

Configuración del clúster de Unified Communication

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

[Certificado SAN para varios servidores de CallManager](#)

[Troubleshoot](#)

[Advertencias conocidas](#)

Introducción

Este documento describe cómo configurar un clúster de Unified Communication con el uso de certificados SAN multiservidor firmados por la autoridad certificadora (CA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Communications Manager (CUCM)
- CUCM IM and Presence versión 10.5

Antes de intentar realizar esta configuración, asegúrese de que estos servicios estén operativos:

- Servicio web de administración de plataformas de Cisco
- Servicio Tomcat de Cisco

Para verificar estos servicios en una interfaz web, navegue hasta **Servicios de página de Serviciabilidad de Cisco Unified > Servicio de red > Seleccionar un servidor**. Para verificarlos en la CLI, ingrese el comando **utils service list**.

Si SSO está activado en el clúster de CUCM, es necesario desactivarlo y volver a activarlo.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

En CUCM versión 10.5 y posteriores, esta solicitud de firma de certificado (CSR) de almacén de confianza puede incluir el nombre alternativo del sujeto (SAN) y dominios alternativos.

1. Tomcat: CUCM e IM&P
2. Cisco CallManager - Solo CUCM
3. Cisco Unified Presence-Extensible Messaging and Presence Protocol (CUP-XMPP) - Solo IM&P
4. CUP-XMPP Server-to-Server (S2S) - Solo IM&P



Es más sencillo obtener un certificado firmado por una CA en esta versión. Solo se requiere que una CSR esté firmada por CA en lugar de la obligación de obtener una CSR de cada nodo de servidor y, a continuación, obtener un certificado firmado por CA para cada CSR y administrarlos individualmente.

Configurar

Paso 1.

Inicie sesión en Administración del sistema operativo (SO) de Publisher y navegue hasta **Seguridad > Administración de certificados > Generar CSR**.

Generate Certificate Signing Request

 Generate  Close

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*	tomcat
Distribution*	cs-ccm-pub.v[redacted].com
Common Name*	cs-ccm-pub.v[redacted].com Multi-server(SAN)
Subject Alternate Names (SANs)	
Parent Domain	[redacted].com
<hr/>	
Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close





*- indicates required item.

Paso 2.

Elija Multi-Server SAN en Distribution.

Generate Certificate Signing Request

 Generate  Close

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*	tomcat
Distribution*	cs-ccm-pub.v[redacted].com
Common Name*	cs-ccm-pub.v[redacted].com Multi-server(SAN)
Subject Alternate Names (SANs)	
Parent Domain	[redacted].com
<hr/>	
Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close



*- indicates required item.


Rellena automáticamente los dominios SAN y el dominio principal.

Verifique que todos los nodos de su clúster estén listados para Tomcat: todos los nodos de CUCM e IM&P b para CallManager: solo los nodos de CUCM están listados.

Generate Certificate Signing Request

Generate Close

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* tomcat

Distribution* Multi-server(SAN)

Common Name* cs-ccm-pub. .com-ms

Subject Alternate Names (SANs)

Auto-populated Domains

- cs-ccm-pub. .com
- cs-ccm-sub. .com
- cs-imp. .com


Parent Domain .com

Other Domains

No file selected.
Please import .TXT file only.
For more information please refer to the notes in the Help Section

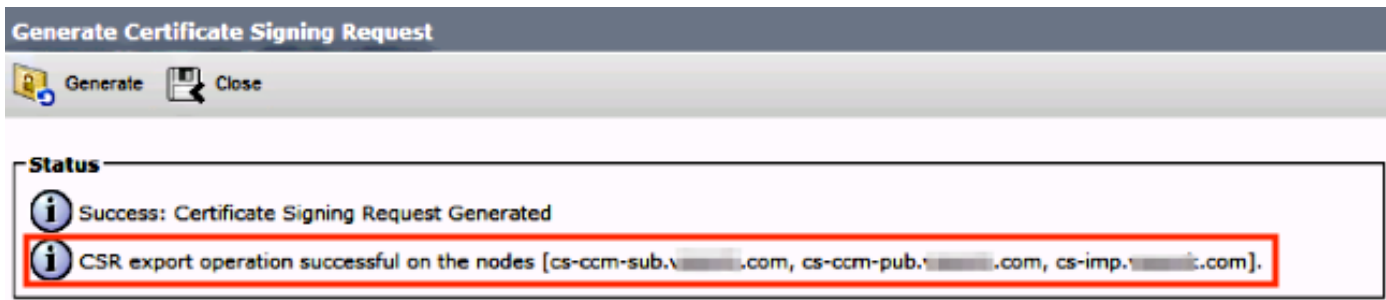
Key Length* 2048

Hash Algorithm* SHA256

 *- indicates required item.

Paso 3.

Haga clic en generar y, una vez que se genere el CSR, compruebe que todos los nodos enumerados en el CSR también se muestran en la lista de CSR exportados correctos.

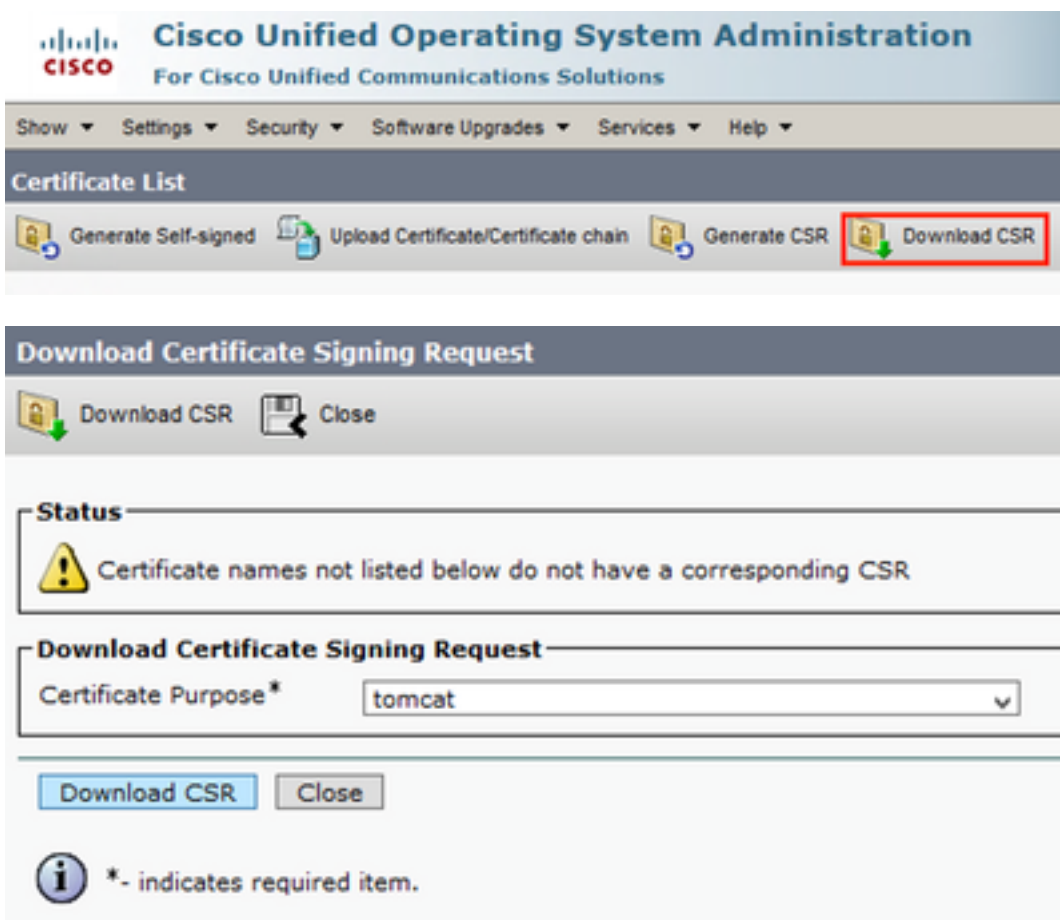


En la Administración de certificados, se genera la solicitud SAN:

Certificate ^	Common Name	Type	Key Type	Distribution	Issued By
tomcat	115pub-ms.	CSR Only	RSA	Multi-server(SAN)	--
tomcat	115pub-ms.	CA-signed	RSA	Multi-server(SAN)

Paso 4.

Haga clic en **Download CSR** y luego elija el propósito del certificado y haga clic en **Download CSR**.



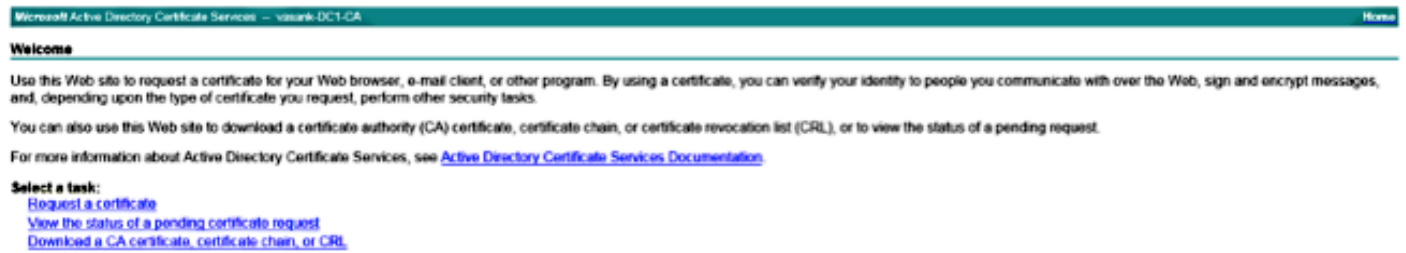
Es posible utilizar la CA local o una CA externa como VeriSign para obtener la CSR (archivo descargado en el paso anterior) firmada.

Este ejemplo muestra los pasos de configuración para una CA basada en Microsoft Windows Server. Si utiliza una CA diferente o una CA externa, vaya al paso 5.

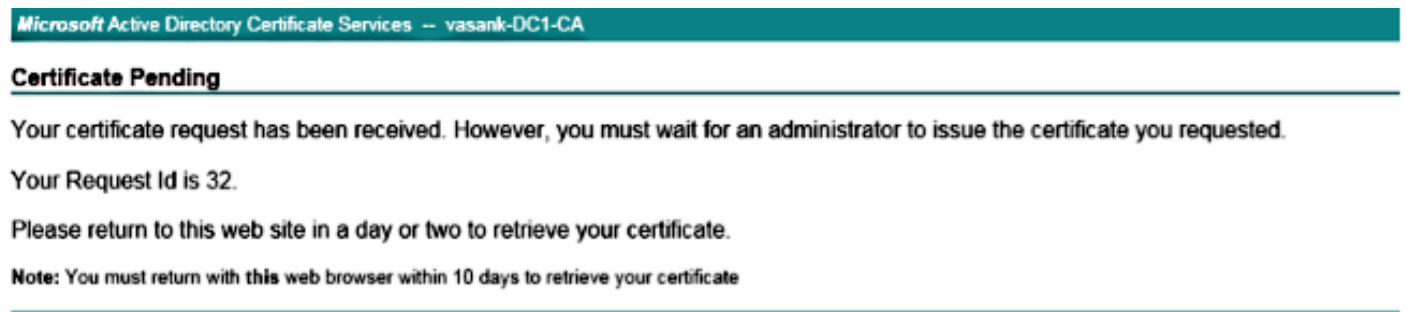
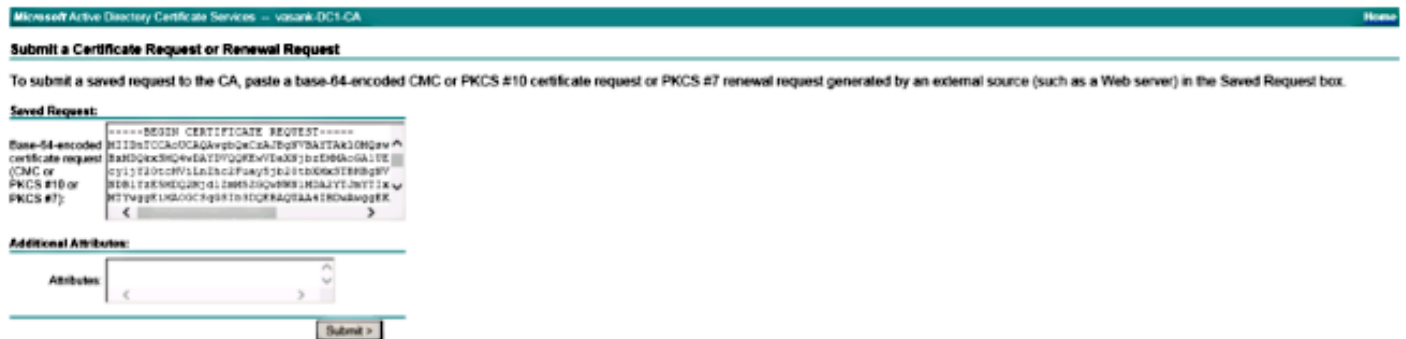
Inicie sesión en <https://<windowsserveripaddress>/certsrv/>

Elija **Solicitar un certificado > Solicitud de certificado avanzada**.

Copie el contenido del archivo CSR en el campo de solicitud de certificado codificado en Base-64 y haga clic en **Enviar**.




Envíe la solicitud de CSR tal y como se muestra aquí.



Paso 5.





Nota: Antes de cargar un certificado Tomcat, verifique que SSO esté inhabilitado. En caso de que esté activado, SSO debe desactivarse y volver a activarse una vez finalizado todo el proceso de regeneración de certificados de Tomcat.

Con el certificado firmado, cargue los certificados de CA como tomcat-trust. Primero el certificado raíz y luego el certificado intermedio si existe.



 **Cisco Unified Operating System Administration**
For Cisco Unified Communications Solutions

Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾


Certificate List

 Generate Self-signed  **Upload Certificate/Certificate chain**  Generate CSR  Download CSR

Upload Certificate/Certificate chain

 Upload  Close

Status

 Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* ▾



Description(friendly name)

Upload File certchain.p7b



Paso 6.

Ahora cargue el certificado firmado de CUCM como Tomcat y verifique que todos los nodos de su clúster aparezcan en la lista "Operación de carga de certificados correcta", como se muestra en la imagen:

Upload Certificate/Certificate chain

 Upload  Close

Status


-  Certificate upload operation successful for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com.
-  Restart Cisco Tomcat Service for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com using the CLI "utils service restart Cisco Tomcat".

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File No file selected.

 *- indicates required item.

La SAN multiservidor aparece en Administración de certificados como se muestra en la imagen:

ipsecc-trust	cs-ccm-pub.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY.cs-ccm-pub.vasank.com	Self-signed	ITLRECOVERY.cs-ccm-pub.com	ITLRECOVERY.cs-ccm-pub.com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.com.ms	CA-signed	Multi-server(SAN)DC1-CA	12/19/2015	Certificate Signed byDC1-CA
tomcat-trust	cs-ccm-pub.com.ms	CA-signed	Multi-server(SAN)DC1-CA	12/19/2015	Trust Certificate
tomcat-trust	cs-ccm-pub.com	Self-signed	gs-ccm-pub.com	gs-ccm-pub.com	04/21/2019	Trust Certificate
tomcat-trust	VerSign_Class_3_Secure_Server_CA_-_G3	CA-signed	VerSign_Class_3_Secure_Server_CA_-_G3	VerSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dc1-ccm-pub.com	Self-signed	dc1-ccm-pub.com	dc1-ccm-pub.com	04/17/2019	Trust Certificate
tomcat-trust	dc1-ccm-pub.com	Self-signed	dc1-ccm-pub.com	dc1-ccm-pub.com	04/18/2019	Trust Certificate
tomcat-trustDC1-CA	Self-signedDC1-CADC1-CA	04/29/2004	Root CA
TVS	gs-ccm-pub.vasank.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/18/2019	Self-signed certificate generated by system

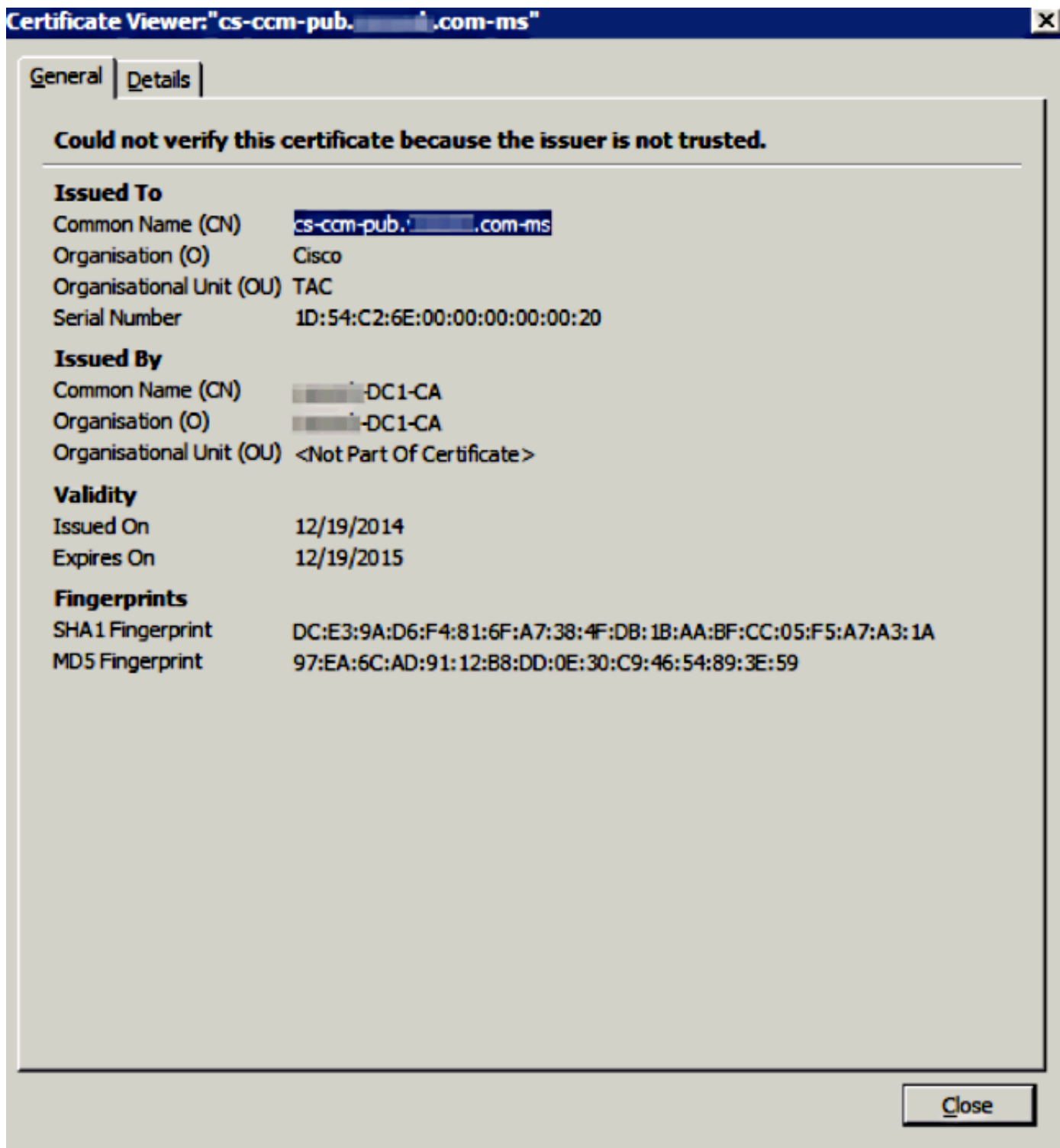
Paso 7.

Reinicie el servicio Tomcat en todos los nodos de la lista SAN (primero en el editor y luego en los suscriptores) a través de CLI con el comando: **utils service restart Cisco Tomcat**.

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

Verificación

Inicie sesión en <http://<fqdnofccm>:8443/ccmadmin> para asegurarse de que se utiliza el nuevo certificado.



Certificado SAN para varios servidores de CallManager

Se puede seguir un procedimiento similar para el certificado de CallManager. En este caso, los dominios que se rellenan automáticamente son solo nodos de CallManager. Si el servicio Cisco CallManager no se está ejecutando, puede optar por mantenerlo en la lista SAN o eliminarlo.

Advertencia: este proceso afecta al registro del teléfono y al procesamiento de llamadas. Asegúrese de programar una ventana de mantenimiento para cualquier trabajo con certificados CUCM/TVS/ITL/CAPF.

Antes del certificado SAN firmado por la CA para CUCM, asegúrese de que:

- El teléfono IP puede confiar en el servicio de verificación de confianza (TVS). Esto se puede verificar con el acceso a cualquier servicio HTTPS desde el teléfono. Por ejemplo, si el acceso al directorio corporativo funciona, significa que el teléfono confía en el servicio TVS.
- Compruebe si el clúster está en modo no seguro o mixto.

Para determinar si se trata de un clúster de modo mixto, elija **Administración de Cisco Unified CM > Sistema > Parámetros empresariales > Modo de seguridad de clúster (0 == No seguro; 1 == Modo mixto)**.

Advertencia: Si se encuentra en un clúster de modo mixto antes de que se reinicien los servicios, se debe actualizar la CTL: [Token](#) o [Tokenless](#).

Después de instalar el certificado emitido por CA, la siguiente lista de servicios debe reiniciarse en los nodos habilitados:

- Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones > TFTP de Cisco
- Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones > Cisco CallManager
- Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones > Cisco CTIManager
- Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red > Servicio Cisco Trust Verification

Troubleshoot

Estos registros pueden ayudar a Cisco Technical Assistance Center a identificar cualquier problema relacionado con la generación CSR de SAN multiservidor y la carga del certificado firmado por CA.

- API de plataforma de Cisco Unified OS
- Tomcat de Cisco
- Registros de IPT Platform CertMgr
- [Proceso de renovación de certificados](#)

Advertencias conocidas

- Id. de error de Cisco [CSCur97909](#): la carga de un certificado multiservidor no elimina los certificados autofirmados en la base de datos
- Id. de error de Cisco [CSCus47235](#): CUCM 10.5.2 no se puede duplicar en SAN para CSR
- Id. de error de Cisco [CSCup28852](#): restablecimiento del teléfono cada 7 minutos debido a la actualización del certificado cuando se utiliza el certificado de varios servidores

Si existe un certificado multiservidor existente, se recomienda la regeneración en estos escenarios:

- Cambio de nombre de host o dominio. Cuando se realiza un cambio de nombre de host o de

dominio, los certificados se vuelven a generar automáticamente como autofirmados. Para cambiarlo a CA-Signed, se deben seguir los pasos anteriores.

- Si se agregó un nuevo nodo al clúster, se debe generar un nuevo CSR para incluir el nuevo nodo.
- Cuando se restaura un suscriptor y no se ha utilizado ninguna copia de seguridad, el nodo puede tener nuevos certificados autofirmados. Se puede requerir una nueva CSR para todo el clúster para incluir el suscriptor. (Hay una solicitud de mejoraID de bug de Cisco [CSCuv75957](#) para agregar esta función.)

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).