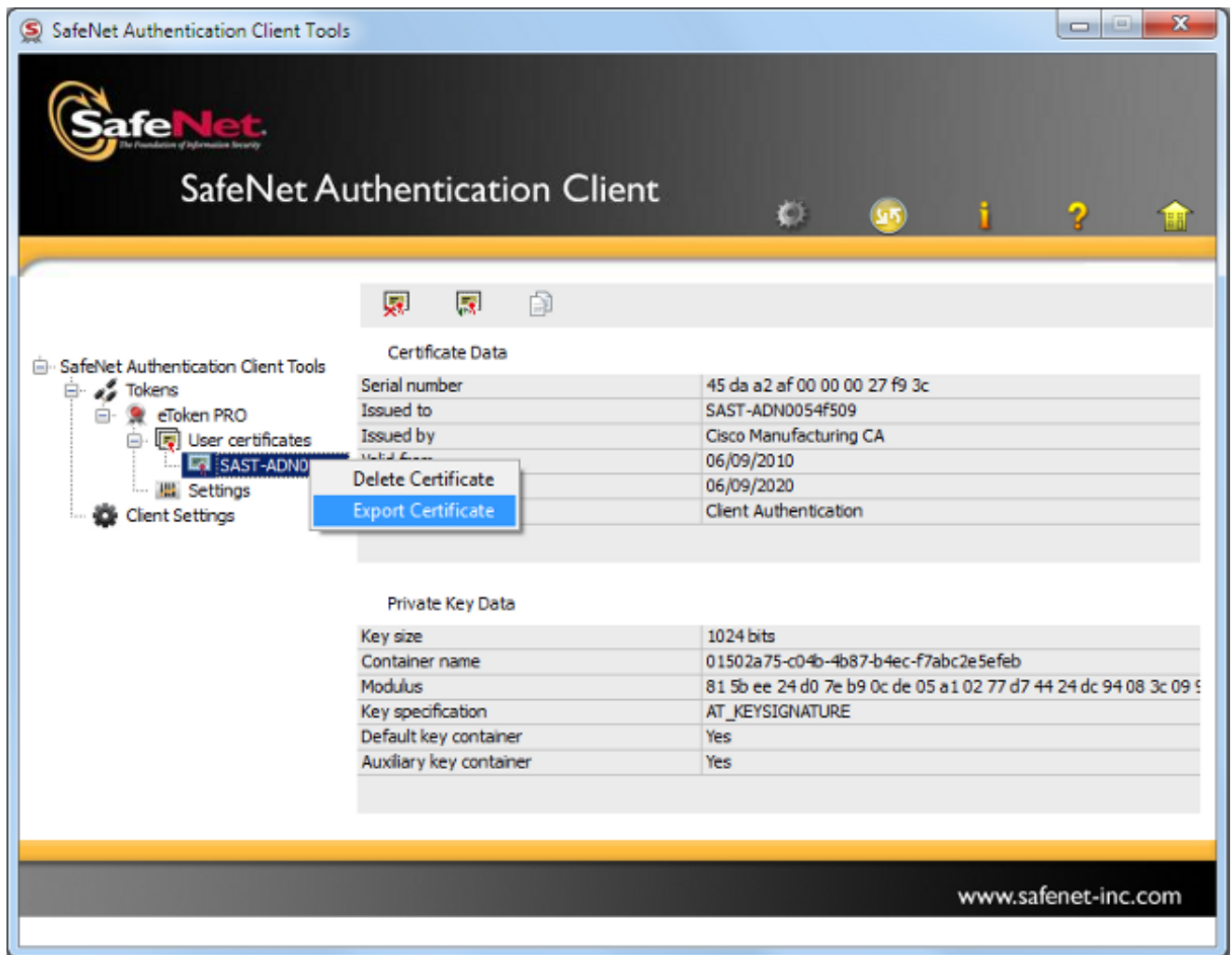


4. In Client di autenticazione SafeNet passare alla visualizzazione avanzata:



5. Inserire il primo eToken USB hardware.

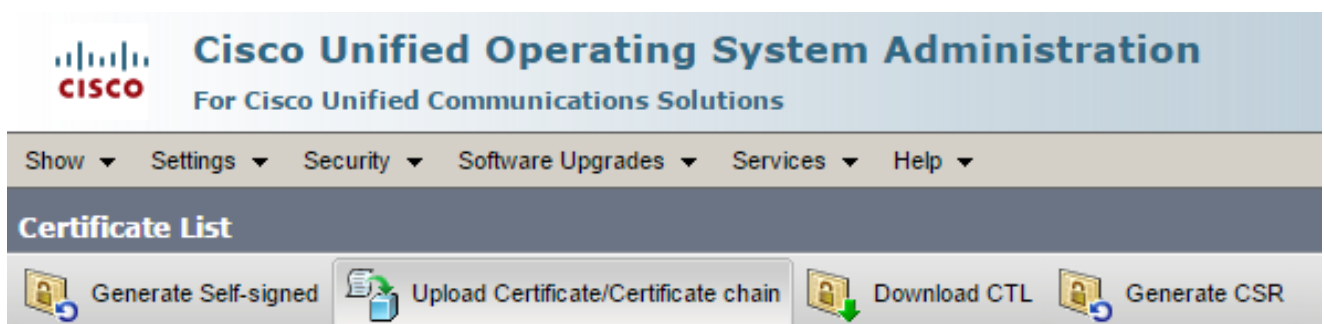
6. Selezionare il certificato nella cartella Certificati utente ed esportarlo nella cartella del PC. Quando viene richiesta una password, utilizzare la password predefinita di Cisco123:



7. Ripetere questi passaggi per il secondo eToken USB hardware in modo che entrambi i certificati vengano esportati nel 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. Accedere a Cisco Unified Operating System (OS) Administration e selezionare Security > Certificate Management > Upload Certificate (Sicurezza > Gestione certificati > Carica certificato):



9. Viene visualizzata la pagina Carica certificato. Scegliere Phone-SAST-trust dal menu a discesa Scopo certificato e selezionare il certificato esportato dal primo eToken:

Upload Certificate/Certificate chain - Google Chrome

<https://10.48.47.155/cmplatform/certificateUpload.do>

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* Phone-SAST-trust

Description(friendly name) 1st eToken Cert

Upload File Wybierz plik SAST-ADN0054f509.cer

Upload Close

i *- indicates required item.

10. Completare i passaggi precedenti per caricare il certificato esportato dal secondo eToken:

Upload Certificate/Certificate chain - Google Chrome

<https://10.48.47.155/cmplatform/certificateUpload.do>

Upload Certificate/Certificate chain

Upload Close

Status

i Success: Certificate Uploaded

Upload Certificate/Certificate chain

Certificate Purpose* Phone-SAST-trust

Description(friendly name) 2nd eToken Cert

Upload File Wybierz plik SAST-ADN008580ef.cer

Upload Close

11. Eseguire il client CTL, fornire l'indirizzo IP o il nome host del nodo di CUCM Publisher e immettere le credenziali di amministratore CCM:

CTL Client v5.0

Cisco CTL Client
For IP Telephony Solutions

CISCO

Cisco Unified Communications Manager Server

Hostname or IP Address: 10.48.47.155 Port: 2444

Username: admin

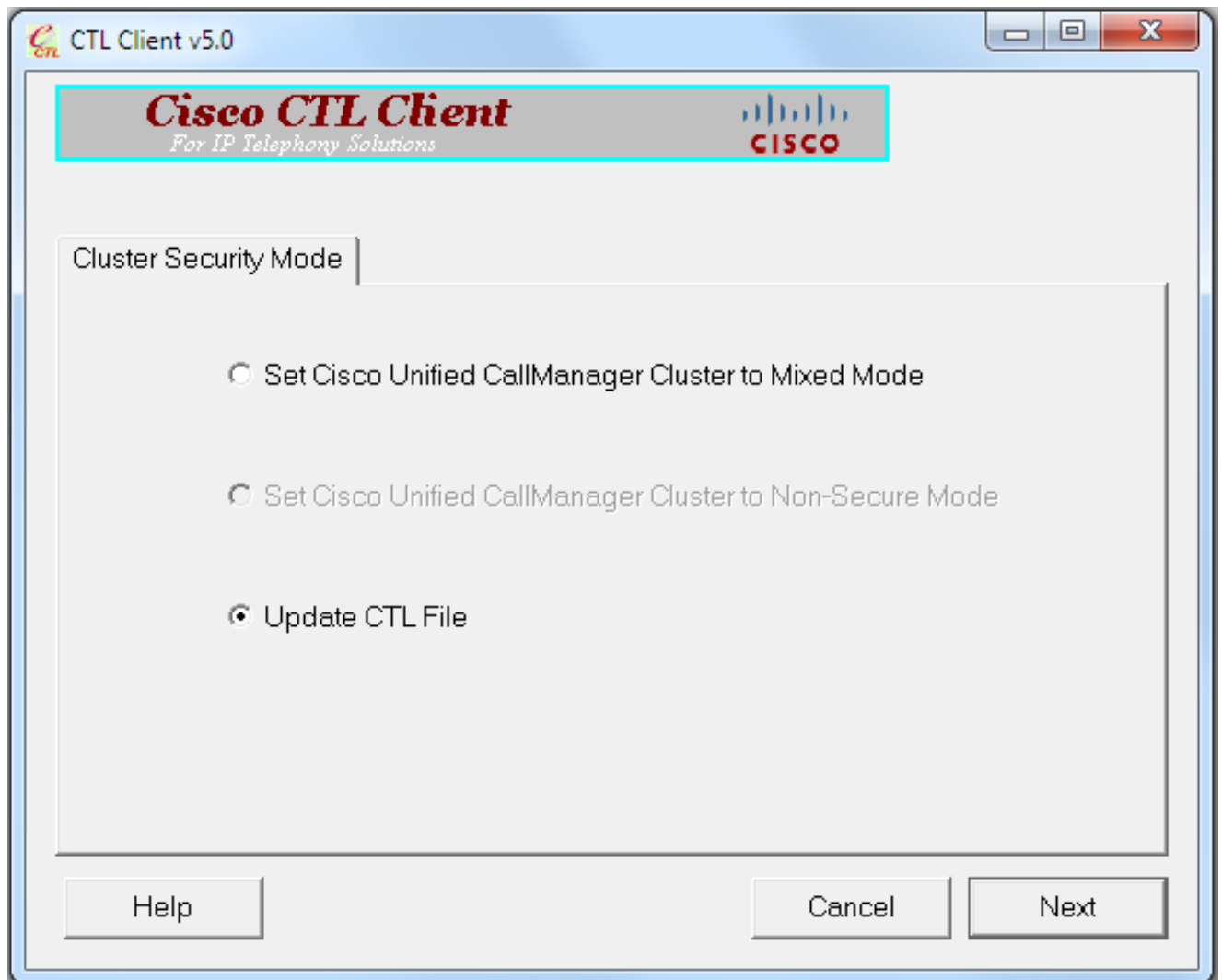
Password: xxxxxxxxxxxx

Help Cancel Next

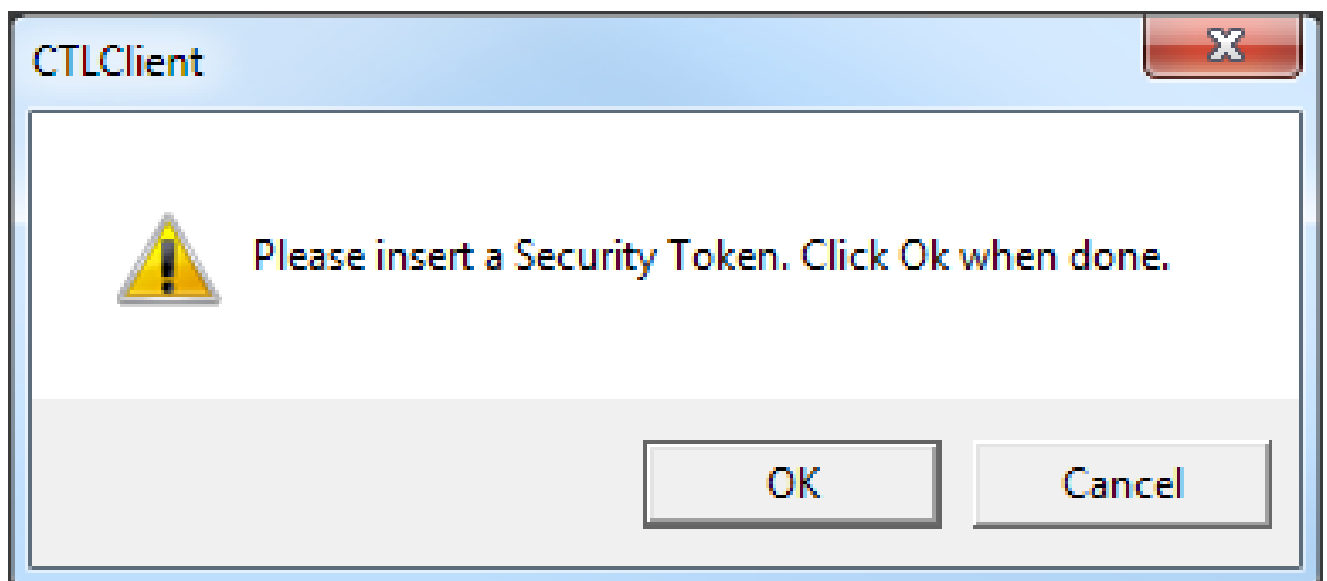
12. Poiché il cluster è già in modalità mista, ma non esiste alcun file CTL nel nodo di Publisher, viene visualizzato questo messaggio di avviso (fare clic su OK per ignorarlo):

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.

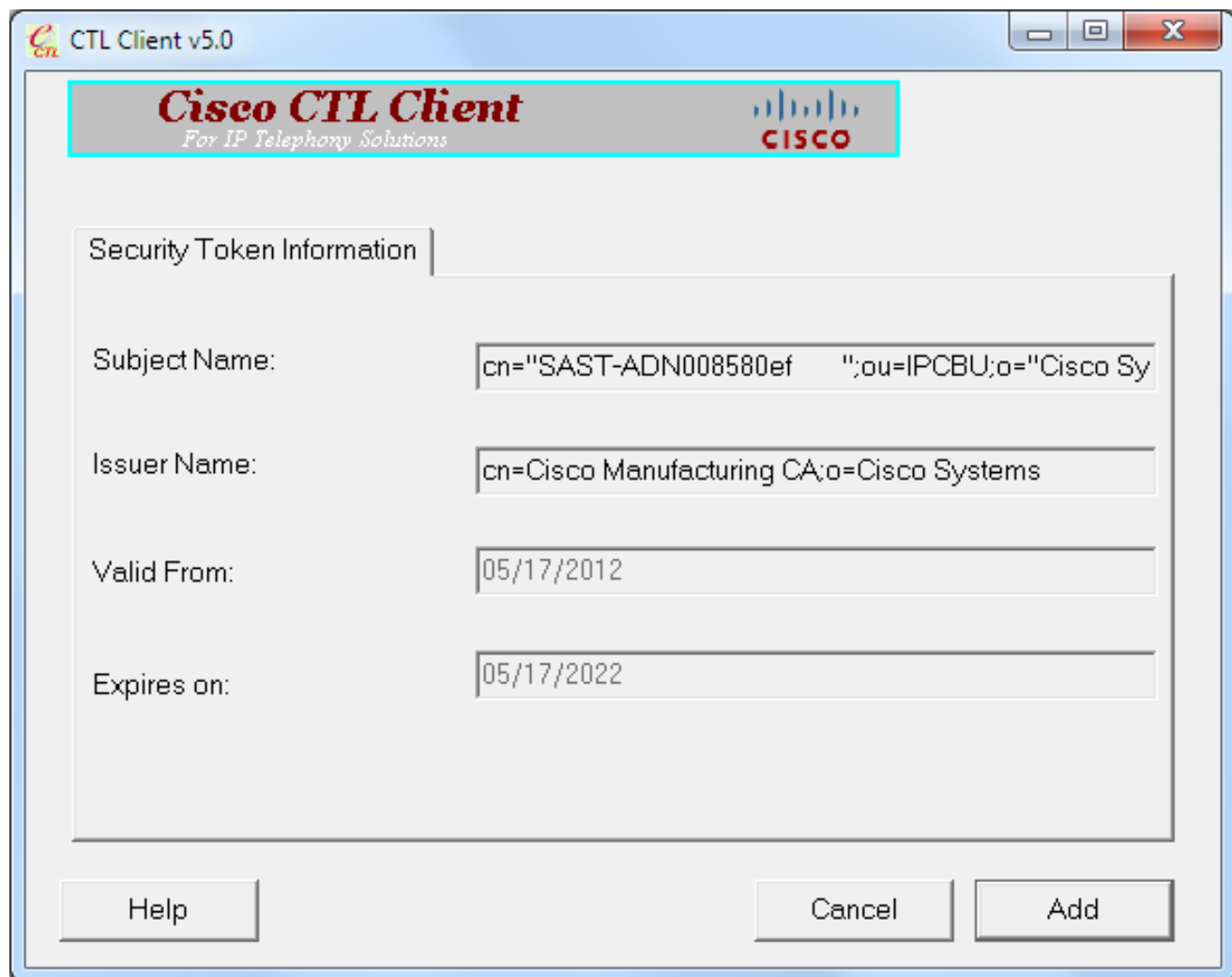
13. Dal client CTL, fare clic sul pulsante di scelta Aggiorna file CTL, quindi fare clic su Avanti:



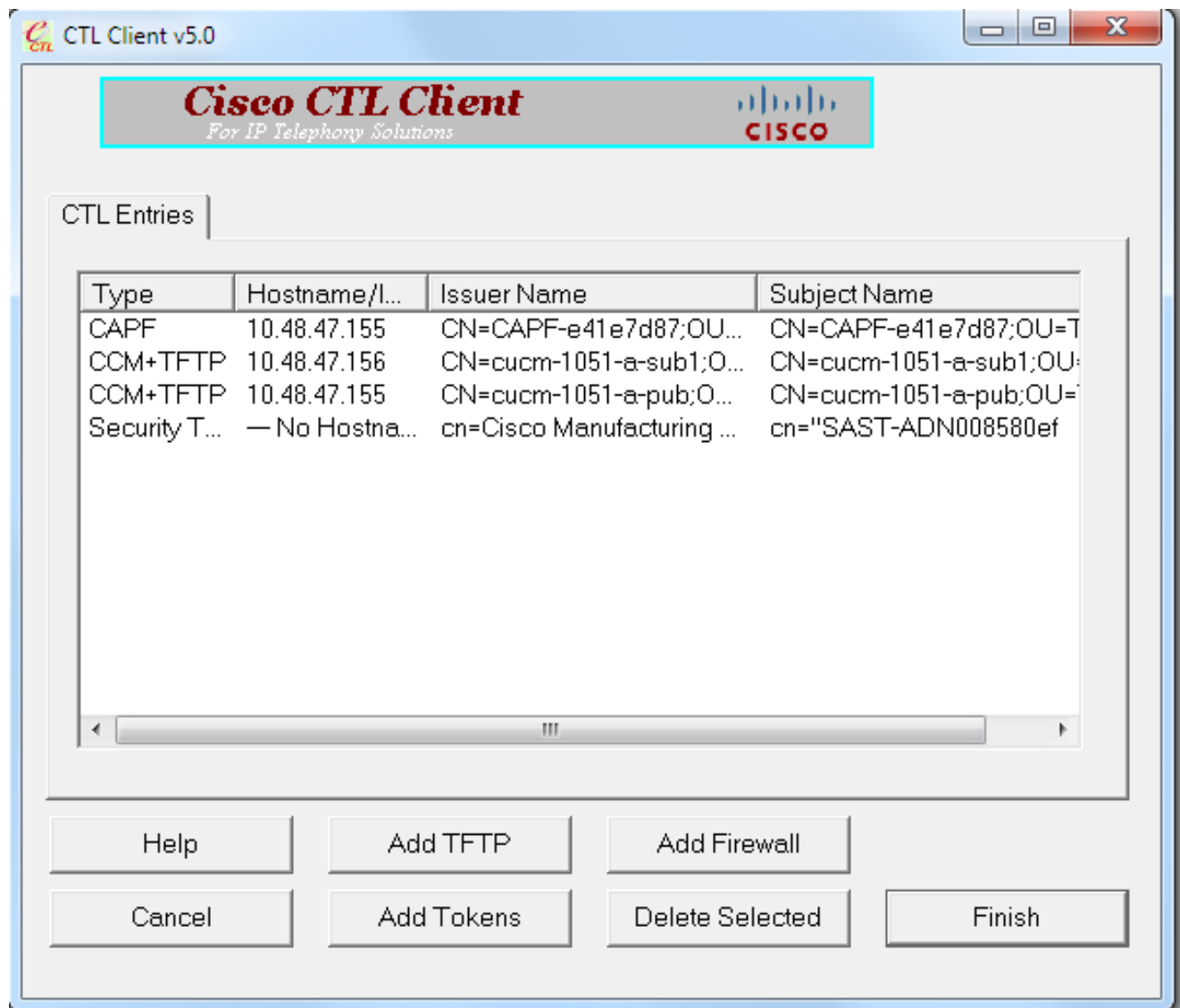
14. Inserire il primo token di sicurezza e fare clic su OK:



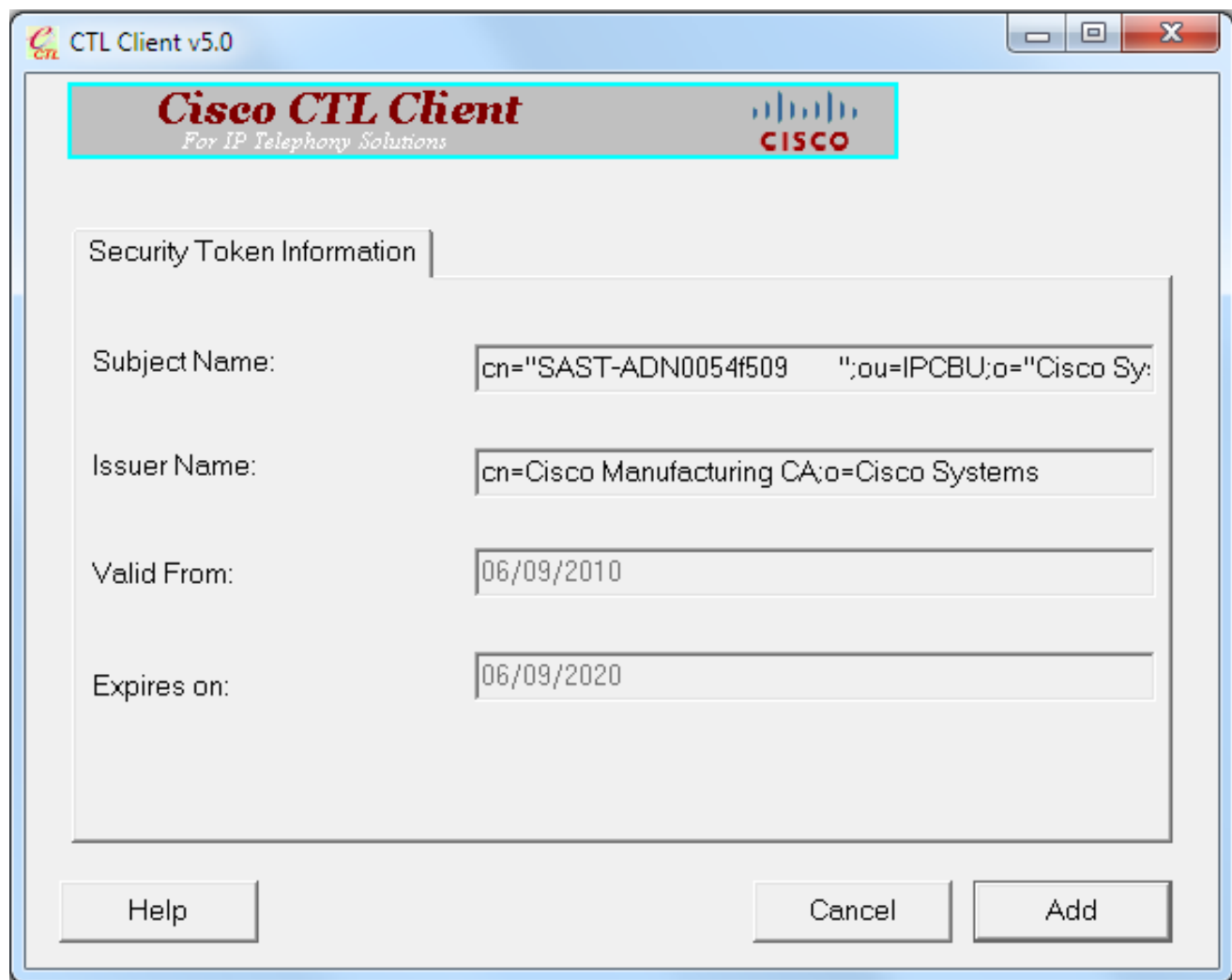
15. Dopo aver visualizzato i dettagli del token di sicurezza, fare clic su Add:



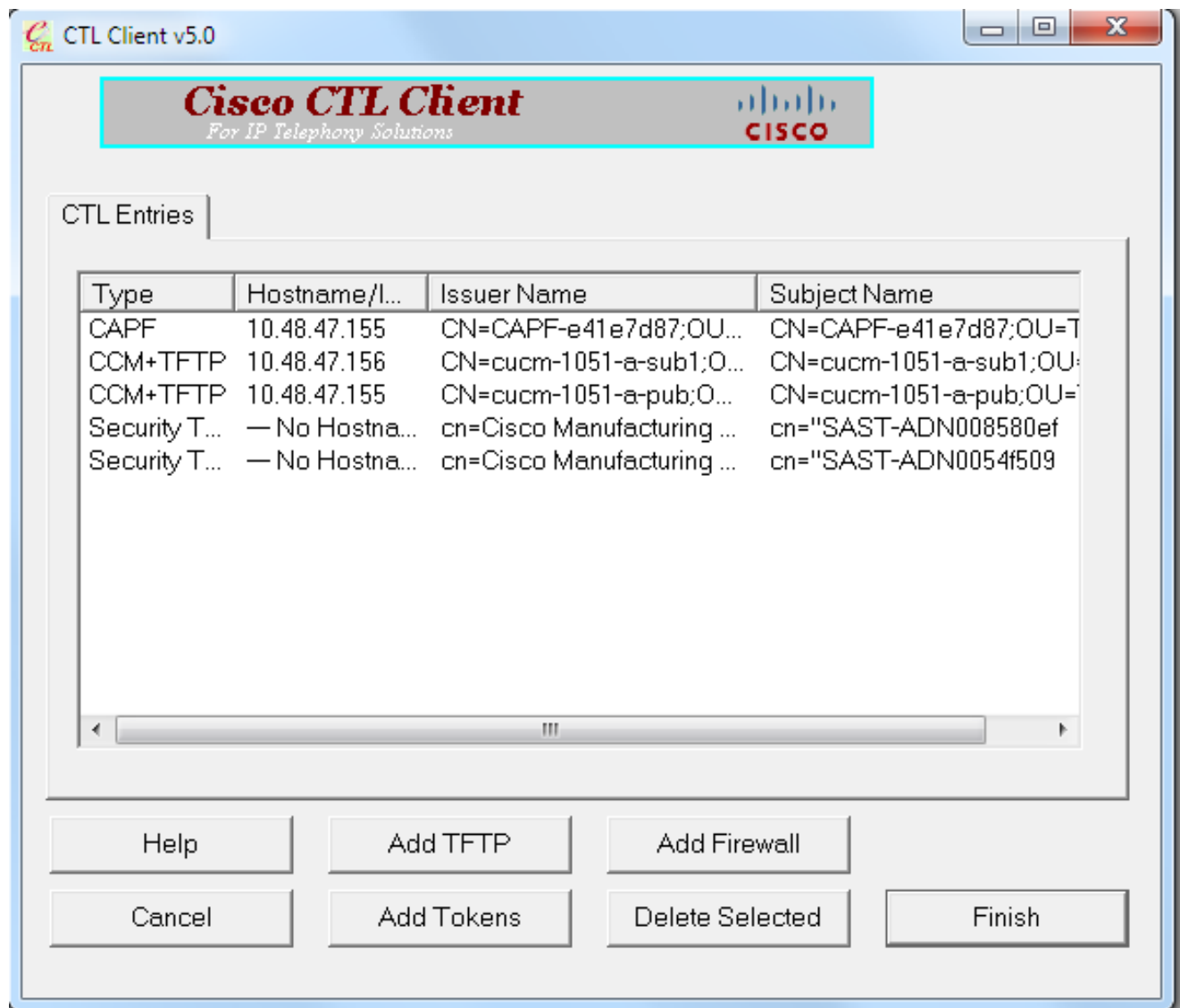
16. Una volta visualizzato il contenuto del file CTL, fare clic su Add Tokens (Aggiungi token) per aggiungere il secondo eToken USB:



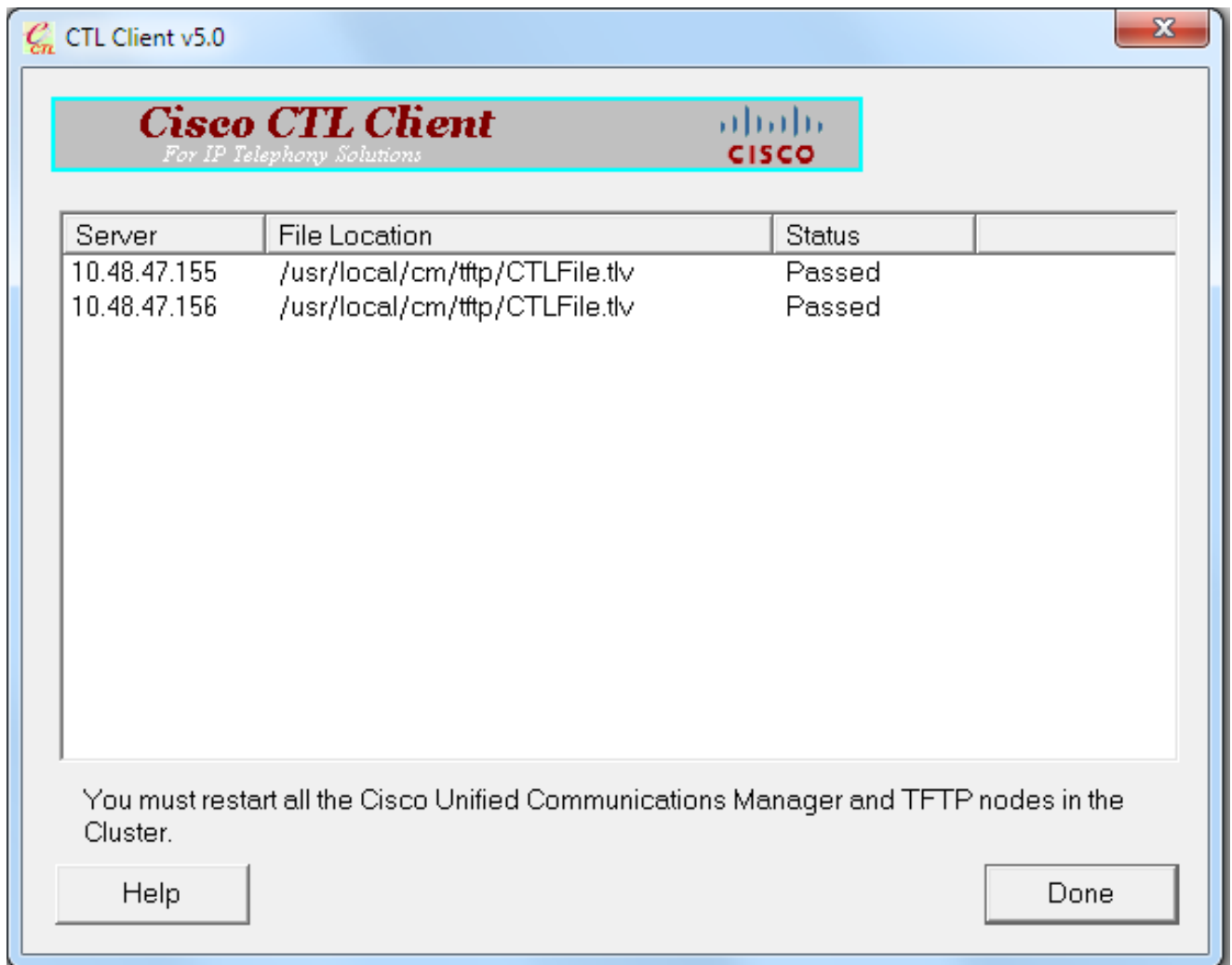
17. Dopo aver visualizzato i dettagli del token di sicurezza, fare clic su Add:



18. Una volta visualizzato il contenuto del file CTL, fare clic su Fine. Quando viene richiesta una password, immettere Cisco123:



19. Quando viene visualizzato l'elenco dei server CUCM su cui è presente il file CTL, fare clic su Fine:



20. Riavviare i servizi TFTP e CallManager in tutti i nodi del cluster che eseguono questi servizi.
21. Riavviare tutti i telefoni IP in modo che possano ottenere la nuova versione del file CTL dal servizio CUCM TFTP.
22. Per verificare il contenuto del file CTL, immettere il comando `show ctl` nella CLI. Nel file CTL è possibile visualizzare i certificati di entrambi gli eToken USB (uno dei due viene utilizzato per firmare il file CTL). Di seguito è riportato un esempio di output:

```
<#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	ISSUENAME	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	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.

23. Dal lato dell'IP Phone, è possibile verificare che dopo il riavvio, i telefoni IP abbiano scaricato la versione aggiornata del file CTL (il checksum MD5 corrisponde all'output del CUCM):



Questa modifica è possibile perché i certificati eToken sono stati precedentemente esportati e caricati nell'archivio di certificati attendibili CUCM e i telefoni IP sono in grado di verificare questo certificato sconosciuto utilizzato per firmare il file CTL rispetto al servizio di verifica della attendibilità (TVS) in esecuzione sul CUCM.

Questo frammento di registro illustra come il telefono IP contatta i televisori CUCM con una richiesta di verifica del certificato eToken sconosciuto, caricato come Phone-SAST-trust e considerato attendibile:

```
<#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
```

Rigenerazione certificati per soluzione CTL senza token


In questa sezione viene descritto come rigenerare un certificato di sicurezza cluster CUCM quando si utilizza la soluzione CTL senza token.

Durante il processo di manutenzione di CUCM, a volte il certificato CallManager del nodo di CUCM Publisher cambia.

Gli scenari in cui questo può verificarsi includono la modifica del nome host, la modifica del dominio o semplicemente la rigenerazione di un certificato (a causa della data di scadenza del certificato chiuso).

Dopo l'aggiornamento, il file CTL viene firmato con un certificato diverso da quelli esistenti nel file CTL installato sui telefoni IP.

Normalmente, questo nuovo file CTL non viene accettato; tuttavia, dopo che il telefono IP ha trovato il certificato sconosciuto utilizzato per firmare il file CTL, contatta il servizio TVS su CUCM.

 Nota: l'elenco dei server TVS si trova nel file di configurazione IP Phone e viene mappato nei server CUCM dal pool di dispositivi IP Phone > Gruppo CallManager.

Una volta completata la verifica sul server TVS, il telefono IP aggiorna il suo file CTL con la nuova versione. Questi eventi si verificano in uno scenario di questo tipo:

1. Il file CTL esiste sul CUCM e sul telefono IP. Il certificato CCM+TFT (server) per il nodo di CUCM Publisher viene utilizzato per firmare il file CTL:

```
<#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=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=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=Malopolska;C=PL
4	FUNCTION	2	

CCM+TFTP

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	

[...]

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
90e586e5945060b109bdf859b4c983cdf21699e3e4abdb0a47ba6f3c04cd7d4f59efeff4a60f6cf3c5db
2ec32988605ae4352e77d647da25fae619dedf9ebb0e0bdd98f8ce70307ba106507a8919df8b8fd9f9
03068a52640a6a84487a90203010001
Extensions: 3 present
```

2. Il file CallManager.pem (certificato CCM+TFTP) viene rigenerato ed è possibile verificare che il numero di serie del certificato cambia:

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. Il comando `utils ctl update CTLFile` viene immesso nella CLI per aggiornare il file CTL:

```
<#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. Il servizio TVS aggiorna la cache dei certificati con i dettagli del nuovo file CTL:

```
<#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. Quando si visualizza il contenuto del file CTL, è possibile verificare che il file sia firmato con il nuovo certificato del server CallManager per il nodo Publisher:

```
<#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. Dalla pagina Manutenzione unificata, i servizi TFTP e Cisco CallManager vengono riavviati su tutti i nodi del cluster che eseguono questi servizi.
7. I telefoni IP vengono riavviati e contattano il server TVS per verificare il certificato sconosciuto che è ora utilizzato per firmare la nuova versione del file CTL:

```
<#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
```

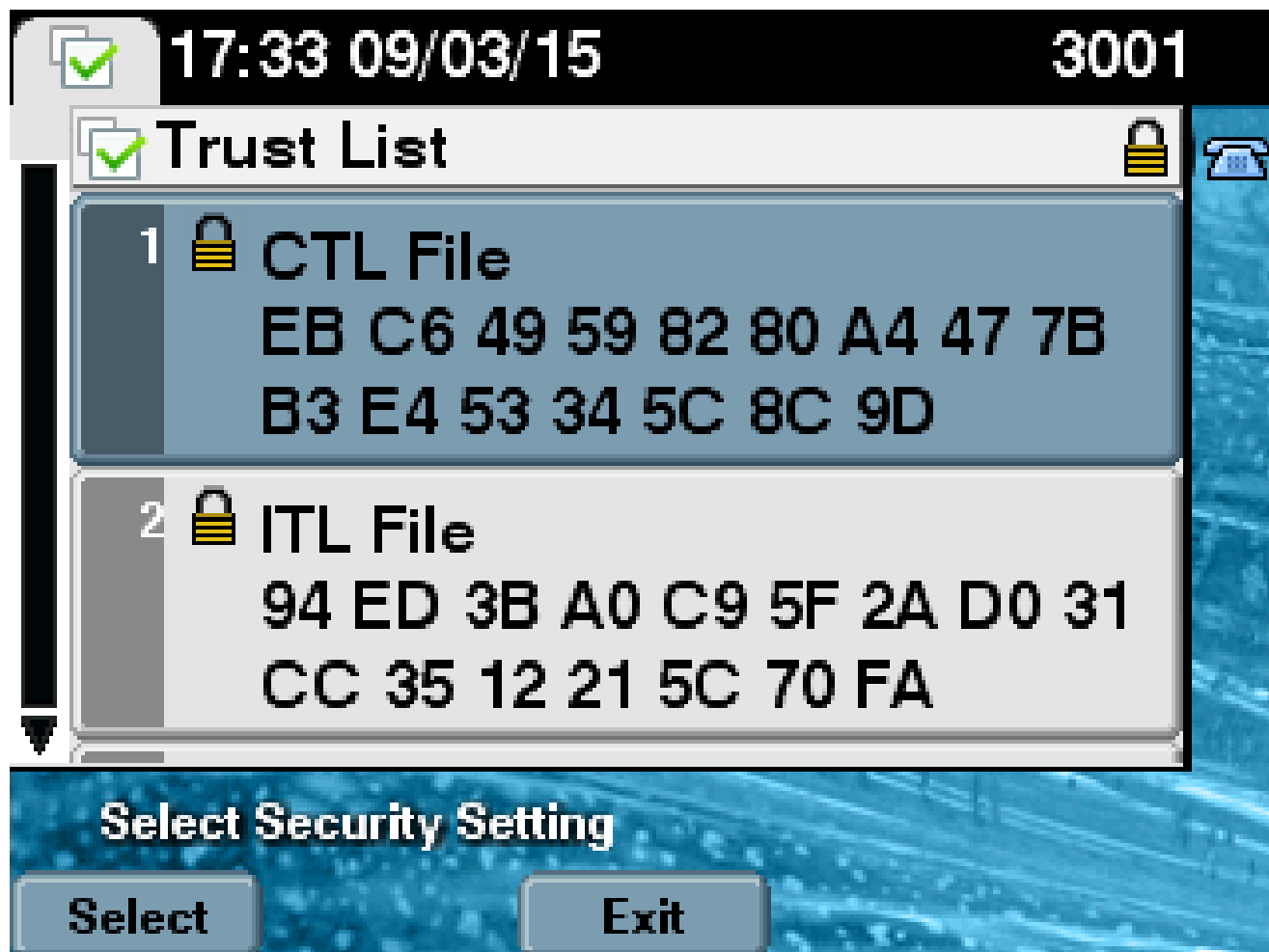
```
//
```

```
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. Infine, sui telefoni IP, è possibile verificare che il file CTL sia aggiornato con la nuova versione e che il checksum MD5 del nuovo file CTL corrisponda a quello del CUCM:



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).