Crear nuevos certificados a partir de certificados de CA firmados

Contenido

Introducción

Este documento describe cómo regenerar los certificados firmados por una autoridad de certificación (CA) en Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

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

Componentes Utilizados

- CUCM versión 10.x, 11.x y 12.x.

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.

Información previa a la comprobación

> **Nota:** Para la regeneración de certificados con firma automática, consulte la Guía de regeneración de certificados. Para la regeneración de certificados Multi-SAN firmados por CA, consulte la Guía de Regeneración de Certificados Multi-SAN.

Para comprender el impacto de cada certificado y su regeneración, consulte la Guía de regeneración autofirmada.

Cada tipo de solicitud de firma de certificado (CSR) tiene diferentes usos de clave, que son obligatorios en el certificado firmado. La Guía de seguridad incluye una tabla con los usos de claves requeridos para cada tipo de certificado.

Para cambiar la configuración del asunto (localidad, estado, unidad organizativa, etc.), ejecute este comando:

- **set web-security** orgunit orgname locality state [country] [alternatehostname]

El certificado Tomcat se regenera automáticamente después de ejecutar el set web-security comando. El nuevo certificado de firma automática no se aplica a menos que se reinicie el servicio Tomcat. Consulte estas guías para obtener más información sobre este comando:

- Guía de referencia de línea de comandos
- Enlace a los pasos de la comunidad de Cisco
- Video

Configurar y regenerar certificados

Los pasos para regenerar certificados de nodo único en un clúster de CUCM firmado por una CA se enumeran para cada tipo de certificado. No es necesario volver a generar todos los certificados del clúster si no han caducado.

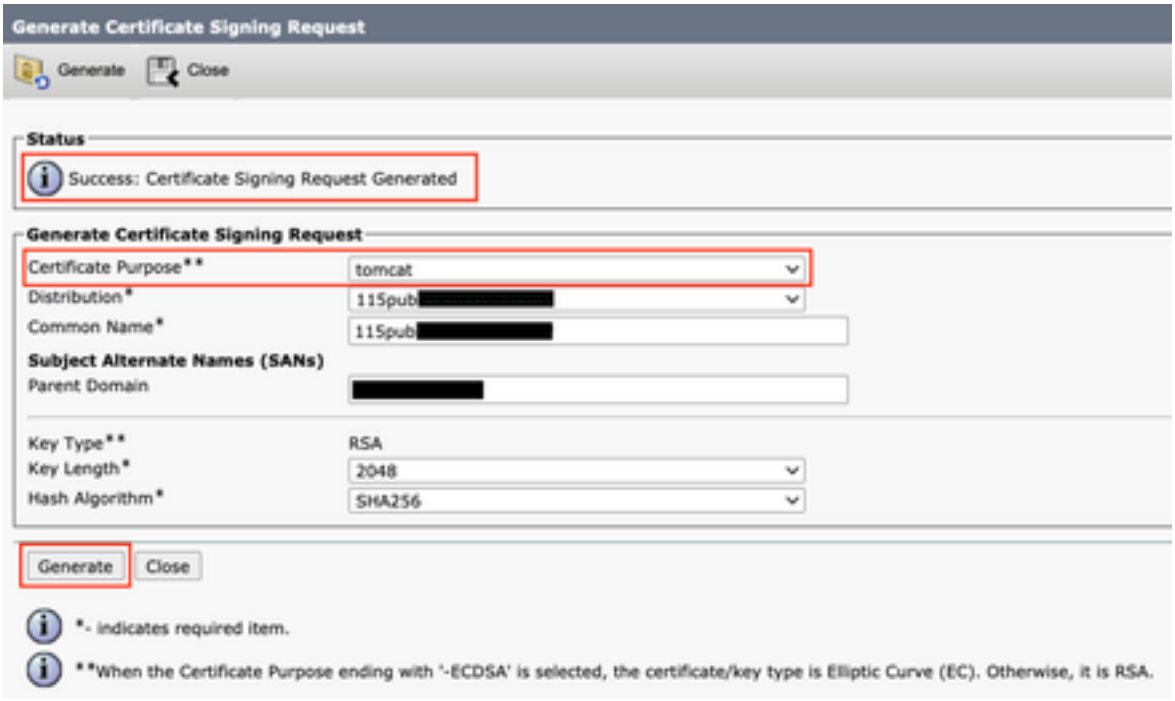
Certificado Tomcat

> **Precaución**: compruebe que SSO está deshabilitado en el clúster (**CM Administration > System > SAML Single Sign-On**). Si SSO está activado, debe desactivarse y, a continuación, activarse una vez finalizado el proceso de regeneración de certificados de Tomcat.

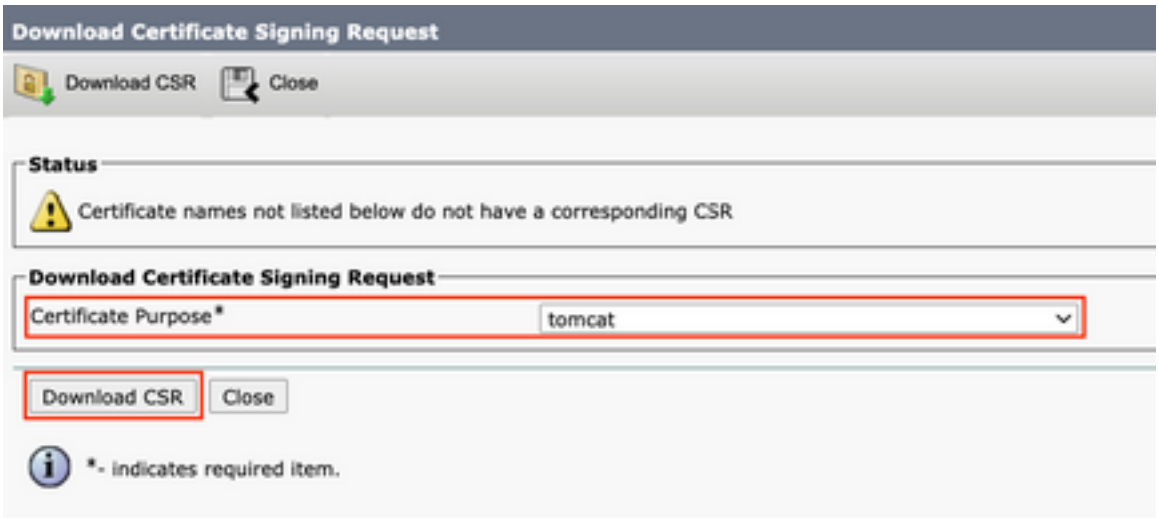
En todos los nodos (CallManager e IM&P) del clúster:

Paso 1. Acceda a **Cisco Unified OS Administration > Security > Certificate Management > Find** y verificar la fecha de vencimiento del certificado Tomcat.

Paso 2. Haga clic en Generate CSR > Certificate Purpose: tomcat. Seleccione la configuración deseada para el certificado y haga clic en **Generate**. Espere a que aparezca el mensaje de confirmación y haga clic en Close.



Paso 3. Descargue el CSR. Haga clic Download CSR , seleccione **Certificate Purpose: tomcat**, y haga clic en Download.



Paso 4. Envíe el CSR a la autoridad certificadora.

Paso 5. La autoridad de certificación devuelve dos o más archivos para la cadena de certificados firmados. Cargue los certificados en este orden:

- Certificado de CA raíz como tomcat-trust. Vaya a **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Establezca la descripción del certificado y examine el archivo de certificado raíz.
- Certificado intermedio como tomcat-trust (opcional). Vaya a **Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust**. Establezca la descripción del certificado y examine el archivo de certificado intermedio.

  Nota: Algunas CA no proporcionan un certificado intermedio; si sólo se proporcionó el certificado raíz, este paso puede omitirse.

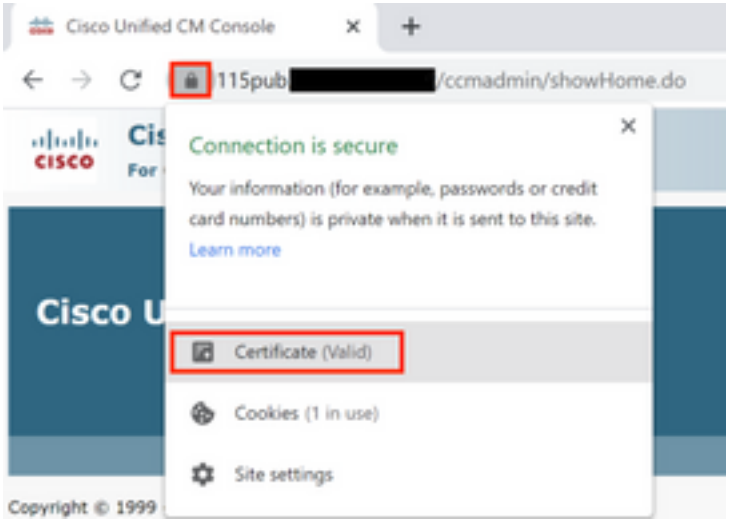
- Certificado firmado por la CA como tomcat. Vaya a **Certificate Management > Upload certificate > Certificate**

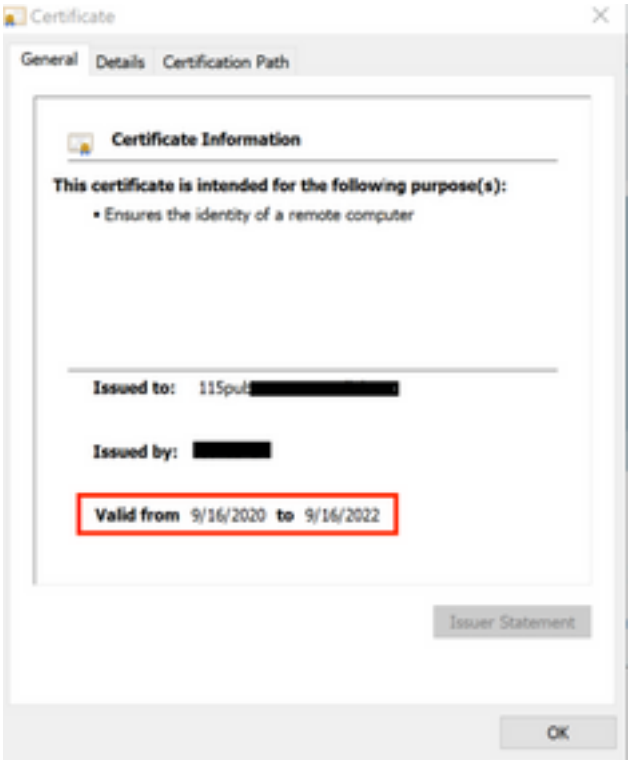
Purpose: tomcat. Establezca la descripción del certificado y busque el archivo de certificado firmado por la CA para el nodo de CUCM actual.

Nota: En este momento, CUCM compara el CSR y el certificado firmado por la CA cargado. Si la información coincide, el CSR desaparece y se carga el nuevo certificado firmado por la CA. Si recibe un mensaje de error después de cargar el certificado, consulte la Upload Certificate Common Error Messages sección.

Paso 6. Para que el nuevo certificado se aplique al servidor, el servicio Cisco Tomcat debe reiniciarse mediante CLI (comience con Publisher y, a continuación, con los suscriptores, de uno en uno); utilice el comando utils service restart Cisco Tomcat.

Para validar el certificado de Tomcat, CUCM lo utiliza ahora. Vaya a la página Web del nodo y seleccione Site Information (Icono de bloqueo) en el Explorador, haga clic en el botón certificate y compruebe la fecha del nuevo certificado.





Certificado de CallManager

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

Nota: para determinar si el clúster está en modo mixto, vaya a **Administración de Cisco Unified CM > Sistema > Parámetros de empresa > Modo de seguridad del clúster (0 == No seguro; 1 == Mixed Mode [Modo mixto])**.

Para todos los nodos CallManager del clúster:

Paso 1. Acceda a Cisco Unified OS Administration > Security > Certificate Management > Find y verifique la fecha de vencimiento del certificado de CallManager.

Paso 2. Haga clic en Generate CSR > Certificate Purpose: CallManager. Seleccione la configuración deseada para el certificado y haga clic en Generate. Espere a que aparezca el mensaje de confirmación y haga clic en Close.

Paso 3. Descargue el CSR. Haga clic **Download CSR**. Select **Certificate Purpose: CallManager** and click **Download**.

Paso 4. Envíe el CSR al Certificate Authority .

Paso 5. La autoridad de certificación devuelve dos o más archivos para la cadena de certificados firmados. Cargue los certificados en este orden:

- Certificado de CA raíz como CallManager-trust. Vaya a Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Establezca la descripción del certificado y examine el archivo de certificado raíz.
- Certificado intermedio como CallManager-trust (opcional). Vaya a Certificate Management > Upload certificate > Certificate Purpose: CallManager-trust. Establezca la descripción del certificado y examine el archivo de certificado intermedio.

Nota: Algunas CA no proporcionan un certificado intermedio; si sólo se proporcionó el certificado raíz, este paso puede omitirse.

- Certificado firmado por la CA como CallManager. Vaya a Certificate Management > Upload certificate > Certificate Purpose: CallManager. Establezca la descripción del certificado y examine el archivo de certificado firmado por la CA para el nodo de CUCM actual.

Nota: En este momento, CUCM compara el CSR y el certificado firmado por la CA cargado. Si la información coincide, el CSR desaparece y se carga el nuevo certificado firmado por la CA. Si recibe un mensaje de error después de cargar el certificado, consulte la sección **Cargar mensajes de error comunes del certificado**.

Paso 6. Si el cluster está en Modo Mixto, actualice la CTL antes de reiniciar los servicios: Token o Tokenless. Si el clúster está en modo no seguro, omita este paso y continúe con el reinicio de los servicios.

Paso 7. Para obtener el nuevo certificado aplicado al servidor, los servicios requeridos deben reiniciarse (sólo si el servicio se ejecuta y está activo). Navegue hasta:

- Cisco Unified Serviceability > Tools > Control Center - Network Services > Cisco Trust Verification Service
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco TFTP
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CallManager
- Cisco Unified Serviceability > Tools > Control Center - Feature Services > Cisco CTIManager

Paso 8. Reinicie todos los teléfonos:

- Vaya a Cisco Unified CM Administration > System > Enterprise Parameters > Reset. Aparecerá una ventana emergente con la indicación Está a punto de restablecer todos los dispositivos del sistema. Esta acción no se puede deshacer. Continúe? seleccionar OK y, a continuación, haga clic en Reset .

Nota: Supervise el registro de dispositivos mediante RTMT. Una vez que todos los teléfonos vuelvan a registrarse, podrá continuar con el siguiente tipo de certificado.

Certificado IPSec

Precaución: Una tarea de copia de seguridad o restauración no debe estar activa cuando se vuelva a generar el certificado IPSec.

Para todos los nodos (CallManager e IM&P) del clúster:

Paso 1. Acceda a Cisco Unified OS Administration > Security > Certificate Management > Find y compruebe la fecha de caducidad del certificado ipsec.

Paso 2. Haga clic en **Generar CSR > Propósito del certificado: ipsec.** Seleccione la configuración deseada para el certificado y haga clic en **Generar**. Espere a que aparezca el mensaje de confirmación y haga clic en **Cerrar**.

Paso 3. Descargue el CSR. Haga clic en **Descargar CSR**. Seleccione Certificate Purpose ipsec y haga clic en **Download**.

Paso 4. Envíe el CSR a la autoridad certificadora.

Paso 5. La autoridad de certificación devuelve dos o más archivos para la cadena de certificados firmados. Cargue los certificados en este orden:

- Certificado de CA raíz como ipsec-trust. Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: ipsec-trust.** Establezca la descripción del certificado y examine el archivo de certificado raíz.
- Certificado intermedio como ipsec-trust (opcional). Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: tomcat-trust**. Establezca la descripción del certificado y examine el archivo de certificado intermedio.

Nota: Algunas CA no proporcionan un certificado intermedio; si sólo se proporcionó el certificado raíz, este paso puede omitirse.

- Certificado firmado por la CA como IPSec. Vaya a **Administración de certificados >**

Cargar certificado > Propósito del certificado: ipsec. Establezca la descripción del certificado y examine el archivo de certificado firmado por la CA para el nodo de CUCM actual.

Nota: En este momento, CUCM compara el CSR y el certificado firmado por la CA cargado. Si la información coincide, el CSR desaparece y se carga el nuevo certificado firmado por la CA. Si recibe un mensaje de error después de cargar el certificado, consulte la sección **Cargar mensajes de error comunes de certificado< /strong>.**

Paso 6. Para obtener el nuevo certificado aplicado al servidor, los servicios requeridos deben reiniciarse (sólo si el servicio se ejecuta y está activo). Navegue hasta:

- **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red > Cisco DRF Master**(Editor)
- **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red > Local de Cisco DRF** (editor y suscriptores)

Certificado CAPF

Nota: para determinar si el clúster está en modo mixto, desplácese a **Administración de Cisco Unified CM > Sistema > Parámetros de empresa > Modo de seguridad del clúster (0 == No seguro; 1 == Mixed Mode [Modo mixto])**.

Nota: el servicio CAPF sólo se ejecuta en el publicador, que es el único certificado utilizado. No es necesario obtener nodos de suscriptor firmados por una CA porque no se utilizan. Si el certificado ha caducado en los suscriptores y desea evitar las alertas de certificados caducados, puede volver a generar los certificados CAPF de suscriptor como de firma automática. Para obtener más información, vea Certificado CAPF como firmado automáticamente.

En el editor:

Paso 1. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find** y verifique la fecha de vencimiento del certificado CAPF.

Paso 2. Haga clic en **Generar CSR > Propósito del certificado: CAPF. Seleccione la configuración deseada para el certificado y haga clic en Generar**. Espere a que aparezca el mensaje de confirmación y haga clic en **Cerrar**.

Paso 3. Descargue el CSR. Haga clic en **Descargar CSR**. Seleccione Certificate Purpose CAPF y haga clic en **Download**.

Paso 4. Envíe el CSR a la autoridad certificadora.

Paso 5. La autoridad de certificación devuelve dos o más archivos para la cadena de certificados firmados. Cargue los certificados en este orden:

- Certificado de CA raíz como CAPF-trust. Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: CAPF-trust.** Establezca la descripción del

certificado y examine el archivo de certificado raíz.
- Certificado intermedio como CAPF-trust (opcional). Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: CAPF-trust**. Establezca la descripción del certificado y examine el archivo de certificado intermedio.

Nota: Algunas CA no proporcionan un certificado intermedio; si sólo se proporcionó el certificado raíz, este paso puede omitirse.

- Certificado firmado por la CA como CAPF. Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: CAPF.** Establezca la descripción del certificado y examine el archivo de certificado firmado por la CA para el nodo de CUCM actual.

Nota: En este momento, CUCM compara el CSR y el certificado firmado por la CA cargado. Si la información coincide, el CSR desaparece y se carga el nuevo certificado firmado por la CA. Si recibe un mensaje de error después de cargar el certificado, consulte la sección **Cargar mensajes de error comunes del certificado**.

Paso 6. Si el cluster está en Modo Mixto, actualice la CTL antes de reiniciar los servicios: Token o Tokenless. Si el clúster está en modo no seguro, omita este paso y continúe con el reinicio del servicio.

Paso 7. Para obtener el nuevo certificado aplicado al servidor, los servicios requeridos deben reiniciarse (sólo si el servicio se ejecuta y está activo). Navegue hasta:

- **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red > Servicio de verificación de confianza de Cisco** (todos los nodos en los que se ejecuta el servicio)
- **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones > Cisco TFTP** (todos los nodos en los que se ejecuta el servicio)
- **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones > Función proxy de Cisco Certificate Authority** (Editor)

Paso 8. Reinicie todos los teléfonos:

- Vaya a **Cisco Unified CM Administration > System > Enterprise Parameters > Reset**. Aparecerá una ventana emergente con la indicación Está a punto de restablecer todos los dispositivos del sistema. Esta acción no se puede deshacer. Continúe? seleccione **Aceptar** y haga clic en **Restablecer**.

Nota: Supervise el registro de dispositivos mediante RTMT. Una vez que todos los teléfonos vuelvan a registrarse, podrá continuar con el siguiente tipo de certificado.

Certificado de TVS

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

TVS.

Para todos los nodos TVS del clúster:

Paso 1. Vaya a **Cisco Unified OS Administration > Security > Certificate Management > Find** y verifique la fecha de vencimiento del certificado de TVS.

Paso 2. Haga clic en **Generar CSR > Propósito del certificado: TVS.** Seleccione la configuración deseada para el certificado y haga clic en **Generar**. Espere a que aparezca el mensaje de confirmación y haga clic en **Cerrar**.

Paso 3. Descargue el CSR. Haga clic en **Descargar CSR**. Seleccione **Certificate Purpose TVS** y haga clic en **Download**.

Paso 4. Envíe el CSR a la autoridad certificadora.

Paso 5. La autoridad de certificación devuelve dos o más archivos para la cadena de certificados firmados. Cargue los certificados en este orden:

- Certificado de CA raíz como TVS-trust. Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: TVS-trust**. Establezca la descripción del certificado y examine el archivo de certificado raíz.
- Certificado intermedio como TVS-trust (opcional). Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: TVS-trust**. Establezca la descripción del certificado y examine el archivo de certificado intermedio.

  Nota: Algunas CA no proporcionan un certificado intermedio; si sólo se proporcionó el certificado raíz, este paso puede omitirse.

- Certificado firmado por la CA como TVS. Vaya a **Administración de certificados > Cargar certificado > Propósito del certificado: TVS.** Establezca la descripción del certificado y examine el archivo de certificado firmado por la CA para el nodo de CUCM actual.

  Nota: En este momento, CUCM compara el CSR y el certificado firmado por la CA cargado. Si la información coincide, el CSR desaparece y se carga el nuevo certificado firmado por la CA. Si recibe un mensaje de error después de cargar el certificado, consulte la sección **Cargar mensajes de error comunes del certificado**.

Paso 6. Para obtener el nuevo certificado aplicado al servidor, los servicios requeridos deben reiniciarse (sólo si el servicio se ejecuta y está activo). Navegue hasta:

- **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones > Cisco TFTP** (Todos los nodos en los que se ejecuta el servicio)
- **Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red > Servicio de verificación de confianza de Cisco** (todos los nodos en los que se ejecuta el servicio)

Paso 7. Reinicie todos los teléfonos:

- Vaya a **Cisco Unified CM Administration > System > Enterprise Parameters > Reset**. Aparecerá una ventana emergente con la indicación Está a punto de restablecer todos los dispositivos del sistema. Esta acción no se puede deshacer. Continúe? seleccione **Aceptar** y haga clic en **Restablecer**.

  Nota: Supervise el registro de dispositivos mediante RTMT. Una vez que todos los teléfonos vuelvan a registrarse, podrá continuar con el siguiente tipo de certificado.

Solucionar problemas de mensajes de error comunes de certificados cargados

En esta sección se enumeran algunos de los mensajes de error más comunes cuando se carga un certificado firmado por CA.

El certificado de la CA no está disponible en el almacén de confianza

Este error significa que el certificado raíz o intermedio no se cargó en CUCM. Verifique que esos dos certificados se hayan cargado como almacén de confianza antes de que se cargue el certificado de servicio.

El archivo /usr/local/platform/.security/tomcat/keys/tomcat.csr no existe

Este error aparece cuando no existe una CSR para el certificado (tomcat, callmanager, ipsec, capf, tvs). Verifique que el CSR se haya creado antes y que el certificado se haya creado en función de ese CSR. Puntos importantes a tener en cuenta:

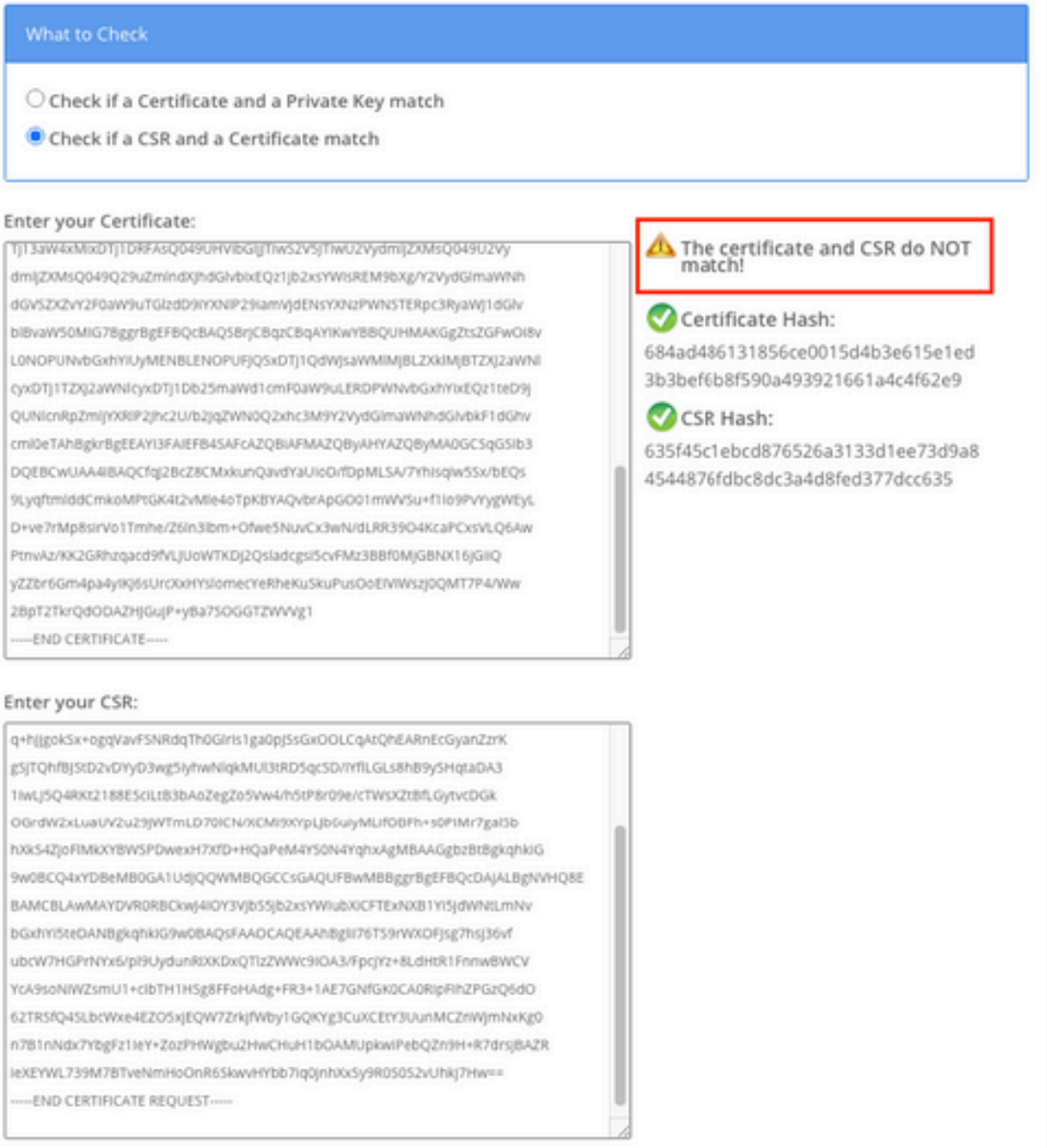
- Solo puede existir 1 CSR por servidor y tipo de certificado. Esto significa que si se crea una nueva CSR, se reemplaza la antigua.
- CUCM no admite certificados comodín.
- No es posible reemplazar un certificado de servicio que está actualmente en vigor sin una nueva CSR.
- Otro posible error para el mismo problema es "No se pudo cargar el archivo /usr/local/platform/upload/certs//tomcat.der." Esto depende de la versión de CUCM.

La clave pública CSR y la clave pública del certificado no coinciden

Este error aparece cuando el certificado proporcionado por la CA tiene una clave pública distinta de la enviada en el archivo CSR. Las posibles razones son:

- Se ha cargado el certificado incorrecto (quizá de otro nodo).
- El certificado de CA se generó con una CSR diferente.
- El CSR se regeneró y reemplazó al CSR antiguo que se utilizó para obtener el certificado firmado.

Para verificar la CSR y la coincidencia de clave pública de certificado, hay varias herramientas en línea como SSL.



Otro posible error para el mismo problema es "No se pudo cargar el archivo /usr/local/platform/upload/certs//tomcat.der." Esto depende de la versión de CUCM.

El nombre alternativo (SAN) del asunto CSR y la SAN del certificado no coinciden

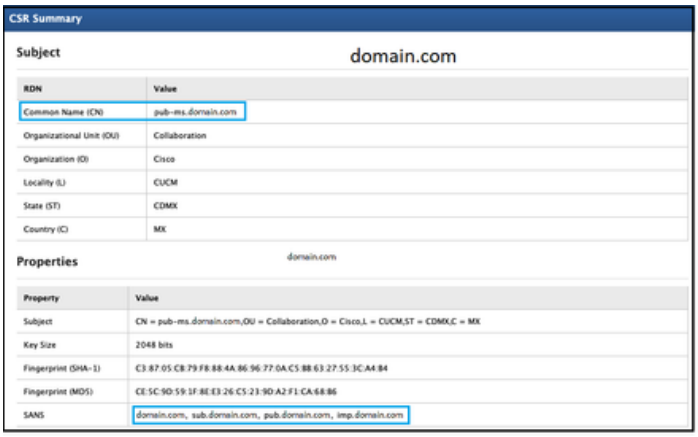
Las SAN entre el CSR y el certificado deben ser iguales. Esto impide la certificación de dominios no permitidos. Para verificar la discordancia de SAN, siga estos pasos:

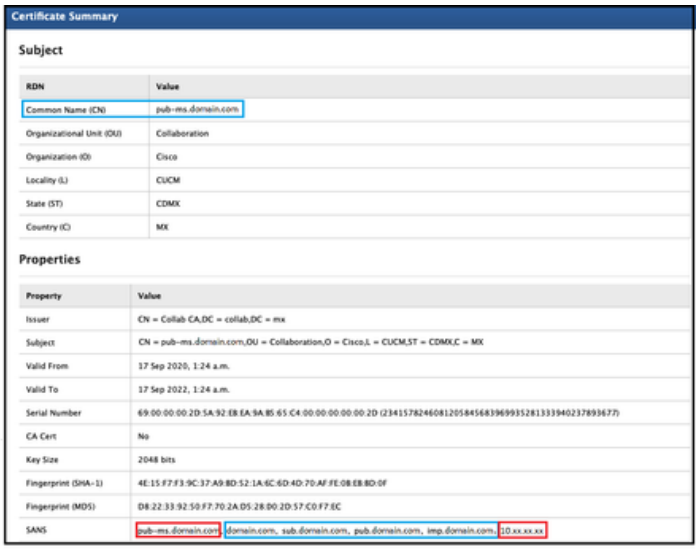
1. Decodificar la RSE y el certificado (base 64). Hay diferentes decodificadores disponibles en línea, como el Decoder.

2. Compare las entradas de SAN y verifique que todas coinciden. El orden no es importante, pero todas las entradas de la CSR deben ser iguales en el certificado.

Por ejemplo, el certificado firmado por la CA tiene agregadas dos entradas SAN adicionales, el

nombre común del certificado y una dirección IP adicional.



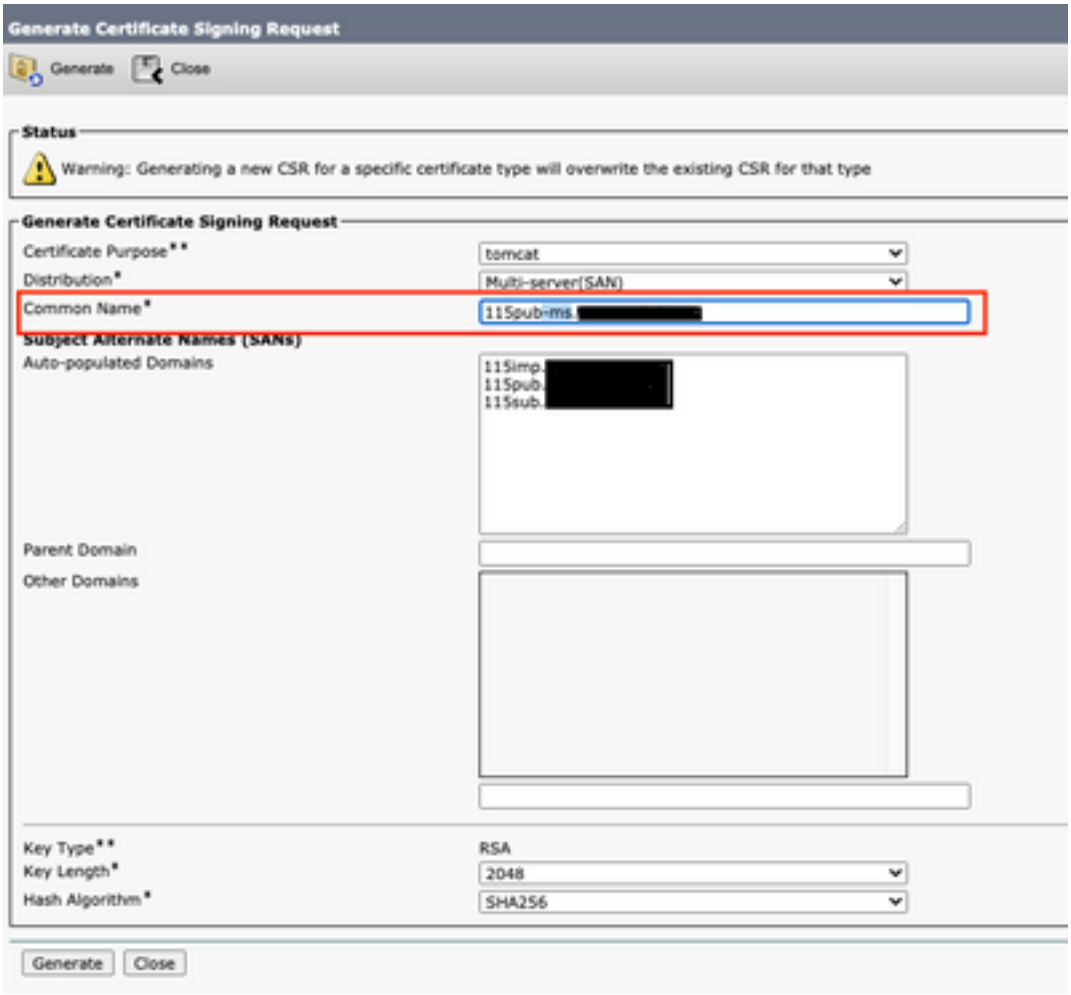


3. Una vez que haya identificado que la SAN no coincide, hay dos opciones para solucionar este problema:

1. Solicite al administrador de la CA que emita un certificado con las mismas entradas de SAN que se envían en el CSR.
2. Cree una CSR en CUCM que cumpla los requisitos de la CA.

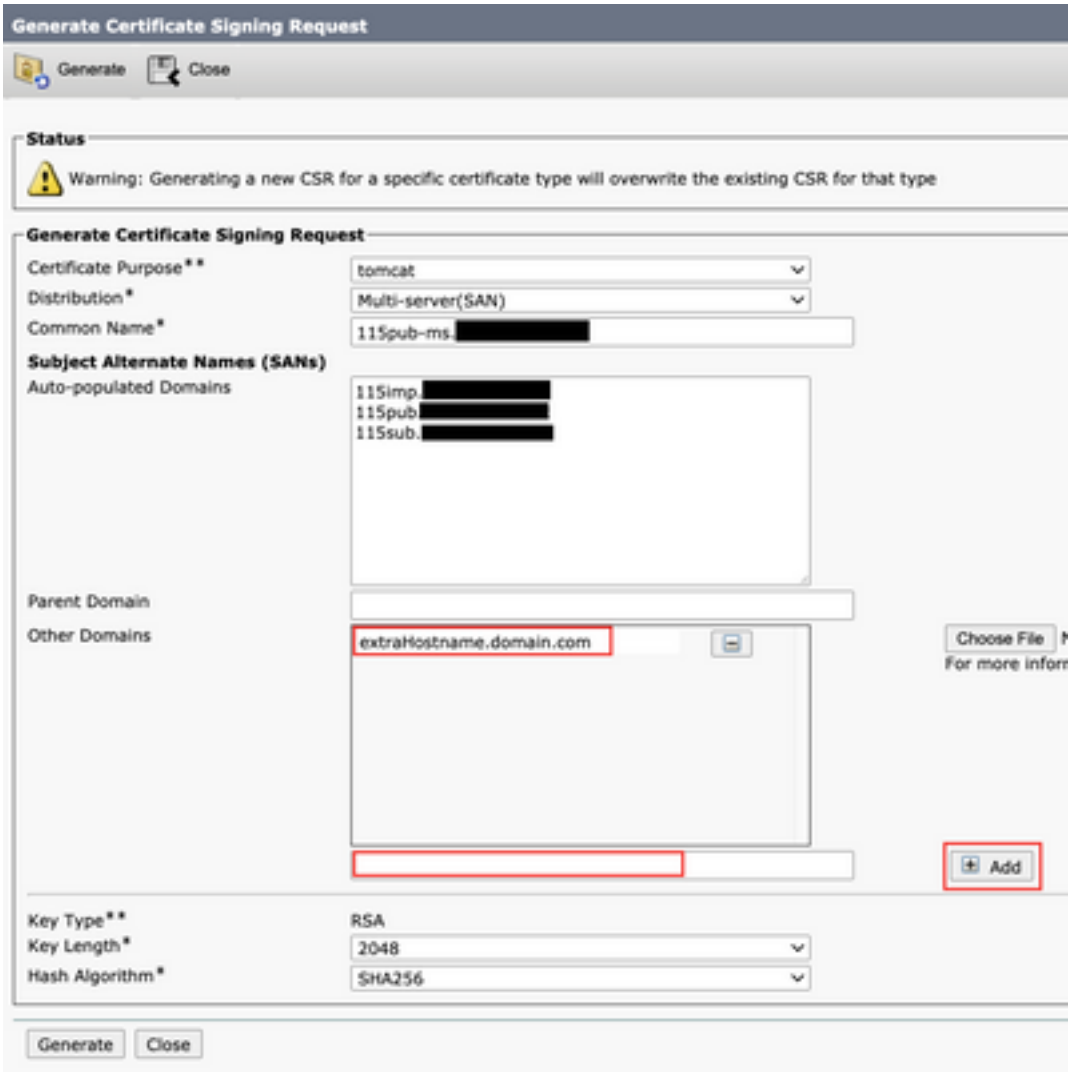
Para modificar la CSR creada por CUCM:

1. Si la CA quita el dominio, se puede crear una CSR en CUCM sin el dominio. Durante la creación de CSR, elimine el dominio que se rellena de forma predeterminada.
2. Si se crea un certificado Multi-SAN, hay algunas CA que no aceptan el "-ms" en el nombre común. El "-ms" se puede quitar del CSR cuando se crea.



3. Para agregar un nombre alternativo aparte de los que CUCM ha completado automáticamente:

    1. Si se utiliza el certificado de varias SAN, se puede agregar más FQDN. (No se aceptan direcciones IP.)



b. Si el certificado es de nodo único, utilice el set web-security comando. Este comando se aplica incluso a los certificados Multi-SAN. (Se puede agregar cualquier tipo de dominio, también se permiten direcciones IP.)

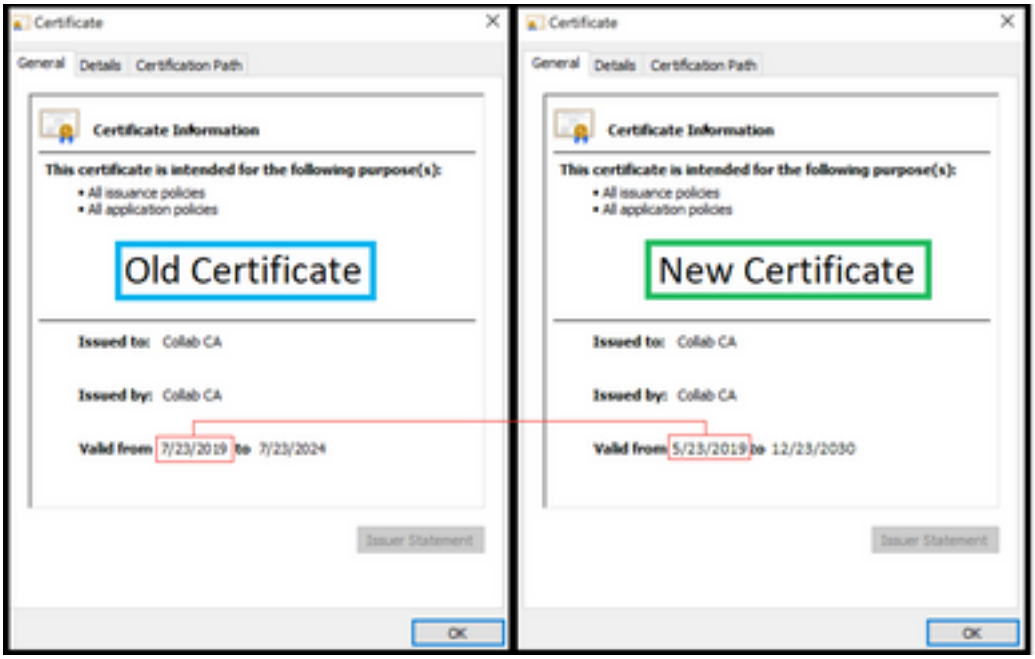
Para obtener más información, vea la Guía de referencia de la línea de comandos.

Los certificados de confianza con el mismo CN no se sustituyen

CUCM se ha diseñado para almacenar sólo un certificado con el mismo nombre común y el mismo tipo de certificado. Esto significa que si un certificado que es tomcat-trust, ya existe en la base de datos y necesita ser reemplazado por uno reciente con el mismo CN, CUCM elimina el certificado antiguo y lo reemplaza por el nuevo.

En algunos casos, CUCM no reemplaza el certificado anterior:

1. El certificado cargado ha caducado: CUCM no permite cargar un certificado caducado.
2. El certificado antiguo tiene una fecha "DESDE" más reciente que el certificado nuevo. CUCM conserva el certificado más reciente y, para tener una fecha "DE" más antigua, lo cataloga como antiguo. Para este escenario, es necesario eliminar el certificado no deseado y luego cargar el nuevo.


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Old Certificate
Issued to: Collab CA
Issued by: Collab CA
Valid from 7/23/2019 to 7/23/2024
Issuer Statement
OK
Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
New Certificate
Issued to: Collab CA
Issued by: Collab CA
Valid from 5/23/2019 to 12/23/2030
Issuer Statement
OK

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).