Modo mezclado CUCM con Tokenless CTL

Contenido

Introducción

Este documento describe la diferencia entre la Seguridad del administrador de las Comunicaciones unificadas de Cisco (CUCM) con y sin el uso de los eTokens del hardware USB. Este documento también describe las situaciones de implementación básicas que implican Tokenless Certificate Trust List (Lista de confianza del certificado) (CTL) y el proceso que se utiliza para asegurarse de que las funciones de sistema correctamente después de los cambios.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento de la versión 10.0(1) o posterior CUCM. Además, asegure eso:

- Usted tiene acceso administrativo al comando line interface(cli) del nodo CUCM Publisher.
- Usted tiene acceso a los eTokens del hardware USB y eso el plugin del cliente CTL está instalada en su PC para los escenarios que le requieren emigrar de nuevo al uso de los eTokens del hardware.
- Hay total conectividad entre todos los Nodos CUCM en el cluster. Esto es muy importante porque el archivo CTL se copia a todos los Nodos en el cluster vía el protocolo FTP de SSH (SFTP).
- La replicación de la base de datos (DB) en el cluster trabaja correctamente y ésa los

servidores replica los datos en el tiempo real.

- Los dispositivos en su despliegue soportan la Seguridad por abandono (los TV). Usted puede utilizar la *lista unificada de la función del teléfono CM del* Cisco unificada señalando el Web page (IP o FQDN>/cucreports/de https:// <CUCM) para determinar los dispositivos que soportan la Seguridad por abandono. **Note**: El Jabber de Cisco y mucho los Teléfonos IP de las 7940/7960 Series del Cisco TelePresence o de Cisco no soporta actualmente la Seguridad por abandono. Si usted despliega Tokenless CTL con los dispositivos que no soportan la Seguridad por abandono, cualquier actualización a su sistema que cambie el certificado del CallManager en el editor evitará que esos dispositivos se registren con el sistema hasta que su CTL se borre manualmente.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 10.5.1.10000-7 (cluster CUCM de dos Nodos)
- Teléfonos IP de las Cisco 7975 Series registradoes vía el protocolo skinny client control (SCCP) con la versión de firmware SCCP75.9-3-1SR4-1S
- Dos tokens del Cisco Security que se utilizan para fijar el cluster al modo mezclado con el uso del software de cliente CTL

Antecedentes

Tokenless CTL es una nueva función en las versiones CUCM 10.0(1) y posterior que permita el cifrado de la señalización de llamada y de los media para los Teléfonos IP sin la necesidad de utilizar los eTokens del hardware USB y al plugin del cliente CTL, que era el requisito en las versiones anteriores CUCM.

Cuando el cluster se pone en el modo mezclado con el uso del comando CLI, el archivo CTL se firma con el certificado CCM+TFTP (servidor) del nodo de Publisher, y hay ningún eToken los Certificados presentes en el archivo CTL.

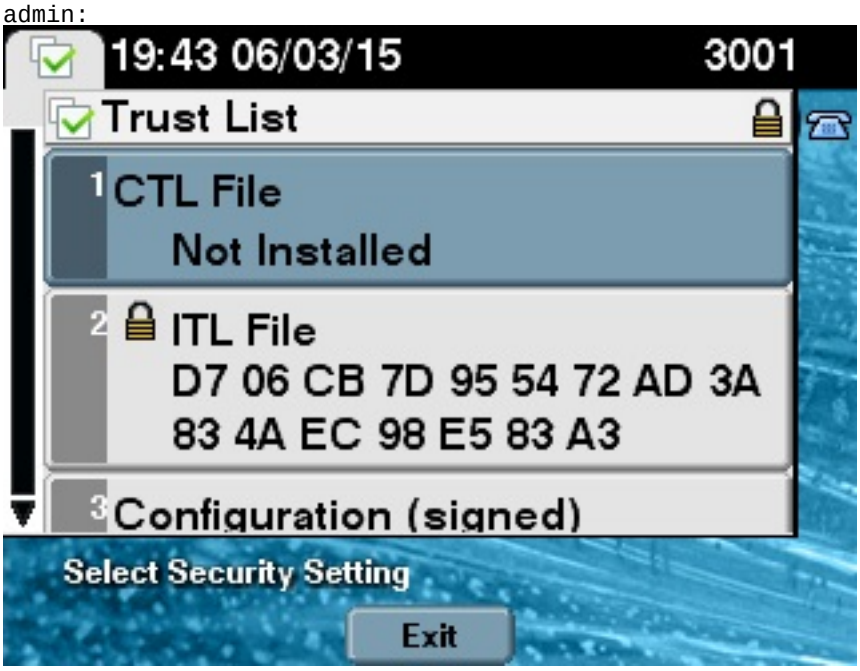
> **Note**: Cuando usted regenera el certificado del CallManager (CCM+TFTP) en el editor, cambia al firmante del archivo. Los teléfonos y los dispositivos que no soportan la Seguridad por abandono no validarán el nuevo archivo CTL a menos que los archivos CTL **se borren manualmente de cada dispositivo**. Refiera al requisito más reciente que se enumera la sección de los requisitos de este documento para más información.

Del modo NON-seguro al modo mezclado (Tokenless CTL)

Esta sección describe el proceso que se utiliza para trasladarse la Seguridad del cluster CUCM al modo mezclado vía el CLI.

Antes de este escenario, el CUCM estaba en el modo NON-seguro, así que significa que no había archivo CTL presente en los Nodos uces de los y que los Teléfonos IP registradoes tenían solamente un archivo de la lista de la confianza de la identidad (ITL) instalado, tal y como se muestra en de estas salidas:

```
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:
```



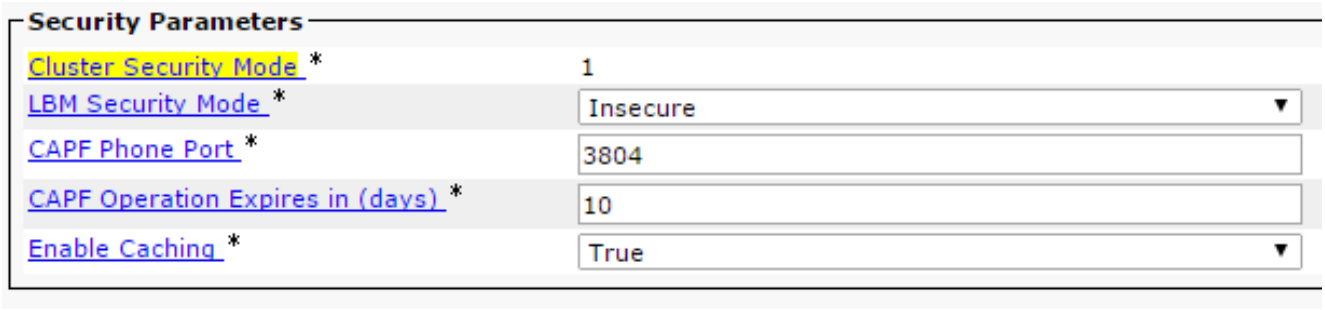
Para trasladarse la Seguridad del cluster CUCM al modo mezclado con el uso de la nueva característica de Tokenless CTL, complete estos pasos:

1. Obtenga el acceso administrativo al nodo CLI CUCM Publisher.

2. Ingrese el comando del conjunto-**cluster mezclado-MODE del ctl del utils** en el CLI:

   ```
   admin:utils ctl set-cluster mixed-mode
   This operation will set 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. Navegue a la **página de administración > al System (Sistema) > Enterprise Parameters (Parámetros Enterprise) CUCM** y verifique si el cluster fue fijado al modo mezclado (un valor de **1** indica el modo mezclado):



4. Recomience el TFTP y los servicios del Cisco CallManager en todos los Nodos en el cluster que dirijan estos servicios.

5. Recomience todos los Teléfonos IP de modo que puedan obtener el archivo CTL del CUCM servicio TFTP.

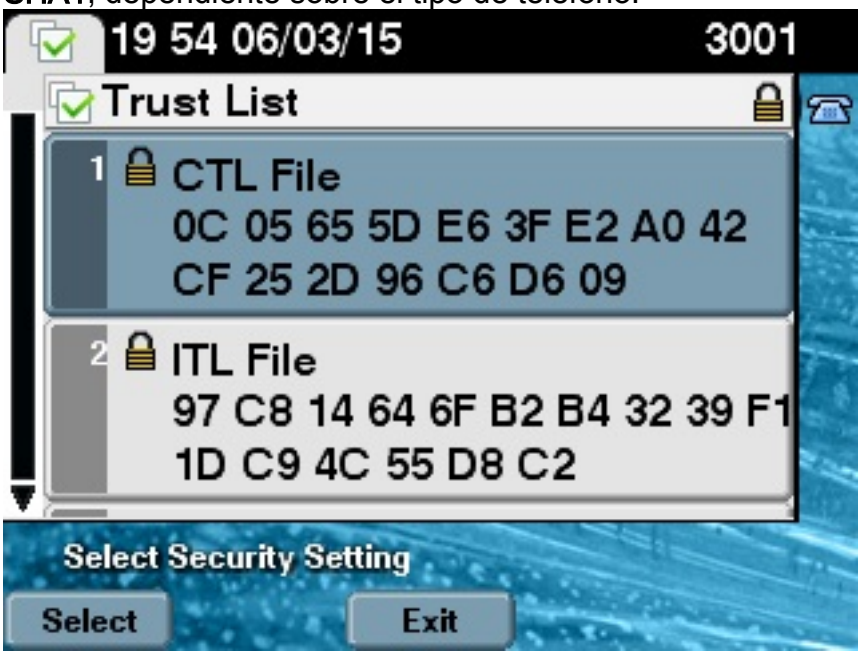
6. Para verificar el contenido del archivo CTL, ingrese el comando del **ctl de la demostración** en el CLI. En el archivo CTL usted puede ver que el certificado CCM+TFTP (servidor) para el nodo CUCM Publisher está utilizado para firmar el archivo CTL (este archivo es lo mismo en todos los servidores en el cluster). Éste es un ejemplo de salida:

```
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=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

[...]

The CTL file was verified successfully.
```

7. En el lado del teléfono del IP, usted puede verificar eso después de que se recomience el servicio, él descarga el archivo CTL, que está presente ahora en el servidor TFTP (la suma de comprobación MD5 hace juego cuando está comparado a la salida del CUCM):

   Note: Cuando usted verifica la suma de comprobación en el teléfono, usted ve el **MD5** o el **SHA1**, dependiente sobre el tipo de teléfono.



De los eTokens del hardware a la solución de Tokenless

Esta sección describe cómo emigrar la Seguridad del cluster CUCM de los eTokens del hardware al uso de la nueva solución de Tokenless.

En algunas situaciones, el modo mezclado se configura ya en el CUCM con el uso del cliente CTL, y los archivos del uso CTL de los Teléfonos IP que contienen los Certificados de los eTokens del hardware USB. Con este escenario, el archivo CTL es firmado por un certificado a partir del uno de los eTokens USB y instalado en los Teléfonos IP. Aquí en un ejemplo:

```
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.
```

Complete estos pasos para mover la Seguridad del cluster CUCM al uso de Tokenless CTL:

1. Obtenga el acceso administrativo al nodo CLI CUCM Publisher.

2. Ingrese el comando CLI de **CTLFile de la actualización del ctl del utils**:

   ```
   admin:utils ctl update CTLFile
   This operation will update 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. Recomience el TFTP y los servicios de CallManager en todos los Nodos en el cluster que dirijan estos servicios.

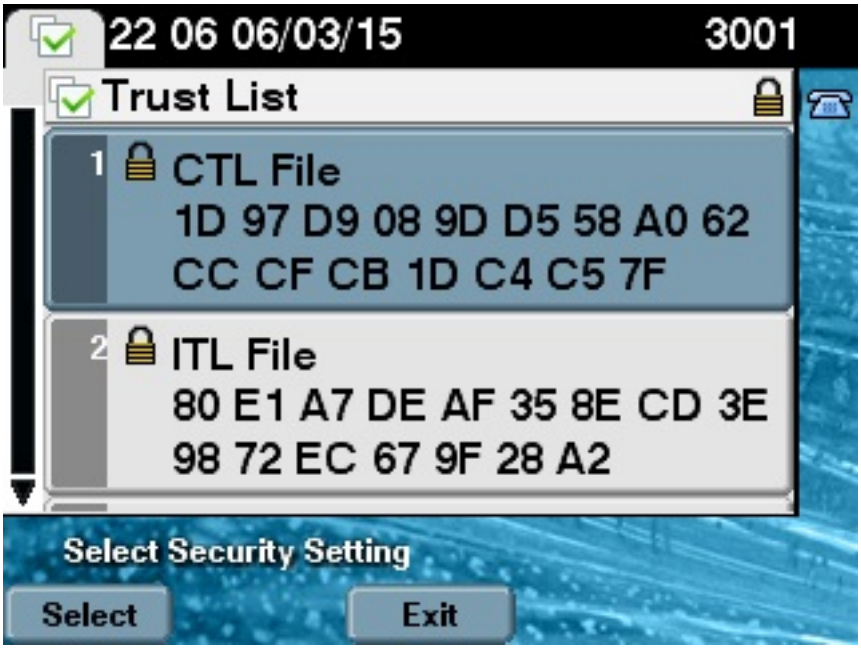
4. Recomience todos los Teléfonos IP de modo que puedan obtener el archivo CTL del CUCM servicio TFTP.

5. Ingrese el comando del **ctl de la demostración** en el CLI para verificar el contenido del archivo CTL. En el archivo CTL, usted puede ver que el certificado CCM+TFTP (servidor) del

nodo CUCM Publisher está utilizado para firmar el archivo CTL en vez del certificado de los eTokens del hardware USB. Una diferencia más importante en este caso es que los Certificados de todos los eTokens del hardware USB están quitados del archivo CTL. Éste es un ejemplo de salida:

```
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=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

[...]

The CTL file was verified successfully.
```

6. En el lado del teléfono del IP, usted puede verificar eso después de que los Teléfonos IP fueran recomenzados, ellos descargó la versión del archivo actualizada CTL (la suma de comprobación MD5 hace juego cuando está comparado a la salida del CUCM):



De la solución de Tokenless a los eTokens del hardware

Esta sección describe cómo emigrar la Seguridad del cluster CUCM lejos de la nueva solución de Tokenless y de nuevo al uso de los eTokens del hardware.

Cuando la Seguridad del cluster CUCM se fija al modo mezclado con el uso de los comandos CLI, y el archivo CTL se firma con el certificado CCM+TFTP (servidor) para el nodo CUCM Publisher, no hay Certificados de los eTokens del hardware USB presentes en el archivo CTL. Por este motivo, cuando usted funciona con al cliente CTL para poner al día el archivo CTL (movimiento de nuevo al uso de los eTokens del hardware), este mensaje de error aparece:

```
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=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

[...]

The CTL file was verified successfully.
```

Esto es determinado importante en los escenarios que incluyen un downgrade (cuando la versión se conmuta detrás) del sistema a una versión pre-10.x que no incluya los comandos del **ctl del utils**. El archivo anterior CTL se emigra (sin los cambios en su contenido) en curso de restauración o Linux a la actualización de Linux (L2), y no contiene los Certificados del eToken, como se mencionó anteriormente. Éste es un ejemplo de salida:

```
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 ISSUERNAME 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:
```

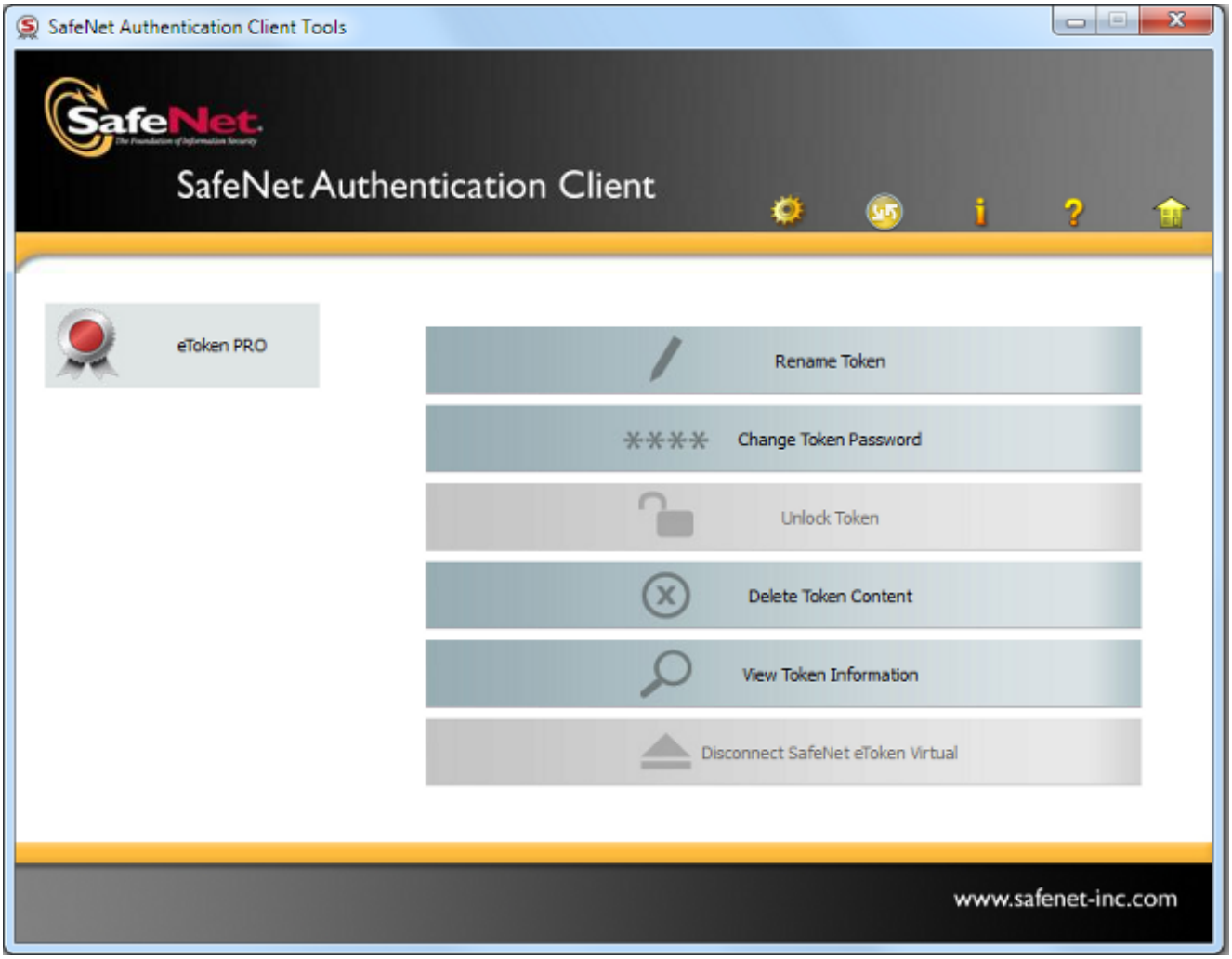
Para este escenario, complete estos pasos para poner al día con seguridad los archivos CTL sin la necesidad de utilizar el procedimiento para los eTokens perdidos, que termina para arriba en la Eliminación manual del archivo CTL de todos los Teléfonos IP:

1. Obtenga el acceso administrativo al nodo CLI CUCM Publisher.

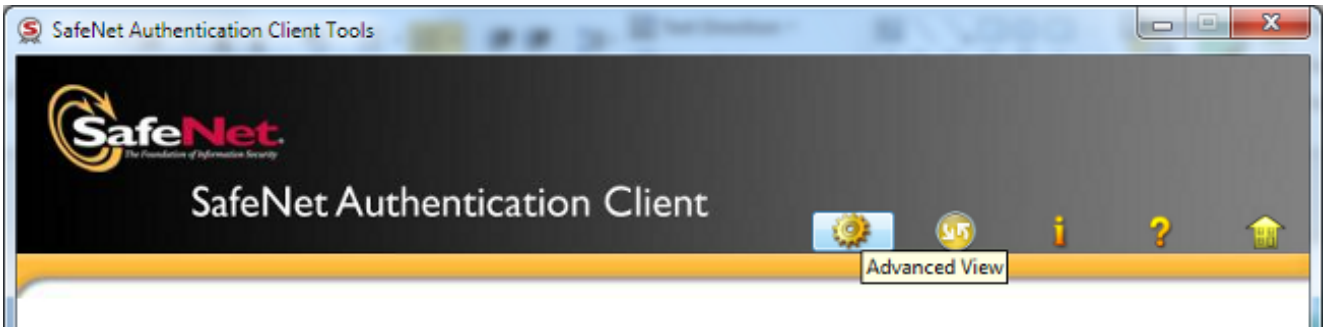
2. Ingrese el **comando del tftp CTLFile.tlv de la cancelación del archivo** en el nodo CLI de Publisher para borrar el archivo CTL:

   ```
   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. Abra a la **Autenticación de clientes de SafeNet** en la máquina de Microsoft Windows que tiene el cliente CTL instalado (está instalada automáticamente con el cliente CTL):

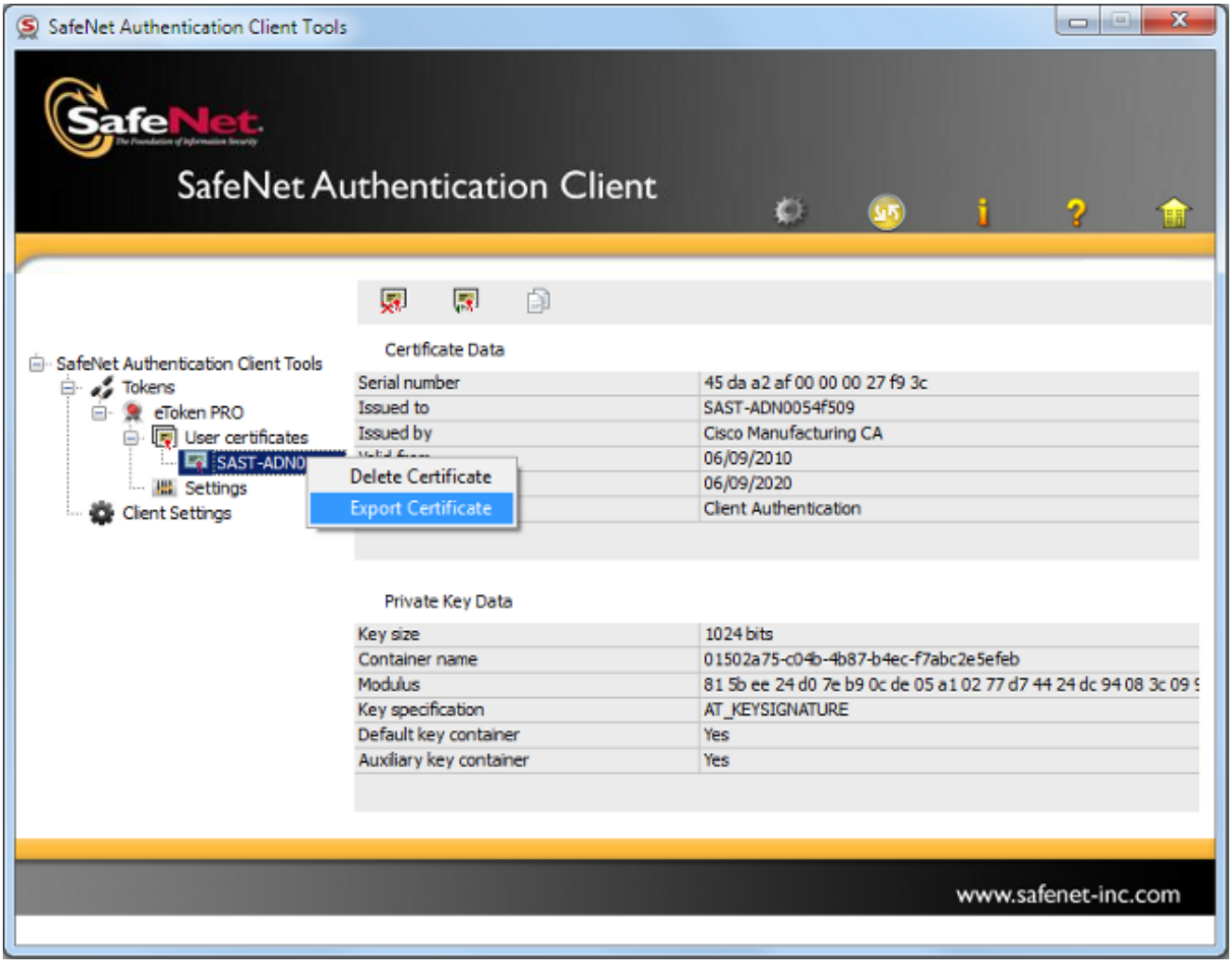


4. En la Autenticación de clientes de SafeNet, navegue a la *visión avanzada*:

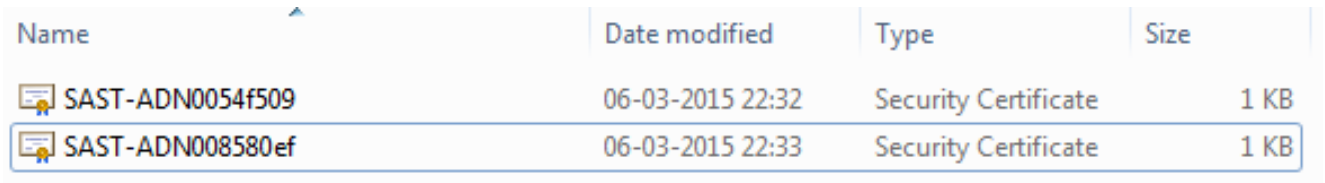


5. Inserte el primer hardware USB eToken.

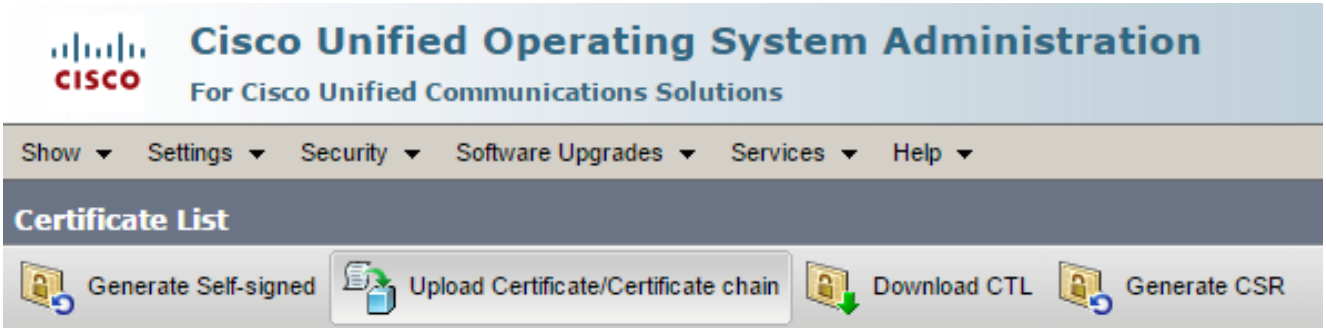
6. Seleccione el certificado bajo la carpeta de los *Certificados de usuario* y expórtelo a la carpeta en el PC. Cuando se le pregunte para una contraseña, utilice la contraseña predeterminada del **cisco123**:



7. Relance estos pasos para el segundo hardware USB eToken para exportar ambos Certificados al PC:

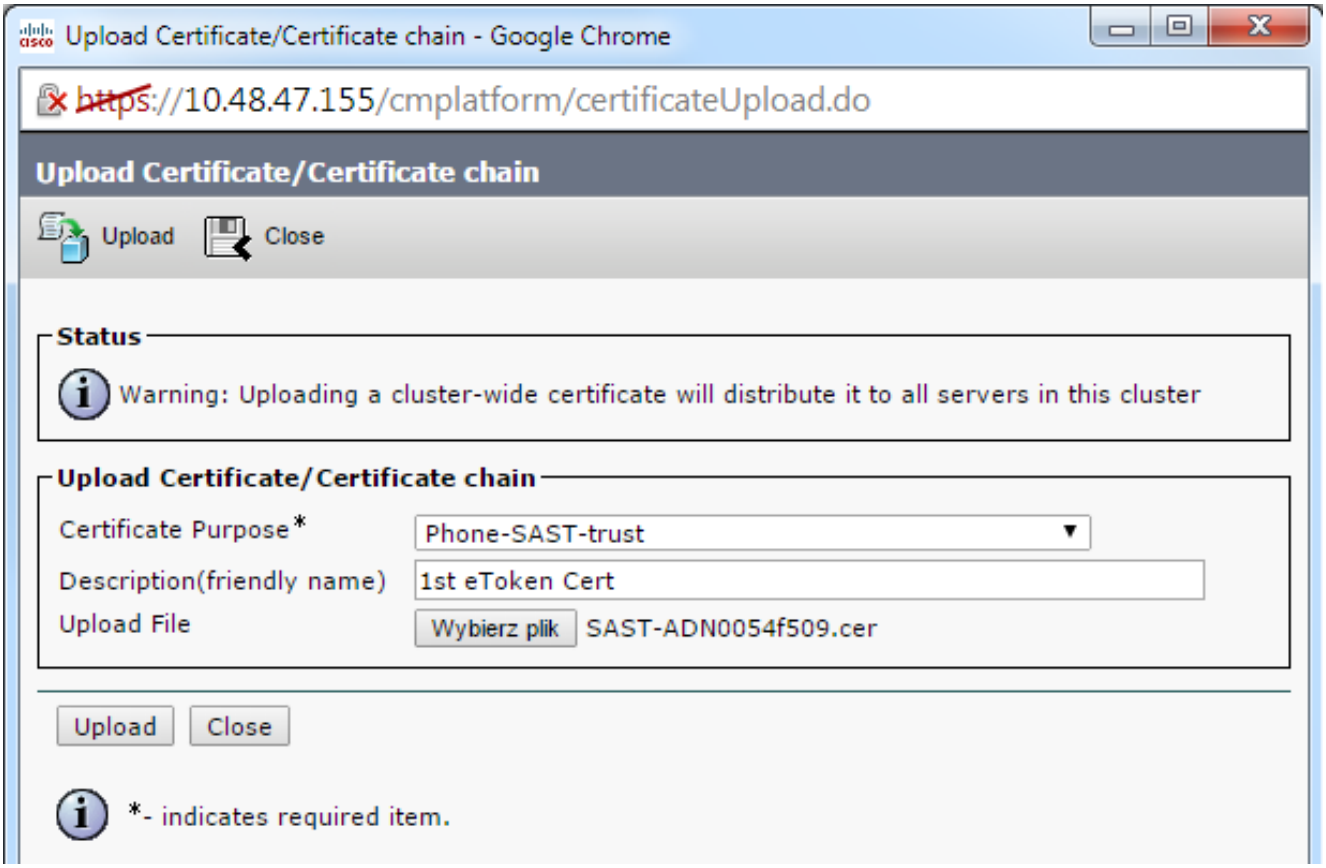


8. El registro en la administración unificada Cisco del operating system (OS) y navega al **Certificate Management (Administración de certificados) de la Seguridad > al certificado de la carga**:

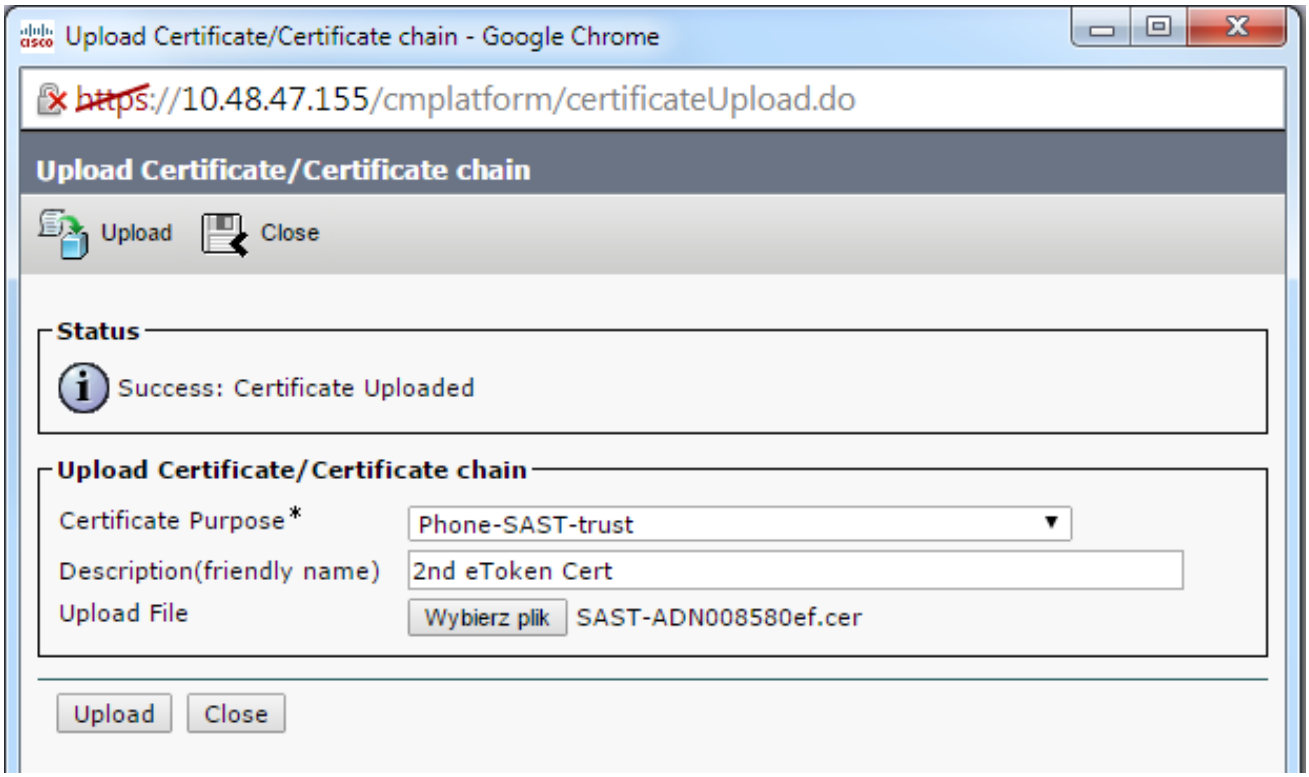


9. La página del certificado de la carga entonces aparece. Elija la Teléfono-SAST-**confianza del**

menú desplegable del propósito del certificado y seleccione el certificado que usted exportó del primer eToken:

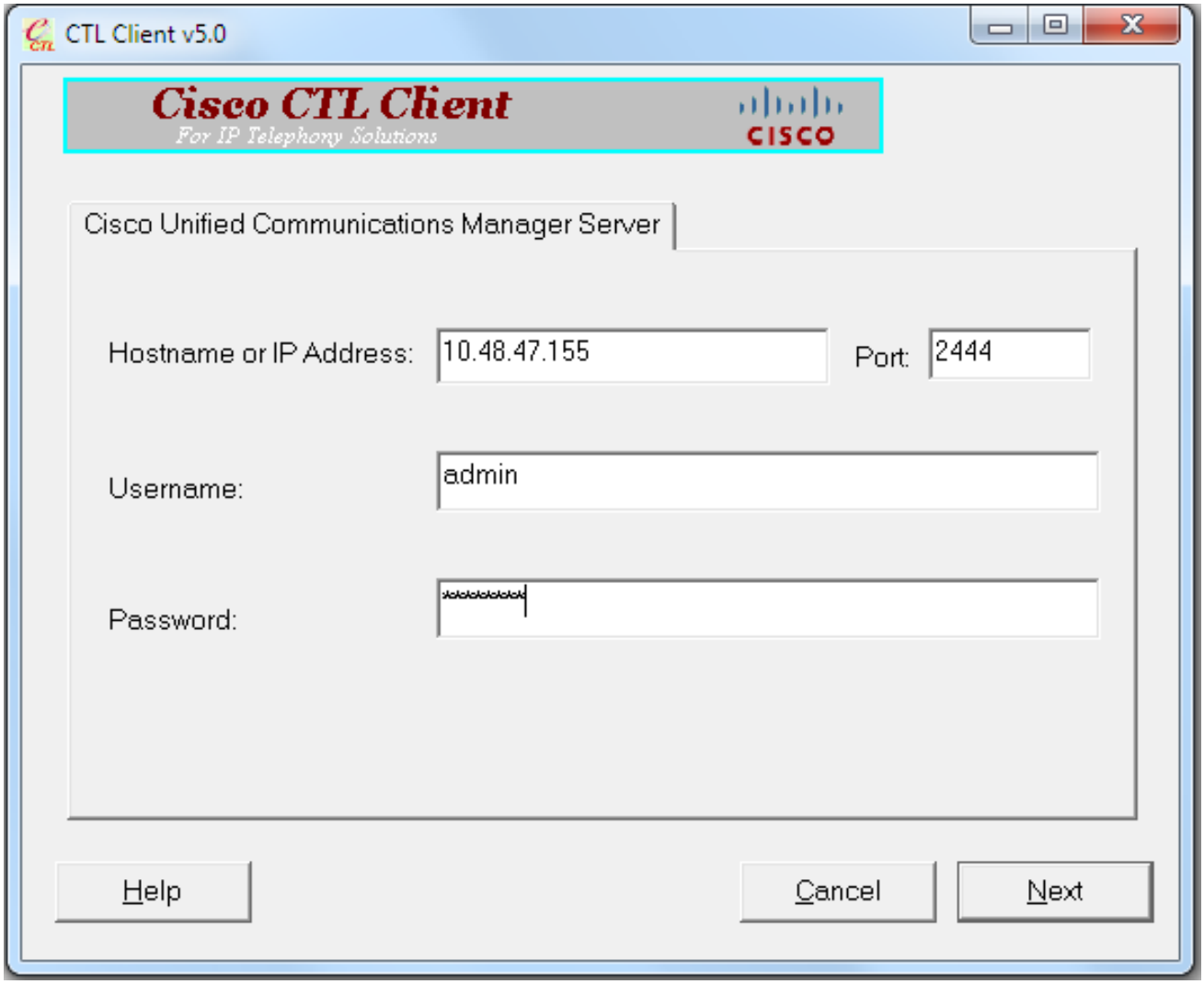


10. Complete los pasos anteriores para cargar el certificado que usted exportó del segundos eToken:



11. Funcione con al cliente CTL, proporcione el IP Address/el nombre de host del nodo CUCM

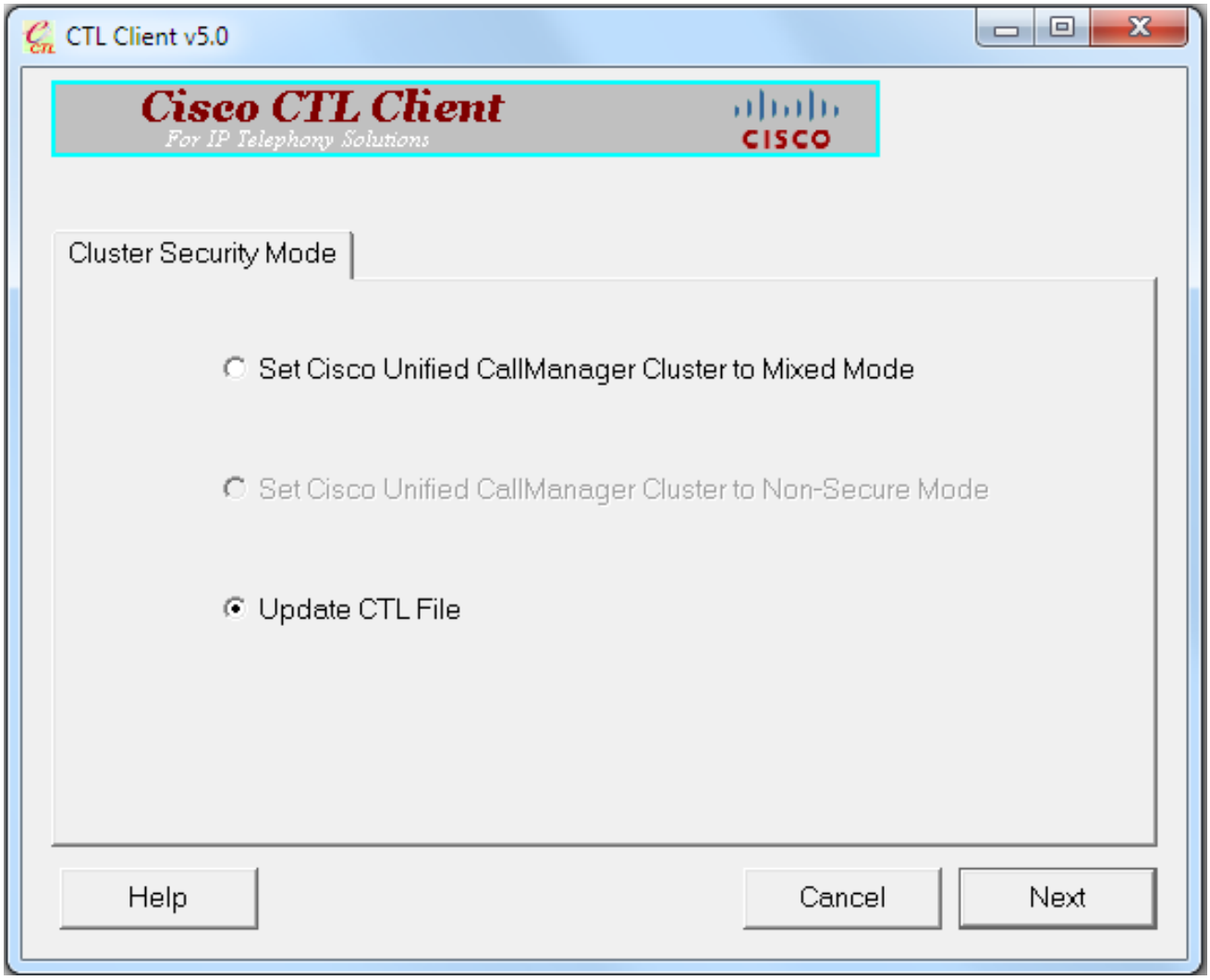
Publisher, y ingrese las credenciales del administrador CCM:



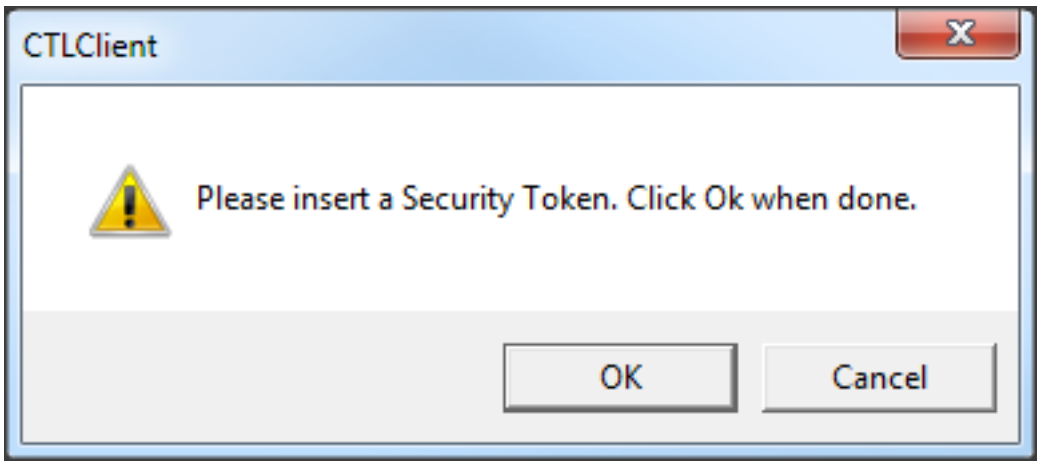
12. Puesto que el cluster está en el modo mezclado ya, pero ningún archivo CTL existe en el nodo de Publisher, este mensaje de advertencia aparece (**AUTORIZACIÓN del** tecleo para ignorarla):

```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1
```

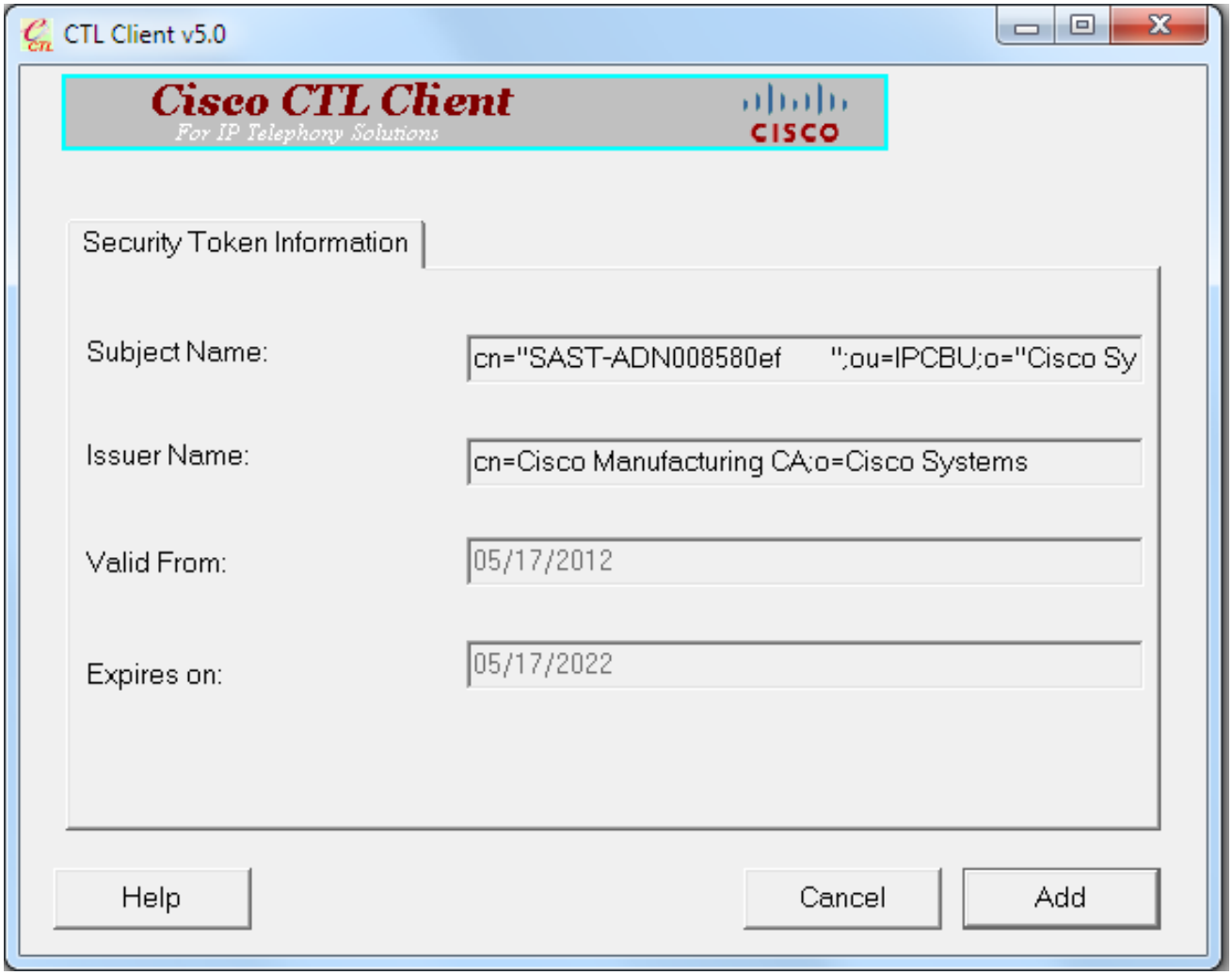
13. Del cliente CTL, haga clic el botón de radio del **archivo de la actualización CTL**, y después haga clic **después**:



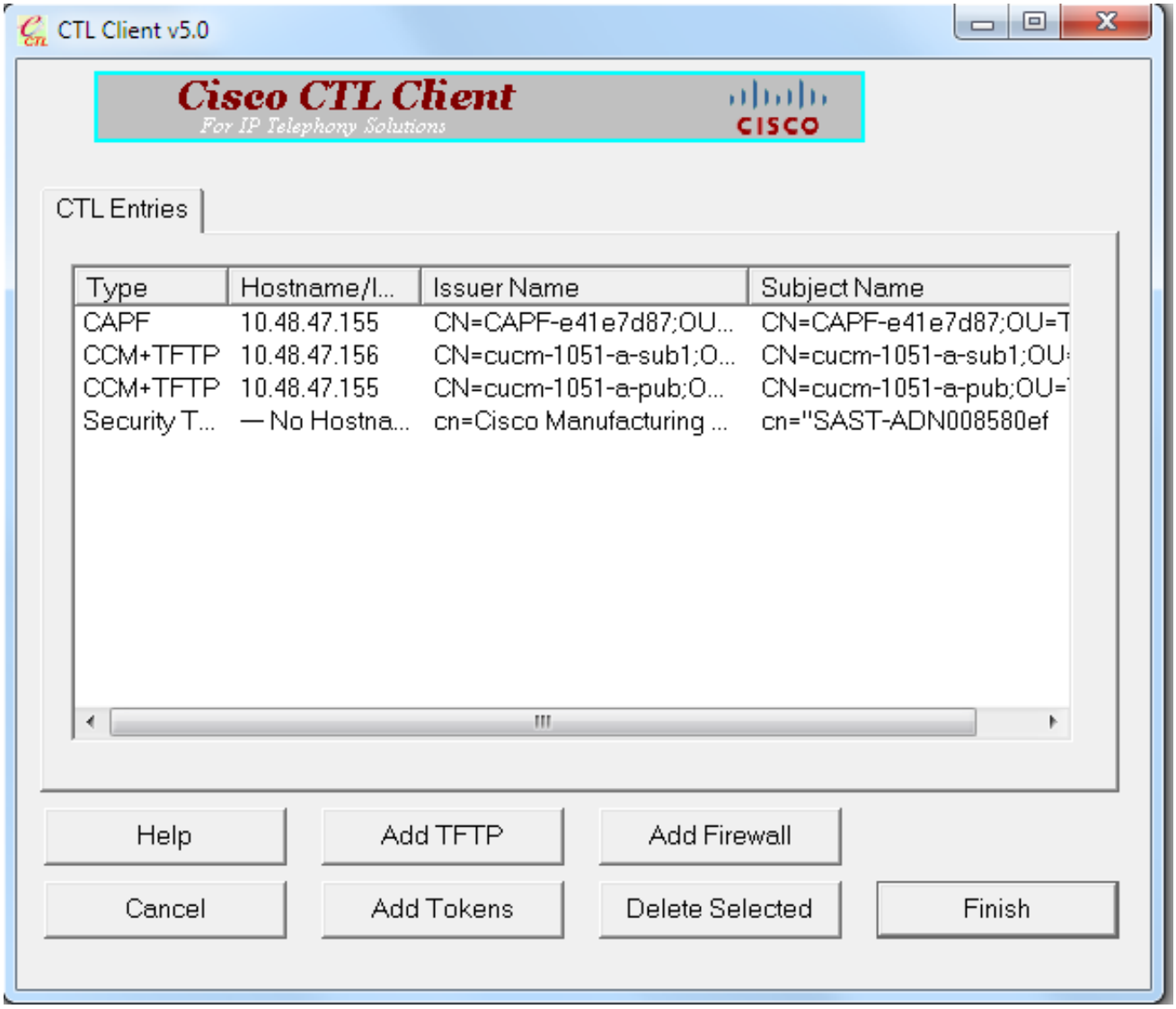
14. Inserte el primer token de seguridad y haga clic la **AUTORIZACIÓN**:



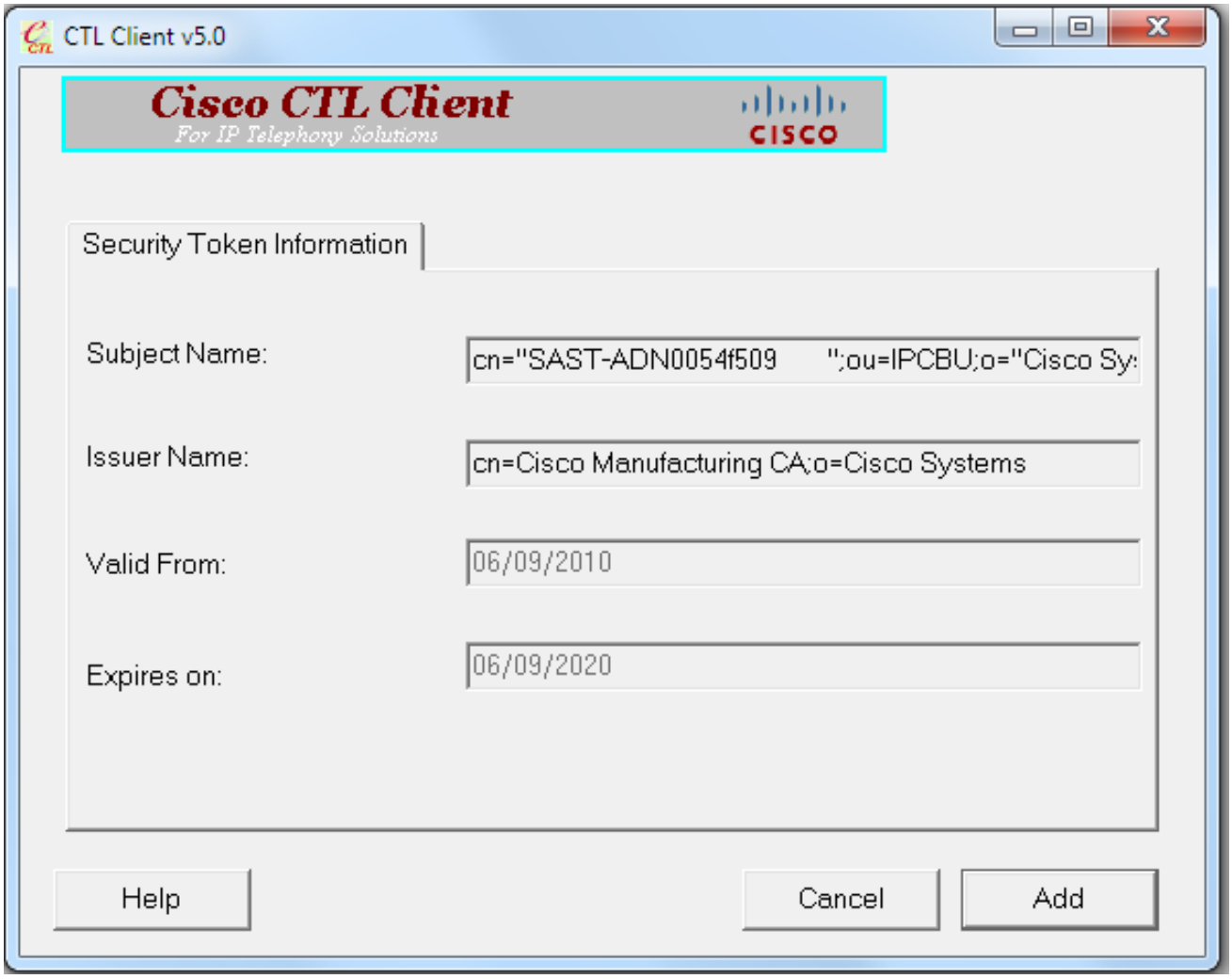
15. Después de que se visualicen los detalles del token de seguridad, el tecleo **agrega**:



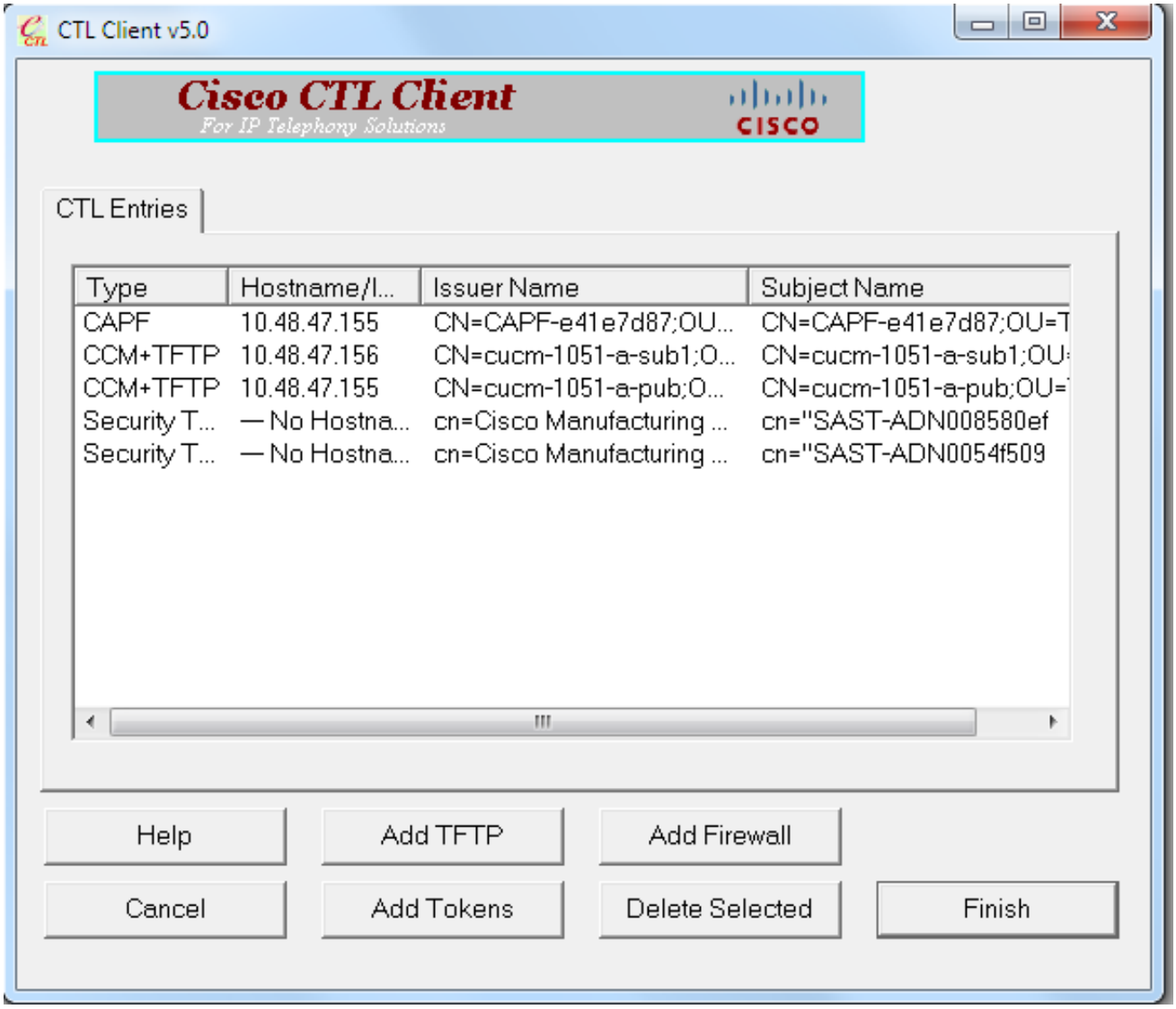
16. El contenido del archivo CTL aparece una vez, tecleo **agrega los tokens** para agregar el segundo USB eToken:



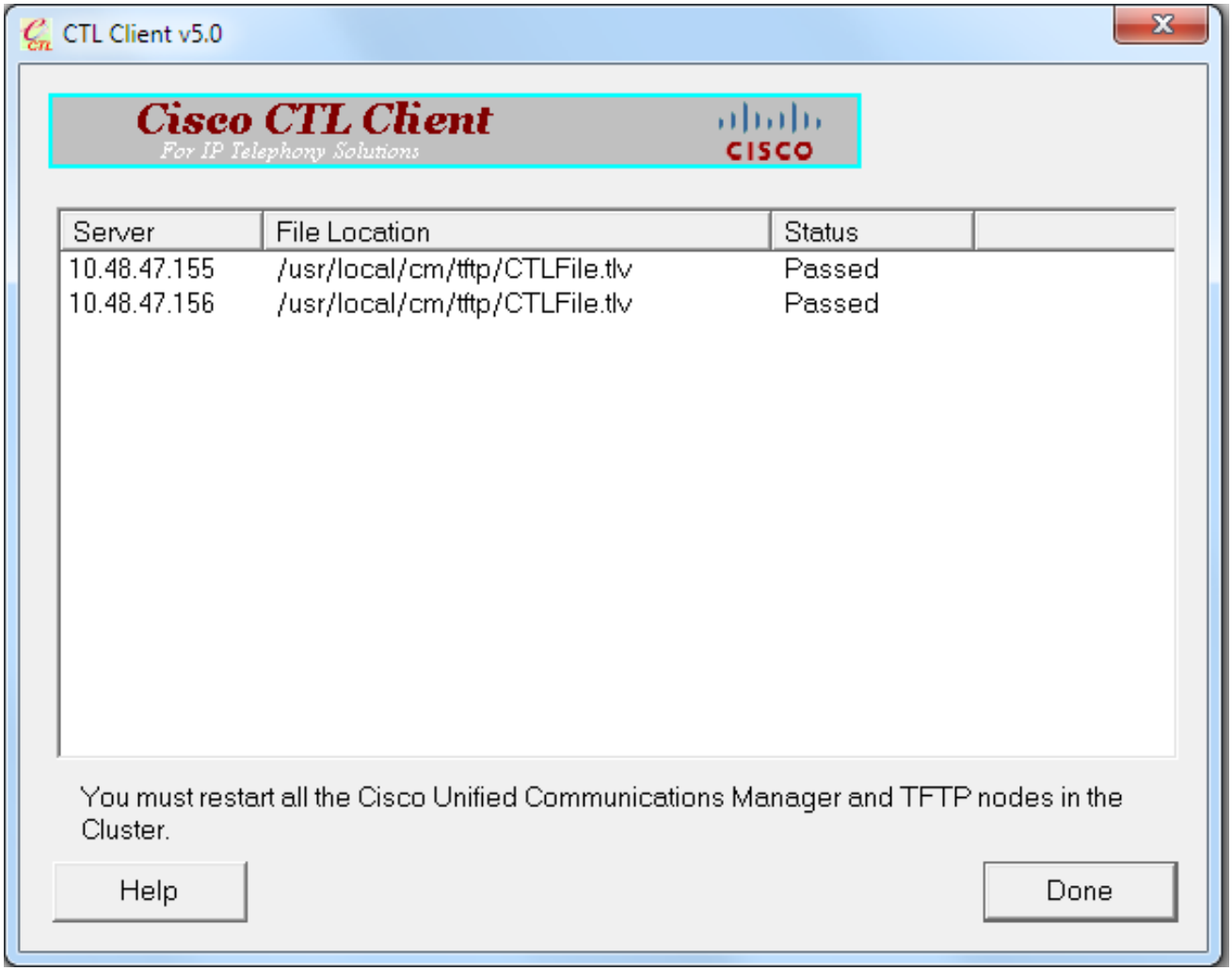
17. Después de que aparezcan los detalles del token de seguridad, el tecleo **agrega**:



18. Después de que aparezca el contenido del archivo CTL, clic en Finalizar. Cuando se le pregunte para una contraseña, ingrese el **cisco123**:



19. Cuando aparece la lista de servidores CUCM en los cuales el archivo CTL exista, tecleo **hecho**:



20. Recomience el TFTP y los servicios de CallManager en todos los Nodos en el cluster que dirijan estos servicios.

21. Recomience todos los Teléfonos IP de modo que puedan obtener la nueva versión del archivo CTL del CUCM servicio TFTP.

22. Para verificar el contenido del archivo CTL, ingrese el comando del **ctl de la demostración** en el CLI. En el archivo CTL usted puede ver los Certificados de ambos eTokens USB (uno de ellos se utiliza para firmar el archivo CTL). Éste es un ejemplo de salida:

```
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. En el lado del teléfono del IP, usted puede verificar eso después de que los Teléfonos IP fueran recomenzados, ellos descargó la versión del archivo actualizada CTL (la suma de comprobación MD5 hace juego cuando está comparado a la salida del CUCM):

Este cambio es posible porque usted exportó y cargó previamente los Certificados del eToken al almacén de la confianza del certificado CUCM, y los Teléfonos IP pueden verificar este certificado desconocido que fue utilizado para firmar el archivo CTL contra el servicio de la verificación de la confianza (TV) esos funcionamientos en el CUCM. Este snippit del registro ilustra cómo el teléfono del IP entra en contacto el CUCM TV con una petición de verificar el desconocido eToken el certificado, que está cargado como Teléfono-SAST-confianza y confiado en:

```
//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: 83E9080000005545AF31
23:00:22.052 | debug CertificateDBCache::getCertificateInformation - Looking up the
certificate cache using Unique MAP ID : 83E9080000005545AF31cn=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 : 83E9080000005545AF31cn=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
```

Regeneración del certificado para la solución de Tokenless CTL

Esta sección describe cómo regenerar un Security Certificate del cluster CUCM cuando se utiliza la solución de Tokenless CTL.

En curso de mantenimiento CUCM, el certificado del CallManager del nodo CUCM Publisher cambia a veces. Los escenarios en los cuales éste puede suceder incluyen el cambio del nombre de host, el cambio del dominio, o simplemente una regeneración del certificado (debida cerrar la fecha del vencimiento del certificado).

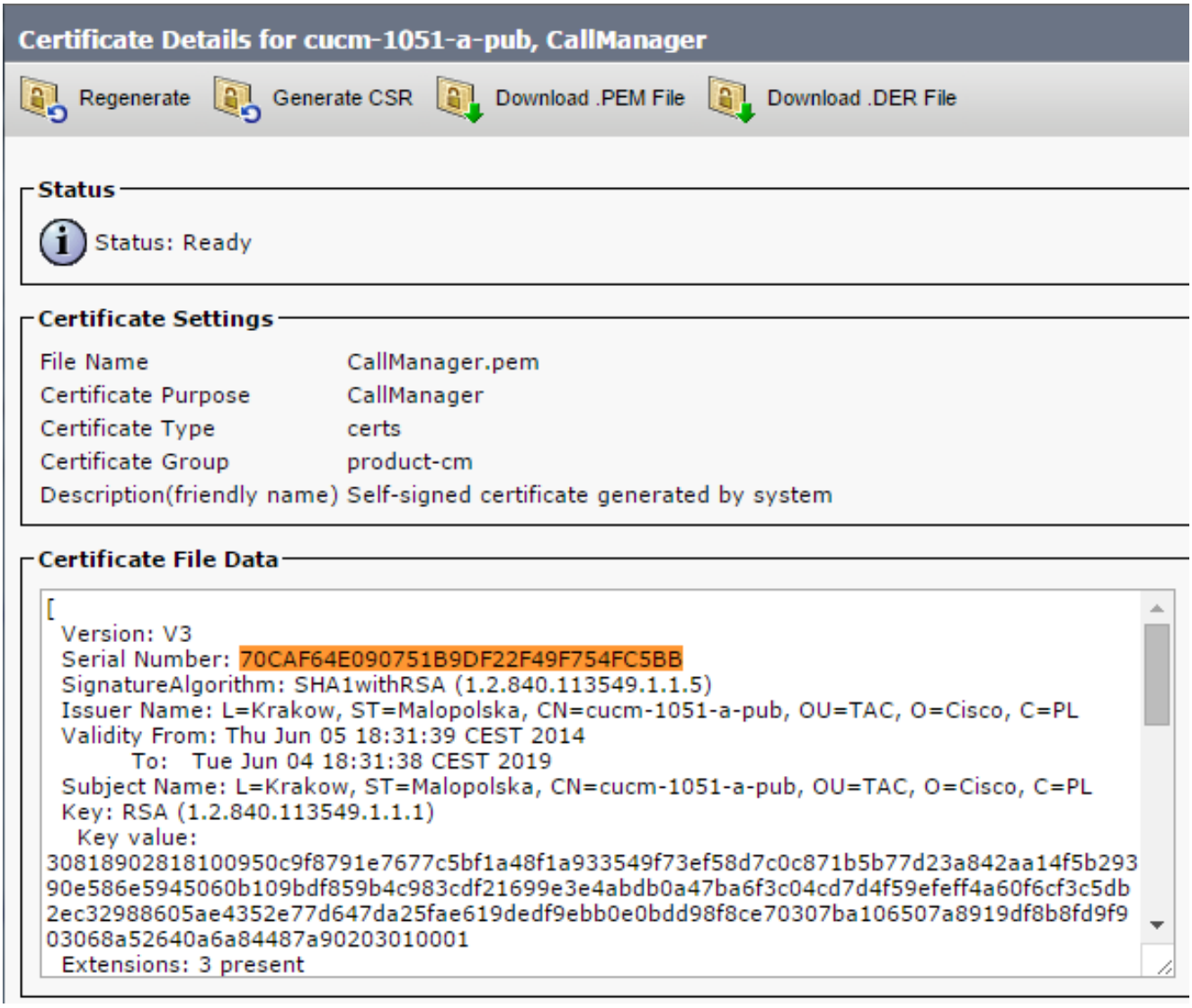
Después de que el archivo CTL sea actualizado, se firma con un diverso certificado que los que existan en el archivo CTL que está instalado en los Teléfonos IP. Normalmente, este nuevo archivo CTL no se valida; sin embargo, después de que el teléfono del IP encuentre el certificado desconocido que se utiliza para firmar el archivo CTL, entra en contacto el servicio TV en el CUCM.

Note: La lista de servidores TV está en Configuración del teléfono IP el archivo y se asocia en los servidores CUCM de la **agrupación de dispositivos > del grupo de CallManager del** teléfono del IP.

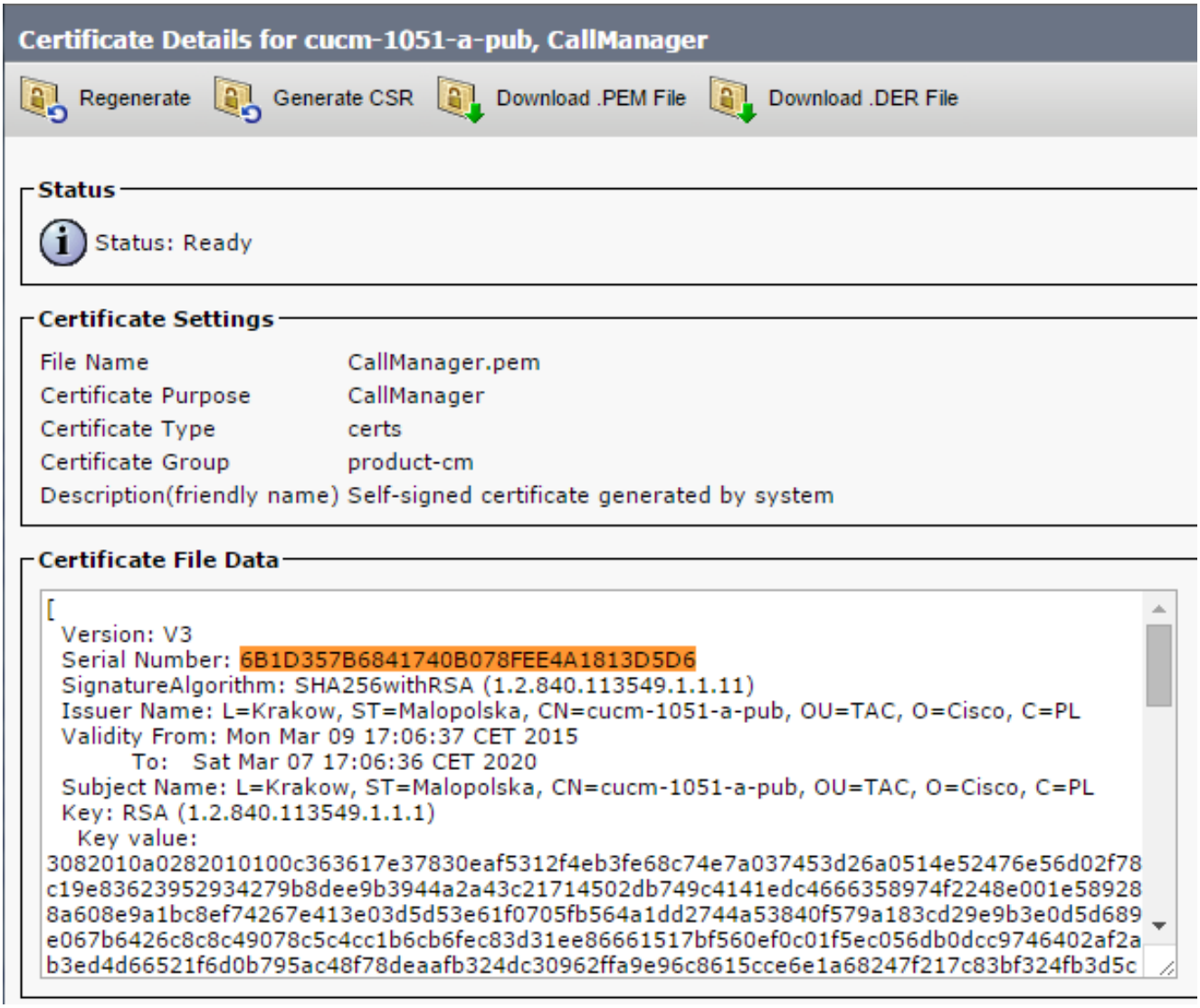
Sobre la verificación exitosa contra el servidor TV, el teléfono del IP pone al día su archivo CTL con la nueva versión. Estos eventos ocurren en tal escenario:

1. El archivo CTL existe en el CUCM y en el teléfono del IP. El certificado CCM+TFT (servidor) para el nodo CUCM Publisher se utiliza para firmar el archivo CTL:

```
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 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

[...]

The CTL file was verified successfully.
```



2. Se regenera el **archivo CallManager.pem** (certificado CCM+TFTP), y usted puede considerar que el número de serie del certificado cambia:



3. El comando de **CTLFile de la actualización del ctl del utils** se ingresa en el CLI para poner al día el archivo CTL:

```
admin:utils ctl update CTLFile
This operation will update 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. El servicio TV pone al día su caché del certificado con los nuevos detalles del archivo CTL:

```
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 ::
6B1D357B6841740B078FEE4A1813D5D6CN=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 ::
6B1D357B6841740B078FEE4A1813D5D6CN=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. Cuando usted ve el contenido del archivo CTL, usted puede ver que el archivo está firmado con el nuevo certificado de servidor del CallManager para el nodo de Publisher:

```
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

[..]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1675
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 6B:1D:35:7B:68:41:74:0B:07:8F:EE:4A:18:13:D5:D6
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 955 5C AF 7D 23 FE 82 DB 87 2B 6F 4D B7 F0 9D D5
86 EE E0 8B FC (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 1675
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 6B:1D:35:7B:68:41:74:0B:07:8F:EE:4A:18:13:D5:D6
7 PUBLICKEY 270
8 SIGNATURE 256
9 CERTIFICATE 955 5C AF 7D 23 FE 82 DB 87 2B 6F 4D B7 F0 9D D5
86 EE E0 8B FC (SHA1 Hash HEX)
10 IPADDRESS 4

[...]

The CTL file was verified successfully.
```

6. De la página unificada de la utilidad, recomienzan a los servicios TFTP y del Cisco CallManager en todos los Nodos en el cluster que dirijan estos servicios.

7. Se recomienzan los Teléfonos IP, y entran en contacto el servidor TV para verificar el certificado desconocido que ahora se utiliza para firmar la nueva versión del archivo CTL:

```
// 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. Finalmente, en los Teléfonos IP, usted puede verificar que el archivo CTL esté puesto al día con la nueva versión y que la suma de comprobación MD5 del nuevo archivo CTL hace juego con la del CUCM: