

# Resolución de problemas comunes con la renovación de certificados en CUCM

## Introducción

Este documento describe problemas comunes después de regenerar certificados en Cisco Unified Communications Manager (CUCM) y cómo resolverlos.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Proceso de renovación de certificados de CUCM
- Interfaz GUI de CUCM
- servidores de Expressway
- Registro de dispositivos con el proceso de CUCM
- Función de proxy de autoridad de certificados
- Guía de seguridad para Cisco Unified Communications Manager

## Componentes Utilizados

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







- CUCM versión 15

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.

## Impacto empresarial

Esta tabla muestra el impacto empresarial de cada renovación de certificado en su operación. Revise la información atentamente. Renueve los certificados requeridos después de horas o en períodos de tranquilidad, en función del nivel de riesgo de cada certificado.

 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	

## Escenario 1: Los teléfonos no se registran después de la renovación de certificados de Call Manager, TVS e ITL



Nota: Esta situación se aplica a las implementaciones en clústeres de modo mixto y no seguro de CUCM, además, se aplica a los certificados autofirmados y a los certificados de CA.

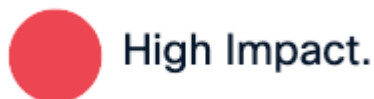
Cuando los certificados de Call Manager , TVS e ITL caducaron y se renovaron al mismo tiempo, hace que todos nuestros teléfonos estén en un estado no registrado que causa un impacto importante en el sistema, se trata de un comportamiento esperado ya que activamos que los teléfonos no confíen en CUCM.

## Verificación

1. Asegúrese de que los certificados ya han caducado en Administración de Cisco Unified OS >Seguridad > Administración de certificados



Este paso afecta a todos los teléfonos, incluidos los registrados. Asegúrese de realizar este paso fuera del horario laboral.



---

## Situación 2: el inicio de sesión único no funciona después de la renovación del certificado de Tomcat

---



Nota: Este escenario se puede aplicar a implementaciones que utilizan un acuerdo de todo el clúster o por nodo para la configuración de inicio de sesión único

---

Inicio de sesión en CUCM con inicio de sesión único (SSO): muestra un mensaje de error "Error al procesar la respuesta pequeña" o "Error al procesar la respuesta pequeña Error al descifrar la clave secreta"

### Verificación

1. Asegúrese de que todos los nodos contengan un certificado tomcat válido si se firmaron automáticamente o si contienen el nuevo certificado tomcat multi-san asociado.
2. Utilice `set samltrace level debug` en todos los nodos de CUCM a través de CLI para activar los registros de SSO en el nivel de depuración
3. Vuelva a crear el problema iniciando sesión en CUCM y utilice el método SSO.
4. Recopile los registros SSO de Tomcat después del incidente y verifique que recibe este mensaje:

- ```
2026-01-10 06:06:31,274 ERROR [http-nio-81-exec-157]  cpi.sso.saml.sp.security.authentication
com.sun.identity.saml2.common.SAML2Exception: Failed to decrypt the secret key.
    at com.sun.identity.saml2.xmlenc.FMEncProvider.getEncryptionKey(FMEncProvider.
    at com.sun.identity.saml2.xmlenc.FMEncProvider.decrypt(FMEncProvider.java:607)
    at com.sun.identity.saml2.assertion.impl.EncryptedAssertionImpl.decrypt(Encryp
...

```

### Solución

Exportación de metadatos de CUCM después de la renovación del certificado de Tomcat e importación al servidor del proveedor de identidad para asegurarse de que tienen el nuevo certificado de Tomcat para esta comunicación.

Procedimiento para renovar tomcat con la implementación de SSO habilitada:



Precaución: El Centro de Asistencia Técnica (TAC) recomienda los siguientes pasos para evitar cualquier problema después de la renovación del certificado de Tomcat, recomiendan realizar este procedimiento después de las horas.

---

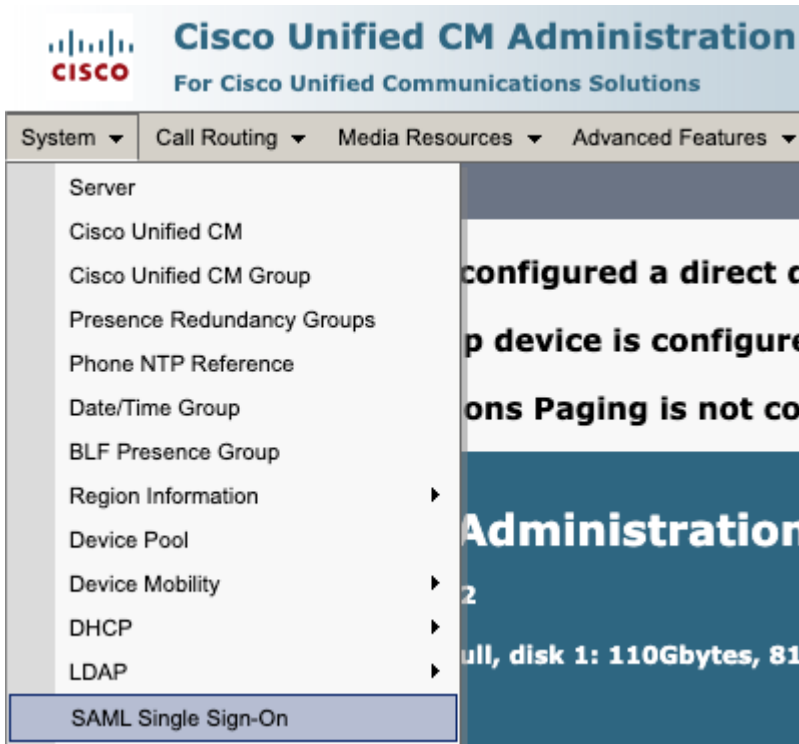


Low Impact

#### 1. Inhabilite SSO en todos los nodos de CUCM



- Acceso a CM administration > System > SAML Single Sign-on



- Seleccione Disable SAML SSO



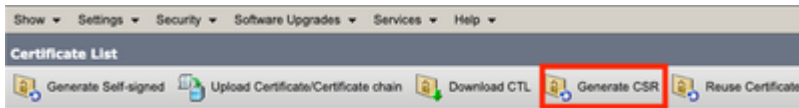
- Este proceso debe realizarse en el resto de los nodos mediante la GUI si se utiliza el acuerdo por nodo.

## 2. Renueve el certificado Tomcat en el clúster de CUCM

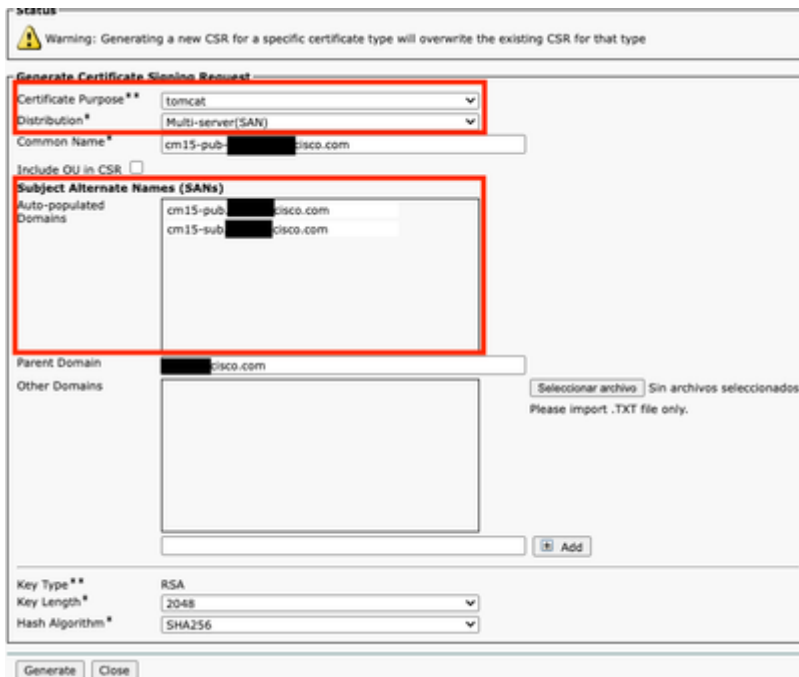


Procedimiento general para renovar el certificado de varias san de Tomcat en un clúster de CUCM:

- Vaya a Administración del SO > Seguridad > Administración de certificados.
- Seleccione Generar CSR.



- Seleccione Tomcat en Propósito de certificado.
- Seleccione Multi-SAN en Distribution.
- Asegúrese de que todos los nodos del clúster aparezcan en Dominios que se rellenan automáticamente.



- Seleccione Generar. Asegúrese de que se ha creado CSR en todos los nodos del clúster.
- Descargue el CSR generado del editor de CUCM y fírmelo con un servidor de la autoridad certificadora (CA).
- Vaya a Administración del SO > Seguridad > Administración de certificados. Seleccione Cargar certificado/cadena de certificado.
- Cargue certificados de CA como Tomcat-trust.
- Repita el paso 6 y ahora cargue el certificado firmado de Tomcat como Tomcat.
- Una vez completado y verificado que todos los nodos tienen el nuevo certificado de Tomcat aplicado, reinicie el servicio Tomcat a través de CLI en todos los nodos del clúster con este comando `utils service restart Cisco Tomcat`.

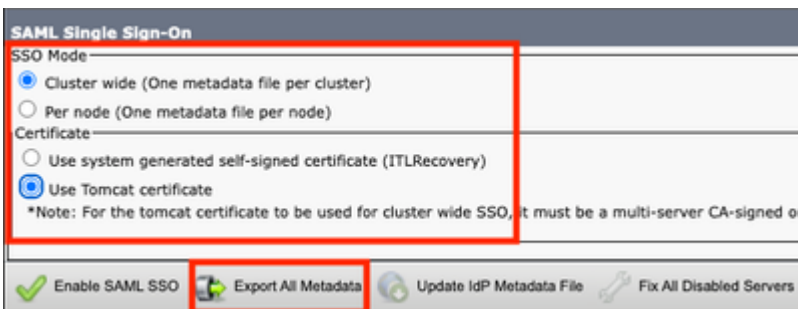
Para obtener más información, consulte esta documentación:

- [Regenere el certificado autofirmado de Tomcat](#)
- [Regenere el certificado firmado por CA de Tomcat.](#)

### 3. Metadatos del proveedor de servicios de exportación (SP)



- Vaya a Administración de CM > Sistema > Inicio de sesión único
- Configure las opciones de SSO (en este caso, en todo el clúster en el modo SSO y Use tomcat certificate en el certificado está configurado como ejemplo) y luego seleccione export all metadata .

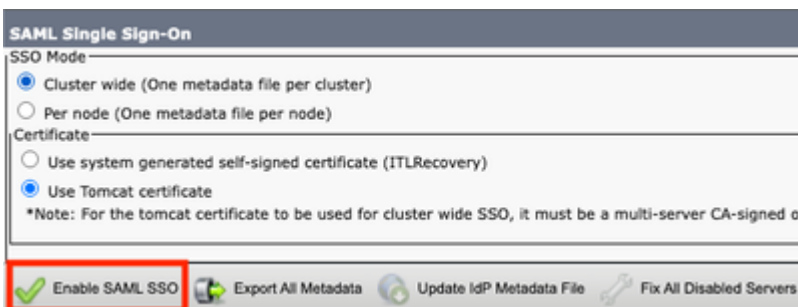



- Importar metadatos SP al servidor del proveedor de identidad (IdP). Para obtener más información, consulte [Configuración de SSO SAML en el Proveedor de Identidad](#)

### 4. Activar SSO en clúster de CUCM




- Vaya a Administración de CM > Sistema > Inicio de sesión único
- Con las mismas opciones de SSO seleccionadas mientras se exportan los metadatos de CUCM, seleccione Enable SAML SSO y continúe.



 Web server connections will be restarted


Enabling SSO and importing the metadata will cause web services to restart upon completion of the wizard. All affected web applications will drop their connection momentarily and need to be logged into again.

 Click "Export All Metadata" button


If the server metadata has not already been uploaded to the IdP, it can be done before running the wizard. You can obtain the server metadata by clicking the "Export All Metadata" button on the main page. Then go to the IdP and upload the file.  
If IDP is provisioned with cluster-wide SP metadata, you need to enable cluster-wide SAML SSO. If IDP is provisioned with per-node SP metadata, you need to enable per-node SAML SSO.

- Si se aplica a todo el clúster, este paso está disponible para comprobar el certificado multi-servidor en todos los nodos, seleccione Test for multi-server tomcat certificate. una vez finalizado, seleccione Next (Siguiente).

**SAML Single Sign-On Configuration**

 Next

**Status**

 Status: Ready

**Test for Multi-Server tomcat certificate**

The criteria for enabling clusterwide SSO is that you must have a multiserver tomcat certificate already deployed. If you have not done this already please follow the below steps:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate CSR
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Download the CSR and get it signed from the CA of your choice
- 7) Once the certificate is issued by the CA, upload it via the "Upload Certificate/ Certificate chain" option on the Certificate Management page
- 8) Restart Tomcat service on all the nodes in the cluster
- 9) Restart TFTP service on all the TFTP nodes in the cluster

For self-signed Multi-server tomcat certificate:

- 1) Login to Cisco Unified OS Administration Page and Navigate to Certificate Management under Security Menu
- 2) Click on Generate self signed Multi-server tomcat certificate
- 3) Select Certificate Purpose as Tomcat
- 4) Select Distribution as "Multi-Server"
- 5) Click Generate
- 6) Restart Tomcat service on all the nodes in the cluster
- 7) Restart TFTP service on all the TFTP nodes in the cluster

If the above steps have been completed, click Test below which will confirm if the multi-server tomcat certificate is deployed before proceeding to the next stage

- Cargar metadatos IdP, seleccionar Importar metadatos IdP y una vez finalizado, seleccionar Siguiente

**SAML Single Sign-On Configuration**

Next

**Status**

 Status: Ready

 Import succeeded for all servers

**Import the IdP Metadata Trust File**

This step uploads the file acquired from the IdP in the previous manual step to the Collaboration servers.

1) Select the IdP Metadata Trust File

 No file chosen

2) Import this file to the Collaboration servers

This action must be successful for at least the Publisher before moving on to the next task in this wizard.

  Import succeeded for all servers


 

- En Probar configuración de SSO, seleccione un usuario con el grupo Superusuarios de CCM estándar asignado y seleccione Ejecutar prueba de SSO hasta obtener el éxito.

**SAML Single Sign-On Configuration**

Back

**Status**


 The server metadata file must be installed on the IdP before this test is run.

**Test SSO Setup**

This test verifies that the metadata files are correctly configured and will allow SSO to start up on the servers. This test can be run on any

1) Pick a valid username to use for this test

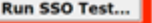
You must already know the password for the selected username.  
This user must have administrator rights and also exist in the IdP.



 Please use one of the Usernames shown below. Using any other Username to log into the IdP may result in administrator lockout.

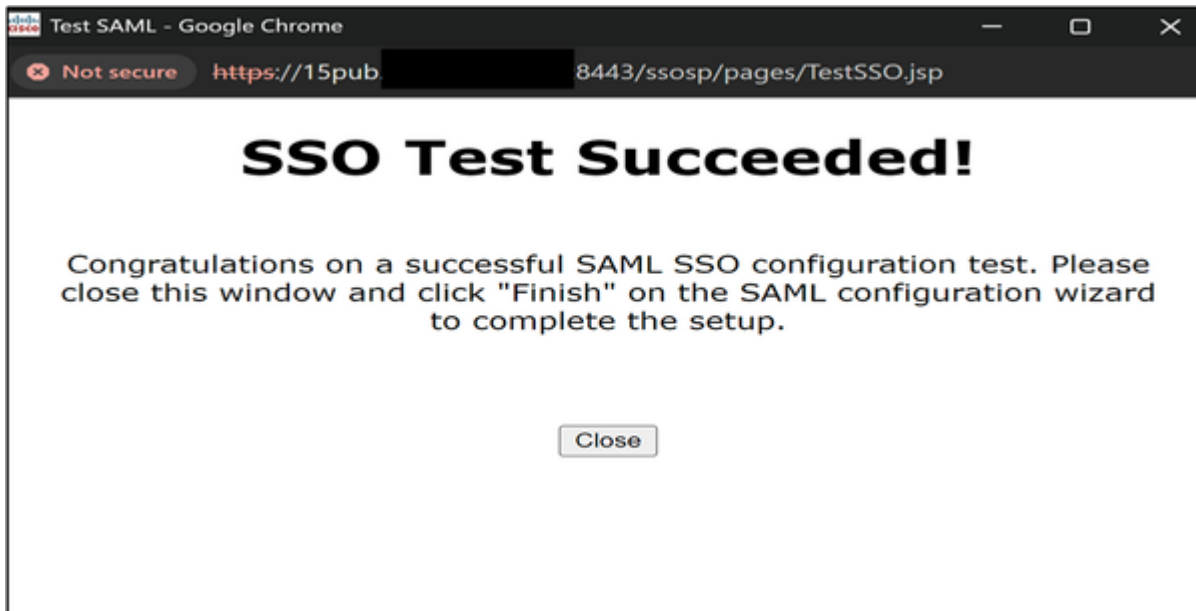
Valid administrator Usernames

admin@ [redacted]

2) Launch SSO test page



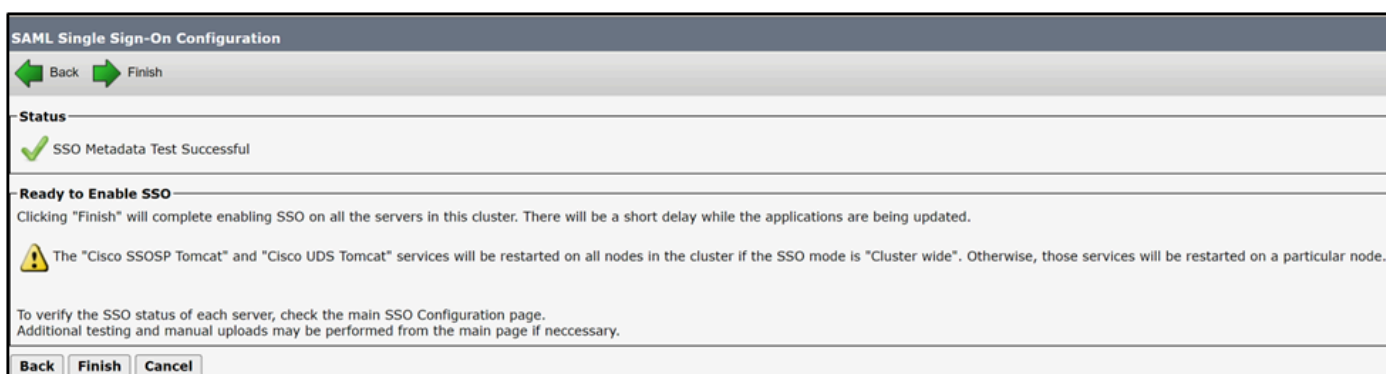
 



4. Reinicie los servicios necesarios después de activar SSO.



- La habilitación de SSO reinicia el servicio tomcat.



Sin embargo, TAC recomienda reiniciar el servicio Tomcat (`utils service restart Cisco Tomcat`) y el servicio UDS Tomcat (`utils service restart CiscoUDSTomcat`) manualmente en todos los nodos después del proceso de habilitación de SSO.

---

## Escenario 3: Problemas de registro de Mobility and Remote Access después de la renovación del certificado

La aplicación Webex no se puede registrar con CUCM a través de Mobility and Remote Access (MRA) después de que Call Manager, Tomcat y los certificados de Expressway C se renueven en implementaciones de modo mixto.

## Verificación

1. CUCM Call Manager y el certificado Tomcat son certificados firmados por CA.
2. La implementación de CUCM y Expressway se ejecuta en modo mixto (TLS).
3. Inspeccionar registros de Expressway-C muestra "rutinas SSL:ssl3\_read\_bytes:tlsv1 alert unknown ca".

<#root>

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]: UTCTime="2026-01-29 19:01:16,974" ModuTe
HTTPMSG:
```

```
|GET /CSFmarcoalh.cnf.xml HTTP/1.1
```

```
Host: expc.cisco.com:6972
```

```
Accept: */*
```

```
Cookie: <CONCEALED>
```

```
User-Agent: WebEx/0.0.0.0
```

```
TrackingID: fxxxxxxx-86f6-4030-8259-0b768c07723e
```

```
Client-ip: xxx.xxx.xxx.xxx
```

```
X-Forwarded-For: xxx.xxx.xxx.xxx, 127.0.0.1
```

```
Via: https/1.1 vcs[0fxxxxxx-c853-xxxx-aa16-0a290bf56fc8] (ATS), http/1.1 vcs[5xxxxxxx-7feb-4xxx-9
```

|

```
2026-01-29T14:01:16.974-05:00 exp-c traffic_server[2030]:[ET_NET 1]ERROR:SSL connection failed for
```

```
SSL routines:ssl3_read_bytes:tlsv1 alert unknown ca
```

## Solución

Exportar e importar certificados entre CUCM y Expressway-C para garantizar la relación de confianza.



Precaución: El TAC recomienda realizar esta operación fuera del horario laboral, ya que este procedimiento requiere el reinicio de los servicios. El impacto empresarial es



**Medium Impact.**

1. Procedimiento para completar la relación de confianza entre CUCM y Expressway con certificados firmados por CA



Navegue hasta Administración del SO > Seguridad > Administración de certificados y descargue el certificado de CA raíz y el intermedio (si lo hubiera) que firma el Call Manager y el certificado Tomcat.

**Certificate List**

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

Status  
18 records found

**Certificate List (1 - 18 of 18)** Rows per Page

Find Certificate List where Certificate begins with callmanager Find Clear Filter

| Certificate           | Common Name/Common Name_SerialNumber                             | Usage    | Type            | Key Type | Distribution      | Issued By |
|-----------------------|------------------------------------------------------------------|----------|-----------------|----------|-------------------|-----------|
| CallManager           | cuem15sub-<br>2766.local: 6f0000000c374e76d635a3840d00000000000c | Identity | CA-<br>signed   | RSA      | Multi-server(SAN) | 2766-ca-1 |
| CallManager-<br>ECDSA |                                                                  |          |                 |          |                   |           |
| CallManager-<br>trust | 2766-ca-<br>1_642238c85deb1c8b48ad6e45d0ab241c                   | Trust    | Self-<br>signed | RSA      | 2766-ca-1         | 2766-ca-1 |

A continuación, navegue hasta Expressway-C > Mantenimiento > Seguridad > Certificado de CA de confianza y cargue el certificado de CA de Call Manager y el certificado Tomcat.

**Maintenance**

- Upgrade
- Logging
- Smart licensing
- Email Notifications
- Tools >
- Security**
  - Trusted CA certificate
  - Server certificate
  - CRL management
  - Client certificate testing
  - Certificate-based authentication configuration
  - Secure traversal test
  - Ciphers
  - SSH configuration
- Backup and restore
- Diagnostics >
- Maintenance mode
- Language
- Restart options

Choose File No file chosen

Upload

Select the file containing trusted CA certificates Choose File No file chosen i

Trusted CA certificate You are here: Maintenance

File uploaded: CA certificate file uploaded. File contents - Certificates: 1, CRLS: 0.

| Type                                 | Issuer               | Subject        | Expiration date | Validity | View                           |
|--------------------------------------|----------------------|----------------|-----------------|----------|--------------------------------|
| <input type="checkbox"/> Certificate | [REDACTED]           | Matches Issuer | Mar 29 2025     | Valid    | <a href="#">View (decoded)</a> |
| <input type="checkbox"/> Certificate | [REDACTED]:2766-ca-1 | Matches Issuer | Feb 09 2025     | Valid    | <a href="#">View (decoded)</a> |

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)



Nota: En escenarios con Call Manager y el certificado Tomcat como autofirmado, descargue el Call Manager y el certificado Tomcat reales y cárguelos en Expressway.



Vaya a Expressway-C > Mantenimiento > Seguridad > Certificado de CA de confianza > Mostrar todo (archivo PEM)

Trusted CA certificate

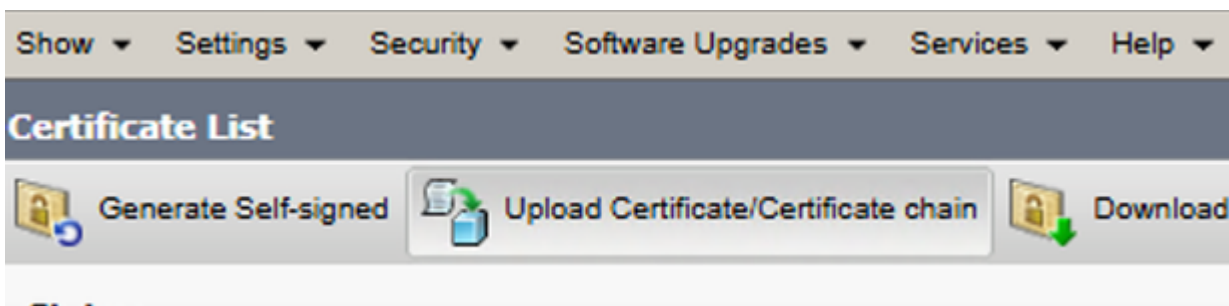
| Type                                 | Issuer                 |
|--------------------------------------|------------------------|
| <input type="checkbox"/> Certificate | [REDACTED] ADSERVER-CA |
| <input type="checkbox"/> Certificate | [REDACTED]:2766-ca-1   |

[Show all \(decoded\)](#) [Show all \(PEM file\)](#) [Delete](#) [Select all](#) [Unselect all](#)

Copie el valor PEM del certificado de CA que firma Expressway-C y guárdelo en un archivo de texto.

```
expcert.pem - Notepad
File Edit Format View Help
-----BEGIN CERTIFICATE-----
MIIDdzCCA1+gAwIBAgIQFBGTWjxDrp1B5NgcCLc0FTANBgkqhkiG9w0BAQsFADBO
MRUwEwYKCZImiZPyLGBGRYFbG9jYWwxZjZAVBgoJkiaJk/IsZAEZFgdicm9qZWRh
[REDACTED]
jsFtVBS1D0ReW61KU5gbIHS19QwbCxZHxd4a
-----END CERTIFICATE-----
```

Navigate to OS administration > Security > Certificate management and select Upload Certificate/Certificate Chain and load the CA certificate of expressway-C as Tomcat-trust and Call Manager-trust



**Upload Certificate/Certificate chain**

Upload Close

**Status**

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

**Upload Certificate/Certificate chain**

Certificate Purpose\* CallManager-trust

Description(friendly name)

Upload File Choose File expcert.pem

Upload Close



Reinicie los servicios necesarios en el clúster de CUCM:

- Navegue hasta Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones y reinicie el servicio Cisco CallManager en todos los nodos que lo ejecutan.
- Navegue hasta Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones y reinicie el servicio Cisco TFTP en todos los nodos que lo ejecutan.
- Reinicie el servicio Tomcat en todos los nodos del clúster a través de CLI con el comando `utils service restart Cisco Tomcat`.
- Reinicie el servicio Cisco HAProxy en todos los nodos del clúster a través de CLI con el comando `utils service restart Cisco HAProxy`.

## Escenario 4: Renovación de la causa del certificado de función proxy de la autoridad certificadora

### Escenario 4.1: Error de autenticación 802.1x

El teléfono no se autentica con ASA después de regenerar el certificado de función proxy de



omita 802.1x para permitir el registro e instalar el certificado LSC en los teléfonos afectados.

Escenario 4.2: Los teléfonos no se registran en CUCM que utiliza el perfil de seguridad en el modo TLS.

Los teléfonos muestran "El teléfono se está registrando" después de regenerar el certificado CAPF en el editor de CUCM.

## Verificación

1. Los teléfonos afectados contienen un perfil de seguridad con el modo TLS activado.

**Phone Security Profile Information**

**Product Type:** Cisco 8845  
**Device Protocol:** SIP  
**Name\*** Cisco 8845 - Secure profile  
**Description** Cisco 8845 - Secure profile  
**Nonce Validity Time\*** 600  
**Device Security Mode** Encrypted  
**Transport Type\*** TLS  
 Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

2. Los teléfonos afectados tienen instalado el certificado LSC.
3. Asegúrese de que el certificado CAPF esté actualizado.

**Certificate List (1 - 15 of 15)**

Find Certificate List where Certificate begins with CAPF Find Clear Filter

Select item or enter search text

| Certificate * | Common Name/Common Name_SerialNumber | Usage    | Type        | Key Type | Distribution        | Issued By     | Expiration |
|---------------|--------------------------------------|----------|-------------|----------|---------------------|---------------|------------|
| CAPF          | CAPF-0bc17206                        | Identity | Self-signed | RSA      | cm15-<br>.cisco.com | CAPF-0bc17206 | 10/01/2028 |

4. Inicie sesión en el publicador de CUCM y utilice el comando show ctl que muestra el número de serie del certificado CAPF antiguo.
5. A continuación, cambie el perfil de seguridad del teléfono a no seguro.

## Solución

Regenere el archivo CTL en CUCM y reinicie los servicios necesarios para asegurarse de que los teléfonos obtengan el nuevo archivo CTL con el archivo CAPF.



Precaución: El TAC recomienda realizar esta operación fuera del horario laboral, ya que este procedimiento requiere el reinicio de los servicios. El impacto empresarial es

## Medium Impact.

Procedimiento para garantizar la renovación de CAPF con éxito.



```
admin:utils ctl update CTLFile
This operation will update the CTLFile. Do you want to continue? (y/n): y

Updating CTL file
CTL file Updated
Please reset all Encrypted and Authenticated phones for the CTL file updates to take effect.
```

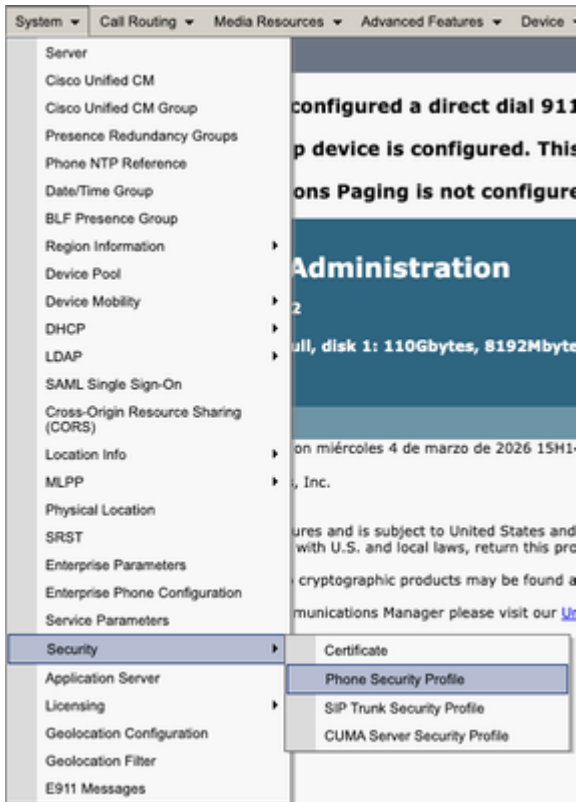
Actualice el archivo CTL después de la regeneración de CAPF. Inicie sesión en la CLI del publicador e introduzca el comando `utils ctl update CTLFile`.



1. Vaya a Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones en CUCM publisher y reinicie el servicio CAPF.
2. Navegue hasta Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de red y reinicie el Servicio de verificación de confianza de Cisco en todos los nodos que lo ejecutan.
3. Navegue hasta Serviciabilidad de Cisco Unified > Herramientas > Centro de control - Servicios de funciones y reinicie el Servicio TFTP de Cisco en todos los nodos que lo ejecutan



- Vaya a Administración CM > Sistema > Seguridad > Perfil de seguridad del teléfono.



- Copie el perfil de seguridad del teléfono actual asignado a los teléfonos requeridos.



- Cambie Name and Device Security Mode a Non Secure y seleccione Save and Apply Config para aplicar este cambio a todos los teléfonos requeridos.

**Phone Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**  
Update successful

**Phone Security Profile Information**

Product Type: Cisco 8845

**Device Protocol:** SIP

Name\*: Cisco 8845 - non Secure profile

Description: Cisco 8845 - Secure profile

Nonce Validity Time\*: 600

Device Security Mode: Non Secure

Transport Type\*: TCP

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

**Phone Security Profile CAPF Information**

Authentication Mode\*: By Null String

Key Order\*: RSA Only

RSA Key Size (Bits)\*: 2048

EC Key Size (Bits): < None >

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

SIP Phone Port\*: 5060

Save Delete Copy Reset Apply Config Add New

- Aplique el perfil de seguridad del dispositivo creado a la configuración de teléfonos necesaria y seleccione Save and Apply Config.

**Protocol Specific Information**

Packet Capture Mode\*: None

Packet Capture Duration: 0

BLF Presence Group\*: Standard Presence group

SIP Dial Rules: < None >

MTP Preferred Originating Codec\*: 711ulaw

Device Security Profile\*: Cisco 8845 - non Secure profile

Rerouting Calling Search Space: < None >

SUBSCRIBE Calling Search Space: < None >

SIP Profile\*: Standard SIP Profile [View Details](#)

Digest User: < None >

Media Termination Point Required  
 Unattended Port  
 Require DTMF Reception



Utilice la sección de información de CAPF en la configuración del dispositivo de los teléfonos afectados para instalar el certificado LSC en los teléfonos requeridos.

- En Información de CAPF, seleccione Install/Upgrade en Certificate Operation.

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Order\*

RSA Key Size (Bits)\*

EC Key Size (Bits)

Operation Completes By     (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Additional CAPF Settings.

- Seleccione Save and Apply Config.
- Espere hasta que Certificate Operation Status muestre Operation completed.



En la sección Información específica de protocolo en Configuración del teléfono, seleccione el perfil de seguridad con TLS habilitado que se creó.

**Protocol Specific Information**

Packet Capture Mode\*

Packet Capture Duration

BLF Presence Group\*

SIP Dial Rules

MTP Preferred Originating Codec\*

Device Security Profile\*

Rerouting Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile\*  [View Details](#)

Digest User

**Phone Security Profile Configuration**

Save Delete Copy Reset Apply Config Add New

**Status**

Status: Ready

**Phone Security Profile Information**

**Product Type:** Cisco 8845  
**Device Protocol:** SIP

Name\* Cisco 8845 - Secure profile  
Description Cisco 8845 - Secure profile  
Nonce Validity Time\* 600  
Device Security Mode Encrypted  
Transport Type\* TLS

Enable Digest Authentication  
 TFTP Encrypted Config  
 Enable OAuth Authentication

## Información Relacionada

- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/214231-certificate-regeneration-process-for-cis.html>
- <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/217138-regeneration-of-cucm-ca-signed-certifica.html>
- <https://www.cisco.com/c/en/us/support/docs/content-networking/certificates/213295-how-to-install-an-lsc-on-a-cisco-ip-phon.html>
- [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X15-2/mra/exwy\\_b\\_mra-deployment-guide-x152.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-2/mra/exwy_b_mra-deployment-guide-x152.html)

## 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).