

Configuración de Tomcat Certificate Reuse para CallManager en CUCM 14

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[1. Establezca el certificado Tomcat como Multi-SAN](#)

[Autofirmado](#)

[Firmado por CA](#)

[2. Reutilice el certificado Tomcat para CallManager](#)

[Verificación](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo reutilizar el certificado Tomcat Multi-SAN para CallManager en un servidor Cisco Unified Communications Manager (CUCM).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- certificados CUCM
- Herramienta de supervisión en tiempo real (RTMT)
- Lista de confianza de identidad (ITL)

Componentes Utilizados

La información de este documento se basa en CUCM 14.0.1.13900-155.

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

Antecedentes

Los dos servicios principales para CUCM son Tomcat y CallManager. En las versiones anteriores, se requerían diferentes certificados para cada servicio para el clúster completo. En la versión 14 de CUCM, también se agregó una nueva función para reutilizar el certificado Tomcat Multi-SAN para el servicio CallManager. Las ventajas de utilizar esta función son:

- Reduce el coste de obtener dos certificados firmados por una autoridad de certificación pública (CA) para un clúster de certificados firmados por CA.
- Esta función reduce el tamaño del archivo ITL y, por lo tanto, la sobrecarga.

 Low Impact  Medium Impact.  High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

Configurar



Precaución: Antes de cargar un certificado Tomcat, compruebe que el inicio de sesión único (SSO) está desactivado. En caso de que esté activado, SSO debe desactivarse y volver a activarse una vez que el proceso de regeneración de certificados de Tomcat haya finalizado.



Low Impact

1. Establezca el certificado Tomcat como Multi-SAN

En CUCM 14, el certificado de Tomcat Multi-SAN puede ser de firma automática o de CA. Si su certificado Tomcat ya es Multi-SAN, omita esta sección.

Autofirmado

Paso 1. Inicie sesión en [Publisher > Operating System \(OS\) Administration](#) y navegue hasta [Security > Certificate Management > Generate Self-Signed](#).

Paso 2. Seleccione Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Se rellenan automáticamente los dominios SAN y el dominio principal.

Generate New Self-signed Certificate

Generate Close

Status

Generating a new certificate will overwrite any existing certificate information. When generating Call Manager, CAPF, or TVS, all devices will be reset automatically.

Generate Self-signed

Certificate Purpose** tomcat

Distribution* Multi-server(SAN)

Common Name* 14pub.

Subject Alternate Names (SANs)

Auto-populated Domains 14pub.
14sub.

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

Validity Period (in years)* 5

Generate Close

i *- Indicates required item.

i **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

Pantalla Generar certificado Tomcat de varias SAN firmado automáticamente

Paso 3. Haga clic en Generate, y valide que todos sus nodos se enumeran bajo el Certificate upload operation successful **mensaje**. Haga clic en Close.

Generate New Self-signed Certificate

Generate Close

Status

i Certificate upload operation successful for the nodes 14sub. ,14pub.

i Restart Cisco Tomcat Service for the nodes 14sub. ,14pub. using the CLI "utils service restart Cisco Tomcat". Restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).

i If SAML SSO is enabled, please disable and re-enable it. Also re-provision the SP metadata on the IDP.

Generar mensaje de Tomcat Multi-SAN autofirmado correcto

Paso 4. Reinicie el servicio Tomcat, abra una sesión CLI en todos los nodos del clúster y ejecute el utils service restart Cisco Tomcat comando.

Paso 5. Desplácese hasta el Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services **y reinicie el** Cisco DRF Master Service **y** Cisco DRF Local Service.

Paso 6. Desplácese hasta cada Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services **y reinicie** Cisco DRF Local Service.

Firmado por CA

Paso 1. Inicie sesión en Publisher > Operating System (OS) Administration **y navegue hasta** Security > Certificate Management > Generate CSR.

Paso 2. Seleccione Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Se rellenan automáticamente los dominios SAN y el dominio principal.

Generate Certificate Signing Request

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose** Distribution* Common Name*

Include OU in CSR

Subject Alternate Names (SANs)

Auto-populated Domains

Parent Domain

Other Domains No file chosen
Please import .TXT file only.

Key Type** RSA
Key Length* 2048
Hash Algorithm* SHA256

 *- indicates required item.

 **When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

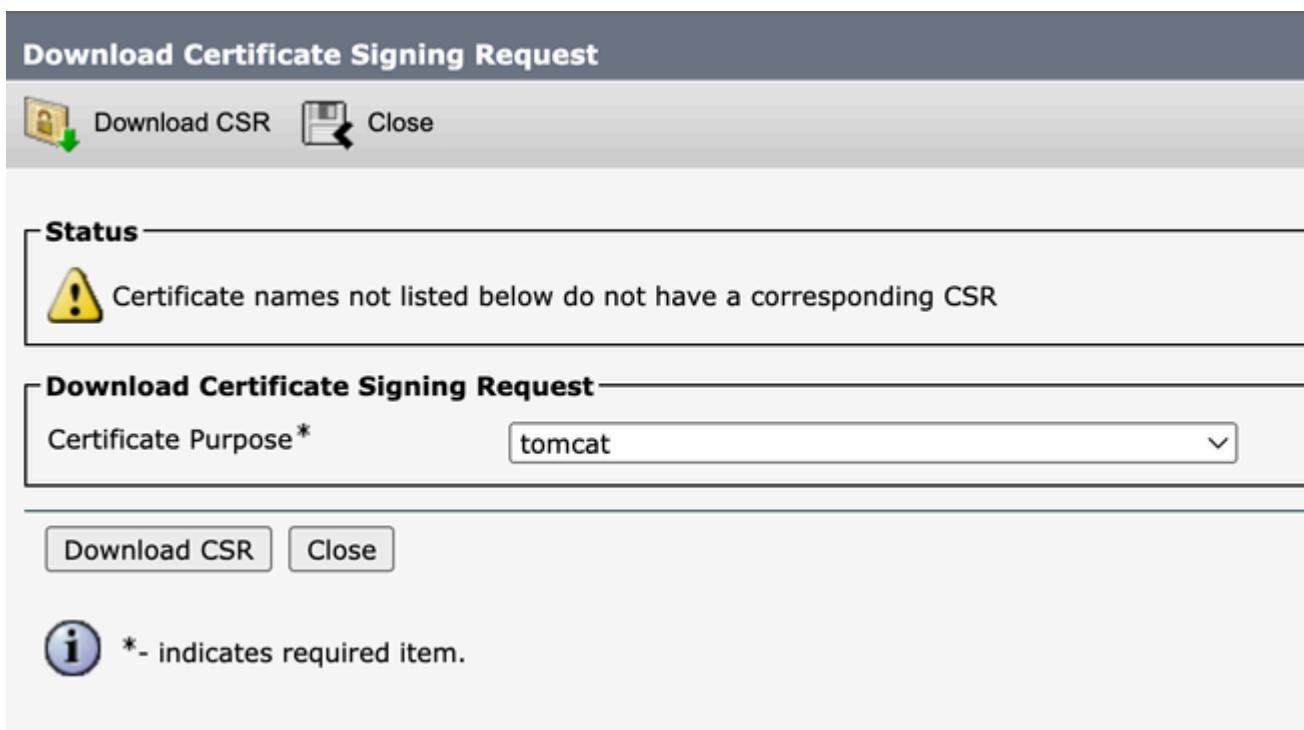
Pantalla Generate Multi-SAN CSR for Tomcat Certificate

Paso 3. Haga clic Generate, y validar todos sus nodos se enumeran bajo el CSR export operation successful mensaje. Haga clic en Close.



Generar mensaje CSR Tomcat correcto de Multi-SAN

Paso 4. Haga clic en Download CSR > Certificate Purpose: tomcat > Download



Descargar la pantalla CSR de Tomcat

Paso 5. Envíe el CSR a la CA para su firma.

Paso 6. Para cargar la cadena de confianza de la CA, navegue por Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Establezca la descripción del certificado y explore los archivos de la cadena de confianza.

Paso 7. Cargue el certificado firmado por la CA y vaya a Certificate Management > Upload certificate > Certificate Purpose: tomcat. Establezca la descripción del certificado y examine el archivo de certificado firmado por la CA.

Paso 8. Reinicie el servicio Tomcat, abra una sesión CLI en todos los nodos del clúster y ejecute el utils service restart Cisco Tomcat comando.

Paso 9. Desplácese hasta el Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services y reinicie

el Cisco DRF Master Service **y** Cisco DRF Local Service.

Paso 10. Desplácese hasta cada uno Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services **y reinicie** Cisco DRF Local Service.

Medium Impact.

2. Reutilice el certificado Tomcat para CallManager



Precaución: Para CUCM 14, se introduce un nuevo parámetro Phone Interaction on Certificate Update empresarial. Utilice este campo para restablecer los teléfonos de forma manual o automática según corresponda cuando se actualice uno de los certificados TVS, CAPF o TFTP (CallManager/ITLRecovery). Este parámetro se establece de forma predeterminada en reset the phones automatically. Después de la regeneración, eliminación y actualización de certificados, asegúrese de reiniciar los servicios adecuados.

Es necesario reiniciar los servicios para una regeneración de certificado de CallManager normal. Marque [Regenerar Certificados En Unified Communications Manager](#).

Paso 1. Vaya al editor de CUCM y, a continuación, a Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Haga clic en Reuse Certificate

Paso 3. En la lista choose Tomcat type desplegable, seleccione tomcat.

Paso 4. Desde el Replace Certificate for the following purpose panel, marque la casilla de verificación.

The screenshot shows a dialog box titled "Use Tomcat Certificate For Other Services".

Status:

- ⚠️ Tomcat-ECDSA Certificate is Not Multi-Server Certificate
- ℹ️ Tomcat Certificate is Multi-Server Certificate

Source:

Choose Tomcat Type* tomcat

Replace Certificate for the following purpose:

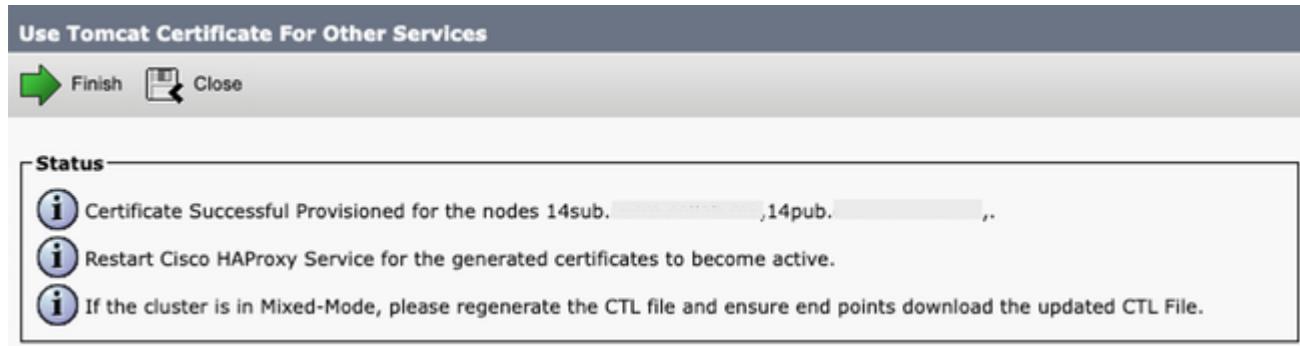
CallManager
 CallManager-ECDSA

Finish Close



Nota: Si elige Tomcat como tipo de certificado, CallManager se habilita como reemplazo. Si elige tomcat-ECDSA como tipo de certificado, CallManager-ECDSA se habilita como reemplazo.

Paso 5. Haga clic **Finish** para reemplazar el certificado de CallManager con el certificado de Tomcat Multi-SAN.



Mensaje de reutilización correcta del certificado Tomcat

Paso 6. Reinicie el servicio Cisco HAProxy, abra una sesión CLI en todos los nodos del clúster y ejecute el `utils service restart Cisco HAProxy` comando.



Nota: Para determinar si el clúster está en modo mixto, navegue hasta Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == No seguro; 1 == Mixed Mode [Modo mixto]).

Paso 7. Si el clúster está en modo mixto, abra una sesión CLI en el nodo del editor, ejecute el `utils ctl update CTLFile` comando y restablezca todos los teléfonos del clúster para que se apliquen las actualizaciones del archivo CTL.

Verificación

Paso 1. Vaya al editor de CUCM y, a continuación, a Cisco Unified OS Administration > Security > Certificate Management.

Paso 2. Filtre por `Find Certificate List where: Usage > begins with: identity` y haga clic en **Find**.

Paso 3. Los certificados de CallManager y Tomcat deben terminar con el mismo `Common Name_Serial Number` valor.

Certificate List

 Generate Self-signed  Upload Certificate/Certificate chain  Generate CSR  Reuse Certificate

Status

 8 records found

Certificate List (1 - 8 of 8)								Rows per Page	50
Find Certificate List where		Usage	Type	Key Type	Distribution	Issued By	Expiration	Description	
		Usage	Type	Key Type	Distribution	Issued By	Expiration	Description	
Certificate	Common Name/Common Name_SerialNumber	Usage	Type	Key Type	Distribution	Issued By	Expiration	Description	
CallManager	14pub..45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Reusing tomcat certificate for CallManager	
CallManager-ECDSA	14pub-EC..56a32bfe30d2996d5c5851a8b7e5731f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system	
CAPF	CAPF-02a10666	Identity	Self-signed	RSA	14pub.cucm.collab.mx	CAPF-02a10666	12/20/2027	Self-signed certificate generated by system	
ipsec	14pub..6f44af5c5cd753d5ffff1538c3879b44	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system	
ITLRecovery	ITLRECOVERY_14pub..727029ee3d929d999ca9bee38720c89e	Identity	Self-signed	RSA	14pub.cucm.collab.mx	ITLRECOVERY_14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system	
tomcat	14pub..45cdf84f42748393feacd6f39c0af1fd	Identity	Self-signed	RSA	Multi-server(SAN)	14pub.cucm.collab.mx	09/25/2028	Multi-server self-signed certificate for tomcat	
tomcat-ECDSA	14pub-EC..6ea1f2fedf8f6183cd6f2994a0f0447f	Identity	Self-signed	EC	14pub.cucm.collab.mx	14pub-EC.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system	
TVS	14pub..768022f66eb2885c34068b7c64126046	Identity	Self-signed	RSA	14pub.cucm.collab.mx	14pub.cucm.collab.mx	05/02/2026	Self-signed certificate generated by system	

 Generate Self-signed  Upload Certificate/Certificate chain  Generate CSR  Reuse Certificate

Verificar reutilización de certificado Tomcat para CallManager



Nota: A partir de SU4, con la reutilización de certificados habilitada, el certificado de Call Manager no se muestra en la GUI, mientras que ambos certificados están visibles en SU2 y SU3.

Información Relacionada

- [Guía de seguridad de Cisco Unified Communications Manager 14](#)
- [Soporte técnico y descargas de Cisco](#)

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).