Regeneración de certificados para CUCM

Contenido

Introducción

Este documento describe el procedimiento para regenerar certificados en Cisco Unified Communications Manager (CUCM) versión 8.X y posteriores.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- *Herramienta de supervisión en tiempo real* (RTMT)
- Certificados de CUCM

Componentes Utilizados

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

- CUCM versión 8.X y superior

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe el procedimiento paso a paso para regenerar certificados en Cisco Unified Communications Manager (CUCM) versión 8.X y posteriores. Sin embargo, esto no refleja los cambios posteriores a 12.0 en la recuperación del DIT.

Instalación de RTMT

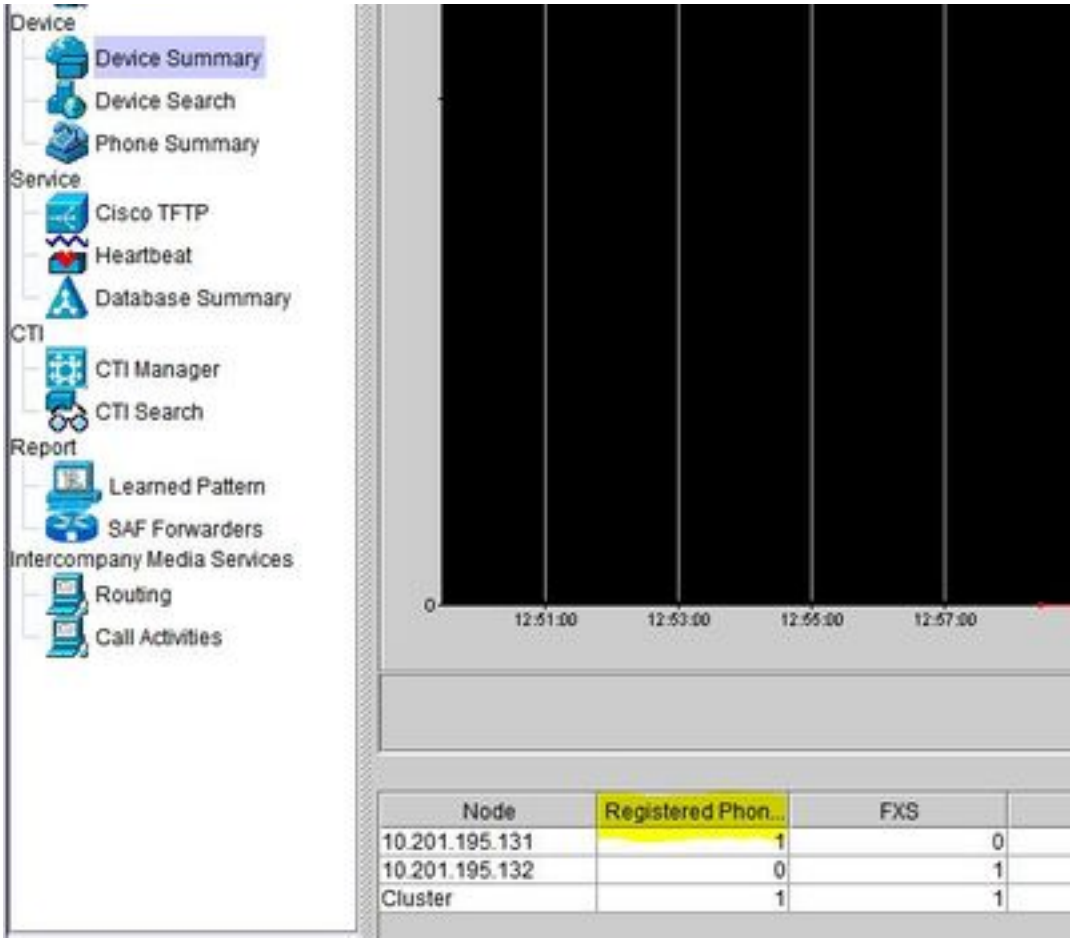
- Descargue e instale la herramienta RTMT desde Call Manager. Desplácese hasta Administración de Call Manager (CM): **Application > Plugins > Find > Herramienta de supervisión en tiempo real de Cisco Unified: Windows > Descargar** Instalación e inicio

Supervisión de terminales con RTMT

- Inicie RTMT e introduzca la dirección IP o el nombre de dominio completo (FQDN); a continuación, introduzca el nombre de usuario y la contraseña para acceder a la herramienta:
- Seleccione la **ficha Voz/Vídeo**.Seleccione **Device Summary**. Esta sección identifica el número total de terminales registrados y cuántos a cada nodoSupervise mientras se restablece el terminal para garantizar el registro antes de la regeneración del siguiente certificado

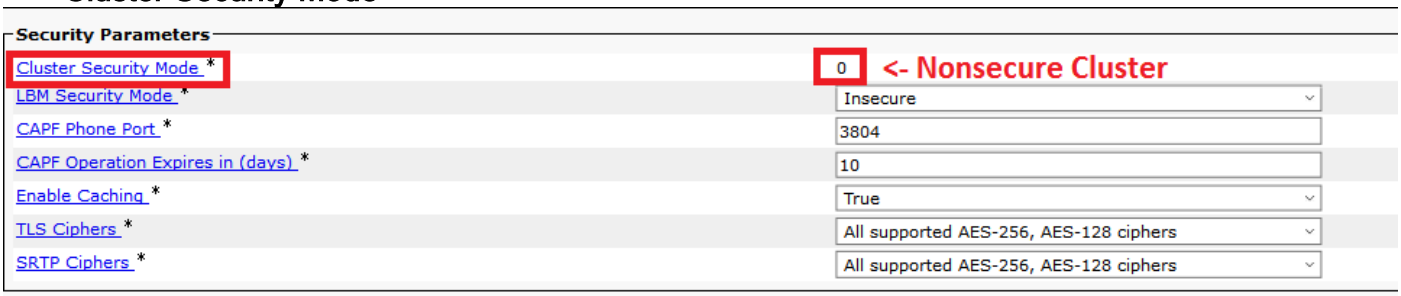
Consejo: El proceso de regeneración de algunos certificados puede afectar al terminal. Considere un plan de acción después del horario laboral habitual debido a la necesidad de reiniciar los servicios y los teléfonos. Se recomienda encarecidamente verificar el registro del teléfono mediante RTMT.

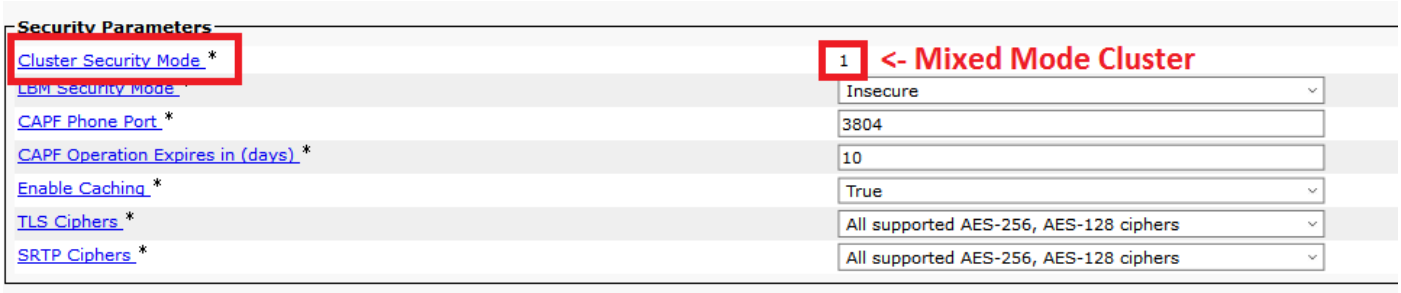
Advertencia: Los terminales con discordancia de ITL actual pueden tener problemas de registro después de este proceso. La eliminación del DIT en el terminal es una solución típica de prácticas recomendadas una vez finalizado el proceso de regeneración y registrados todos los demás teléfonos.



Identifique si el clúster está en modo mixto o en modo no seguro

- Vaya a Administración de CM. **System > Enterprise Parameters > Security Parameters > Cluster Security Mode**





Impacto del almacén de certificados

Es fundamental que todos los certificados del clúster de CUCM se actualicen correctamente para que el sistema funcione correctamente. Si los certificados han caducado o no son válidos, pueden afectar considerablemente al funcionamiento normal del sistema. El impacto puede variar según

la configuración del sistema. Aquí se muestra una lista de servicios para los certificados específicos que no son válidos o que han caducado:

CallManager.pem

- Los teléfonos cifrados/autenticados no se registran
- El protocolo de transferencia de archivos trivial (TFTP) no es de confianza (los teléfonos no aceptan archivos de configuración firmados ni archivos ITL)
- Los servicios telefónicos pueden verse afectados
- Los enlaces troncales del protocolo de inicio de sesión seguro (SIP) o los recursos multimedia (puentes de conferencia, punto de terminación de medios (MTP), codificadores X, etc.) no se registran ni funcionan.
- Falla la solicitud de AXL.

Tomcat.pem

- Los teléfonos no pueden acceder a servicios HTTPs alojados en el nodo de CUCM, como Directorio corporativo
- CUCM puede tener varios problemas web, como no poder acceder a páginas de servicio desde otros nodos del clúster
- Problemas de Extension Mobility (EM) o Extension Mobility entre clústeres
- Inicio de sesión único (SSO)
- Si se integra UCCX (Unified Contact Center Express), debido al cambio de seguridad de CCX 12.5, es necesario tener cargado el certificado Tomcat de CUCM (autofirmado) o el certificado raíz e intermedio Tomcat (para CA firmada) en el almacén de confianza Tomcat de UCCX, ya que afecta a los inicios de sesión de escritorio de Finesse.

CAPF.pem

- Los teléfonos no se autentican para VPN de teléfono, 802.1x o proxy de teléfono
- No se pueden emitir certificados de certificado de importancia local (LSC) para los teléfonos.
- Los archivos de configuración cifrados no funcionan

IPSec.pem

- El Sistema de recuperación ante desastres (DRS)/Marco de recuperación ante desastres (DRF) no funciona correctamente
- No funcionan los túneles IPsec a gateway (GW) a otros clústeres de CUCM

TVS (Trust Verification Service)

El servicio de verificación de confianza (TVS) es el componente principal de la seguridad de forma predeterminada. TVS permite a los teléfonos IP de Cisco Unified autenticar los servidores de aplicaciones, como los servicios de EM, el directorio y MIDlet, cuando se establece HTTPS.

TVS proporciona estas características:

- Escalabilidad: el número de certificados de confianza no afecta a los recursos del teléfono IP de Cisco Unified.
- Flexibilidad: la adición o eliminación de certificados de confianza se refleja automáticamente en el sistema.
- Security by Default (Seguridad predeterminada): las funciones de seguridad de señales y no multimedia forman parte de la instalación predeterminada y no requieren la intervención del usuario.

ITL y CTL

- ITL contiene la función de certificado para el TFTP de Call Manager, todos los certificados de TVS en el clúster y la función de proxy de autoridad certificadora (CAPF) cuando se ejecuta.
- CTL contiene entradas para el token de seguridad del administrador del sistema (SAST), Cisco CallManager y los servicios TFTP de Cisco que se ejecutan en el mismo servidor, CAPF, servidor o servidores TFTP y firewall del dispositivo de seguridad adaptable (ASA). No se hace referencia a TVS en CTL.

Proceso de regeneración de certificados

> **Nota:** Todos los terminales deben encenderse y registrarse antes de la regeneración de certificados. De lo contrario, los teléfonos no conectados requieren la eliminación del DIT.

Certificado Tomcat

Identificar si se están utilizando certificados de terceros:

1. Vaya a cada servidor del clúster (en pestañas independientes del explorador web) y comience por el editor, seguido de cada suscriptor. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Observar desde la columna Descripción si Tomcat indica Certificado autofirmado generado por el sistema. Si Tomcat está firmado por terceros, siga el enlace proporcionado y realice estos pasos después de la regeneración de Tomcat.Certificados firmados por terceros, consulte Carga de certificados GUI web de CCMAdmin de CUCM.
2. Seleccione **Find** para mostrar todos los certificados: Seleccione el certificado **Tomcat pem**.Una vez abierto, seleccione **Regenerar** y espere hasta que vea la ventana emergente Éxito, luego cierre la ventana emergente o vuelva y seleccione **Buscar/Lista**.
3. Continúe con cada suscriptor subsiguiente, siga el mismo procedimiento en el paso 2 y complete en todos los suscriptores de su clúster.
4. Una vez que todos los nodos hayan regenerado el certificado Tomcat, reinicie el servicio tomcat en todos los nodos. Comience con el editor y, a continuación, los suscriptores. Para reiniciar Tomcat necesita abrir una sesión CLI para cada nodo y ejecutar el comando **utils service restart Cisco Tomcat**.

5. Estos pasos son necesarios desde el entorno CCX si procede:

- Si se utiliza un certificado autofirmado, cargue los certificados Tomcat de todos los nodos del clúster de CUCM en el almacén de confianza de Tomcat de Unified CCX.
- Si se utiliza un certificado firmado por CA o firmado por CA privada, cargue el certificado de CA raíz de CUCM en el almacén de confianza Tomcat de Unified CCX.
- Reinicie los servidores como se menciona en el documento de regeneración de certificados para CCX.

Referencias adicionales:

- Guía de administración de certificados de la solución UCCX
- Utilidad de comprobación de estado de Unified CCX

Certificado IPSEC

Nota: CUCM/Mensajería instantánea y presencia (IM&P) antes de la versión 10.X del DRF Master El agente se ejecuta tanto en CUCM Publisher como en IM&P Publisher. El servicio local DRF se ejecuta en los suscriptores respectivamente. Versiones 10.X y posteriores, DRF Master El agente se ejecuta solo en el publicador de CUCM y en el servicio local de DRF en los suscriptores de CUCM y en los publicadores y suscriptores de IM&P.

Nota: El sistema de recuperación ante desastres utiliza una comunicación basada en Secure Socket Layer (SSL) entre el Master Agente y agente local para la autenticación y el cifrado de datos entre los nodos de clúster de CUCM. DRS utiliza los certificados IPSec para el cifrado de clave pública/privada. Tenga en cuenta que si elimina el archivo IPSEC truststore (hostname.pem) de la página Administración de certificados, DRS no funcionará como se espera. Si elimina el archivo de confianza IPSEC manualmente, debe asegurarse de cargar el certificado IPSEC en el almacén de confianza IPSEC. Para obtener más información, consulte la página de ayuda de administración de certificados en las guías de seguridad de Cisco Unified Communications Manager.

1. Vaya a cada servidor del clúster (en pestañas independientes del explorador web) y comience por el editor, seguido de cada suscriptor. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find**:
   Seleccione el certificado **IPSEC pem**.Una vez abierto, seleccione **Regenerar** y espere hasta que vea la ventana emergente Éxito, luego cierre la ventana emergente o vuelva y seleccione **Buscar/Lista**.
2. Continuar con los suscriptores subsiguientes; siga el mismo procedimiento en el paso 1 y complete en todos los suscriptores de su clúster.
3. Después de que todos los nodos hayan regenerado el certificado IPSEC, reinicie los servicios.
   Vaya a Publisher **Cisco Unified Serviceability**. **Serviciabilidad de Cisco Unified >**

Herramientas > Centro de control - Servicios de red.Seleccione **Reiniciar** en **Cisco DRF Master**servicio.Una vez que se complete el reinicio del servicio, seleccione **Restart** en el **Servicio local de Cisco DRF** en el editor, luego continúe con los suscriptores y seleccione **Restart** en el **Servicio local de Cisco DRF**.

El certificado IPSEC.pem del editor debe ser válido y estar presente en todos los suscriptores como almacenes de confianza IPSEC. El certificado IPSEC.pem de los suscriptores no estará presente en el editor como almacén de confianza IPSEC en una implementación estándar. Para verificar la validez, compare los números de serie del certificado IPSEC.pem del PUB con la confianza IPSEC en los SUB. Deben coincidir.

Certificado CAPF

Advertencia: Asegúrese de haber identificado si el clúster está en modo mixto antes de continuar. Consulte la sección **Identificación de si su clúster está en modo mixto o modo no seguro**.

1. Vaya a **Cisco Unified CM Administration > System > Enterprise Parameters**.
   Compruebe la sección Parámetros de Seguridad y compruebe si el modo de seguridad de cluster está establecido en 0 o 1. Si el valor es 0, el cluster está en modo no seguro. Si es 1, el clúster está en modo mixto y debe actualizar el archivo CTL antes de reiniciar los servicios. Consulte Vínculos sin token y token.
2. Vaya a cada servidor del clúster (en pestañas independientes del explorador web), comience por el editor y, a continuación, por cada suscriptor. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Seleccione el certificado **pem CAPF**.Una vez abierto, seleccione **Regenerar** y espere hasta que vea la ventana emergente Éxito. A continuación, cierre la ventana emergente o vuelva y seleccione **Buscar/Lista**
3. Continuar con los suscriptores subsiguientes; siga el mismo procedimiento en el paso 2 y complete en todos los suscriptores de su clúster. Si el cluster está en Modo Mixto SOLAMENTE y el CAPF ha sido regenerado - Actualice el CTL antes de continuar con Token - Sin Tokens.Si el clúster está en modo mixto, el servicio Call Manager también debe reiniciarse antes del reinicio de otros servicios.
4. Después de que todos los nodos hayan regenerado el certificado CAPF, reinicie los servicios.
   Vaya a **Serviciabilidad de Cisco Unified** del editor. **Serviciabilidad de Cisco Unified > Herramientas > Centro de control: servicios de funciones**.Comience con el publicador y seleccione **Restart** en el **Servicio de función proxy de Cisco Certificate Authority** sólo donde esté activo.
5. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red**. Empiece con el editor y continúe con los suscriptores; seleccione **Restart** en **Cisco Trust Verification** . Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones**.Comience con el editor y luego continúe con los suscriptores, reinicie el **servicio TFTP de Cisco** sólo donde esté activo.
6. Reinicie todos los teléfonos: **Cisco Unified CM Administration > System > Enterprise Parameters**Seleccione **Reset** y verá una ventana emergente con la declaración **You are about to reset all devices in the system. Esta acción no se puede deshacer. ¿Desea continuar?,**seleccione **Aceptar** y, a continuación, seleccione **Restablecer**.

Los teléfonos se restablecerán. Supervise sus acciones mediante la herramienta RTMT para asegurarse de que el restablecimiento se ha realizado correctamente y de que los dispositivos se vuelven a registrar en CUCM. Espere a que se complete el registro del teléfono antes de continuar con el siguiente certificado. Este proceso de registro de teléfonos puede llevar algún tiempo. Tenga en cuenta que los dispositivos que tenían ITL incorrectos antes del proceso de regeneración no se vuelven a registrar en el clúster hasta que se elimina.

Certificado de CallManager

> **Advertencia:** Asegúrese de haber identificado si el clúster está en modo mixto antes de continuar. Consulte la sección **Identificación de si su clúster está en modo mixto o modo no seguro**.

> **Advertencia:** No regenere los certificados CallManager.PEM y TVS.PEM al mismo tiempo. Esto provoca una discordancia irrecuperable con el ITL instalado en los terminales que requieren la eliminación del ITL de TODOS los terminales del clúster. Termine todo el proceso para CallManager.PEM y una vez que los teléfonos se registren nuevamente, inicie el proceso para TVS.PEM.

1. Vaya a **Cisco Unified CM Administration > System > Enterprise Parameters**: Compruebe la sección Parámetros de Seguridad y compruebe si el modo de seguridad de cluster está establecido en 0 o 1. Si el valor es 0, el cluster está en modo no seguro. Si es 1, el clúster está en modo mixto y debe actualizar el archivo CTL antes de reiniciar los servicios. Consulte Vínculos sin token y token.
2. Vaya a cada servidor del clúster (en pestañas independientes del explorador web), comience por el editor y, a continuación, por cada suscriptor. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find**.
   Seleccione el certificado pem de CallManager.Una vez abierto, seleccione **Regenerar** y espere hasta que vea la ventana emergente Éxito, luego cierre la ventana emergente o vuelva y seleccione **Buscar/Lista**.
3. Continuar con los suscriptores subsiguientes; siga el mismo procedimiento en el paso 2 y complete en todos los suscriptores de su clúster. Si el clúster está en modo mixto SOLAMENTE y el certificado de CallManager se ha regenerado - Actualice el CTL antes de continuar con Token - Tokenless
4. Inicie sesión en Publisher Cisco Unified Serviceability: Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones**.Comience con el editor y luego continúe con los suscriptores, reinicie el **servicio Cisco CallManager** donde esté activo.
5. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones**
   Empiece con el publicador y continúe con los suscriptores; reinicie el servicio **Cisco CTIManager** sólo si está activo.
6. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red**.
   Empiece con el publicador, continúe con los suscriptores y reinicie **Cisco Trust Verification Service**.
7. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones**.
   Comience con el editor y luego continúe con los suscriptores, reinicie el **servicio TFTP de**

Cisco sólo donde esté activo.

8. Reinicie todos los teléfonos: **Cisco Unified CM Administration > System > Enterprise Parameters**Seleccione **Reset** y verá una ventana emergente con la declaración **You are about to reset all devices in the system. Esta acción no se puede deshacer. ¿Desea continuar?,**seleccione **Aceptar** y, a continuación, seleccione **Restablecer**

Los teléfonos se restablecerán. Supervise sus acciones mediante la herramienta RTMT para asegurarse de que el restablecimiento se ha realizado correctamente y de que los dispositivos se vuelven a registrar en CUCM. Espere a que se complete el registro del teléfono antes de continuar con el siguiente certificado. Este proceso de registro de teléfonos puede llevar algún tiempo. Tenga en cuenta que los dispositivos que tenían ITL incorrectos antes del proceso de regeneración no se vuelven a registrar en el clúster hasta que se elimina ITL.

Certificado de TVS

Advertencia: No regenere los certificados CallManager.PEM y TVS.PEM al mismo tiempo. Esto provoca una discordancia irrecuperable con el ITL instalado en los terminales que requieren la eliminación del ITL de TODOS los terminales del clúster.

Nota: TVS autentica certificados en nombre de Call Manager. Regenere este certificado en último lugar.

Vaya a cada servidor del clúster (en pestañas independientes del explorador web), comience por el editor y, a continuación, por cada suscriptor. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find**:

- Seleccione el certificado **TVS pem**.
- Una vez abierto, seleccione **Regenerar** y espere hasta que vea la ventana emergente Éxito, luego cierre la ventana emergente o vuelva y seleccione **Buscar/Lista**.

1. Continuar con los suscriptores subsiguientes; siga el mismo procedimiento en el paso 1 y complete en todos los suscriptores de su clúster. Una vez que todos los nodos hayan regenerado el certificado de TVS, reinicie los servicios: Inicie sesión en Publisher **Cisco Unified Serviceability**. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red**.En el editor, seleccione **Restart** en **Cisco Trust Verification Service**.Una vez que se complete el reinicio del servicio, continúe con los suscriptores y reinicie el **Servicio de verificación de confianza de Cisco**.
2. Comience con el publicador y luego continúe con los suscriptores, reinicie el servicio **Cisco TFTP** solo donde esté activo.
3. Reinicie todos los teléfonos: **Cisco Unified CM Administration > System > Enterprise Parameters**.Seleccione **Reset** y verá una ventana emergente con la declaración **You are about to reset all devices in the system. Esta acción no se puede deshacer. ¿Desea continuar?,**seleccione **Aceptar** y, a continuación, seleccione **Restablecer**.

Los teléfonos se restablecerán. Supervise sus acciones mediante la herramienta RTMT para asegurarse de que el restablecimiento se ha realizado correctamente y de que los dispositivos se vuelven a registrar en CUCM. Espere a que se complete el registro del teléfono antes de continuar con el siguiente certificado. Este proceso de registro de teléfonos puede llevar algún tiempo. Tenga en cuenta que los dispositivos que tenían ITL incorrectos antes del proceso de regeneración no se vuelven a registrar en el clúster hasta que se elimina ITL.

ITLRecrecovery Certificate

Nota: El certificado de recuperación ITL se utiliza cuando los dispositivos pierden su estado de confianza. El certificado aparece tanto en el DIT como en la CTL (cuando el proveedor de CTL está activo).
Si los dispositivos pierden su estado de confianza, puede utilizar el comando **utils itl reset localkey** para clústeres no seguros y el comando **utils ctl reset localkey** para clústeres de modo mixto. Lea la guía de seguridad de su versión de Call Manager para familiarizarse con el uso del certificado ITLRecrecovery y el proceso necesario para recuperar el estado de confianza.
Si el clúster se ha actualizado a una versión que admite una longitud de clave de 2048 y los certificados de servidor de clústeres se han vuelto a generar a 2048 y no se ha vuelto a generar ITLRecrecovery y actualmente tiene una longitud de clave de 1024, el comando de recuperación ITL no funciona y no se utiliza el método ITLRecrecovery.

1. Vaya a cada servidor del clúster (en pestañas independientes del explorador web), comience por el editor y, a continuación, por cada suscriptor. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find**:
   Seleccione el certificado **ITLRecrecovery pem**.Una vez abierto, seleccione **Regenerar** y espere hasta que vea la ventana emergente Éxito, luego cierre la ventana emergente o vuelva y seleccione **Buscar/Lista**.
2. Continuar con los suscriptores subsiguientes; siga el mismo procedimiento en el paso 2 y complete en todos los suscriptores de su clúster.
3. Después de que todos los nodos hayan regenerado el certificado ITLRecrecovery, los servicios deben reiniciarse en el orden siguiente: Si se encuentra en el modo mixto: actualice la CTL antes de continuar con Token - Tokenless.Inicie sesión en Publisher **Cisco Unified Serviceability**. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red**.En el editor, seleccione **Restart** en **Cisco Trust Verification Service**. Una vez que se complete el reinicio del servicio, continúe con los suscriptores y reinicie el **Servicio de verificación de confianza de Cisco**.
4. Comience con el publicador y luego continúe con los suscriptores, reinicie el servicio **Cisco TFTP** solo donde esté activo.
5. Reinicie todos los teléfonos: **Cisco Unified CM Administration > System > Enterprise Parameters**Seleccione **Reset** y verá una ventana emergente con la declaración **You are about to reset all devices in the system. Esta acción no se puede deshacer. ¿Desea continuar?,**seleccione **Aceptar** y, a continuación, seleccione **Restablecer**.
6. Los teléfonos cargan ahora el nuevo ITL/CTL mientras se restablecen.

Eliminar certificados de confianza caducados

Nota: Identifique los certificados de confianza que deben eliminarse, ya no son necesarios o han caducado. No elimine los cinco certificados base que incluyen CallManager.pem, tomcat.pem, ipsec.pem, CAPF.pem y TVS.pem. Los certificados de confianza se pueden eliminar cuando sea necesario. El siguiente servicio que se reinicia está diseñado para borrar la información de los certificados heredados dentro de esos servicios.

1. Vaya a **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de**

red. En la lista desplegable, seleccione el publicador de CUCM.Seleccione **Detener** Notificación de cambio de certificado.Repita este procedimiento para cada nodo de Call Manager del clúster.Si tiene un servidor IMP: En el menú desplegable, seleccione los servidores IMP de uno en uno y seleccione **Detener administración de plataforma Servicios web y Cisco Intercluster Sync Agent**.

2. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find**. Busque los certificados de confianza caducados. (Para las versiones 10.X y posteriores, puede filtrar por vencimiento. Para las versiones inferiores a 10.0, debe identificar los certificados específicos manualmente o a través de las alertas de RTMT si se reciben.)El mismo certificado de confianza puede aparecer en varios nodos. Debe eliminarse de forma individual de cada nodo.Seleccione el certificado de confianza que desea eliminar (dependiendo de su versión, obtendrá una ventana emergente o accederá al certificado en la misma página) Seleccione **Eliminar**. (Aparece una ventana emergente que comienza con "va a eliminar permanentemente este certificado".)Seleccione **Aceptar**.
3. Repita el proceso para cada certificado de confianza que desee eliminar.
4. Al finalizar, es necesario reiniciar los servicios relacionados directamente con los certificados eliminados. No es necesario reiniciar los teléfonos en esta sección. Call Manager y CAPF pueden afectar a los terminales. Tomcat-trust: reinicie el servicio Tomcat mediante la línea de comandos (consulte la sección Tomcat)CAPF-trust: restart Cisco Certificate Authority Proxy Function (consulte la sección CAPF) No reinicie los terminales.CallManager-trust: CallManager Service/CTIManager (Vea la Sección CallManager) No reinicie los terminales. Afecta a los terminales y provoca reinicios.Confianza IPSEC: DRF Master/DRF Local (Consulte la sección IPSEC).TVS (autofirmado) no tiene certificados de confianza.
5. Reinicie los servicios que se detuvieron anteriormente en el paso 1.

Verificación

El procedimiento de verificación no está disponible para esta configuración.

Troubleshoot

Los procedimientos de solución de problemas no están disponibles para esta configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).