Cisco Jabber y modo OAuth SIP

Contenido

Introducción

Este documento describe los pasos de configuración y de solución de problemas básicos para implementar el modo OAuth SIP con Cisco Jabber.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Registro de softphone Jabber
- Unified Communications Manager (UCM)
- Solución Mobile and Remote Access (MRA)

Componentes Utilizados

Versión de software mínima para admitir el modo OAuth de SIP:

- Cisco UCM 12.5
- Cisco Jabber 12.5
- Cisco Expressway X12.5

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.

Restricción

Cuando el modo OAuth SIP está habilitado, las opciones Enable Digest Authentication y TFTP Encrypted Config no son compatibles.

Antecedentes

Ventajas clave

La protección de la señalización SIP y los medios para el softphone Cisco Jabber implica actualmente varios pasos de configuración. La más difícil es instalar y renovar los certificados de cliente (LSC), especialmente si un dispositivo Cisco Jabber está cambiando entre las instalaciones y fuera de ellas, y mantener los certificados del archivo CTL actualizados.

El modo OAuth de SIP permite que el teléfono virtual Cisco Jabber utilice tokens autodescriptivos de OAuth en lugar del certificado LSC del cliente para la autenticación en una interfaz SIP segura. La compatibilidad con OAuth en la interfaz SIP de UCM permite la señalización y los medios seguros para las implementaciones de Jabber en las instalaciones y MRA sin necesidad del modo mixto ni del funcionamiento de CAPF.

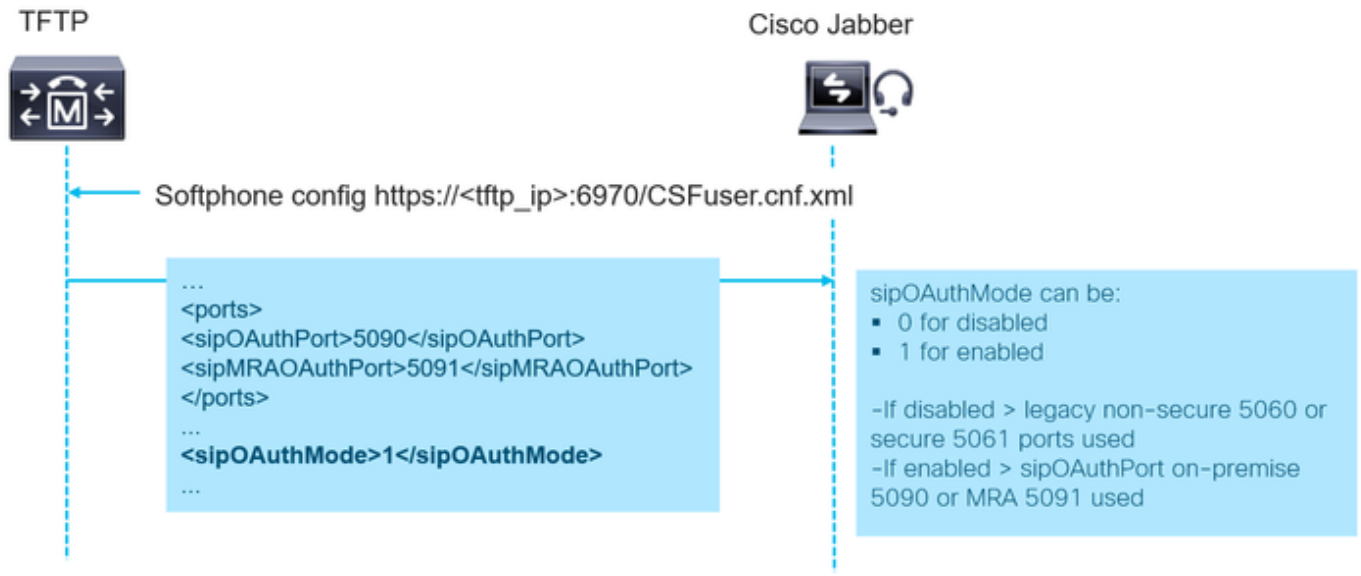
Ventajas clave de la compatibilidad con el modo OAuth SIP de Cisco Jabber:

- Habilita el cifrado siempre activo sin cargas administrativas adicionales.
- Señalización y medios seguros para Cisco Jabber sin necesidad del modo mixto (sin actualizaciones de CTL, mantenimiento de certificados, etc.)
- No es necesario instalar y mantener el LSC en los clientes Jabber.

- Retos con LSC en varios dispositivos (portátiles/dispositivos móviles...)
- El funcionamiento de CAPF es necesario siempre que se instala Jabber en un dispositivo nuevo.
- Operación CAPF no admitida en MRA.

Arquitectura general

El dispositivo Cisco Jabber reconoce que la autenticación OAuth está habilitada en la interfaz SIP mediante el análisis del archivo de configuración CSF (http://<cucmIP>:6970/<CSF-device-name>.cnf.xml), ejemplo de archivo de configuración (algunas líneas se omiten por motivos de brevedad):



Cisco Jabber lee el parámetro sipOAuthMode para determinar si el modo OAuth de SIP está o no habilitado. Este parámetro puede asumir uno de los valores siguientes:

- 0 - SIP OAuth está inhabilitado
- 1 - SIP OAuth está habilitado

Si el modo OAuth de SIP está habilitado, Jabber utiliza uno de estos parámetros para determinar el puerto para la conexión TLS de SIP: sipOAuthPort para las implementaciones in situ o sipMARAOAuthPort para las implementaciones basadas en MRA. El ejemplo presenta los valores predeterminados: sipOAuthPort 5090 y sipMARAOAuthPort 5091. Estos valores se pueden configurar y pueden ser diferentes en cada nodo de CUCM.

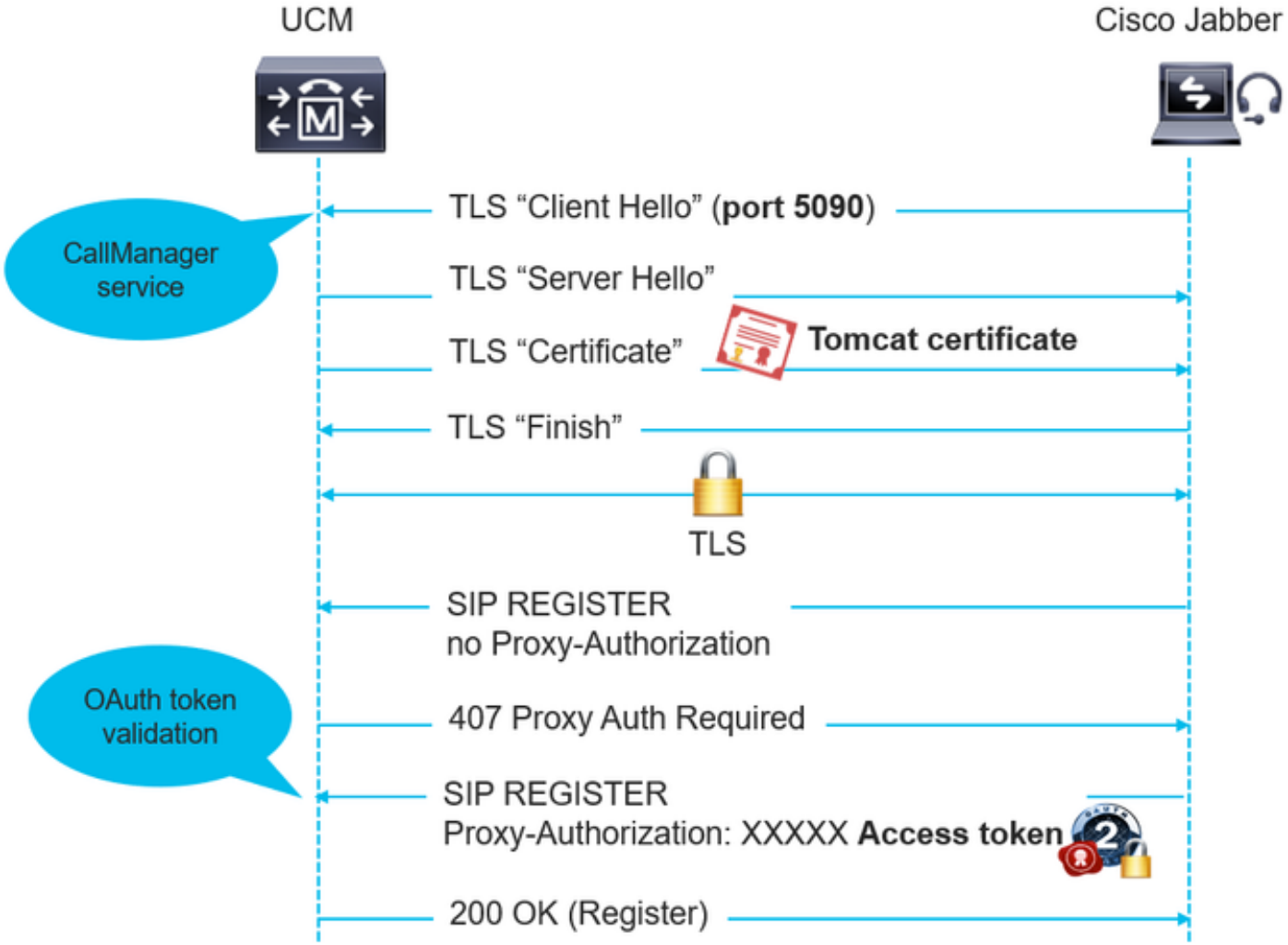
Si el modo OAuth de SIP está desactivado, Jabber utiliza puertos no seguros (5060) o seguros (5061) heredados para el registro de SIP.

Nota: Cisco UCM utiliza el puerto OAuth del teléfono SIP (5090) para escuchar el registro de la línea SIP desde los dispositivos en las instalaciones de Jabber a través de TLS. Sin embargo, UCM utiliza el puerto de acceso remoto móvil SIP (predeterminado, 5091) para escuchar los registros de línea SIP desde Jabber a través de Expressway a través de mLTS. Ambos puertos son configurables. Consulte la sección de configuración.

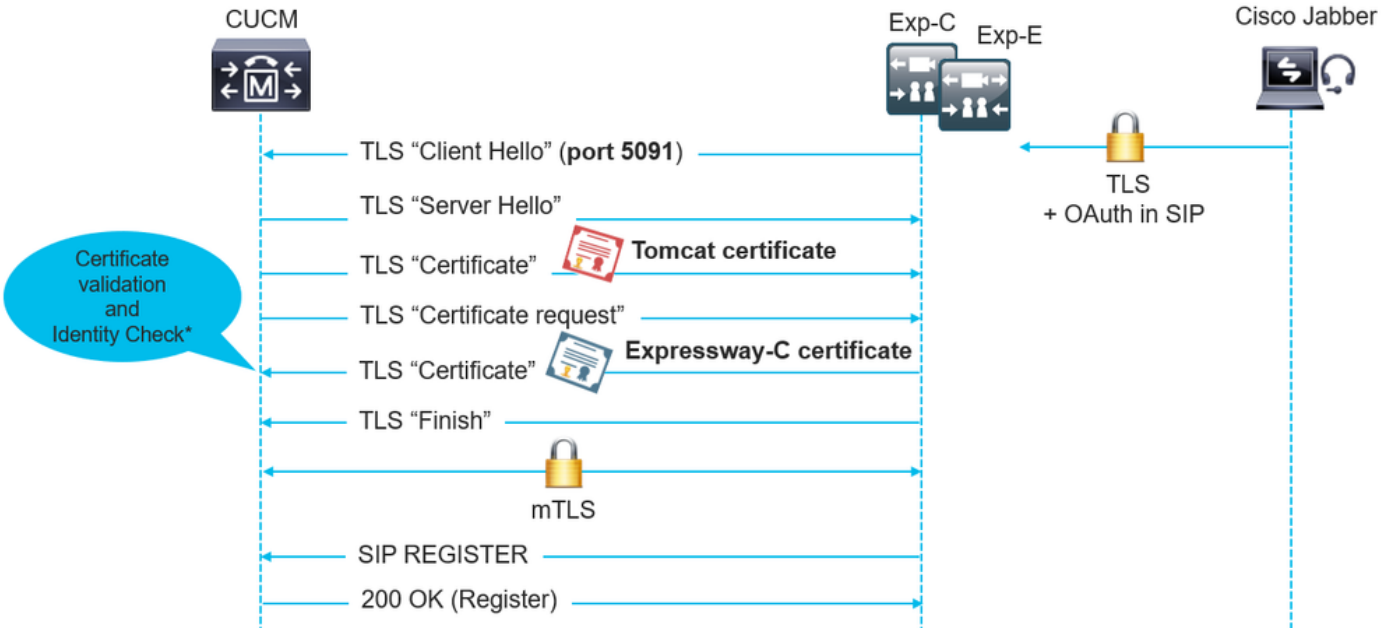
El servicio CallManager escucha tanto sipOAuthPort como sipMARAOAuthPort. Sin embargo, ambos puertos utilizan el certificado Tomcat y Tomcat-trust para conexiones TLS/mTLS entrantes. Asegúrese de que el almacén de confianza de Tomcat pueda comprobar el certificado de Expressway-C para el modo OAuth de SIP para que MRA funcione correctamente.

En situaciones, cuando se vuelve a generar el certificado Tomcat, el proceso de CallManager también debe reiniciarse en los nodos afectados posteriormente. Esto es necesario para que el proceso CCM cargue y utilice nuevos certificados en los puertos sipOAuth.

En esta imagen se muestra el registro de Cisco Jabber mientras se encuentra en las instalaciones:



Esta imagen muestra el registro de Cisco Jabber sobre MRA:



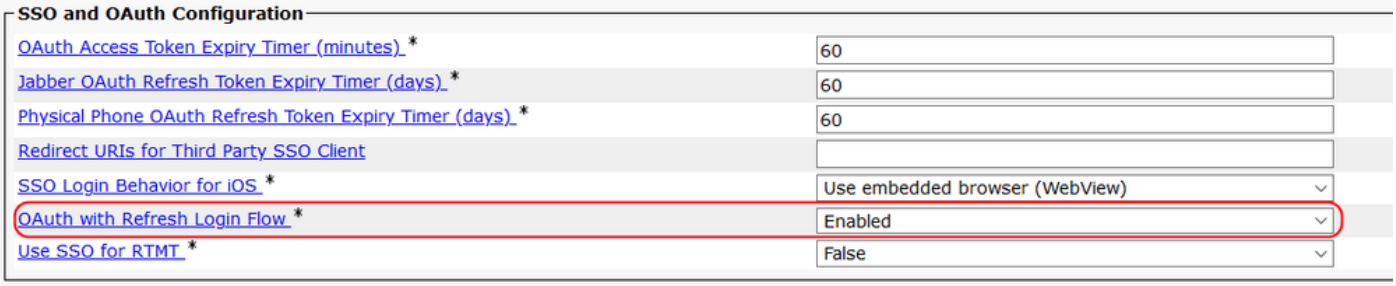
*Los nodos de Expressway-C utilizan la API AXL para informar a UCM del CN/SAN en su certificado. UCM utiliza esta información para validar el certificado Exp-C cuando se establece una conexión TLS mutua.

Configuración: Jabber in situ

Nota:
Asegúrese de completar los puntos siguientes antes de la configuración del modo OAuth SIP:
- MRA está configurado y la conexión se establece entre Unified Communication Manager (UCM) y Expressway (aplicable solo si MRA está en uso).
- UCM está registrado en una cuenta inteligente o virtual con funcionalidad de exportación controlada.

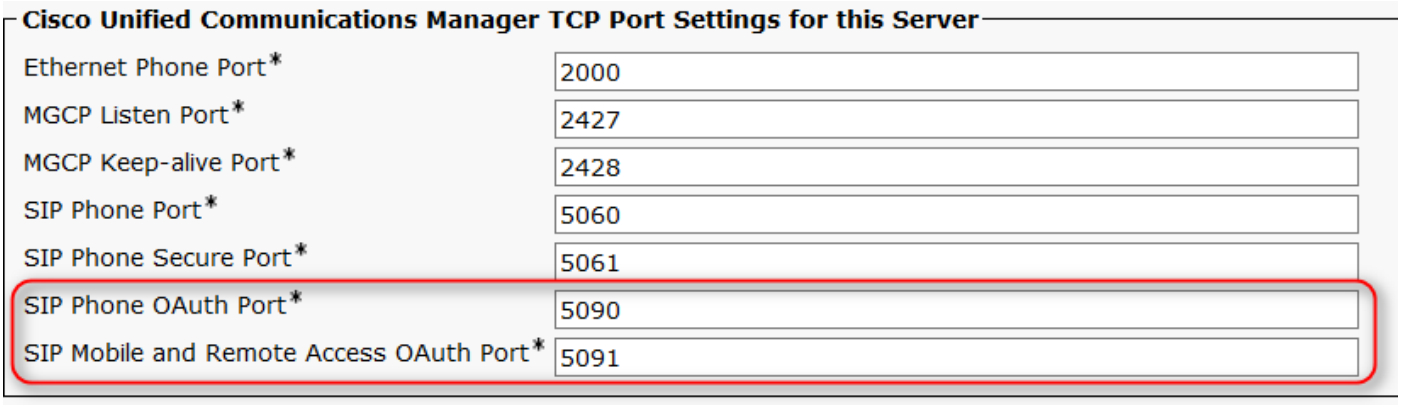
1. Configure los Logins de Actualización.

Configure los inicios de sesión de actualización con tokens de acceso de OAuth y tokens de actualización para los clientes de Cisco Jabber. En Administración de Cisco Unified CM, seleccione Sistema > Parámetros de empresa.



2. Configure los puertos OAuth.

Elija System > Cisco Unified CM. Este es un paso opcional. La imagen presenta los valores predeterminados. El intervalo configurable aceptable es de 1024 a 49151. Repita el mismo procedimiento para cada servidor.



3. Active el modo OAuth SIP.

Utilice la Interfaz de línea de comandos del editor para habilitar el modo SIP OAuth globalmente. Ejecute el comando: utils sipOAuth-mode enable.

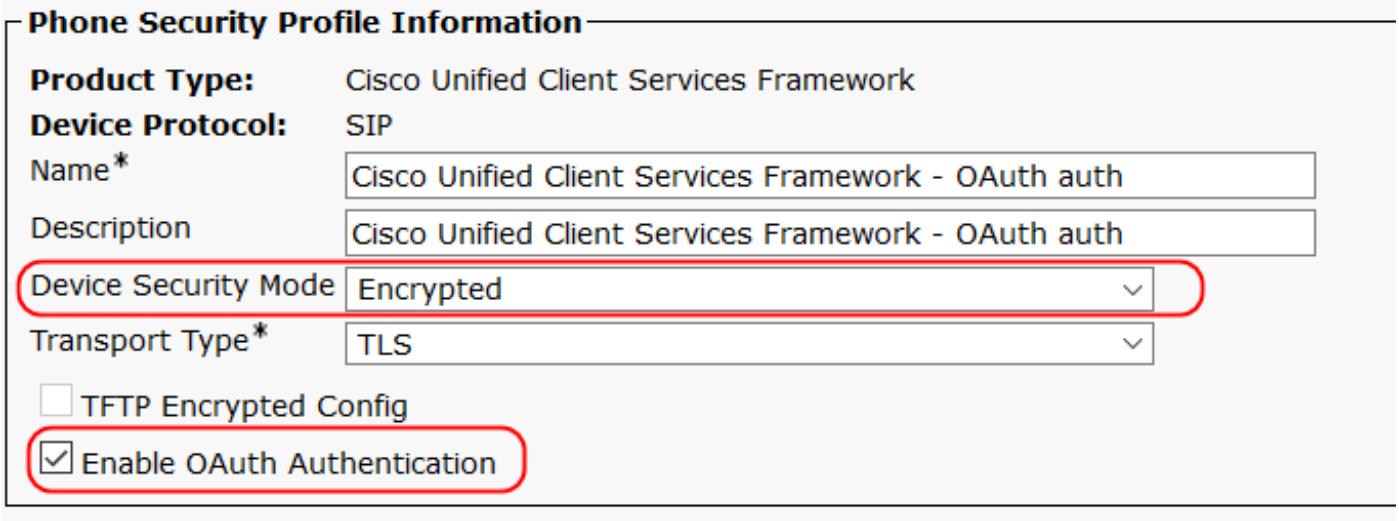
```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

4. Reinicie el servicio Cisco CallManager.

En Serviciabilidad de Cisco Unified, elija Herramientas > Centro de control - Servicios de funciones. Seleccione y reinicie el servicio Cisco CallManager en todos los nodos donde el servicio está activo.

5. Configure el Soporte de OAuth en el Perfil de Seguridad.

En Administración de Cisco Unified CM, elija Sistema > Perfil de seguridad del teléfono. Seleccione Enable OAuth Authentication para habilitar la compatibilidad con OAuth SIP para el terminal.



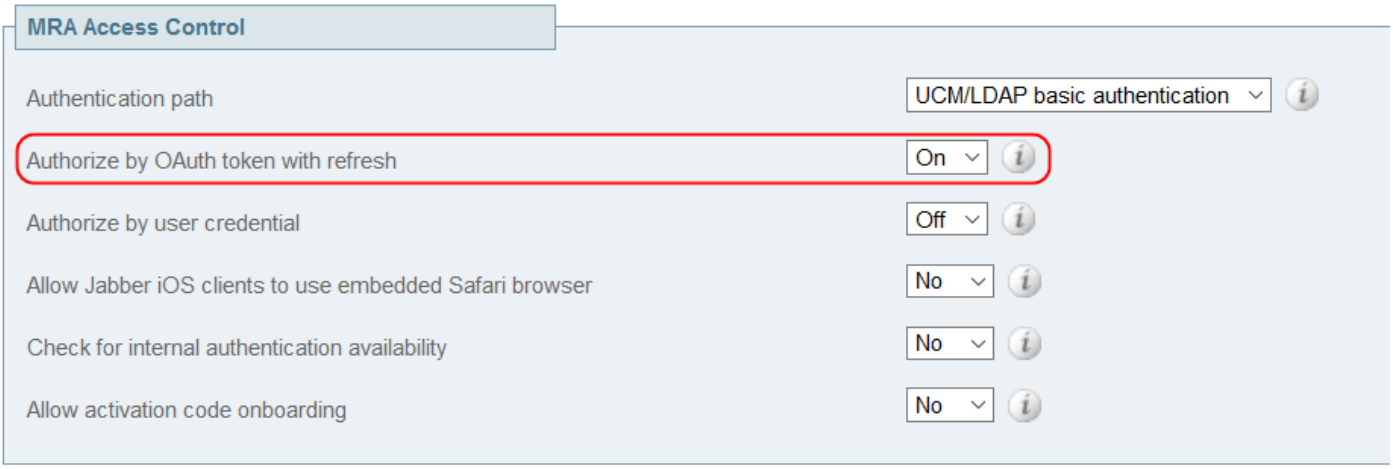
Configuración - Jabber sobre MRA

Prerrequisitos

Antes de configurar el modo OAuth SIP para Jabber sobre MRA, complete los pasos 1-4 del capítulo Configuración - Jabber en las instalaciones de este artículo.

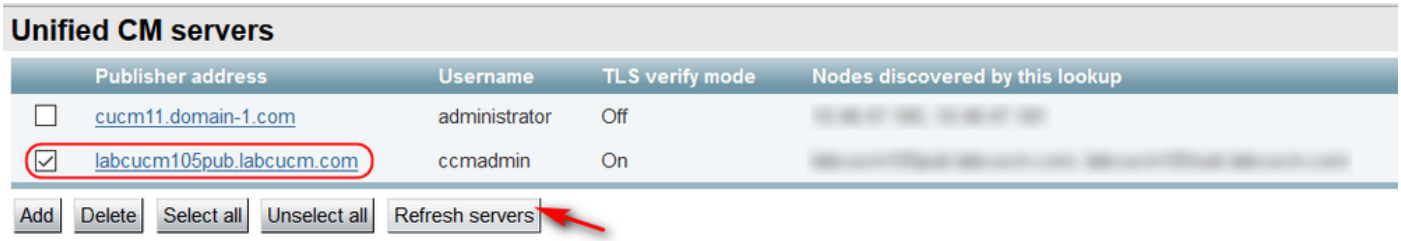
Paso 1. Habilite Refresh Login over MRA.

Los inicios de sesión de actualización deben estar habilitados en Expressway (también llamados tokens autodescriptivos) antes de la configuración de la autenticación OAuth SIP con Cisco Jabber sobre MRA. En Expressway-C, navegue hasta Configuración > Unified Communications > Configuración y asegúrese de que el parámetro Authorize by OAuth Token with refresh esté configurado en On.



Paso 2. Actualice los nodos de Unified CM en Expressway-C.

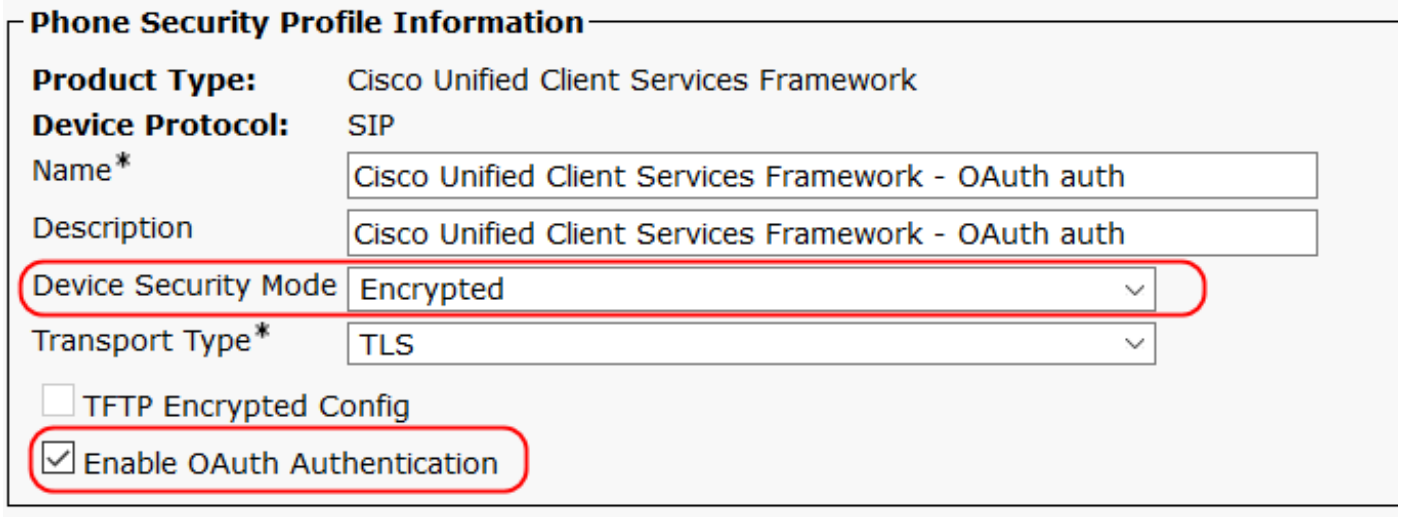
Vaya a Configuration > Unified Communications > Unified CM servers. Descubra o actualice los nodos de Unified CM en Expressway-C.



Nota: Se crea automáticamente una nueva zona de CEOAuth (TLS) en Expressway-C. Por ejemplo, CEOAuth <nombre de Unified CM>. Se crea una regla de búsqueda para proxy las solicitudes SIP que se originan en Jabber a través de MRA hacia el nodo de Unified CM. Esta zona utiliza conexiones TLS independientemente de si Unified CM está configurado con el modo mixto. Para establecer la confianza, Expressway-C también envía el nombre de host y los detalles del nombre alternativo del sujeto (SAN) al clúster de Unified CM. Consulte la parte de verificación de este artículo para asegurarse de que se ha establecido la configuración adecuada.

Paso 3. Configure el Soporte de OAuth en el Perfil de Seguridad.

En Administración de Cisco Unified CM, elija Sistema > Perfil de seguridad del teléfono. Habilite la compatibilidad con OAuth en el perfil asignado a Cisco Jabber.



Verificación

1. Compruebe si el modo OAuth de SIP está activado globalmente.

Verifique el modo OAuth desde Cisco Unified CM Administration, elija System > Enterprise Parameters.

Como alternativa, utilice Admin CLI - Ejecute el comando: run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'

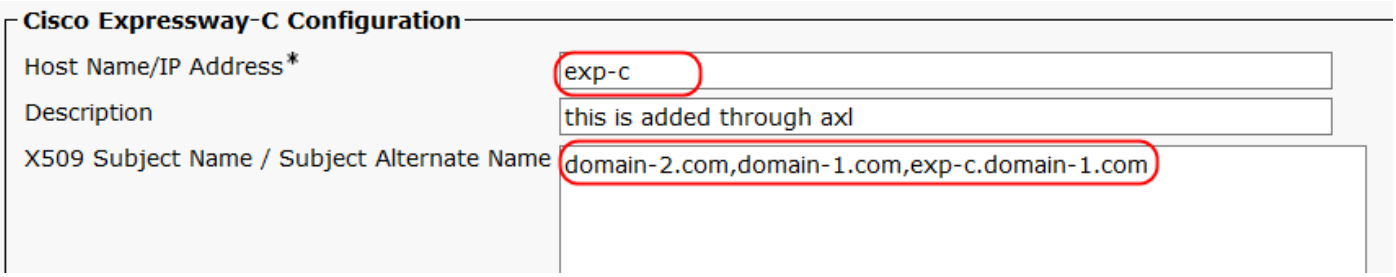
```
admin:run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'
paramvalue
==========
1
admin:
```

Valores posibles: 0 - para Desactivado (valor predeterminado), 1 - para Activado.

2. Compruebe que las entradas de SAN de Expressway-C se han enviado correctamente a CUCM.

Expressway-C envía los detalles CN/SAN de su certificado a UCM a través de AXL. Estos detalles se guardan en la tabla de configuración de expresswayc. Este proceso se invoca cada vez que detecta o actualiza los nodos de Unified CM en Expressway-C. Estas entradas se utilizan para establecer la confianza entre UCM y Expressway-C. El campo CN/SAN del certificado de Expressway-C se compara con esas entradas durante la conexión MTLS al puerto OAuth de MRA SIP (5091 de forma predeterminada). Si la verificación no se realiza correctamente, la conexión MTLS falla.

Verifique las entradas de Cisco Unified CM Administration, elija Device > Expressway-C (disponible a partir de UCM 12.5.1Su1)

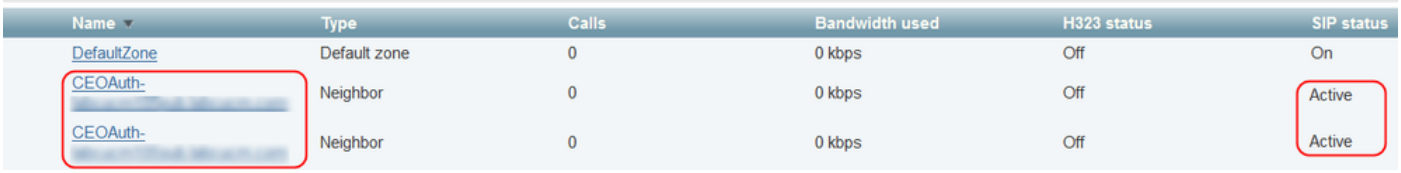


Como alternativa, utilice Admin CLI - Ejecutar el comando: run sql select * from expresswaycconfiguration

```
admin:run sql select * from expresswaycconfiguration
pkid                                 hostnameorip description              x509subjectnameoraltname
==================================== ============ ======================== ========================================================
d5fd15d5-b049-c5b5-0197-bd11a5641640 exp-c        this is added through axl domain-2.com,secure-phone-profile,domain-1.com,exp-c.domain-1.com
admin:
```

3. Verifique las zonas de CEOAuth en Expressway-C.

Vaya a Expressway-C > Configuration > Zones > Zones. Asegúrese de que todas las zonas de CEOAuth recién creadas se encuentran en el estado activo.



4. Verificar que el Proceso de CallManager escuche en los Puertos OAuth SIP.

Ejecute el comando desde la CLI de administración: show open ports regexp 5090 (puerto OAuth SIP predeterminado)

```
admin:show open ports regexp 5090

Executing.. please wait.
ccm       30622    ccmbase  364u  IPv4  207160      0t0  TCP 10.48.[redacted]:5090 (LISTEN)
```

Ejecute el comando desde la CLI de administración: show open ports regexp 5091 (puerto OAuth SIP MRA predeterminado)

```
admin:show open ports regexp 5091

Executing.. please wait.
ccm       30622    ccmbase  351u  IPv4  207155      0t0  TCP 10.48.[redacted]:5091 (LISTEN)
```

Troubleshoot

Ejemplo de registro de Jabber (en las instalaciones)

Ejemplo de registro para el registro OAuth SIP in situ en el puerto 5090 desde la perspectiva del registro de Jabber.

CSF configuration retrieved 2020-03-30 13:03:18,278 DEBUG [0x000012d8] [src\callcontrol\ServicesManager.cpp(993)] [csf.ecc] [csf::ecc::ServicesManager::fetchDeviceConfig] - fetchDeviceConfig() retrieved config for CSFrado 2020-03-30 13:03:18,278 DEBUG [0x000012d8] [rc\callcontrol\ServicesManager.cpp(1003)] [csf.ecc] [csf::ecc::ServicesManager::fetchDeviceConfig] - Device Config:

10.10.10.1

ccm12pub

2000

5060

5061

5090

5091

…

1
Setting SIP oauth mode to 1 2020-03-30 13:03:18,747 DEBUG [0x00002968] [ig\CertificateVerificationHelper.cpp(35)] [csf.ecc] [csf::ecc::CertificateVerificationHelper::setSipOauthMode] - sip OAuth Mode=1 ## Setting OAuth ports (5090 and 5091) for each UCM server 13:03:19,013 INFO [0x00002484] [\core\ccapp\config\config_parser.c(1491)] [csf.sip-call-control] [config_process_ccm_properties] - ccm0=10.10.10.1 ccm1=10.10.10.2 ccm2= sip_oauth_port_0=5090 sip_oauth_port_1=5090 sip_oauth_port_2=5090 length=0 13:03:19,013 INFO [0x00002484] [\core\ccapp\config\config_parser.c(1494)] [csf.sip-call-control] [config_process_ccm_properties] - sip_mar_oauth_port_0=5091 sip_mar_oauth_port_1=5091 sip_mar_oauth_port_2=5091 ## Open TLS connection to 5090 2020-03-30 13:03:18,528 DEBUG [0x00000e2c] [sipstack\sip_transport_connection.c(431)] [csf.sip-call-control] [sip_create_transport_connection] - [SIP][CONN][0] create TLS connection 10.10.10.10:5061-----10.10.10.1:5090. ## Sending register message 2020-03-30 13:03:19,200 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-sent---> REGISTER sip:10.10.10.1 SIP/2.0 Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00001188 From:

;tag=8823234512340890000003bdd-00005eff To:

Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Max-Forwards: 70 Date: Mon, 30 Mar 2020 11:03:19 GMT CSeq: 2270 REGISTER User-Agent: Cisco-CSF Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-config,X-cisco-sis-7.0.0,X-cisco-xsi-8.5.1,X-cisco-graceful-reg,X-cisco-duplicate-reg ## 407 Proxy Authentication Required 2020-03-30 13:03:19,310 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-recv<--- SIP/2.0 407 Proxy Authentication Required Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00001188 From:

;tag=8823234512340890000003bdd-00005eff To:

;tag=441122775 Date: Mon, 30 Mar 2020 11:03:31 GMT Call-ID: 88232345-12340017-

00001c0b-00000cfa@10.10.10.10 Server: Cisco-CUCM12.5 CSeq: 2270 REGISTER Proxy-Authenticate: Bearer realm="ccmsipline" Content-Length: 0 ## Register with OAuth token included in the Proxy-Authorization header 2020-03-30 13:03:19,310 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-sent---> REGISTER sip:10.10.10.1 SIP/2.0 Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00004a82 From:

;tag=882323451234089000003bdd-00005eff To:

Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Max-Forwards: 70 Date: Mon, 30 Mar 2020 11:03:19 GMT CSeq: 2271 REGISTER User-Agent: Cisco-CSF Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video Proxy-Authorization: Bearer token="

" Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-config,X-cisco-sis-7.0.0,X-cisco-xsi-8.5.1,X-cisco-graceful-reg,X-cisco-duplicate-reg Reason: SIP;cause=200;text="cisco-alarm:111 Name=CSFrado ActiveLoad=Jabber_for_Windows-12.8.0.51973 InactiveLoad=Jabber_for_Windows-12.8.0.51973 Last=Application-Requested-Destroy" Expires: 3600 Content-Type: multipart/mixed; boundary=uniqueBoundary Mime-Version: 1.0 Content-Length: 1271 # 200 OK for Register 2020-03-30 13:03:19,325 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-recv<--- SIP/2.0 200 OK Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00004a82 From:

;tag=882323451234089000003bdd-00005eff To:

;tag=1915868308 Date: Mon, 30 Mar 2020 11:03:31 GMT Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Server: Cisco-CUCM12.5 CSeq: 2271 REGISTER Expires: 120 Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video;x-cisco-newreg Supported: X-cisco-srtp-fallback,X-cisco-sis-9.1.0 Content-Type: application/x-c

Situación 1: discrepancia del puerto de registro de OAuth SIP

El dispositivo Jabber en las instalaciones en modo OAuth SIP no se puede registrar con UCM. UCM envía 403 para el mensaje Register (Registrar):

SIP/2.0 403 Forbidden Via: SIP/2.0/TLS 10.5.10.121:50347;branch=z9hG4bK00005163 From:

;tag=005056867e66010a00006698-00002a32 To:

;tag=1946377502 Date: Fri, 03 Aug 2018 05:00:18 GMT Call-ID: 00505686-7e660005-0000216b-0000366f@10.5.10.121 Server: Cisco-CUCM12.5 CSeq: 363 REGISTER Retry-After: 35 Warning: 399 UCM2-PUB "SIP OAuth Registration port Mismatch" Content-Length: 0

Posible solución: Asegúrese de que se cumplen las siguientes condiciones:

- El modo OAuth está habilitado globalmente
- El perfil de seguridad del dispositivo asociado al dispositivo tiene habilitada la compatibilidad con OAuth
- Mensaje recibido en el puerto 5090 sobre TLS en lugar de mTLS

Situación 2: CA desconocida de Expressway

Expressway-C no puede establecer el intercambio de señales mTLS con UCM en sipMARAOuthport (valor predeterminado 5091). Expressway-C no confía en el certificado compartido por UCM y responde con el mensaje CA desconocida durante la configuración de mTLS.

Posible solución: El servicio CallManager envía su certificado Tomcat durante el intercambio de señales mTLS. Asegúrese de que Expressway-C confía en el firmante del certificado Tomcat de UCM.

Situación 3: CA desconocida de UCM

Expressway-C no puede establecer el intercambio de señales mTLS con UCM en sipMARAOuthport (valor predeterminado 5091). UCM no confía en el certificado compartido por

Expressway y responde con el mensaje CA desconocida durante la configuración de mTLS.

Captura de paquetes de esta comunicación (UCM 10.x.x.198, Expressway-C 10.x.x.182):

Time	Source	Destination	Protocol	Source por	Destinati	Length	Info
11:16:29.659235	10.[redacted].182	10.[redacted].198	TCP	25161	5091	74	25161 → 5091 [SYN] Seq=0 Win=64240 Len=0 MSS=1
11:16:29.659609	10.[redacted].198	10.[redacted].182	TCP	5091	25161	74	5091 → 25161 [SYN, ACK] Seq=0 Ack=1 Win=28960
11:16:29.659627	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=1 Ack=1 Win=64256 Len=0
11:16:29.714501	10.[redacted].182	10.[redacted].198	TLSv1.2	25161	5091	260	Client Hello
11:16:29.715316	10.[redacted].198	10.[redacted].182	TCP	5091	25161	66	5091 → 25161 [ACK] Seq=1 Ack=195 Win=30080 Len
11:16:29.737063	10.[redacted].198	10.[redacted].182	TLSv1.2	5091	25161	1514	Server Hello
11:16:29.737091	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=195 Ack=1449 Win=64128
11:16:29.737137	10.[redacted].198	10.[redacted].182	TLSv1.2	5091	25161	1081	Certificate, Server Key Exchange, Certificate
11:16:29.737149	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=195 Ack=2464 Win=63488
11:16:29.753375	10.[redacted].182	10.[redacted].198	TLSv1.2	25161	5091	2878	Certificate, Client Key Exchange, Certificate
11:16:29.754116	10.[redacted].198	10.[redacted].182	TCP	5091	25161	66	5091 → 25161 [ACK] Seq=2464 Ack=3007 Win=35712
11:16:29.758710	10.[redacted].198	10.[redacted].182	TLSv1.2	5091	25161	73	Alert (Level: Fatal, Description: Unknown CA)
11:16:29.758743	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=3007 Ack=2471 Win=64128
11:16:29.758780	10.[redacted].198	10.[redacted].182	TCP	5091	25161	66	5091 → 25161 [RST, ACK] Seq=2471 Ack=3007 Win=

Posible solución: UCM utiliza el almacén de confianza de Tomcat para verificar los certificados entrantes durante el intercambio de señales mTLS en los puertos OAuth SIP. Asegúrese de que el certificado del firmante para Expressway-C esté cargado correctamente en UCM.

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).