Ejemplo de configuración de clúster de CUCM cambiado de modo mixto a modo no seguro

Contenido

Introducción

En el documento se describen los pasos necesarios para cambiar el modo de seguridad de Cisco Unified Communications Manager (CUCM) del modo Mixto al modo No seguro. También muestra cómo cambia el contenido de un archivo de lista de confianza de certificados (CTL) cuando se completa este movimiento.

Hay tres partes principales para cambiar el modo de seguridad de CUCM:

1 bis. Ejecute el cliente CTL y seleccione la variante deseada del modo de seguridad.
1 ter. Ingrese el comando CLI para seleccionar la variante deseada del modo de seguridad.
2. Reinicie los servicios Cisco CallManager y Cisco TFTP en todos los servidores CUCM que ejecuten estos servicios.
3. Reinicie todos los teléfonos IP para que puedan descargar la versión actualizada del archivo CTL.

> **Nota:** Si el modo de seguridad del clúster se cambia del modo Mixto al modo No seguro, el archivo CTL sigue existiendo en los servidores y en los teléfonos, pero el archivo CTL no contiene ningún certificado CCM+TFTP (servidor). Dado que los certificados CCM+TFTP (servidor) no existen en el archivo CTL, esto obliga al teléfono a registrarse como No seguro con CUCM.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de la versión 10.0(1) de CUCM o una posterior. Además, asegúrese de lo siguiente:

- El servicio Proveedor de CTL está activo y se ejecuta en todos los servidores TFTP activos del clúster. De forma predeterminada, el servicio se ejecuta en el puerto TCP 2444, pero esto se puede modificar en la configuración del parámetro de servicio de CUCM.
- Los Servicios de función proxy de autoridad certificadora (CAPF) están activos y se ejecutan en el nodo de editor.
- La replicación de la base de datos (DB) en el clúster funciona correctamente y los servidores replican los datos en tiempo real.

Componentes Utilizados

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

- Clúster de dos nodos CUCM Release 10.0.1.11900-2
- Teléfono IP Cisco 7975 (registrado con el protocolo de control de llamadas skinny (SCCP), versión de firmware SCCP75.9-3-1SR3-1S)
- Se necesitan dos tokens de seguridad de Cisco para establecer el clúster en modo mixto
- Uno de los Tokens de Seguridad listados anteriormente es necesario para establecer el clúster en el modo No Seguro

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Para ejecutar el complemento Cliente de CTL, es necesario tener acceso al menos a un token de seguridad que se insertó para crear o actualizar el archivo de CTL más reciente que exista en el servidor de CUCM Publisher. En otras palabras, al menos uno de los certificados de eToken que existe en el archivo CTL actual en CUCM debe estar en el token de seguridad que se utiliza para cambiar el modo de seguridad.

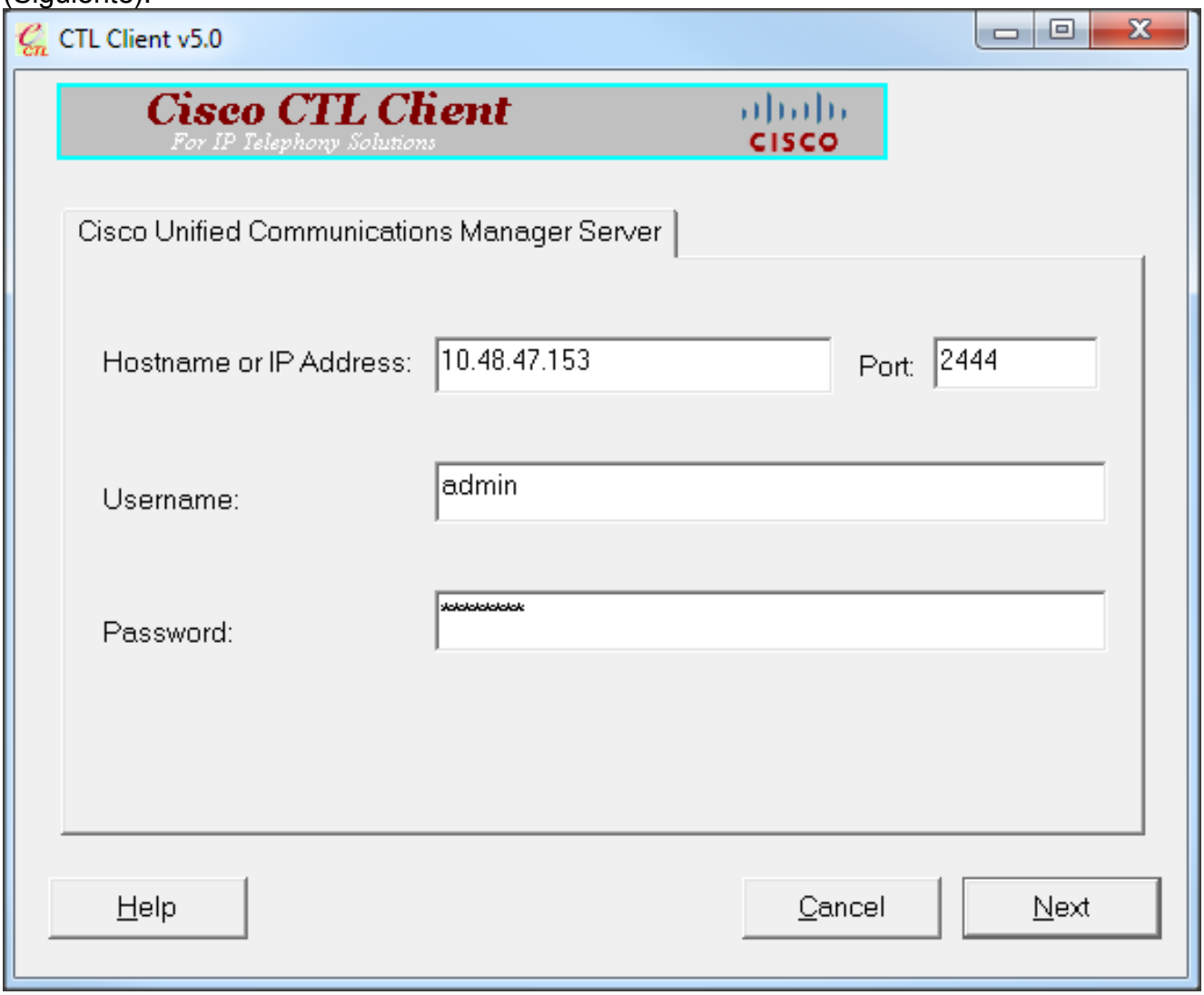
Configurar

Cambie la seguridad del clúster de CUCM del modo mixto al modo no seguro con el cliente CTL

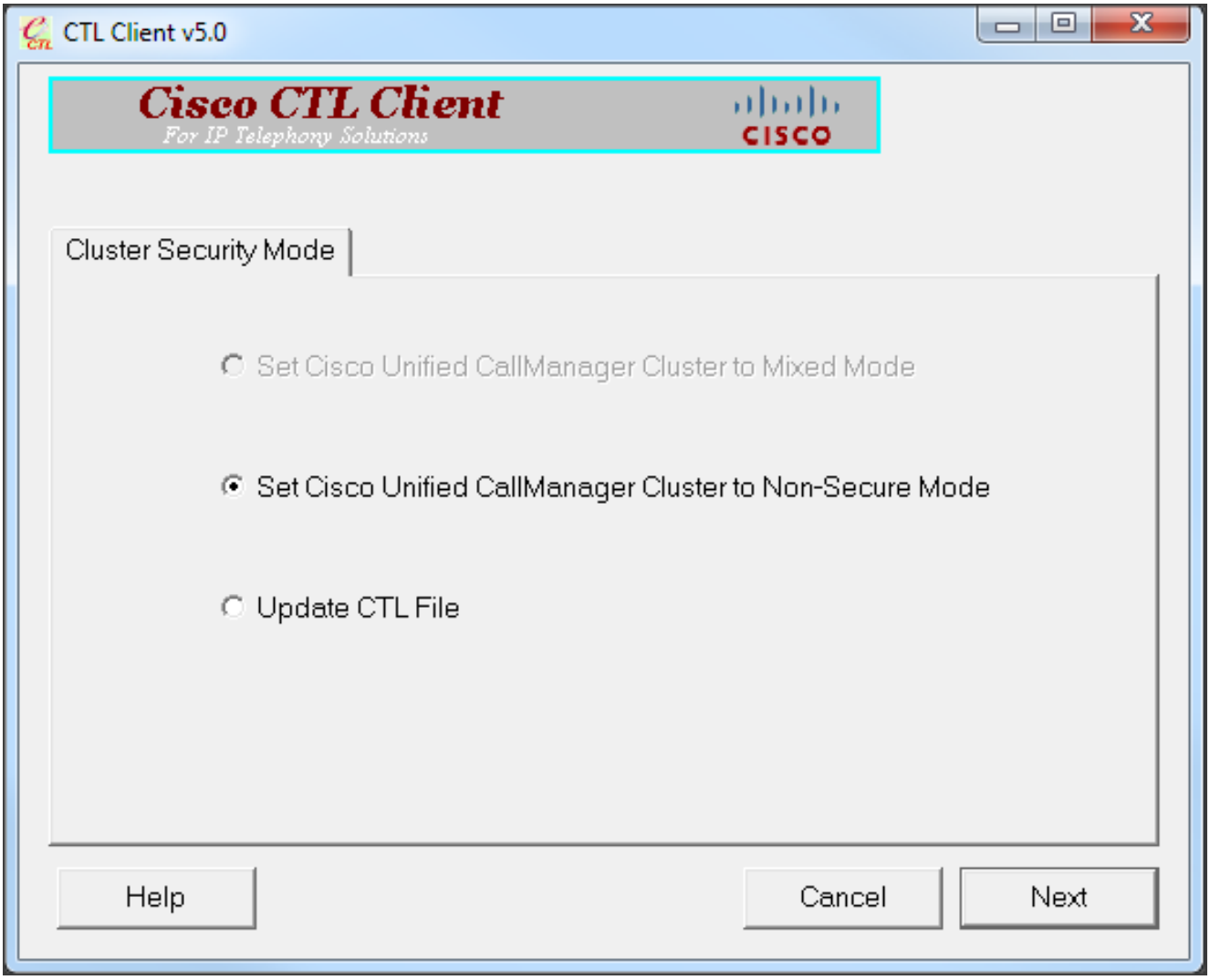
Complete estos pasos para cambiar la seguridad del clúster de CUCM del modo Mixto al modo

No Seguro con el cliente CTL:

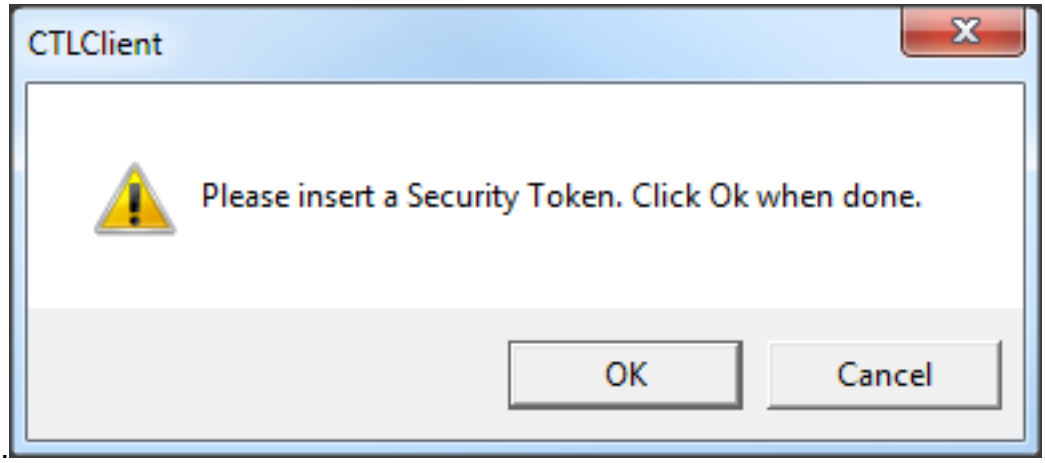
1. Obtenga un token de seguridad que insertó para configurar el archivo CTL más reciente.
2. Ejecute el cliente CTL. Proporcione el nombre de host/dirección IP de la publicación de CUCM y las credenciales del administrador de CCM. Haga clic en Next (Siguiente).



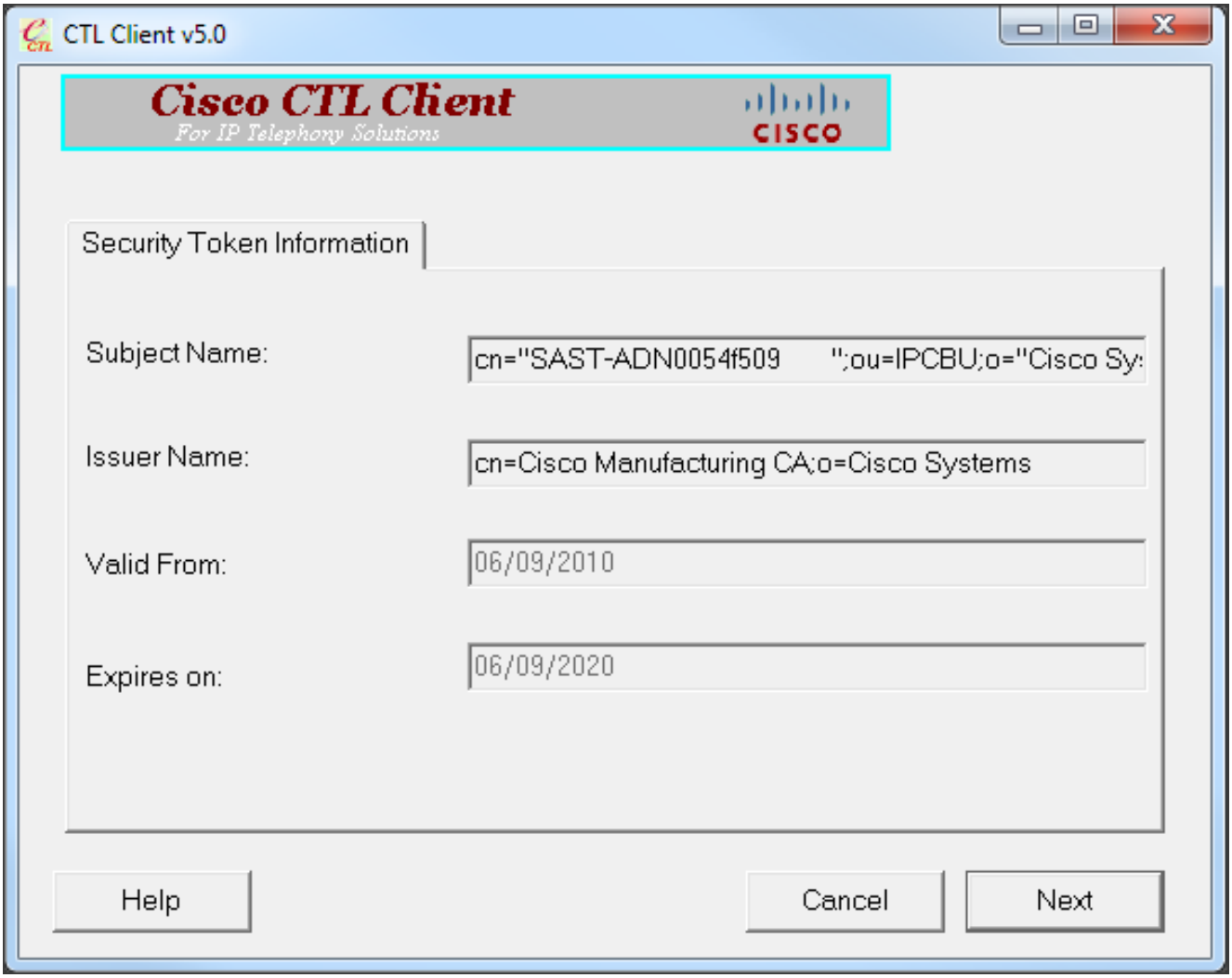
3. Haga clic en el botón de opción **Set Cisco Unified CallManager Cluster to Non-Secure Mode**. Haga clic en Next (Siguiente).



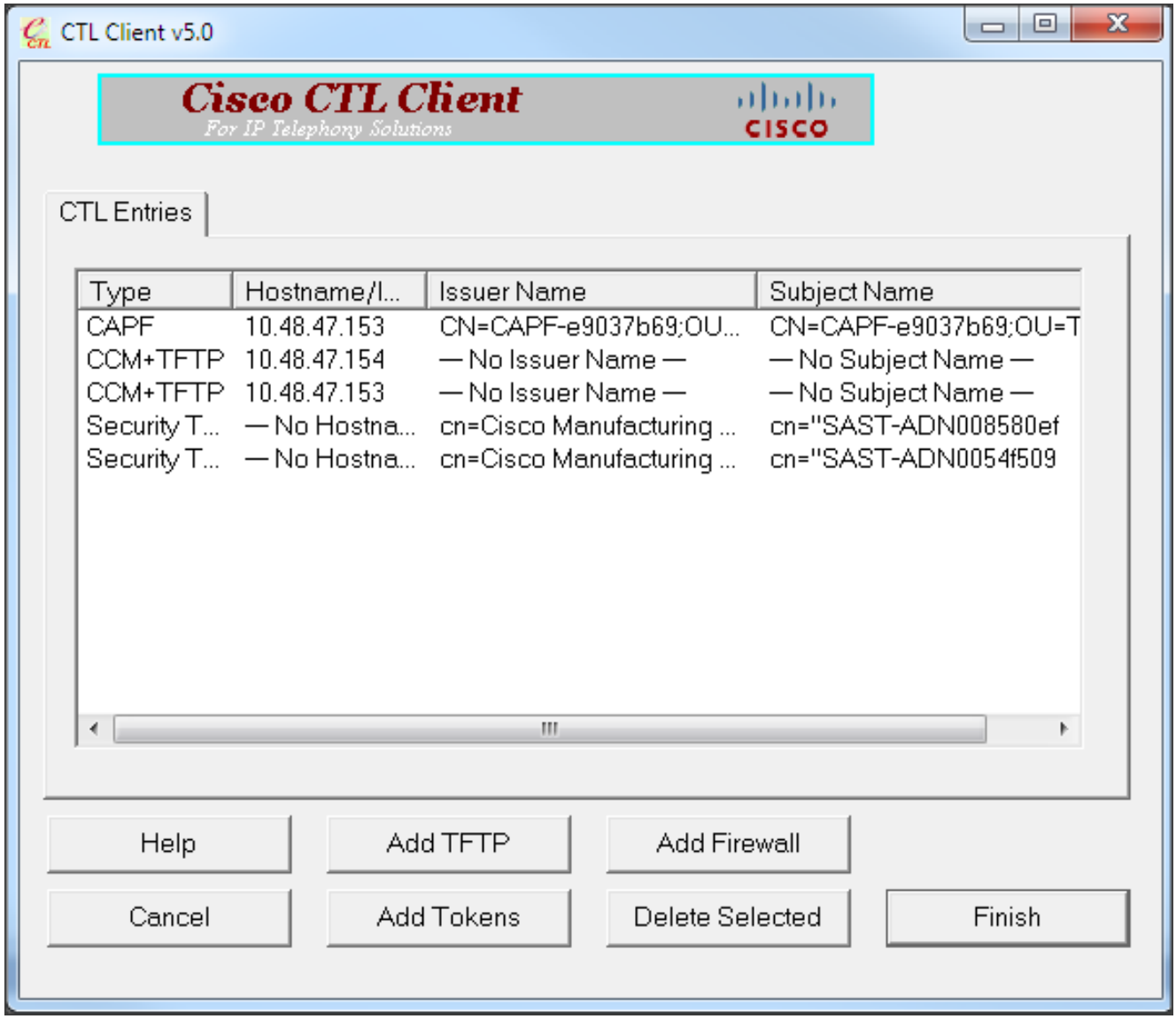
4. Inserte un token de seguridad que se insertó para configurar el archivo CTL más reciente y haga clic en **Aceptar**. Este es uno de los tokens que se utilizaron para rellenar la lista de certificados en CTLFile.tlv.



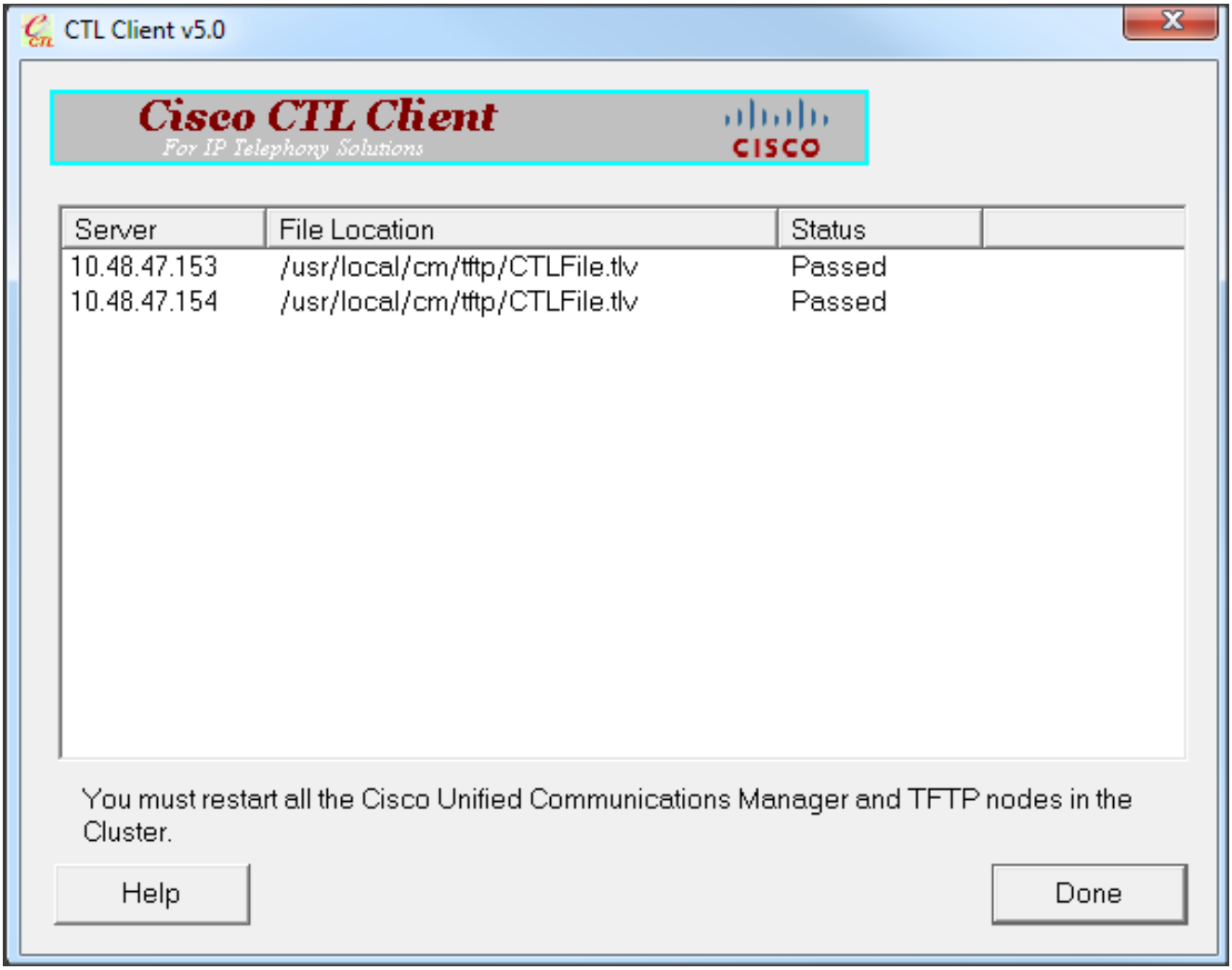
5. Se muestran los detalles del token de seguridad. Haga clic en Next (Siguiente).



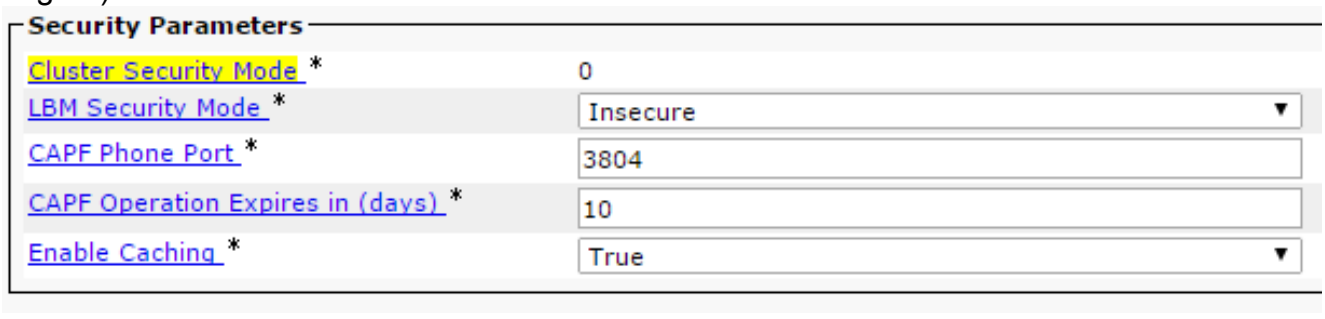
6. Se muestra el contenido del archivo CTL. Haga clic en Finish (Finalizar). Cuando se le solicite la contraseña, introduzca **Cisco123**.



7. Se muestra la lista de servidores CUCM en los que se encuentra el archivo CTL. Haga clic en Done
(Listo).



8. Elija **CUCM Admin Page > System > Enterprise Parameters** y verifique que el cluster se haya configurado en modo no seguro ("0" indica no seguro).



9. Reinicie los servicios TFTP y Cisco CallManager en todos los nodos del clúster que ejecutan estos servicios.
10. Reinicie todos los teléfonos IP para que puedan obtener la nueva versión del archivo CTL de CUCM TFTP.

Cambie la seguridad del clúster de CUCM del modo mixto al modo no seguro con la CLI

Esta configuración es solo para CUCM versión 10.X y posteriores. Para establecer el modo de seguridad de clúster de CUCM en No seguro, ingrese el comando **utils ctl set-cluster non-secure-**

mode en la CLI de Publisher. Una vez que se haya completado, reinicie los servicios TFTP y Cisco CallManager en todos los nodos del clúster que ejecutan estos servicios.

Este es un ejemplo de salida de CLI que muestra el uso del comando.

```
admin:utils ctl set-cluster non-secure-mode
This operation will set the cluster to non secure mode. Do you want to continue? (y/n):

Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that
run these services
admin:
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Para verificar CTLFIle.tlv, puede utilizar uno de estos dos métodos:

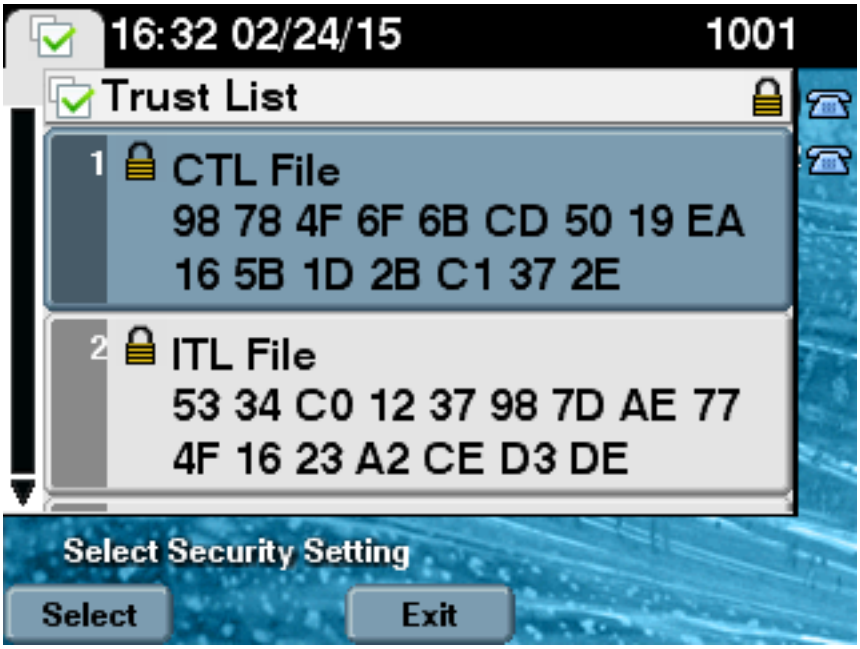
- Para verificar el contenido y la suma de comprobación MD5 del archivo CTLFIle.tlv presente en el lado TFTP de CUCM, ingrese el comando **show ctl** en la CLI de CUCM. El archivo CTLFIle.tlv debe ser el mismo en todos los nodos de CUCM.
- Para verificar la suma de comprobación MD5 en el teléfono IP 7975, elija **Settings > Security Configuration > Trust List > CTL File**.

  Nota: Al comprobar la suma de comprobación en el teléfono, verá MD5 o SHA1, según el tipo de teléfono.

Conjunto de clústeres de CUCM en modo de seguridad: suma de comprobación de archivos CTL

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

En el lado del teléfono IP, puede ver que tiene el mismo archivo CTL instalado (la suma de comprobación MD5 coincide cuando se compara con la salida de CUCM).



Clúster de CUCM establecido en modo no seguro - Contenido de archivo CTL

Este es un ejemplo de un archivo CTL de un clúster de CUCM establecido en modo no seguro. Puede ver que los certificados CCM+TFTP están vacíos y no contienen ningún contenido. El resto de los certificados de los archivos CTL no se modifican y son exactamente iguales que cuando CUCM se configuró en el modo Mixto.

```
admin:show ctl
The checksum value of the CTL file:
7879e087513d0d6dfe7684388f86ee96(MD5)
be50e5f3e28e6a8f5b0a5fa90364c839fcc8a3a0(SHA1)


Length of CTL file: 3746
The CTL File was last modified on Tue Feb 24 16:37:45 CET 2015

Parse CTL File
----------------

Version: 1.2
HeaderLength: 304 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 117
4 SIGNERNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
5 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45
6 CANAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
45 ec 5 c 9e 68 6d e6
5d 4b d3 91 c2 26 cf c1
ee 8c b9 6 95 46 67 9e
19 aa b1 e9 65 af b4 67
```

```
36 7e e5 ee 60 10 b 1b
58 c1 6 64 40 cf e2 57
aa 86 73 14 ec 11 b a
3b 98 91 e2 e4 6e 4 50
ba ac 3e 53 33 1 3e a6
b7 30 0 18 ae 68 3 39
d1 41 d6 e3 af 97 55 e0
5b 90 f6 a5 79 3e 23 97
fb b8 b4 ad a8 b8 29 7c
1b 4f 61 6a 67 4d 56 d2
5f 7f 32 66 5c b2 d7 55
d9 ab 7a ba 6d b2 20 6
14 FILENAME 12
15 TIMESTAMP 4

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45
7 PUBLICKEY 140
9 CERTIFICATE 902 19 8F 07 C4 99 20 13 51 C5 AE BF 95 03 93 9F F2 CC 6D 93 90 (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.

CTL Record #:2
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93 3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was not used to sign the CTL file.

CTL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.153
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

CTL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1004
2 DNSNAME 13 10.48.47.153
3 SUBJECTNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
4 FUNCTION 2 CAPF
5 ISSUERNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
6 SERIALNUMBER 16 79:59:16:C1:54:AF:31:0C:0F:AE:EA:97:2E:08:1B:31
```

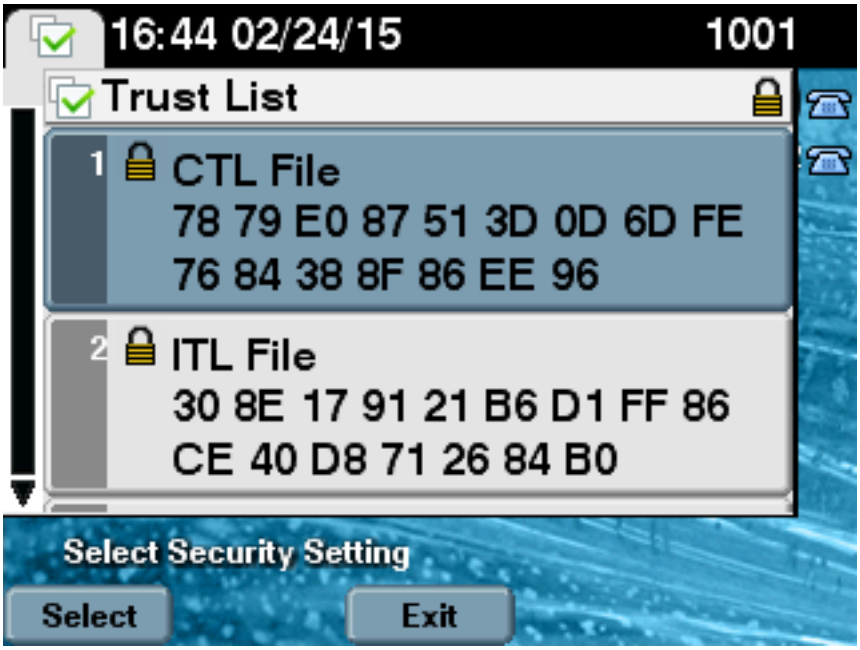
```
7 PUBLICKEY 140
9 CERTIFICATE 680 A0 A6 FC F5 FE 86 16 C1 DD D5 B7 57 38 9A 03 1C F7 7E FC 07 (SHA1 Hash HEX)
10 IPADDRESS 4

CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.154
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

The CTL file was verified successfully.

admin:
```

En el lado del teléfono IP, después de reiniciarlo y descargar la versión actualizada del archivo CTL, puede ver que la suma de comprobación MD5 coincide cuando se compara con la salida de CUCM.



Ponga la seguridad del clúster de CUCM del modo mixto al modo no seguro cuando se pierden tokens USB

Los tokens de seguridad de los clústeres seguros podrían perderse. En esa situación, debe considerar estos dos escenarios:

- El clúster ejecuta la versión 10.0.1 o posterior
- El clúster ejecuta una versión anterior a 10.x

En el primer escenario, complete el procedimiento descrito en la sección Cambiar la seguridad del clúster de CUCM del modo mixto al modo no seguro con la CLI para recuperarse del problema. Dado que el comando CLI no requiere un token CTL, se puede utilizar incluso si el clúster se puso en modo mixto con el cliente CTL.

La situación se vuelve más compleja cuando se utiliza una versión anterior a 10.x de CUCM. Si pierde u olvida la contraseña de uno de los tokens, todavía puede utilizar el otro para ejecutar el

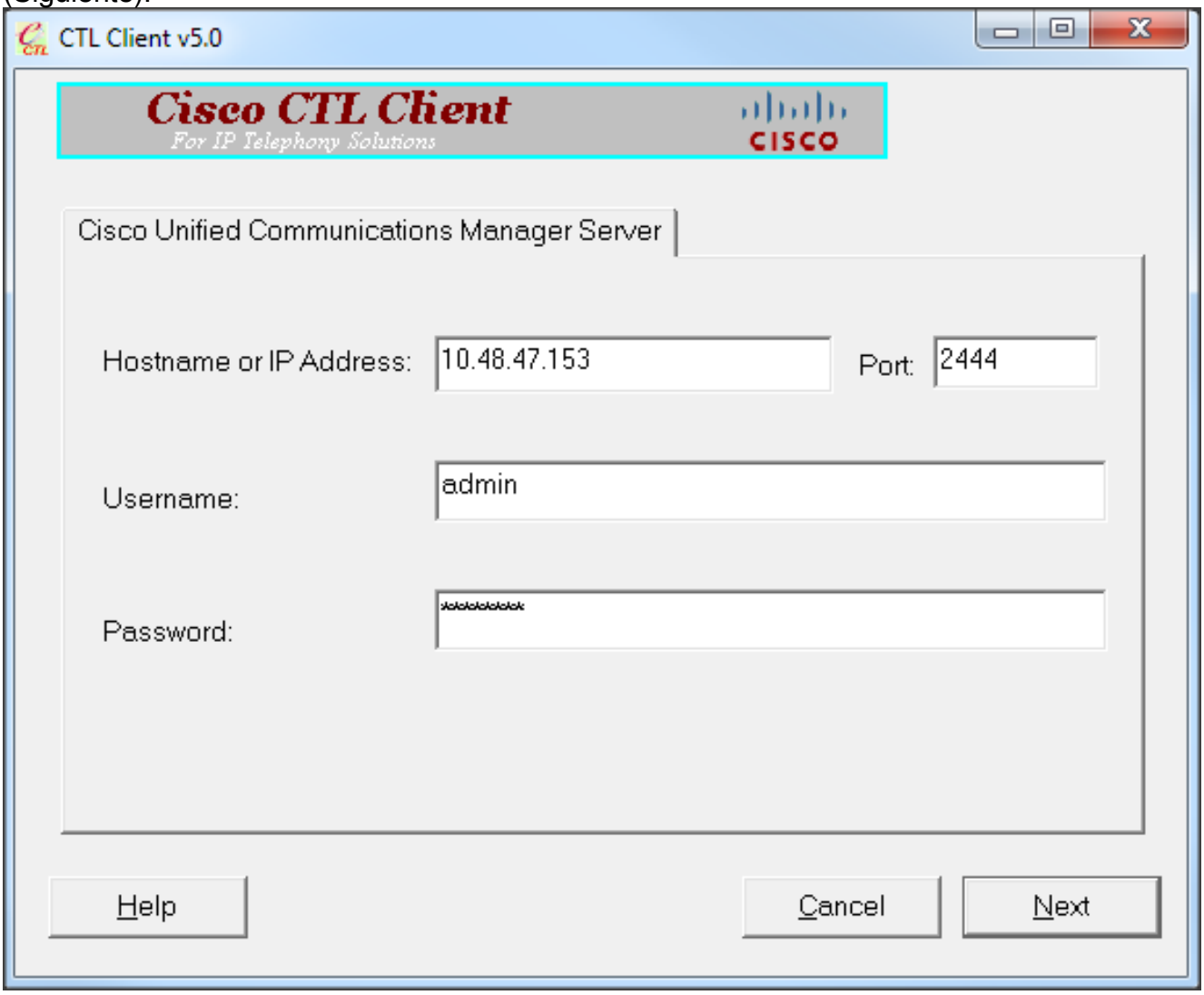
cliente CTL con los archivos CTL actuales. Se recomienda encarecidamente obtener otro eToken y agregarlo al archivo CTL tan pronto como sea posible en aras de la redundancia. Si pierde u olvida las contraseñas de todos los eTokens enumerados en su archivo CTL, necesita obtener un nuevo par de eTokens y ejecutar un procedimiento manual como se explica aquí.

1. Ingrese el comando **file delete tftp CTLFile.tlv** para eliminar el archivo CTL de todos los servidores TFTP.

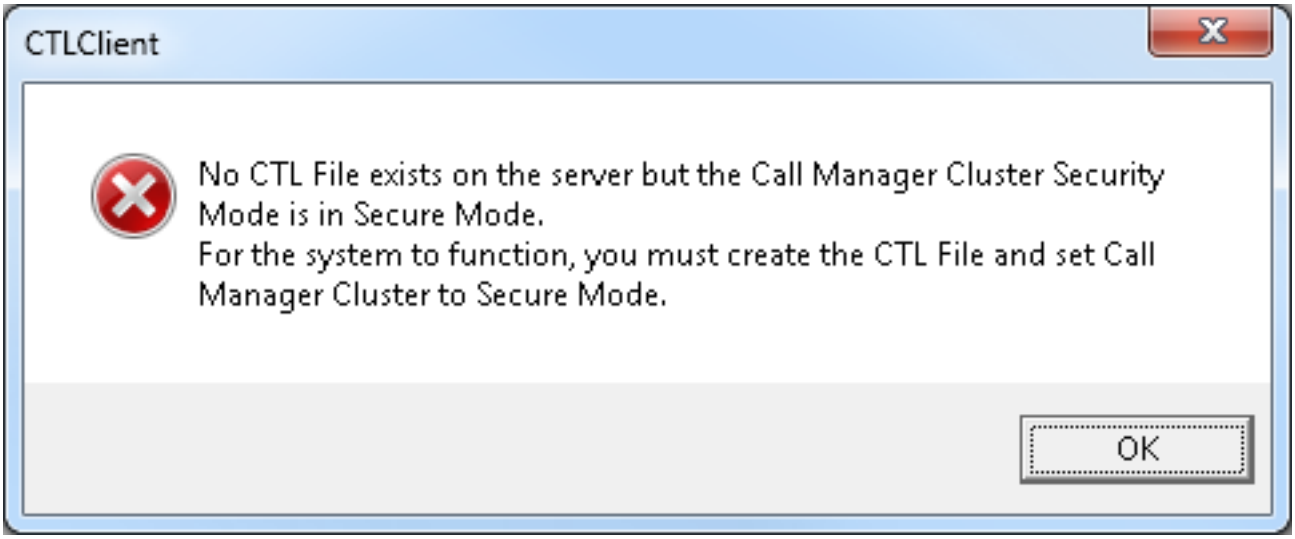
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

admin:show ctl
Length of CTL file: 0
CTL File not found. Please run CTLClient plugin or run the CLI - utils ctl..
to generate the CTL file.
Error parsing the CTL File.
```

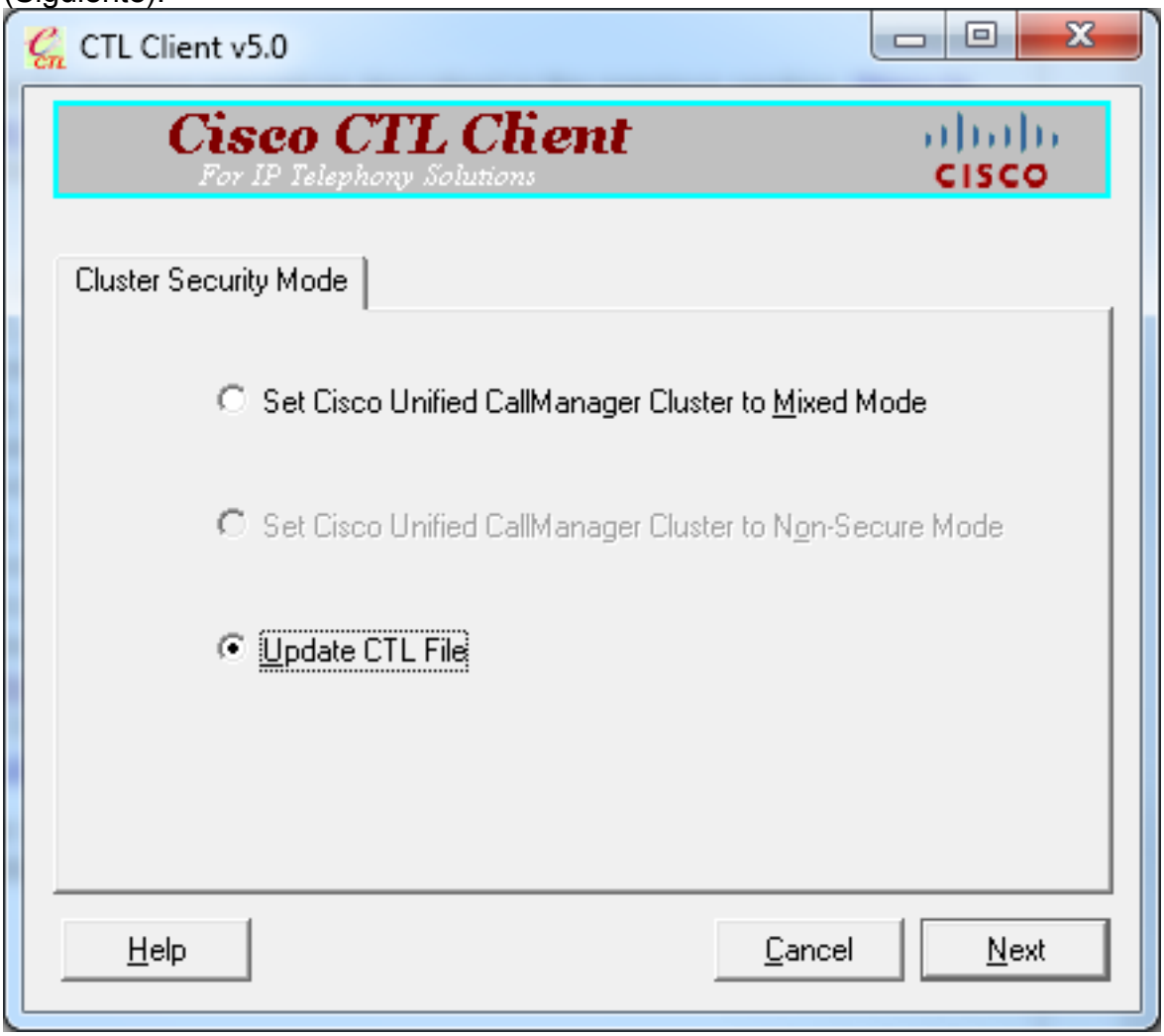
2. Ejecute el cliente CTL. Introduzca el nombre de host/dirección IP de la base de datos de publicaciones de CUCM y las credenciales del administrador de CCM. Haga clic en Next (Siguiente).



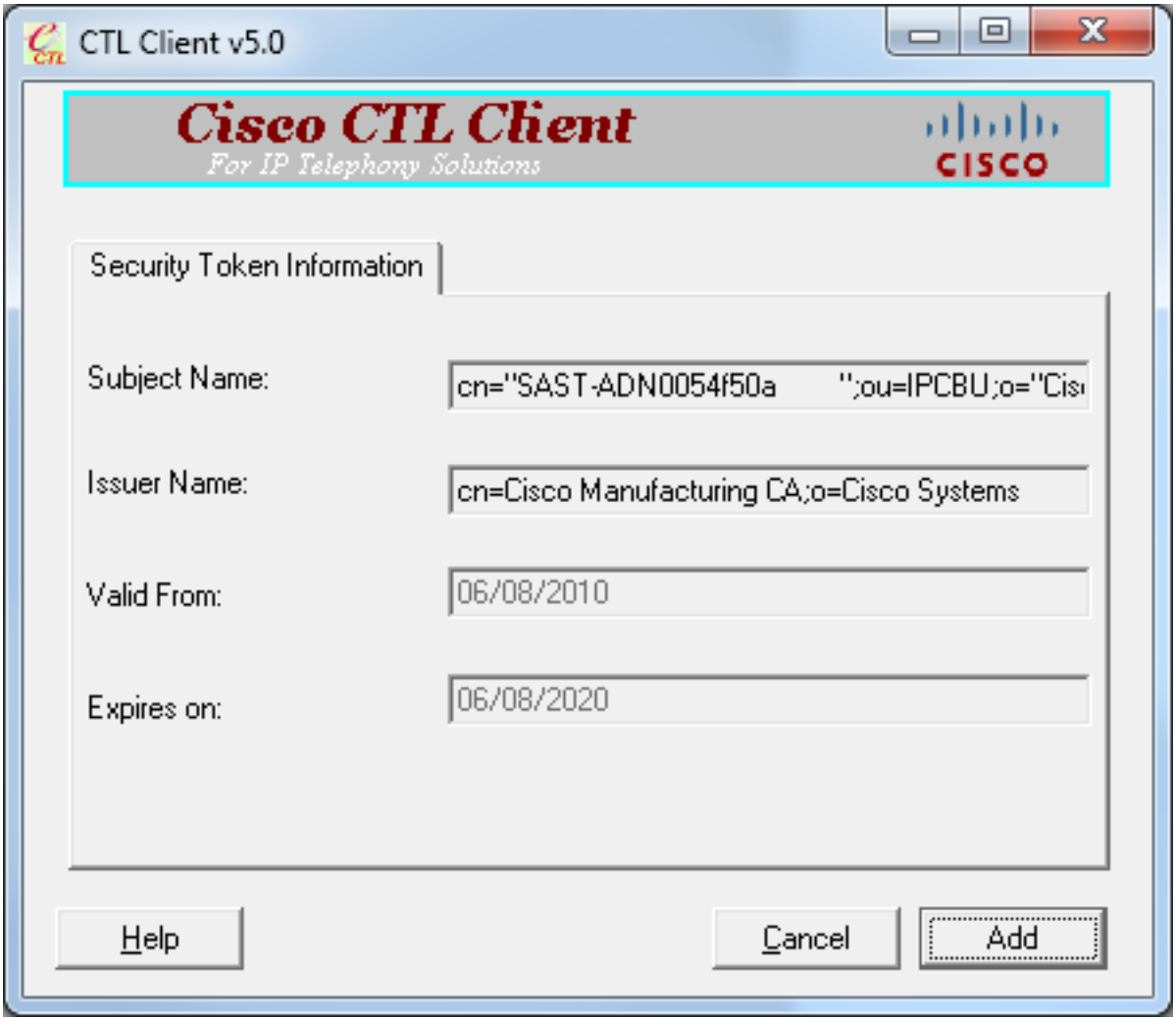
3. Puesto que el clúster está en modo Mixto, sin embargo no existe ningún archivo CTL en Publisher, se muestra esta advertencia. Haga clic en **Aceptar** para ignorarlo y continuar.



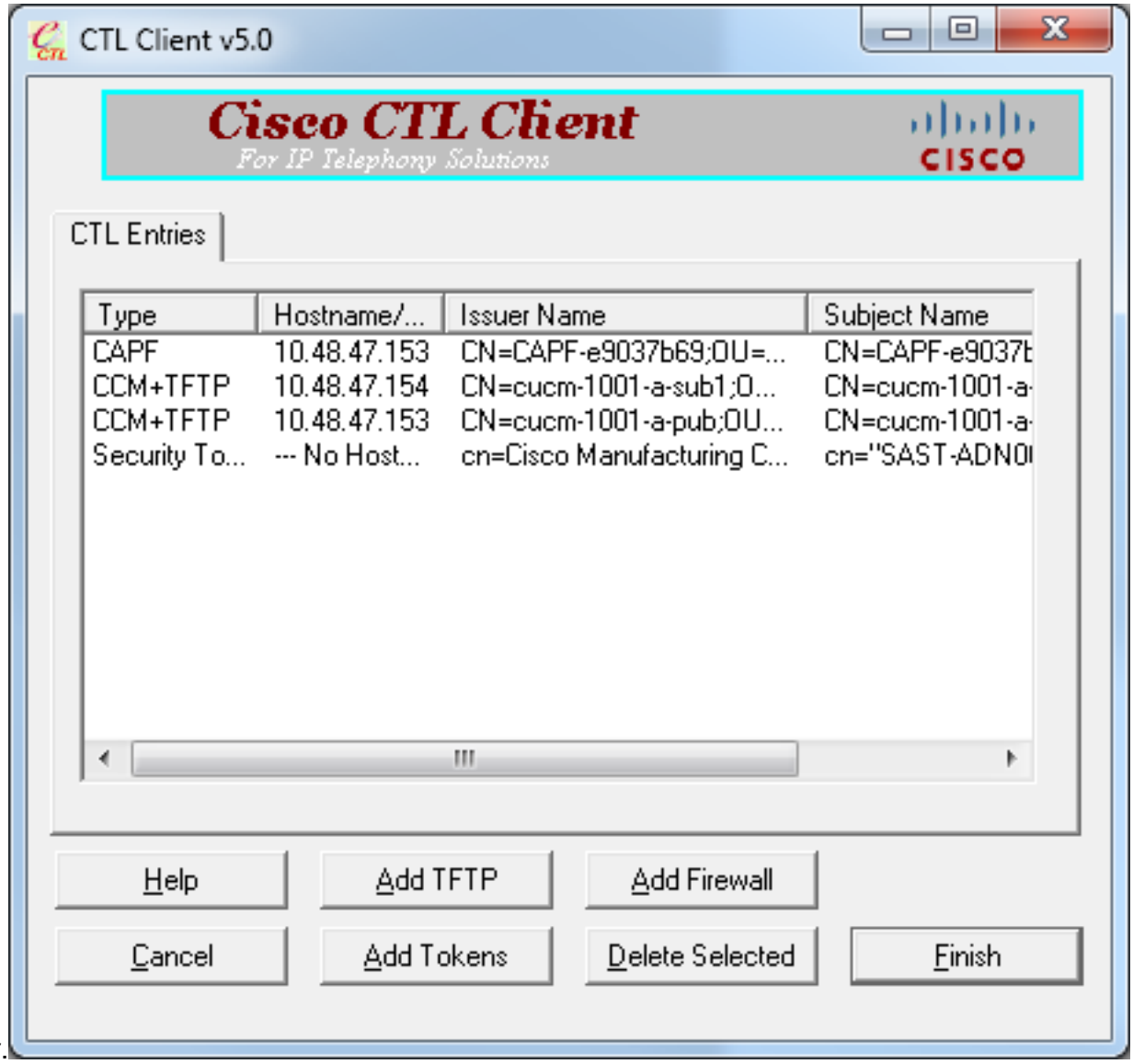
4. Haga clic en el botón de opción **Update CTL File**. Haga clic en Next (Siguiente).



5. El cliente CTL solicita agregar un token de seguridad. Haga clic en **Agregar** para continuar.

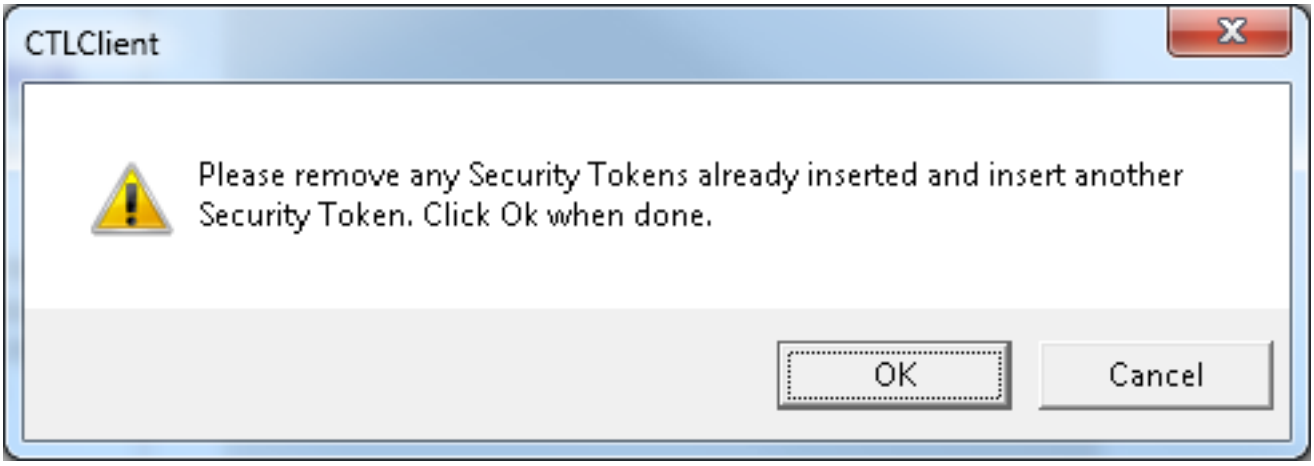


6. La pantalla muestra todas las entradas de la nueva CTL. Haga clic en **Add Tokens** para agregar el segundo token del nuevo

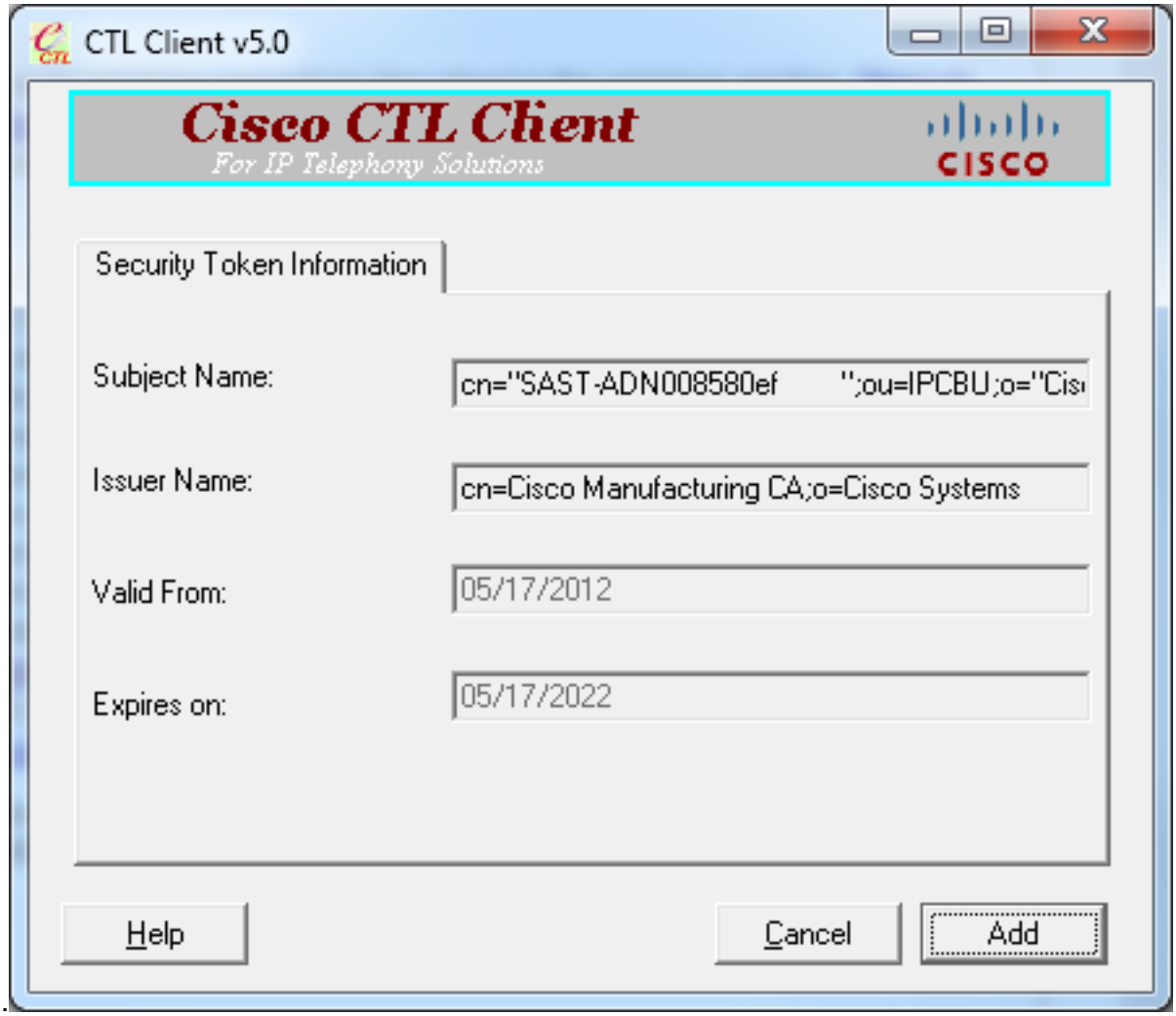


par.

7. Se le pedirá que quite el token actual e inserte uno nuevo. Haga clic en **Aceptar** una vez hecho.

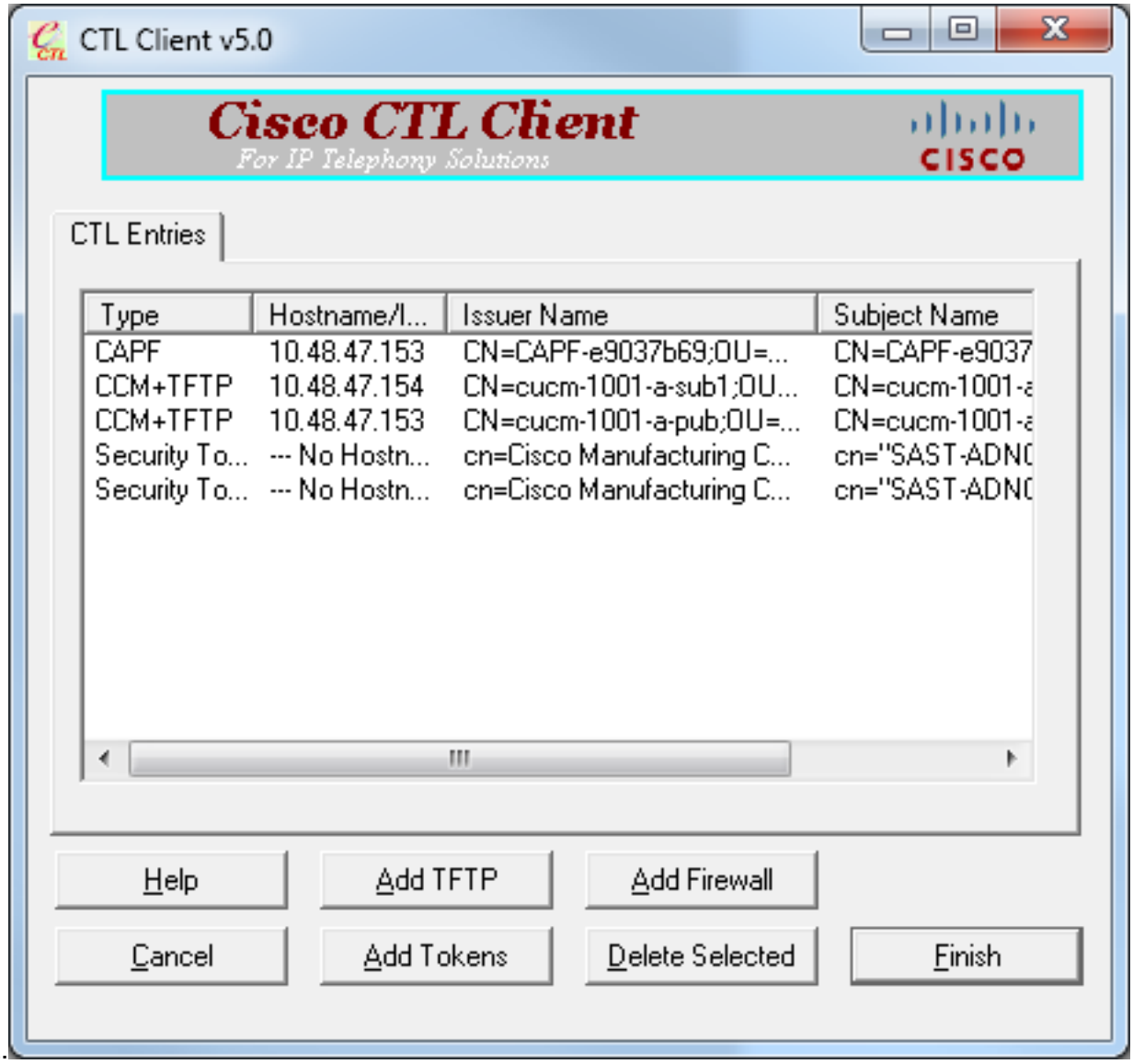


8. Se muestra una pantalla que muestra los detalles del nuevo token. Haga clic en **Agregar** para confirmarlos y agregar este



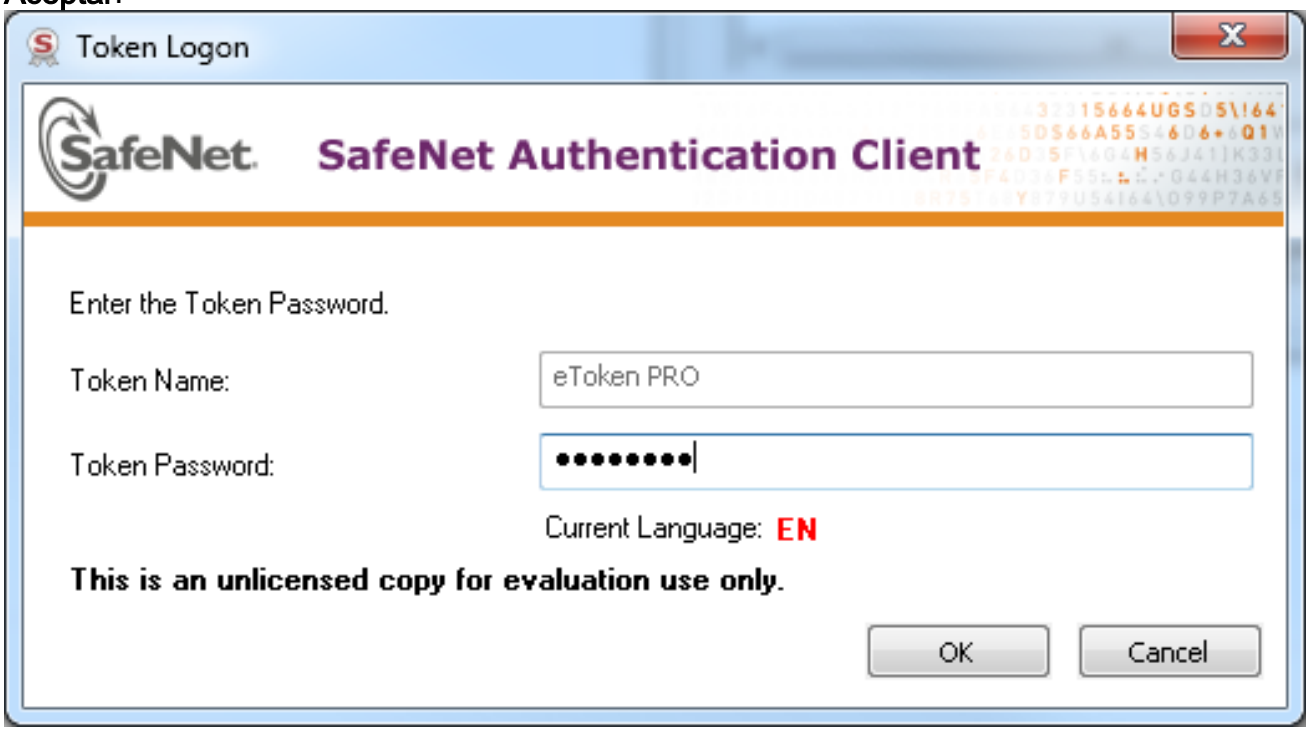
token.

9. Se le presentará una nueva lista de entradas de CTL que muestra ambos Tokens agregados. Haga clic en **Finalizar** para generar nuevos archivos

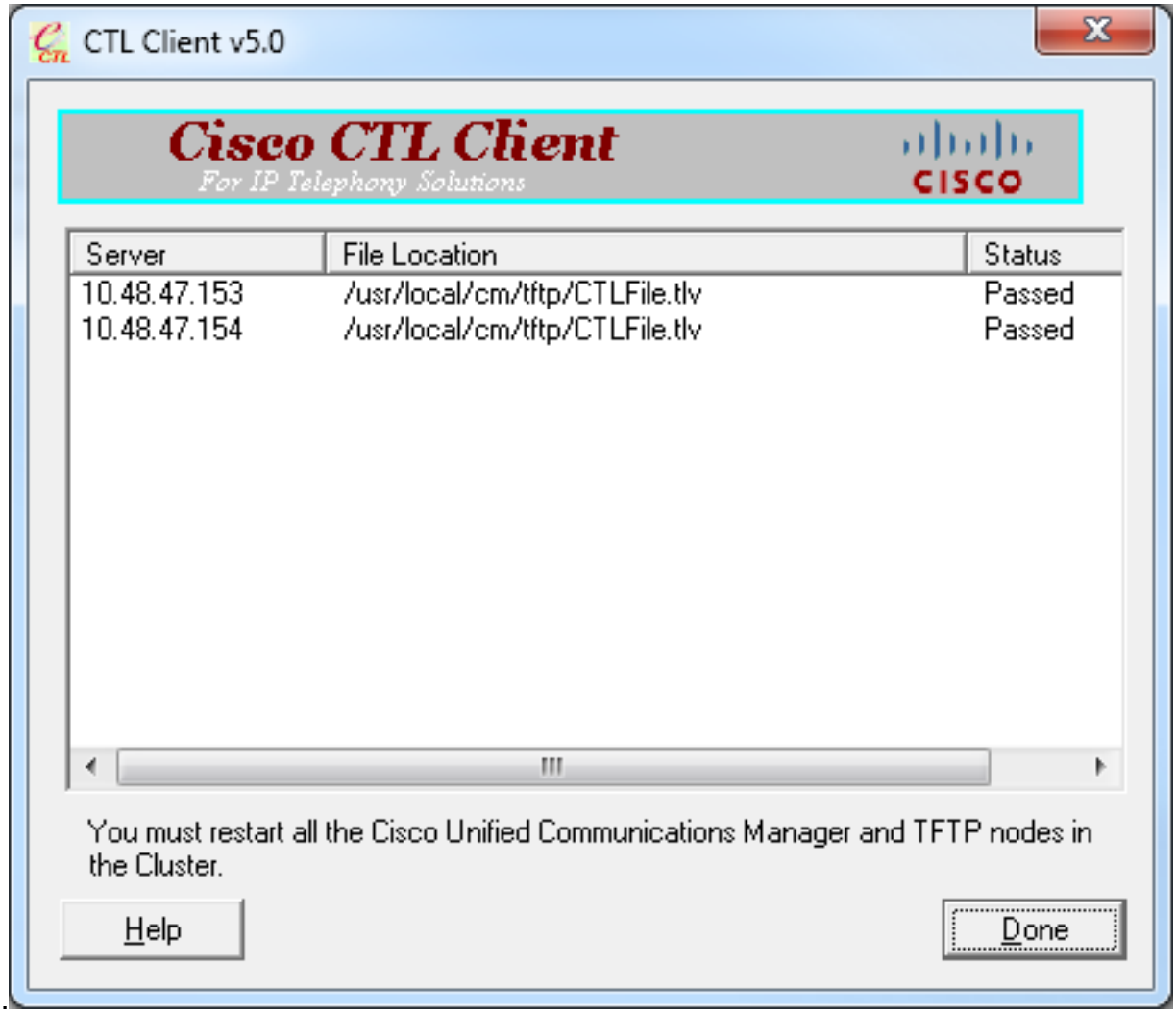


CTL.

10. En el campo Contraseña de Token, ingrese **Cisco123**. Haga clic en **Aceptar**.



11. Verá la confirmación de que el proceso se ha realizado correctamente. Haga clic en **Finalizado** para confirmar y salir del cliente



CTL.

12. Reinicie Cisco TFTP seguido del servicio CallManager (Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones). Se debe generar el nuevo archivo CTL. Ingrese el comando **show ctl** para la verificación.

```
admin:show ctl
The checksum value of the CTL file:
68a954fba070bbcc3ff036e18716e351(MD5)
4f7a02b60bb5083baac46110f0c61eac2dceb0f7(SHA1)


Length of CTL file: 5728
The CTL File was last modified on Mon Mar 09 11:38:50 CET 2015
```

13. Elimine el archivo CTL de cada teléfono del clúster (este procedimiento puede variar según el tipo de teléfono; consulte la documentación para obtener más información, como la Guía de administración de los teléfonos IP 8961, 9951 y 9971 de Cisco Unified).**Nota:** Es posible que los teléfonos aún puedan registrarse (en función de la configuración de seguridad del teléfono) y funcionar sin continuar con el paso 13. Sin embargo, tendrán instalado el archivo CTL antiguo. Podría causar problemas si se regeneran los certificados, se agrega otro servidor al clúster o se reemplaza el hardware del servidor. No se recomienda dejar el clúster en este estado.
14. Mueva el clúster a No seguro. Vea la sección Cambio de la seguridad del clúster de CUCM del modo mixto al modo no seguro con el cliente CTL para obtener detalles.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.