Vencimiento del certificado y cancelacíon del CallManager

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Problema](#)
[Solución](#)
[Regeneración del certificado para las versiones 8.x CUCM y posterior](#)
[CAPF](#)
[IPSec](#)
[CM](#)
[TV](#)
[Certificados de la cancelación](#)

Introducción

Este documento describe un problema con el Cisco CallManager (CM) donde usted recibe el **CertExpiryEmergency: Certifique el** mensaje de alarma del **vencimiento EMERGENCY_ALARM del** cliente de la herramienta del monitoreo en tiempo real (RTMT), y ofrece una solución al problema.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de las versiones 6.x CM con 9.x, y que su sistema:

- No tiene una configuración del Domain Name System (DNS). Esto se hace para la simplicidad del documento, pero muchos sistemas lo tienen configurado que sea ACEPTABLE.
- Tiene un certificado que se expire y deba ser regenerado, o un certificado que se programe para expirar.

  Nota: El IP Address del sistema no importa si usted ingresa el **nuevo** o **regenerado** comando de la **generación** después de que usted cambie el nombre del host o el IP Address.

Componentes Utilizados

La información en este documento se basa en el servidor del CM de Cisco con las páginas de

administración.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Problema

Usted recibe un **CertExpiryEmergency: Certifique el** mensaje de alarma del **vencimiento EMERGENCY_ALARM** RTMT adentro del CM:

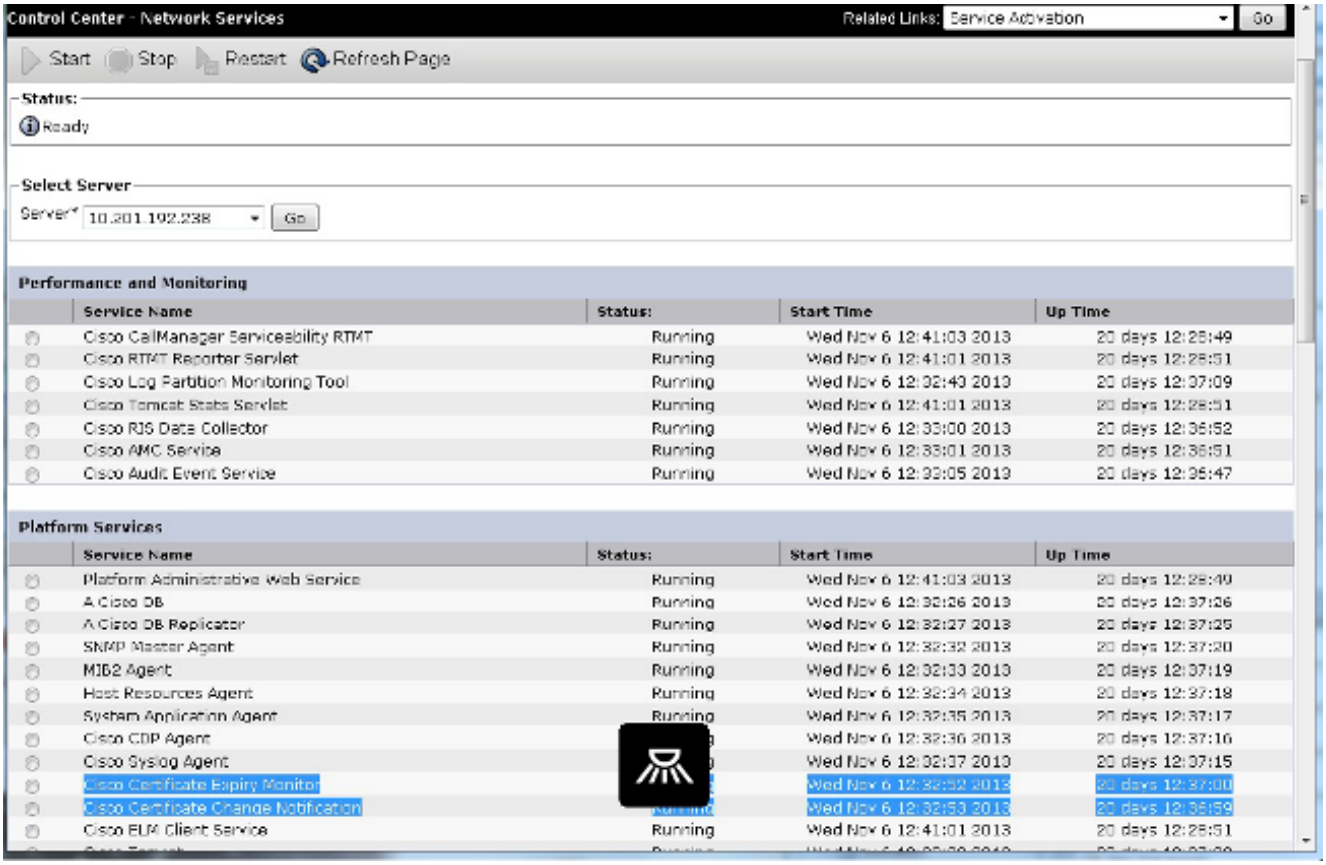
```
Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 629: Jul 30 17:00:00.352 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification.
 Certificate name:CAPF Unit:CAPF Type:own-cert
Expiration:Fri Dec 28 12:14:42:000 EST 2012 / App ID:Cisco Certificate
Monitor Cluster ID:Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 630: Jul 30 17:00:00.353 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CallManager-trust Type:trust-cert Expiration:Fri Dec 28 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 631: Jul 30 17:00:00.354 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CAPF-trust Type:trust-cert Expiration:Fri Dec 28 12:14:4 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI
```

Solución

Utilice la información en esta sección para resolver el problema del mensaje de alarma CM.

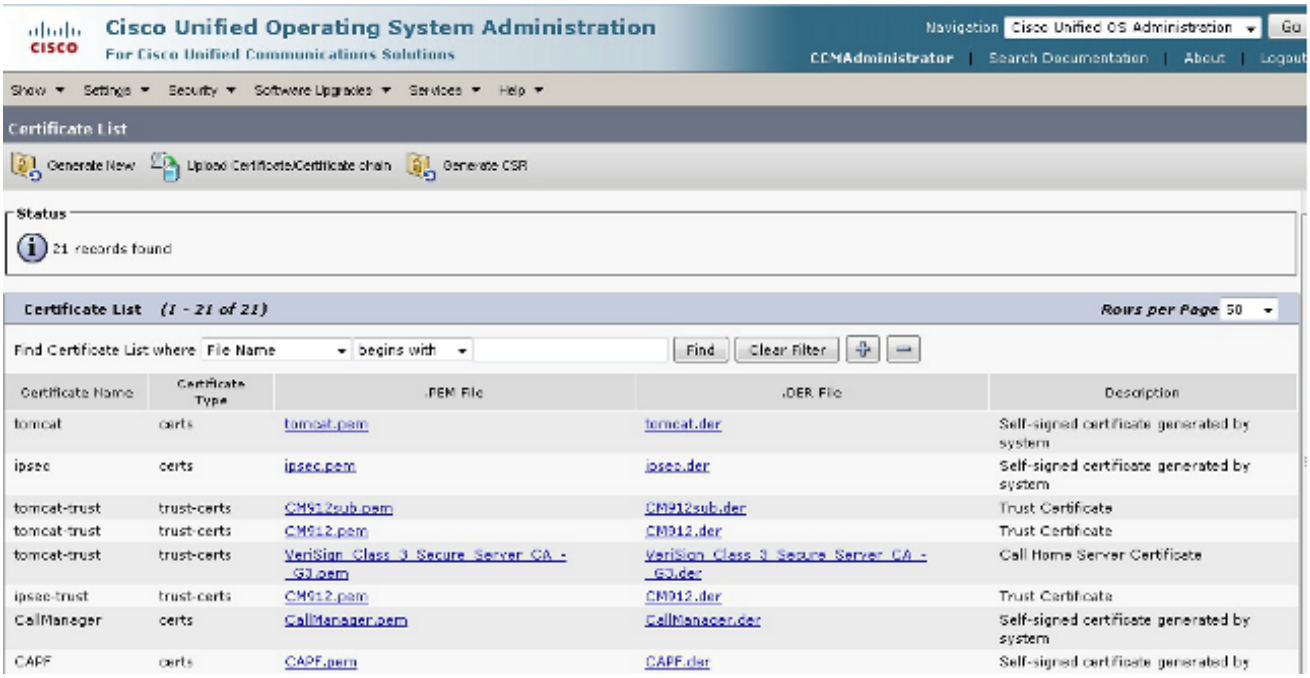
1. Del CM la página unificada GUI de la utilidad, navega al **Tools (Herramientas) > Control Center (Centro de control) - los servicios de red**.

2. Pare los servicios de la **notificación de cambio del monitor del vencimiento del certificado de Cisco** y del **certificado de Cisco** en todos los servidores en el cluster:



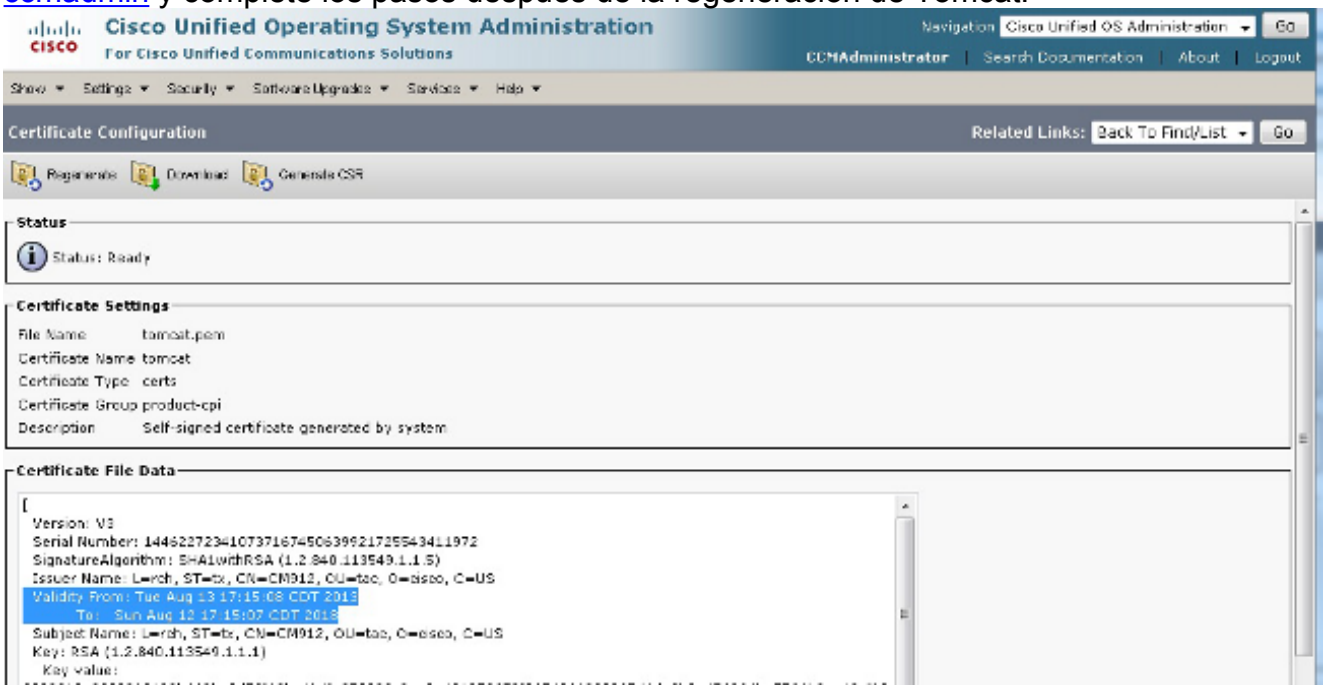
3. De la administración GUI del operating system (OS), navegue al **Certificate Management (Administración de certificados) de la Seguridad**, y este las visualizaciones de la pantalla:

4. Haga clic el **hallazgo** para visualizar todos los Certificados en un servidor determinado:

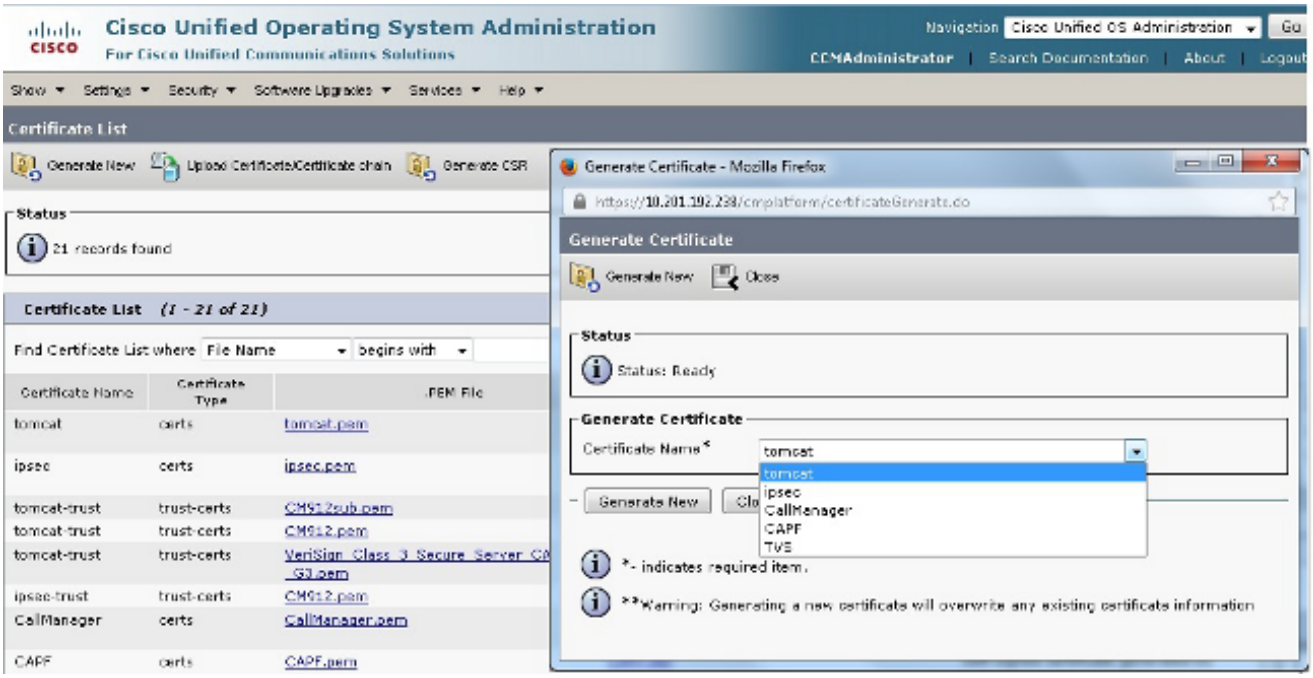


5. Haga clic cualquier certificado (un certificado de Tomcat en este caso) y vea la fecha, según lo resaltado en la imagen siguiente. Para los Certificados de Tomcat, verifique si el servidor utiliza un certificado de tercera persona para el login de la página del **ccmadmin**. Usted puede marcar esto cuando usted registra en la página de un navegador.

   Nota: Si es un certificado firmado de tercera persona, refiérase al CUCM que carga el artículo de la comunidad del soporte de Cisco de los Certificados de la red GUI del ccmadmin y complete los pasos después de la regeneración de Tomcat.

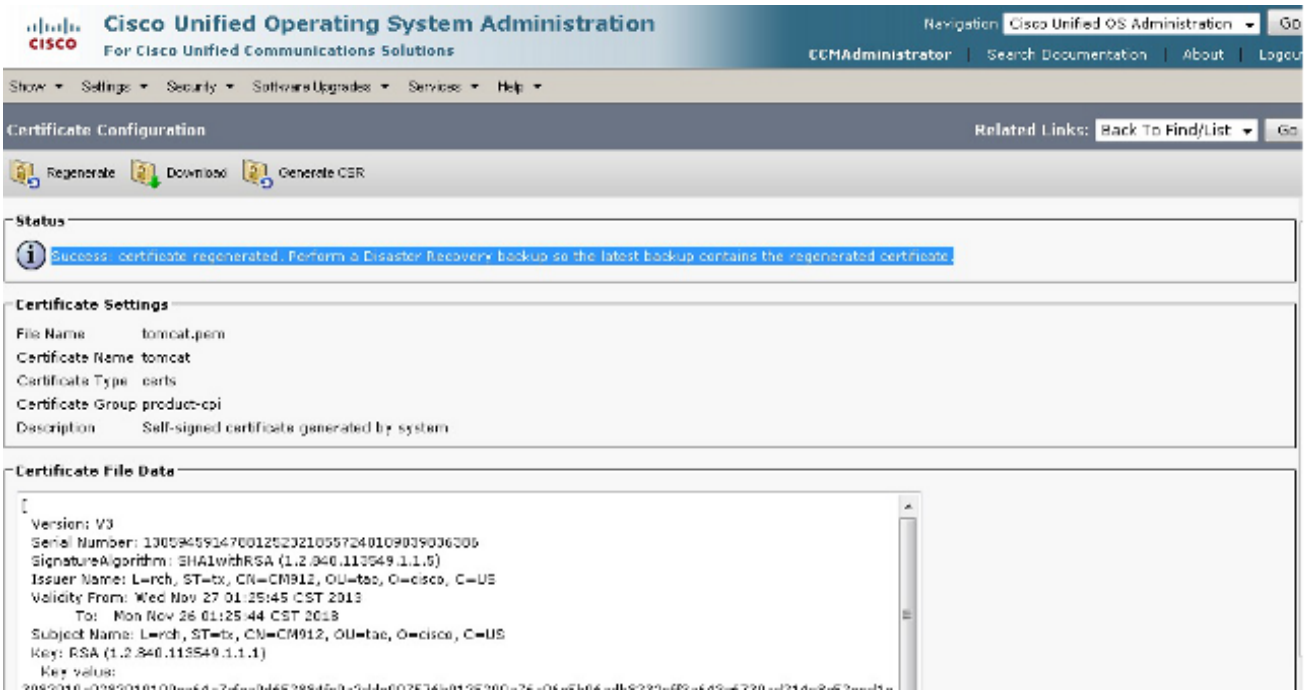


6. Navegue a la página de la **administración de certificados** en Publisher. Encuentre y haga clic el **archivo tomcat.pem**, y después haga clic el regenerado:



7. Para recomenzar el servicio del tomcat en ese nodo, abrir un CLI en el nodo y ingresar el comando del **tomcat de Cisco del reinicio del servicio del utils**. Una vez que se genera el certificado, un mensaje surge para confirmar que el certificado es actual.

   Nota: El certificado también es verificado por la información de la fecha descrita en los pasos anteriores.



8. Complete este proceso para cada uno de los suscriptores en el cluster para regenerar los Certificados del tomcat.

Certifique la regeneración para las versiones 8.x CUCM y posterior

Utilice la información en esta sección para regenerar los certificados vencidos para las versiones 8.x del administrador de las Comunicaciones unificadas de Cisco (CUCM) y posterior.

Nota: Regenere los Certificados después de las horas hábiles normales, porque usted debe recomenzar los servicios y reiniciar los teléfonos en el proceso.

CAPF

Para la regeneración de la función de proxy del Certificate Authority (CAPF), asegúrese de que el cluster no esté en un modo seguro del cluster: navegue al **System (Sistema) > Enterprise Parameters (Parámetros Enterprise) de la** página Web de administración CM, y de la búsqueda para el **modo seguro del cluster**. Si el valor es **0**, después el cluster no está en un modo seguro del cluster. Si el valor es cualquier número con excepción de cero, después el cluster está en un modo seguro, y usted debe utilizar Certificate Trust List (Lista de confianza del certificado) al cliente (CTL) para poner al día el archivo CTL.

Nota: Refiérase al artículo de la comunidad de la Seguridad del teléfono del IP y del soporte CTL (Certificate Trust List (Lista de confianza del certificado)) Cisco para más información.

1. De Publisher, navegue a la página de la administración de certificados.
2. Abra el **archivo CAPF.pem** y haga clic el regenerado**. Esto** renueva el certificado y crea dos nuevos archivos de la confianza: uno es la CM-confianza y la otra es la CAPF-confianza.
3. El página de la utilidad, navegue a las **herramientas > a los servicios de la característica**.
4. Si el servicio del CAPF se activa bajo **servicios de la característica**, después recomience el servicio. Si el servicio del CAPF no se activa, después un reinicio no es necesario.
5. Navegue a las **herramientas > a los servicios de red de la** página de la utilidad, y recomience el servicio del servicio de la verificación de la confianza (TV).
6. Navegue a las **herramientas > a los servicios de la característica de la** página de la utilidad, especifique el nodo, y recomience servicio TFTP.
7. Una vez que recomienzan a los servicios, reinicie los teléfonos de modo que puedan extraer el archivo actualizado de la lista de la confianza de la identidad (ITL).
8. Vuelva a la página de la administración de certificados y borre los dos viejos archivos de la confianza. Éstos son los dos archivos expirados de la confianza que usted recibió del resultado del error. Los nuevos Certificados tienen un número de serie que haga juego el **archivo CAPF.pem**.
9. Complete los pasos anteriores para cada suscriptor.

IPSec

Los Certificados de la seguridad de protocolos en Internet (IPSec) afectan al master del error de la Recuperación tras desastres (DRF) y locales, que se ocupa de las funciones de reserva y del restore.

1. Navegue a la página de administración OS en Publisher.

2. Navegue al **Certificate Management (Administración de certificados) de la Seguridad** y haga clic el **archivo IPSEC.pem**.

3. Haga clic el **regenerado** para poner al día el archivo de la confianza.

4. Reinicie el servidor que el certificado fue regenerado encendido. Se requiere esto porque cada servicio se debe recomenzar después de cualquier regeneración/actualización de cualquier certificado. Sin embargo, el IPSec no tiene una capacidad del reinicio del servicio con excepción de reiniciar el nodo entero. Si otros Certificados necesitan ser puestos al día/ser regenerados, complete todos los pasos y después reinicie el nodo después de todo que los Certificados se han procesado a través. Esto permite que el servidor tenga todos los Certificados actualizados en el truststore y lea adentro correctamente.

CM

1. Navegue a la página de administración OS en Publisher.

2. Navegue a la página de la administración de certificados, haga clic el **hallazgo**, haga clic el **archivo CallManager.pem**, y después haga clic el regenerado**.**

3. Navegue a las **herramientas > al servicio de la característica** en la página de la utilidad, encuentre el nodo especificado, y recomience el servicio del CM de Cisco.

4. De la página de la utilidad, navegue a las **herramientas > a los servicios de red**, y recomience el servicio TV.

5. De la página de la utilidad, navegue a las **herramientas > a los servicios de la característica**, especifique el nodo, y recomience los servicios CM y CTI.

6. Reinicie los teléfonos de modo que puedan extraer el archivo actualizado ITL.

7. Complete los pasos anteriores para cada suscriptor.

TV

1. Navegue a la página de administración OS en Publisher.

2. Navegue al **Certificate Management (Administración de certificados) de la Seguridad**, haga clic el **hallazgo**, haga clic el **archivo TVS.pem**, y después haga clic el regenerado**.**

3. De la página de la utilidad, navegue a las **herramientas > a los servicios de red**, y recomience el servicio TV.

4. De la página de la utilidad, navegue a las **herramientas > a los servicios de la característica**, especifique el nodo, y recomience servicio TFTP.

5. Reinicie los teléfonos de modo que puedan extraer el archivo actualizado ITL.

6. Complete los pasos anteriores para cada suscriptor.

Borre los Certificados

Cuando usted borra los Certificados, asegúrese de que paren a los servicios previamente mencionados, y de que los Certificados que usted borra no están utilizados actualmente ni están expirados realmente.

También, marque siempre toda la información dentro del certificado, porque usted no puede salvarlo después de la cancelacíon.