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.

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	

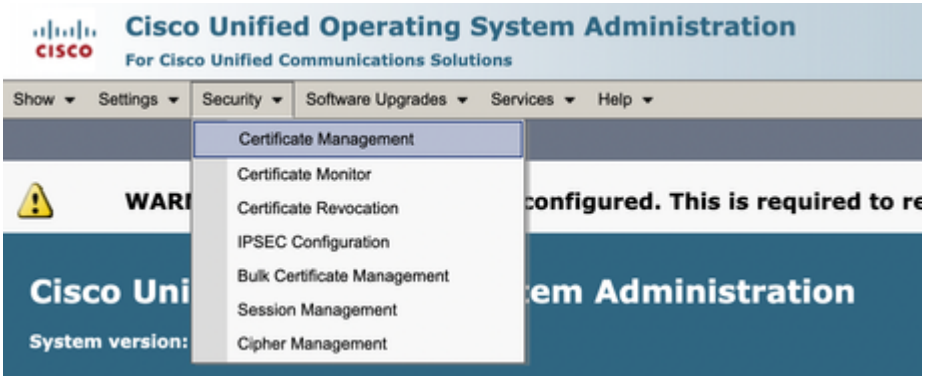
Escenario 1: Los teléfonos no se registran después de la renovación de certificados de Call Manager, TVS e ITL

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.

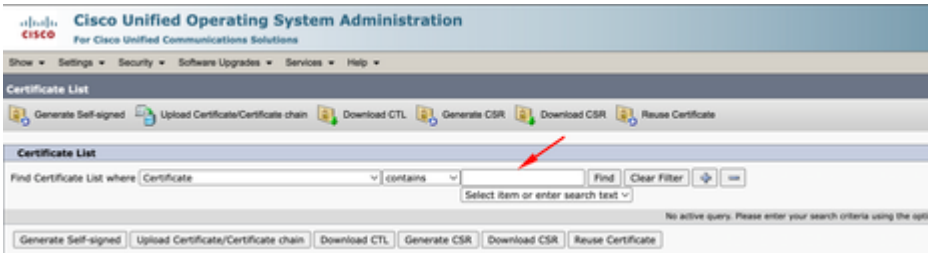
Cuando los certificados de Call Manager , TVS e ITL caducaron y se renovaron al mismo tiempo, hace que todos nuestros teléfonos estén en un estado no registrado que causa un impacto importante en el sistema, se trata de un comportamiento esperado ya que activamos que los teléfonos no confíen en CUCM.

Verificación

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

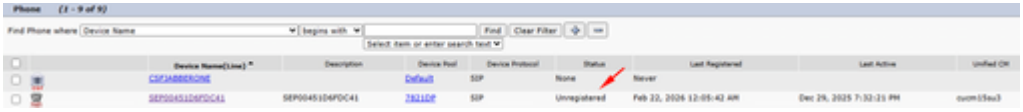


2. Busque por Callmanager, TVS o ITL bajo el filtro en la parte superior de la página y utilice las opciones contiene o comienza con:



3. Los certificados deberán estar actualizados y comprobados en la columna Vencimiento (igual para los certificados de TVS e ITL)

4. Una vez verificado todo es bueno después de la renovación del certificado, los teléfonos se muestran como el estado Unregistered.



Solución

Hay dos opciones para solucionar el problema:

1. Realice un restablecimiento de fábrica del teléfono que permita que el teléfono borre la configuración de seguridad actual y permita que el teléfono obtenga los nuevos certificados
2. Actualice los certificados ITL y CTL desde CLI en el nodo de editor y utilice el comando utils itl reset localkey.

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.authenticatio
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.

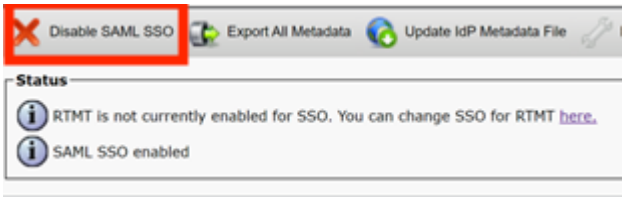
Procedimiento para renovar tomcat con la implementación de SSO habilitada:

⚠ 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.

1. Inhabilite SSO en todos los nodos de CUCM

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

- Seleccione Disable SAML SSO

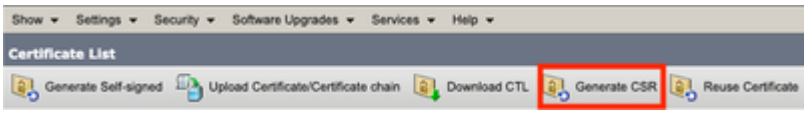


- Este proceso debe realizarse en el resto de los nodos mediante la GUI si se utiliza el acuerdo por nodo.

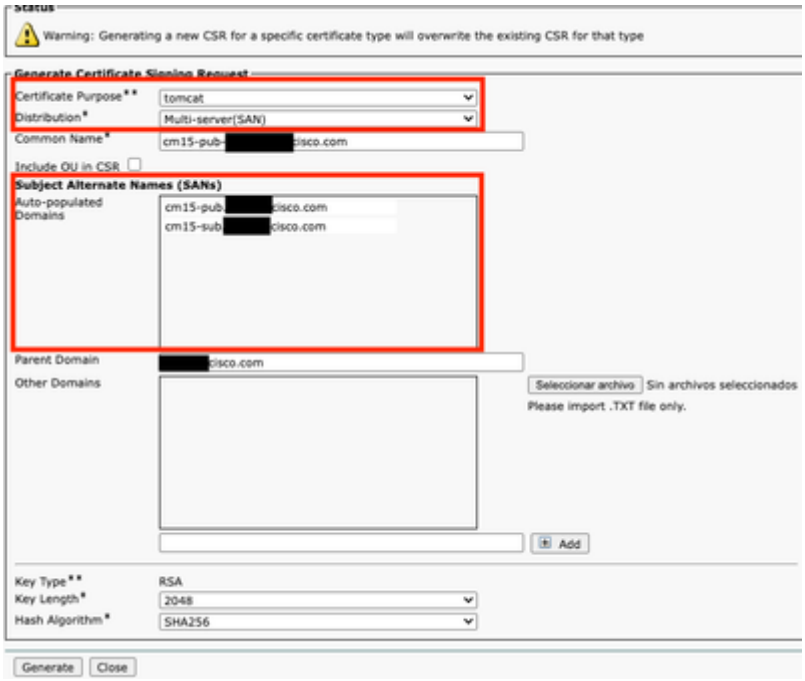
2. Renueve el certificado Tomcat en el clúster de CUCM

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.

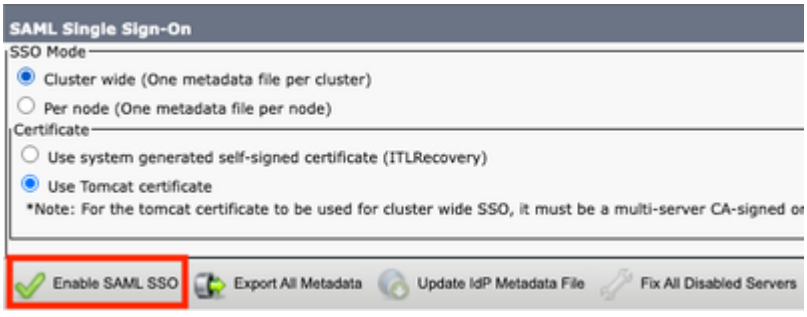
3. Metadatos del proveedor de servicios de exportación (SP)

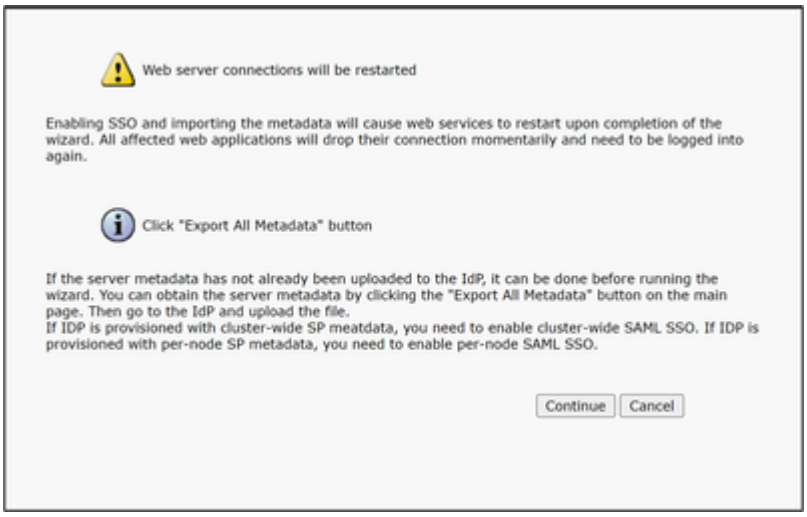
- Vaya a Administración de CM > Sistema > Inicio de sesión único
- Configure las opciones de SSO (en este caso, en todo el clúster en el modo SSO y Use tomcat certificate en el certificado está configurado como ejemplo) y luego seleccione export all metadata .

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

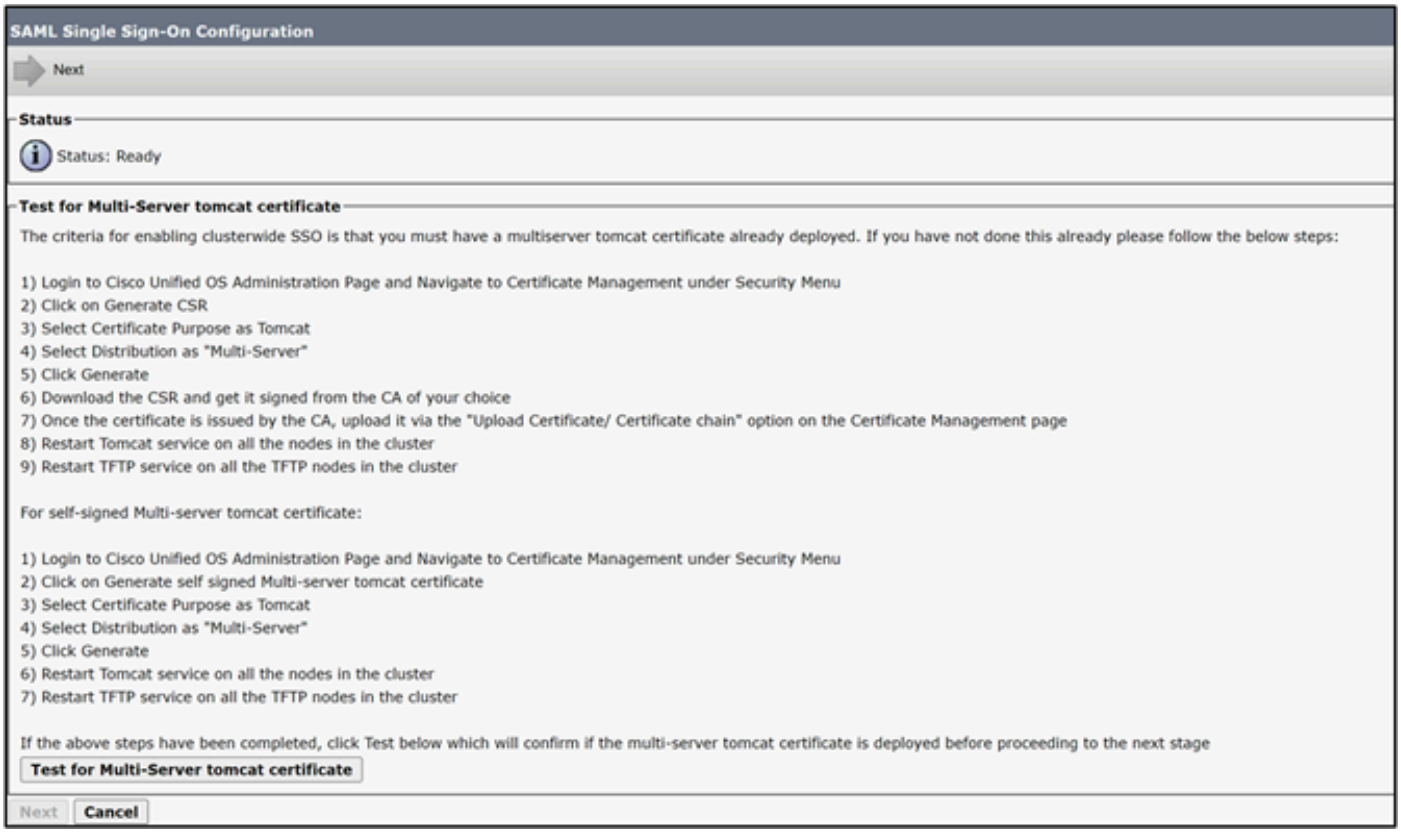
4. Activar SSO en clúster de CUCM

- 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 continue.

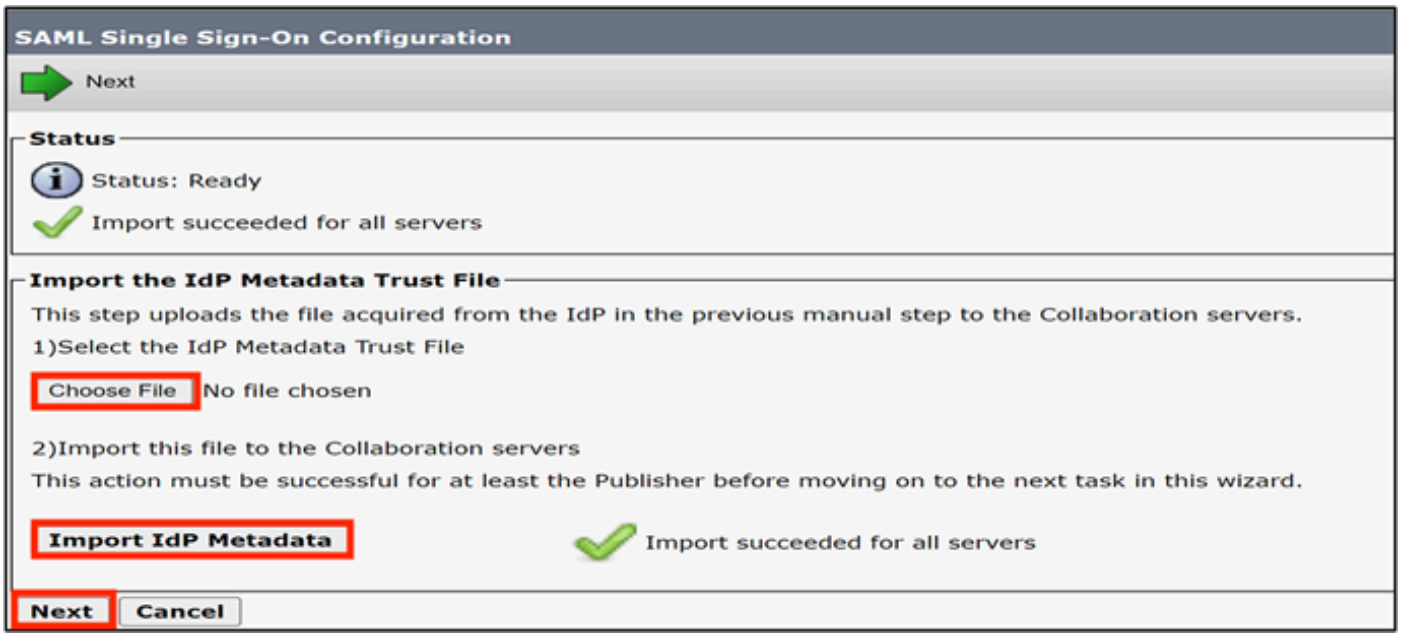




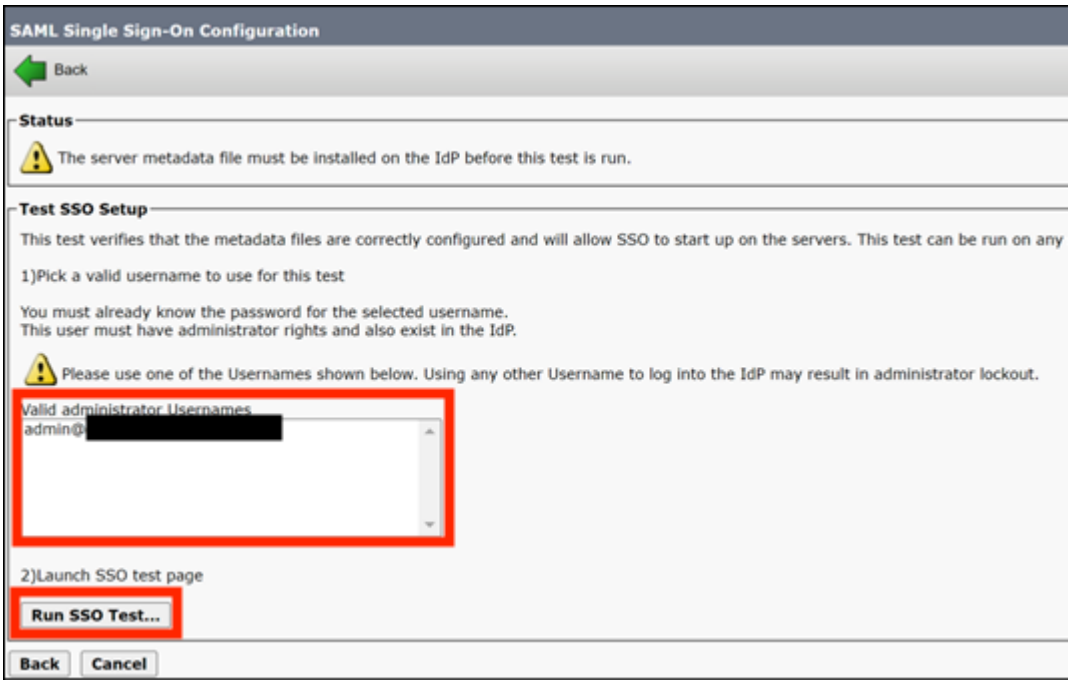
- Si se aplica a todo el clúster, este paso está disponible para comprobar el certificado multi-san en todos los nodos, seleccione Test for multi-server tomcat certificate. una vez finalizado, seleccione Next (Siguiente).

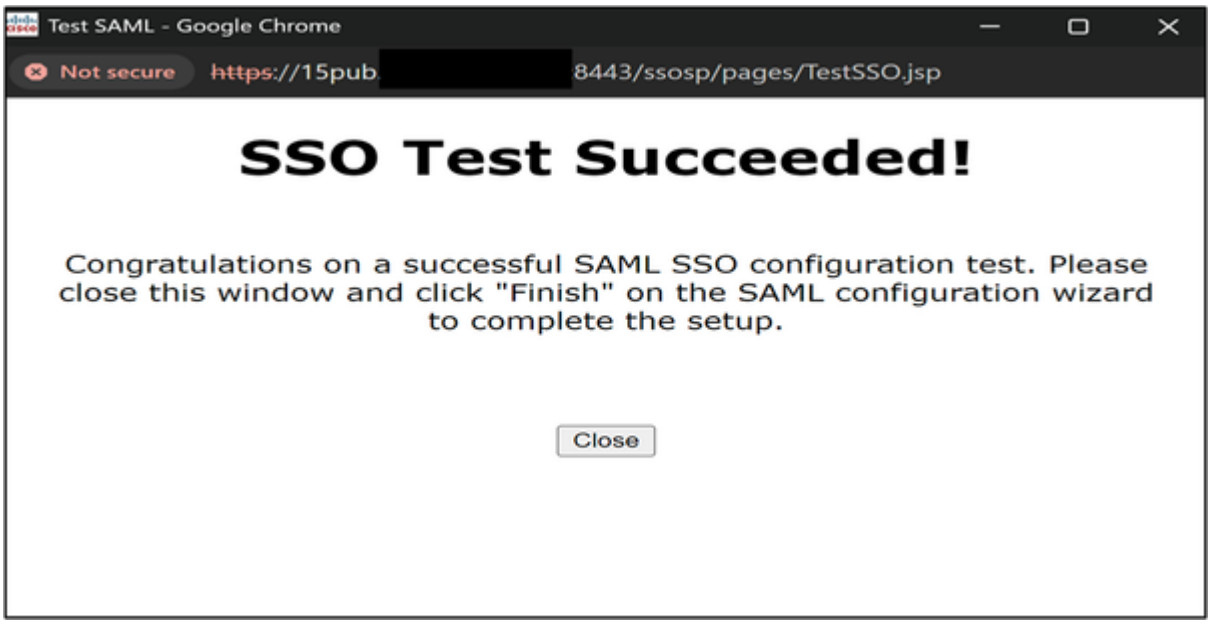


- Cargar metadatos IdP, seleccionar Importar metadatos IdP y una vez finalizado, seleccionar Siguiente



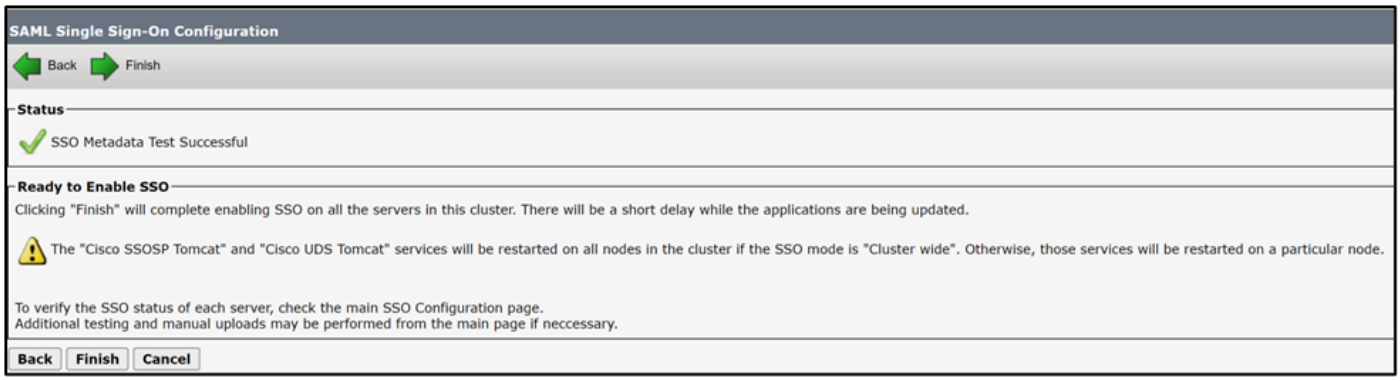
- En Probar configuración de SSO, seleccione un usuario con el grupo Superusuarios de CCM estándar asignado y seleccione Ejecutar prueba de SSO hasta obtener el éxito.





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" Module
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.

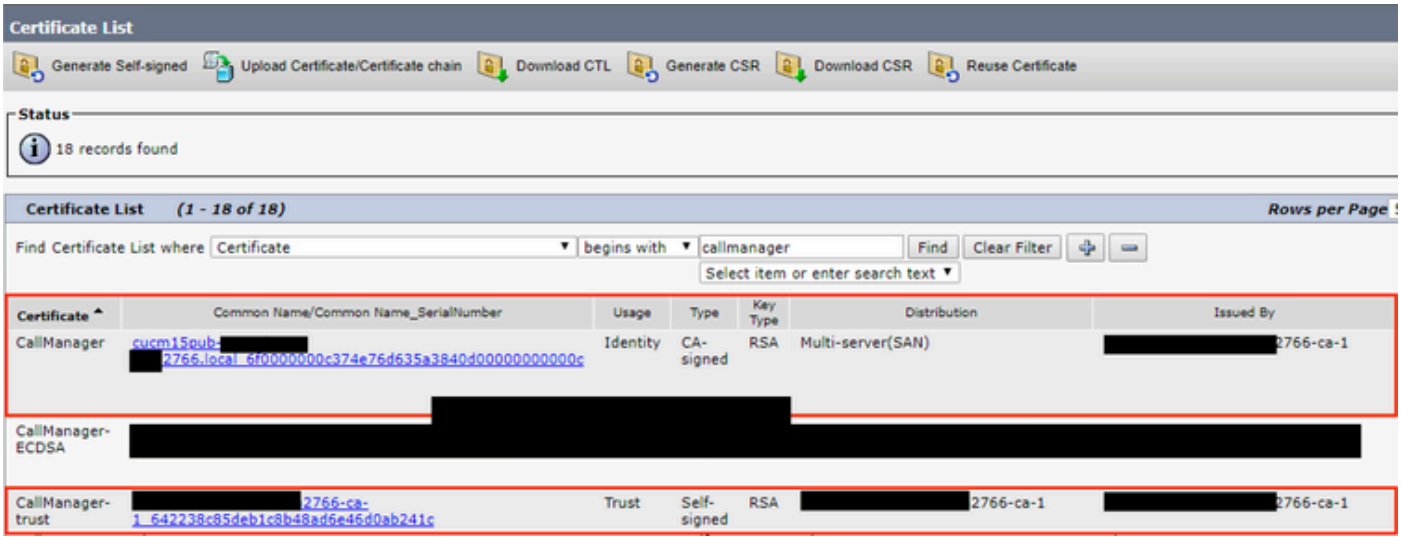
⚠ Precaución: El TAC recomienda realizar esta operación fuera del horario laboral, ya que este procedimiento requiere el reinicio de los servicios. El impacto empresarial es

---

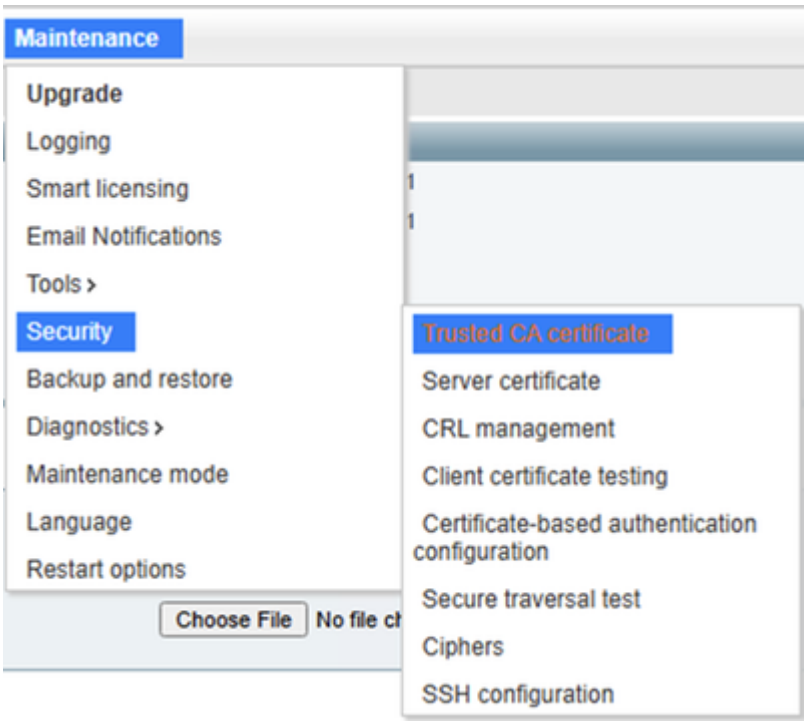
Medium Impact.

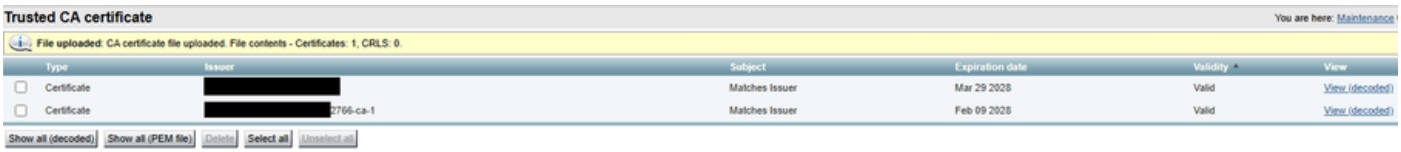
1. Procedimiento para completar la relación de confianza entre CUCM y Expressway con certificados firmados por CA

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.



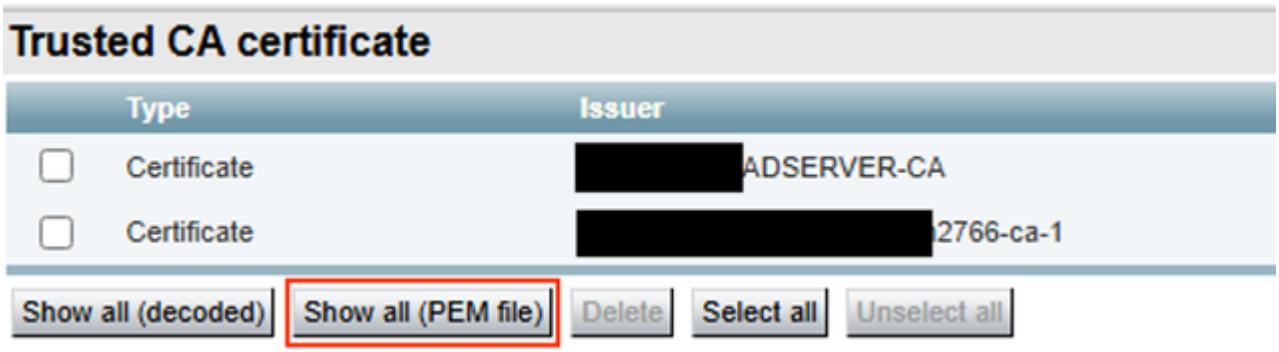
A continuación, navegue hasta Expressway-C > Mantenimiento > Seguridad > Certificado de CA de confianza y cargue el certificado de CA de Call Manager y el certificado Tomcat.



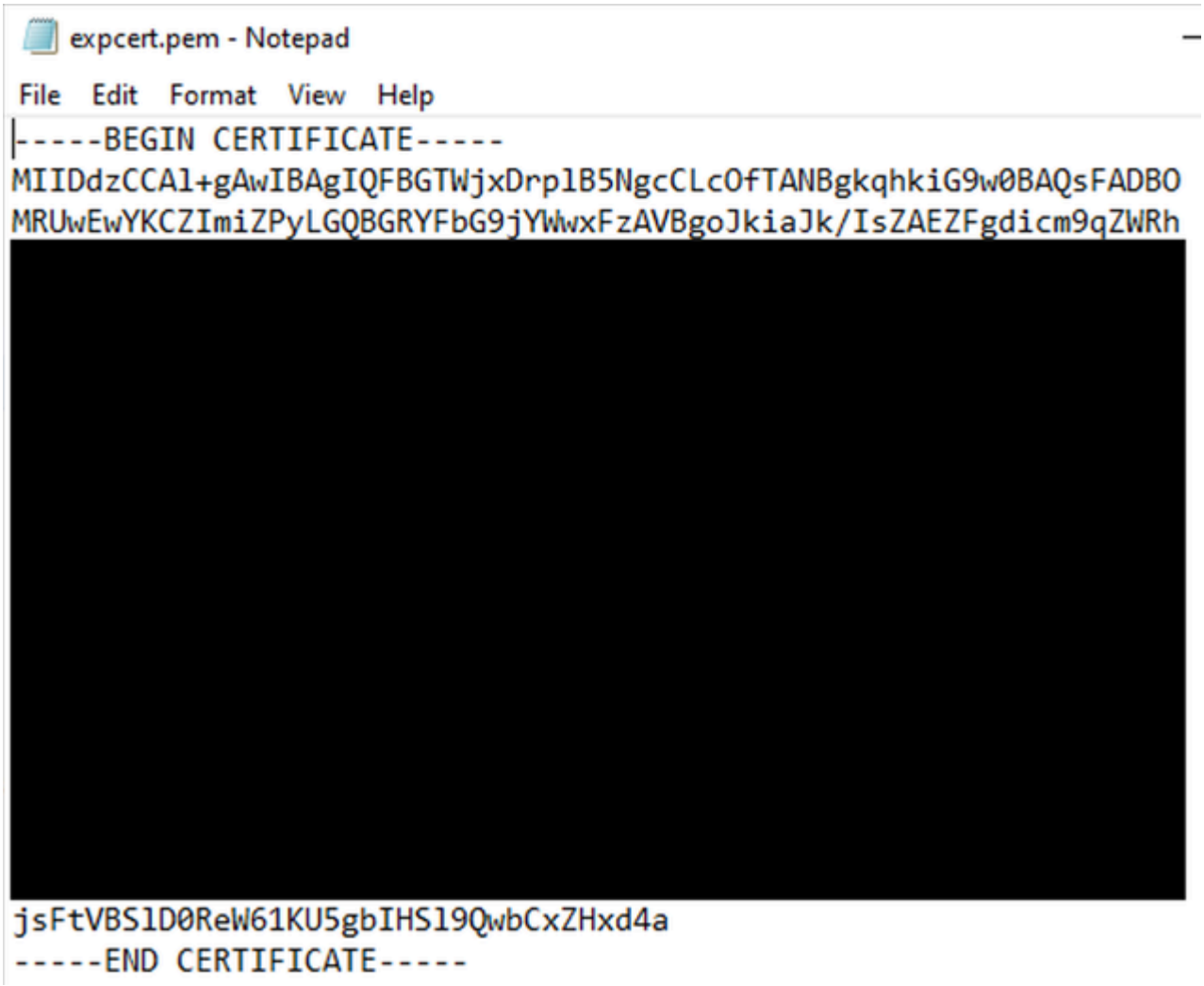


Nota: En escenarios con Call Manager y el certificado Tomcat como autofirmado, descargue el Call Manager y el certificado Tomcat reales y cárguelos en Expressway.

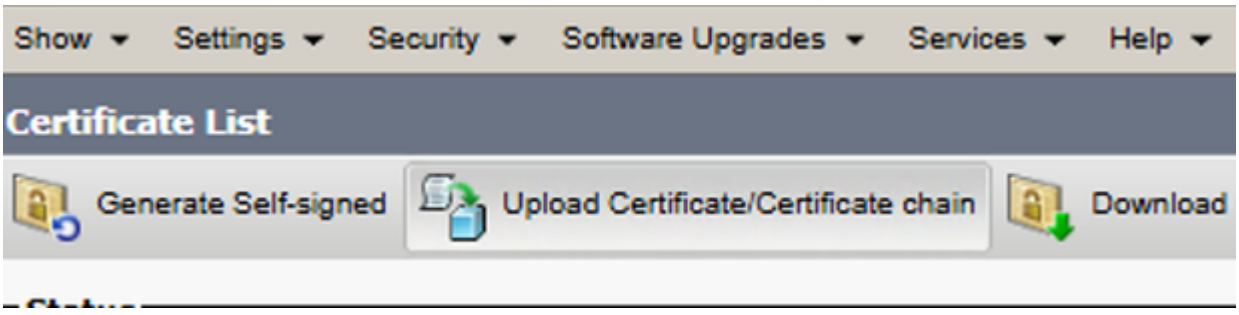
Vaya a Expressway-C > Mantenimiento > Seguridad > Certificado de CA de confianza > Mostrar todo (archivo PEM)

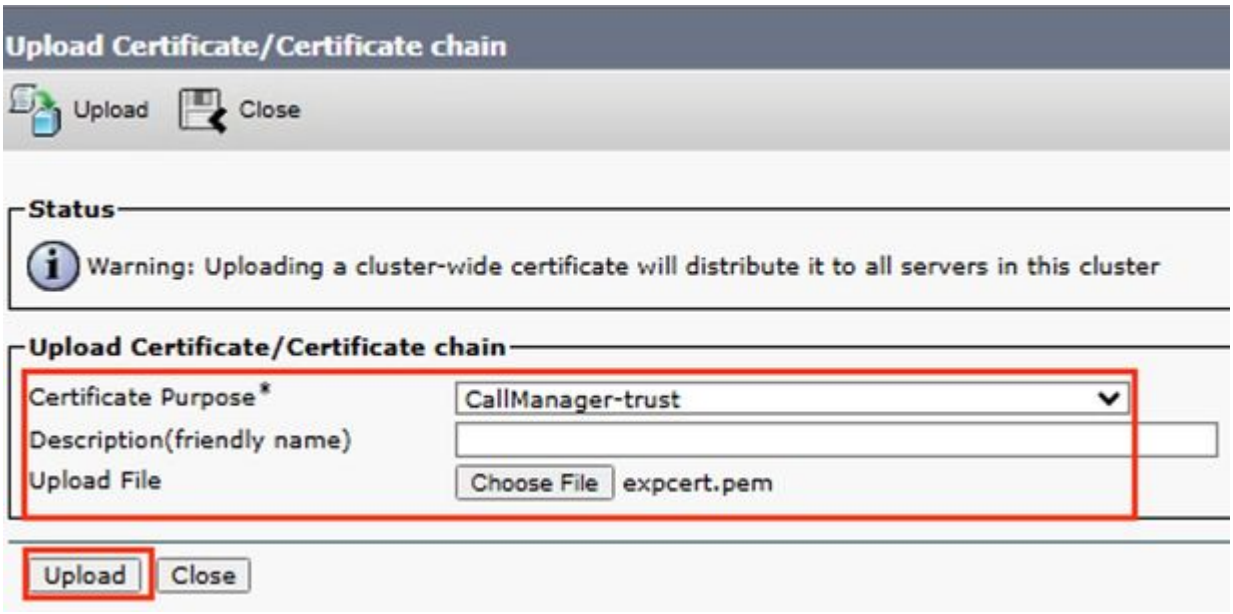


Copie el valor PEM del certificado de CA que firma Expressway-C y guárdelo en un archivo de texto.



Navegue hasta OS administration > Security > Certificate management y seleccione Upload Certificate/Certificate Chain y cargue el certificado de CA de expressway-C como Tomcat-trust y Call Manager-trust





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

autoridad certificadora (CAPF) en el editor de CUCM.

Verificación

1. Los mensajes de estado del teléfono muestran "Autenticación 802.1x: Error"

2. Inspeccione los registros telefónicos del servidor afectado y encuentre "SSL_ERROR_WANT_READ"

```
4592 NOT Feb 17 11:01:25.041733 (349-349) PAE: -Secure Connection Handshake in progress - status SSL_ER
4593 NOT Feb 17 11:01:25.041826 (349-349) PAE: -EV_REQUEST_REC, ST_AUTHENTICATING->ST_AUTHENTICATING
++ EAP-Failure
4594 NOT Feb 17 11:01:25.041898 (349-349) PAE: -send EAP-Resp/TLS - id 9
4595 NOT Feb 17 11:01:25.042032 (349-349) PAE: -authWhile timer set: 30 sec
4596 NOT Feb 17 11:01:27.061822 (349-349) PAE: -[0001-0] 08-cc-a7-1c-bb-ae vid=0xfff=4095 static=0 pri=
4597 NOT Feb 17 11:01:27.061950 (349-349) PAE: -port=0
4598 NOT Feb 17 11:01:27.062009 (349-349) PAE: -cprCdpGetPort address:  8:CC:A7:1C:BB:AE  Phyport=0 app
4599 NOT Feb 17 11:01:27.062068 (349-349) PAE: - >>>>>>>>>>>>> port obtained = 0 for mac macAddress 08:
4600 NOT Feb 17 11:01:27.062134 (349-349) PAE: -rcvd EAP-Failure
4601 NOT Feb 17 11:01:27.062189 (349-349) PAE: -EV_FAILURE, ST_AUTHENTICATING->ST_HELD
4602 WRN Feb 17 11:01:27.062462 (349-349) PAE: -802.1X auth FAILED
4603 NOT Feb 17 11:01:27.062550 (349-349) PAE: -paeInfoToInetd: PAE info sent to NETSD
4604 NOT Feb 17 11:01:27.062717 (1786-1880) JAVA-Calling handleNetSDEvent
4605 WRN Feb 17 11:01:27.062953 (1786-1880) JAVA-Thread-11|cip.sec.Security:? - Security: Received a pr
4606 DEB Feb 17 11:01:27.063039 (1786-1880) JAVA-openQue(): que->/tmp/pae_msg_que, key->0x101019ab
4607 DEB Feb 17 11:01:27.063069 (1786-1880) JAVA-openQue(): que->/tmp/pae_rsp_que, key->0x10101c4c
4608 DEB Feb 17 11:01:27.063091 (1786-1880) JAVA-getpaeinfo: send pae info message paeCmd.mtype=1880, p
4609 DEB Feb 17 11:01:27.063121 (1786-1880) JAVA-getpaeinfo: recv pae info resp ret=-1, errno=No messag
4610 NOT Feb 17 11:01:27.063306 (349-349) PAE: -paeInfoToInetd: Netsd event NETSD_EV_PAE sent to NETSD
4611 NOT Feb 17 11:01:27.063370 (349-349) PAE: - PAE RE-AUTH, not sending SEC_DOWN Netsd event for CDP
4612 NOT Feb 17 11:01:27.063423 (349-349) PAE: -paeSetLastSupStatus: LastSupStatus 0
4613 NOT Feb 17 11:01:27.063475 (349-349) PAE: -heldWhile timer set: 60 sec
4614 NOT Feb 17 11:01:27.064074 (349-349) PAE: -paeNetsdRcvMsg(349): PAE event: status: FAIL : Resource
```

Solución

Descargue el certificado CAPF del editor de CUCM y cárguelo en el servidor de autenticación;

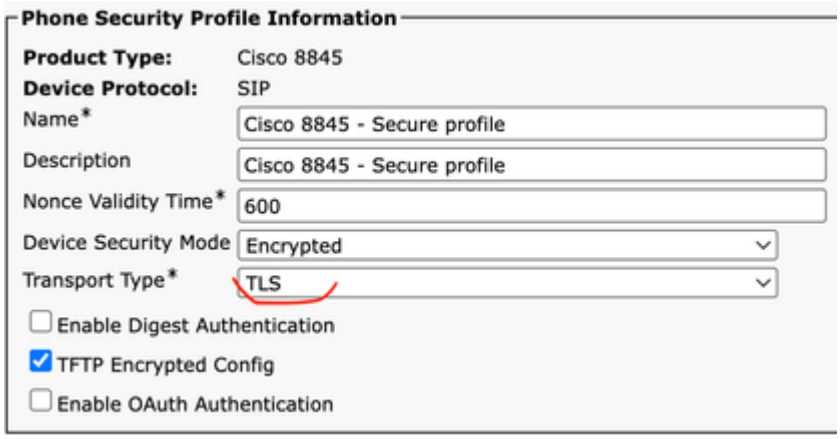
omita 802.1x para permitir el registro e instalar el certificado LSC en los teléfonos afectados.

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.



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

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.
```

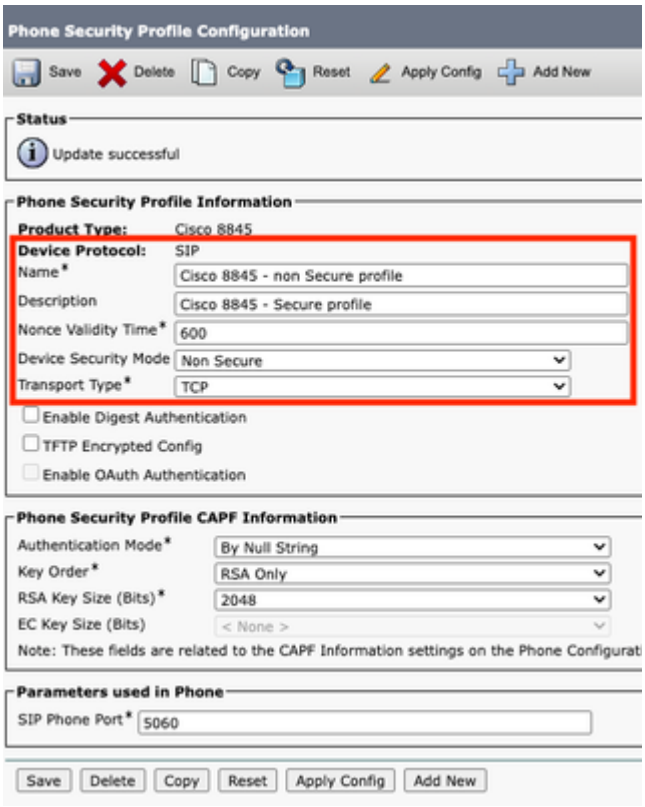
Actualice el archivo CTL después de la regeneración de CAPF. Inicie sesión en la CLI del publicador e introduzca el comando utils ctl update CTLFile.

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

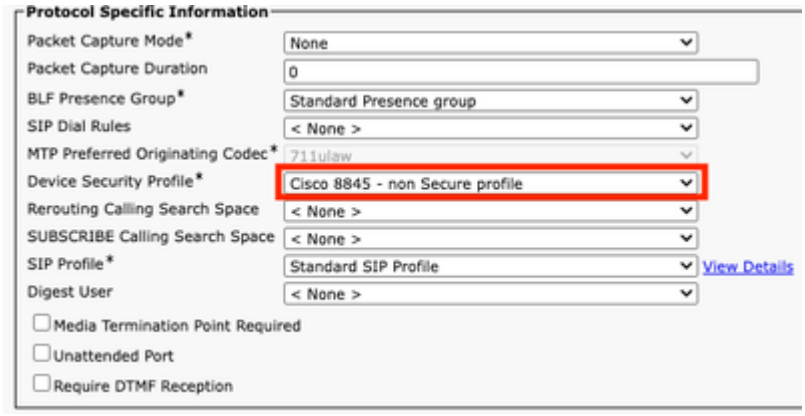
- Vaya a Administración CM > Sistema > Seguridad > Perfil de seguridad del teléfono.

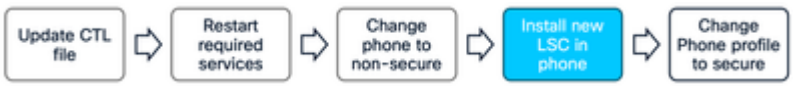
- Copie el perfil de seguridad del teléfono actual asignado a los teléfonos requeridos.

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



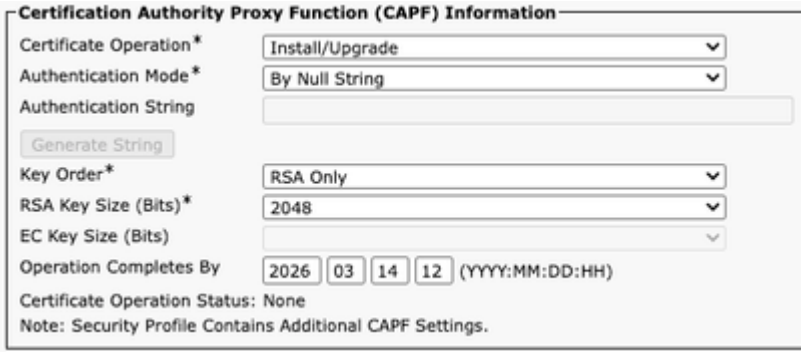
- Aplique el perfil de seguridad del dispositivo creado a la configuración de teléfonos necesaria y seleccione Save and Apply Config.





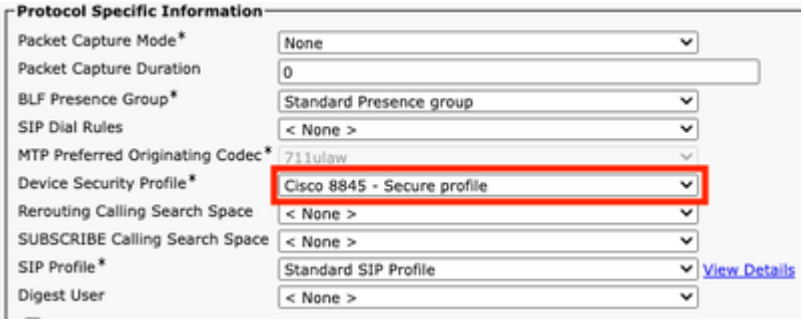
Utilice la sección de información de CAPF en la configuración del dispositivo de los teléfonos afectados para instalar el certificado LSC en los teléfonos requeridos.

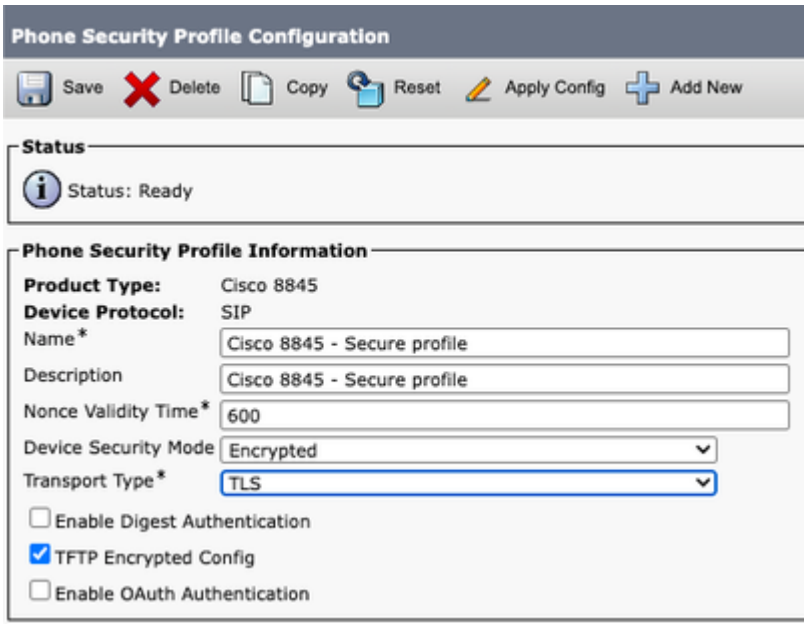
- En Información de CAPF, seleccione Install/Upgrade en Certificate Operation.



- 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.





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

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).