Habilitar ActiveControl sobre MRA/Expressway

Contenido

Introducción

Este documento describe las diferentes opciones para habilitar el protocolo ActiveControl para clientes de acceso móvil y remoto (MRA) y para llamadas desde terminales en las instalaciones a Webex Meetings a través de Expressway. MRA es una solución de implementación para la capacidad de terminales y Jabber sin red privada virtual (VPN). Esta solución permite a los usuarios finales conectarse a recursos internos de la empresa desde cualquier lugar del mundo. El protocolo ActiveControl es un protocolo propiedad de Cisco que permite una experiencia de conferencia más enriquecedora con funciones en tiempo de ejecución como listas de reuniones, cambios de diseño de vídeo, opciones de silencio y grabación.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Expressway (llamadas MRA y B2B)

Componentes Utilizados

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

- Expressway X12.5
- Cisco Meeting Server (CMS) 2.9
- Cisco Unified Communications Manager 12.5

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.

Antecedentes

En este documento, el enfoque principal se centra en la conexión del cliente MRA a Cisco Meeting Server (CMS), pero lo mismo se aplica a otros tipos de plataformas o conexiones, como por ejemplo, cuando se conecta a Webex Meetings. La misma lógica se puede aplicar para el siguiente tipo de flujos de llamadas:

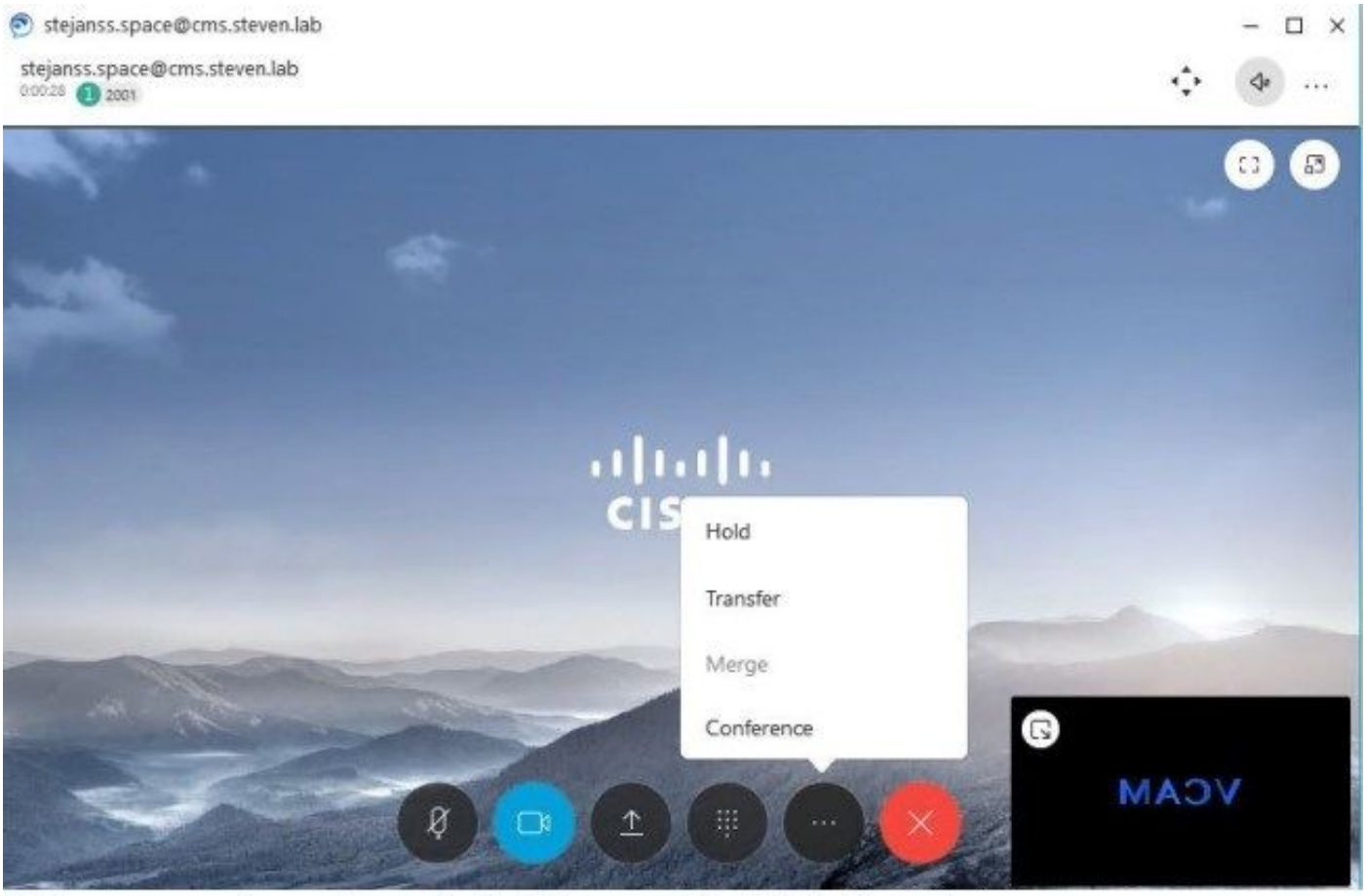
- Terminal - CUCM - Expressway-C - Expressway-E - Reunión Webex
- Terminal MRA - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Reunión Webex

  Nota: las funciones de ActiveControl admitidas por Webex Meetings son diferentes a las de CMS en este momento y son solo un subconjunto limitado.

La plataforma Cisco Meeting Server ofrece a los participantes de la reunión la posibilidad de controlar su experiencia de reunión directamente desde su terminal de conferencia a través de ActiveControl sin necesidad de aplicaciones u operadores externos. ActiveControl utiliza el protocolo de medios iX en dispositivos Cisco y se negocia como parte de la mensajería SIP de una llamada. A partir de la versión 2.5 de CMS, las principales funciones habilitadas son las siguientes (aunque pueden depender del tipo de terminal y de la versión de software en uso):

- Visualización de una lista de todos los participantes (lista o lista de participantes) conectados a la reunión
- Silenciar o dejar de silenciar a otros participantes
- Agregar o quitar otro participante de la reunión
- Iniciar o detener la grabación de una reunión
- Hacer que un participante sea importante
- Indicador para el participante que es el orador activo en la reunión
- Indicador para el participante que comparte actualmente contenido o presentación en la reunión
- Bloqueo o desbloqueo de la reunión

En la primera imagen se ve una vista de usuario de un cliente Jabber que colocó una llamada en un espacio CMS sin ActiveControl, mientras que la segunda imagen muestra la vista de usuario más rica en funciones donde Jabber ha podido negociar ActiveControl con el servidor CMS.



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl es un protocolo basado en XML que se transfiere mediante el protocolo iX que se negocia en el protocolo de descripción de sesión (SDP) de las llamadas del protocolo de inicio de sesión (SIP). Se trata de un protocolo de Cisco (eXtensible Conference Control Protocol (XCCP)) y se negocia solo en SIP (de modo que las llamadas interconectadas no tienen ActiveControl) y aprovecha UDP/UDT (UDP-based Data Transfer Protocol) para la transferencia de datos. La negociación segura se realiza a través de la TLS de datagrama (DTLS) que se puede considerar

como TLS en una conexión UDP. Aquí se muestran algunos ejemplos de las diferencias en la negociación.

Sin Cifrar

m=application xxxxx UDP/UDT/IX *****
a=ixmap:11 **xccp**

Cifrado (lo mejor que puede hacer es probar el cifrado, pero permitir el repliegue a una conexión no cifrada)

m=application xxxx UDP/UDT/IX *****

a=ixmap:2 **xccp**

a=**huella dactilar**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

Cifrado (forzar cifrado: no permitir el repliegue a una conexión no cifrada)

m=application xxxx UDP/**DTLS**/UDT/IX *****

a=ixmap:2 **xccp**

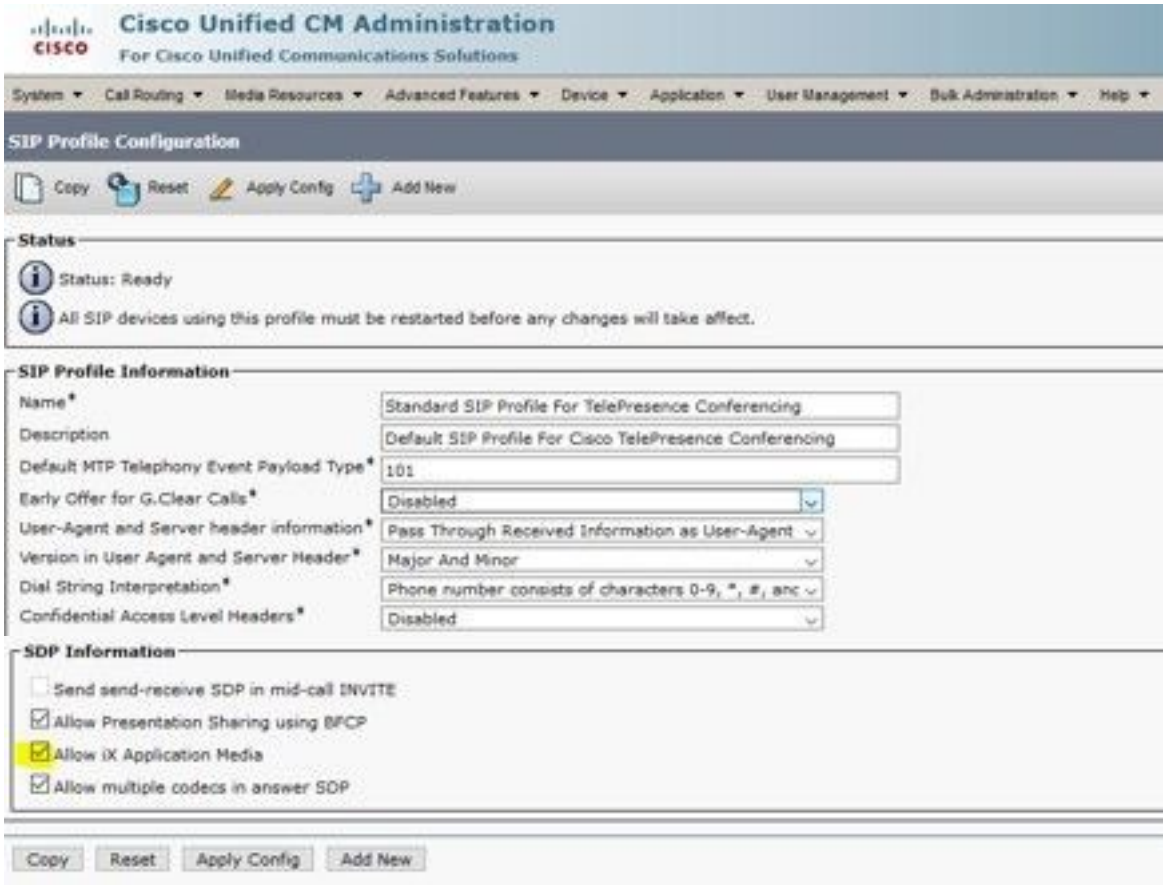
a=**huella dactilar**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

Existen algunas versiones de software mínimas requeridas para la compatibilidad total con ActiveControl como se indica a continuación:

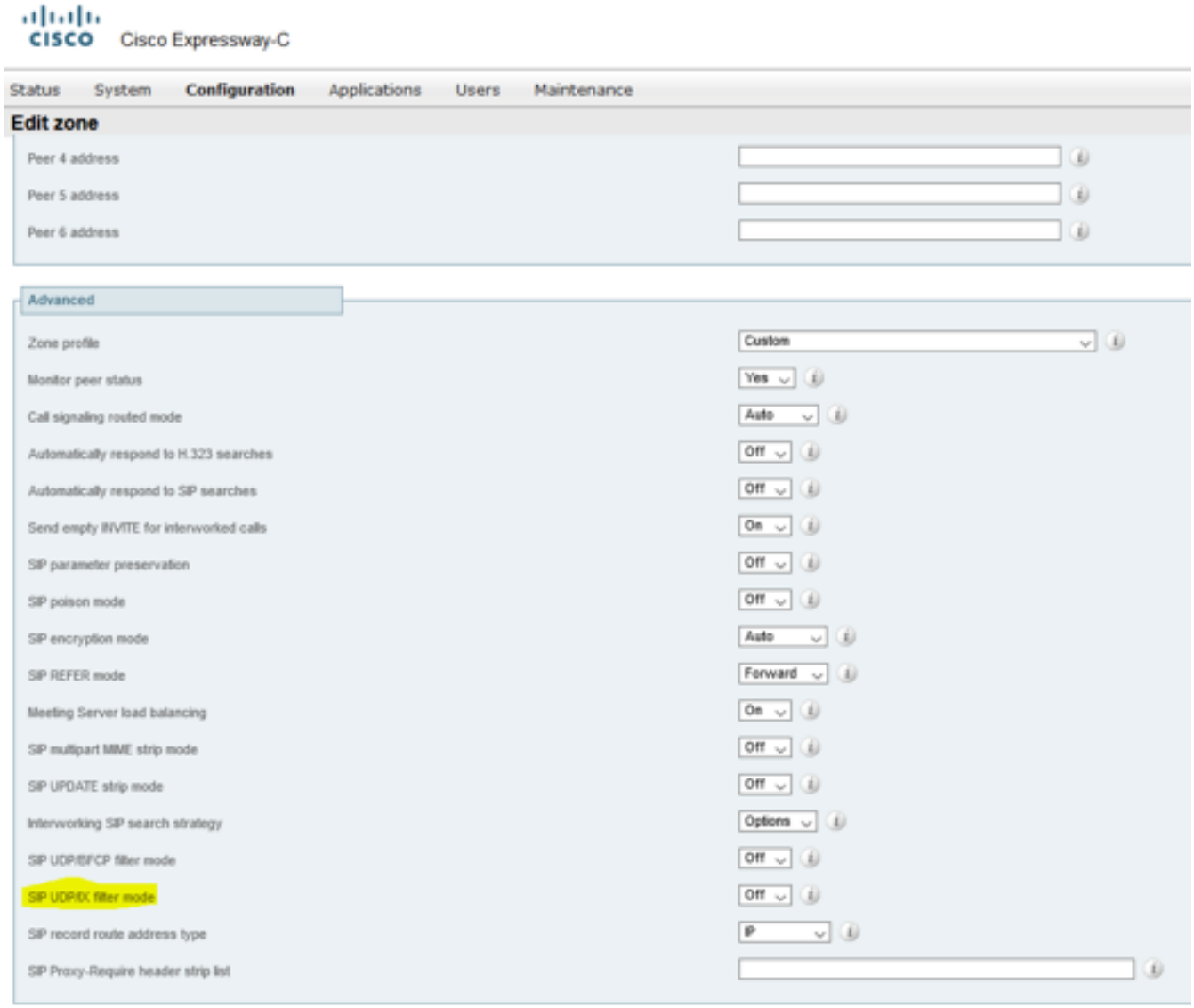
- Jabber versión 12.5 o posterior (notas de la versión)
- Terminales CE 8.3 o posterior, 9.6.2 o posterior recomendados según la Guía de control activo de CMS (CE9.3.1 o posterior para Webex según el enlace de ayuda de Webex)
- CUCM 10.5 o posterior (para compatibilidad con Jabber 12.5 ActiveControl) (11.5(1) o posterior para Webex según el enlace)
- Se recomienda CMS 2.1 o posterior, 2.5 o posterior según la guía de control activo de CMS
- Expressway X12.5 o posterior (notas de la versión) para permitir la compatibilidad en clientes MRA no cifrados

Hay algunas opciones de configuración que se deben tener en cuenta:

- En CUCM, asegúrese de que los enlaces troncales SIP relevantes (a Expressway-C y CMS) estén configurados con un perfil SIP que tenga activada la opción 'Permitir medios de aplicación iX'



- En CMS está habilitado de forma predeterminada a partir de 2.1, pero puede inhabilitarlo a través de un CompatibilityProfile en el que puede establecer *sipUDT* en false
- En Expressway, en la configuración de zona en la configuración avanzada (cuando se usa un perfil de zona "personalizado"), asegúrese de que el *modo de filtro UDP/IX SIP* esté configurado en "Desactivado" si desea permitir que iX pase



Problema

Información general

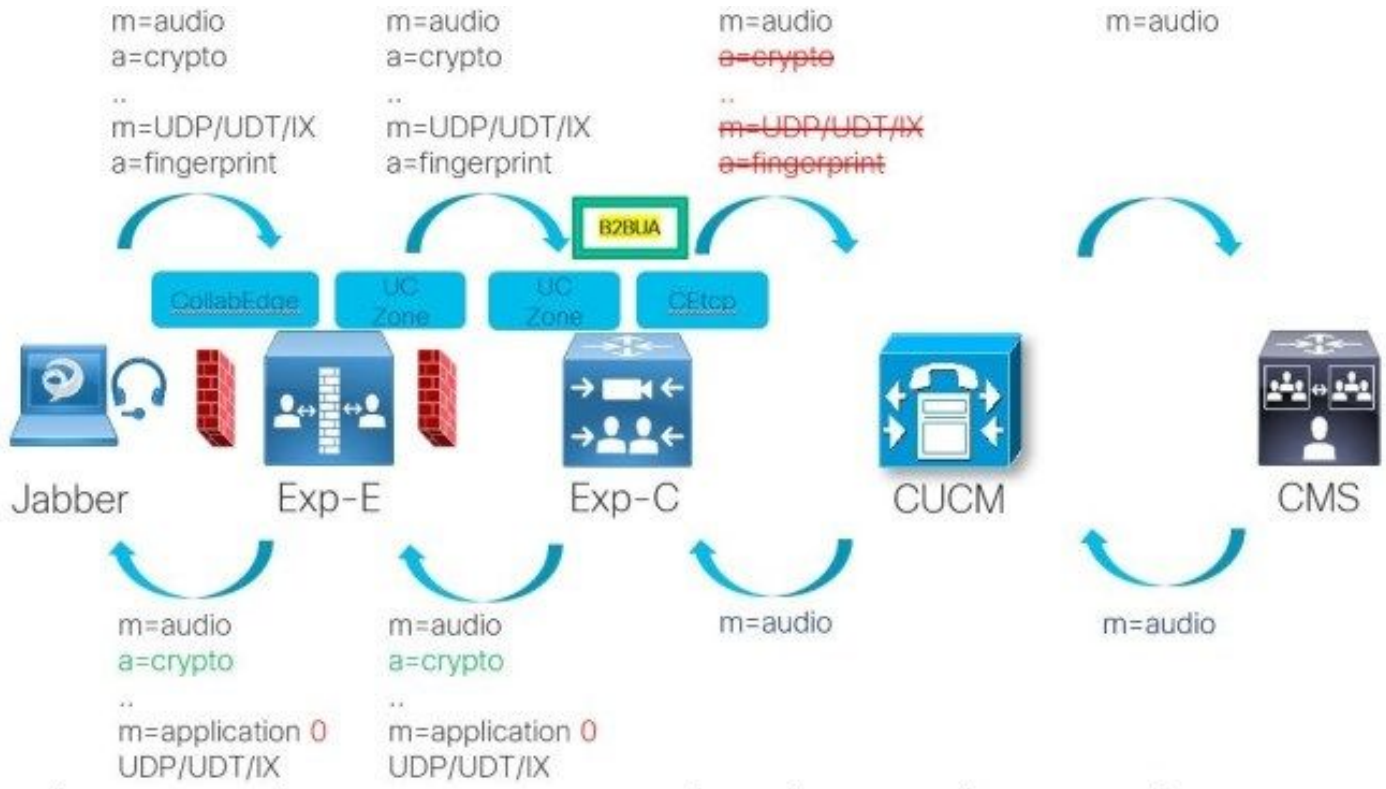
ActiveControl se está negociando de forma segura de forma diferente que otros canales de medios. Para otros canales de medios como el audio y el video, por ejemplo, el SDP se agrega con líneas crypto que se utilizan para anunciar al partido remoto la clave de encripción que se utilizará para este canal. Por lo tanto, el canal del protocolo de transporte en tiempo real (RTP) se puede hacer seguro y, por tanto, se puede considerar como RTP seguro (SRTP). Para el canal iX, utiliza el protocolo DTLS para cifrar la secuencia de medios XCCP de modo que utilice un mecanismo diferente.

El software Expressway no finaliza el protocolo DTLS. Esto se indica en la sección *Limitaciones* en *Funcionalidad no admitida* de las notas de la versión de Expressway.

- Expressway does not terminate DTLS. We do not support DTLS for securing media and SRTP is used to secure calls. Attempts to make DTLS calls through Expressway will fail. The DTLS protocol is inserted in the SDP but only for traversing the encrypted iX protocol.

Versiones de Expressway anteriores a X12.5

Cuando se ejecuta una versión de Expressway anterior a X12.5, si hay una conexión entrante con un canal iX cifrado que pasa a través de una zona TCP no segura, Expressway elimina las líneas criptográficas de los canales multimedia normales así como todo el canal iX. Esto se muestra visualmente para un cliente de MRA que se conecta a un espacio CMS donde se ve que la conexión es segura desde el cliente de MRA a Expressway-C pero luego, dependiendo del perfil de seguridad del teléfono configurado en CUCM para el dispositivo, o bien no está cifrado (y se envía a través de la zona CEtcp) o cifrado (y se envía a través de la zona CEtls). Cuando no está cifrado como se muestra en la imagen, verá que Expressway-C elimina las líneas criptográficas para todos los canales de medios e incluso elimina todo el canal de medios iX porque no puede terminar el protocolo DTLS. Esto sucede a través del agente de usuario back-to-back (B2BUA) porque la configuración de zona para la zona CEtcp se configura con el cifrado de medios 'Forzar descifrado'. En la dirección opuesta (sobre la zona transversal de UC con cifrado de medios 'Forzar cifrado') cuando se recibe la respuesta SDP, agrega las líneas criptográficas para las líneas de medios normales y pone a cero el puerto para el canal iX, lo que resulta en una negociación de ActiveControl. Internamente, cuando los clientes se registran directamente en CUCM, permite tanto canales de medios iX cifrados como no cifrados, ya que CUCM no se está colocando en la ruta de medios.



Media negotiation when using Expressway versions lower than X12.5 and CEtcp SIP trunk

El mismo tipo de lógica se aplica a las conexiones de llamadas de Expressway a Webex Meetings. Requiere que la ruta completa sea segura de extremo a extremo ya que los servidores de Expressway (antes de X12.5) solo pasan por la información de conexión DTLS pero no terminan en ella ellos mismos para iniciar una nueva sesión o para cifrar/descifrar el canal de medios en los diferentes tramos de llamada.

Versiones de Expressway de X12.5 y posteriores

Cuando se ejecuta una versión de Expressway de X12.5 o superior, el comportamiento ha cambiado, ya que ahora pasa por el canal iX a través de la conexión de zona TCP como cifrado forzado (UDP/DTLS/UDT/IX) para que pueda seguir negociando el canal iX, pero solo cuando el extremo remoto también utiliza cifrado. Aplica el cifrado porque Expressway no finaliza la sesión

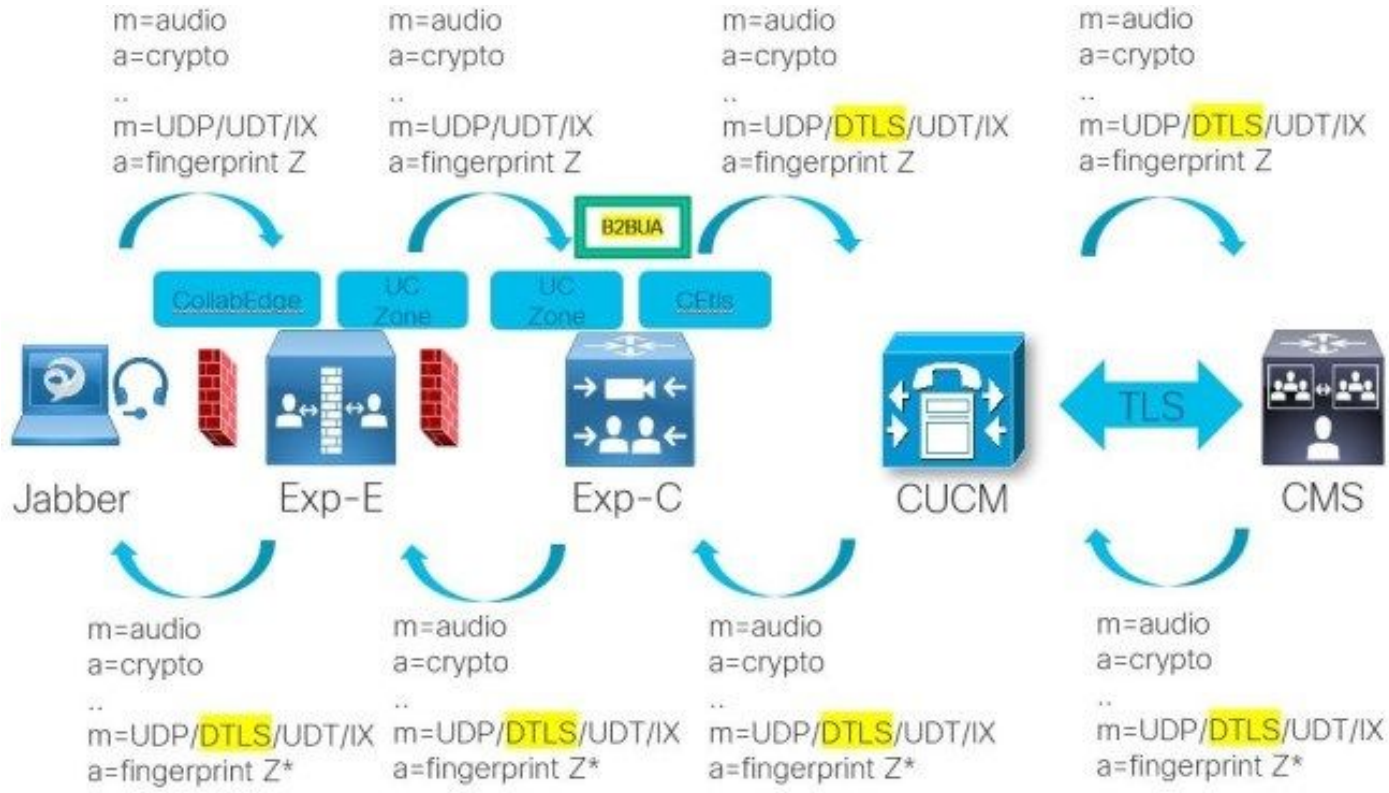
DTLS y, por lo tanto, solo actúa en el paso a través, por lo que depende del extremo remoto para iniciar o finalizar la sesión DTLS en ese momento. Las líneas criptográficas se eliminan a través de la conexión TCP por motivos de seguridad. Este cambio de comportamiento se trata en las notas de la versión según la sección de 'MRA: Support for Encrypted iX (for ActiveControl)'. Lo que sucede después de eso, depende de la versión de CUCM, ya que ese comportamiento cambió en 12.5(1)SU1, donde permite pasar a través del canal iX, así como en conexiones entrantes no seguras. Incluso cuando hubiera un troncal SIP de TLS seguro a CMS, cuando se ejecuta la versión de CUCM inferior a 12.5(1)SU1, se eliminaría el canal iX antes de pasarlo a CMS, lo que finalmente resultaría en un puerto de salida a cero de CUCM a Expressway-C.

MRA: Support for Encrypted iX (for ActiveControl)

ActiveControl over MRA is already supported with encrypted phone profiles. This feature will allow MRA video endpoints and Jabber clients with non-secure phone security profiles to negotiate ActiveControl so that users can see roster lists, layouts, and other iX-dependent ActiveControl features in video meetings.

There are no configuration or interface changes for this feature. However, you may need to rediscover your Cisco Unified Communications Manager servers after you upgrade the Expressway.

Con una ruta de medios y señalización de llamadas segura de extremo a extremo, el canal iX se puede negociar directamente (a través de diferentes saltos de servidores Expressway) entre el cliente (MRA) y la solución de conferencias (CMS o Webex Meeting). La imagen muestra el mismo flujo de llamadas para el cliente MRA que se conecta a un espacio CMS, pero ahora con un perfil de seguridad de teléfono seguro configurado en CUCM y un enlace troncal SIP de TLS seguro a CMS. Puede ver que la trayectoria es segura de extremo a extremo y que el parámetro de huella dactilar DTLS se pasa por encima de toda la trayectoria.

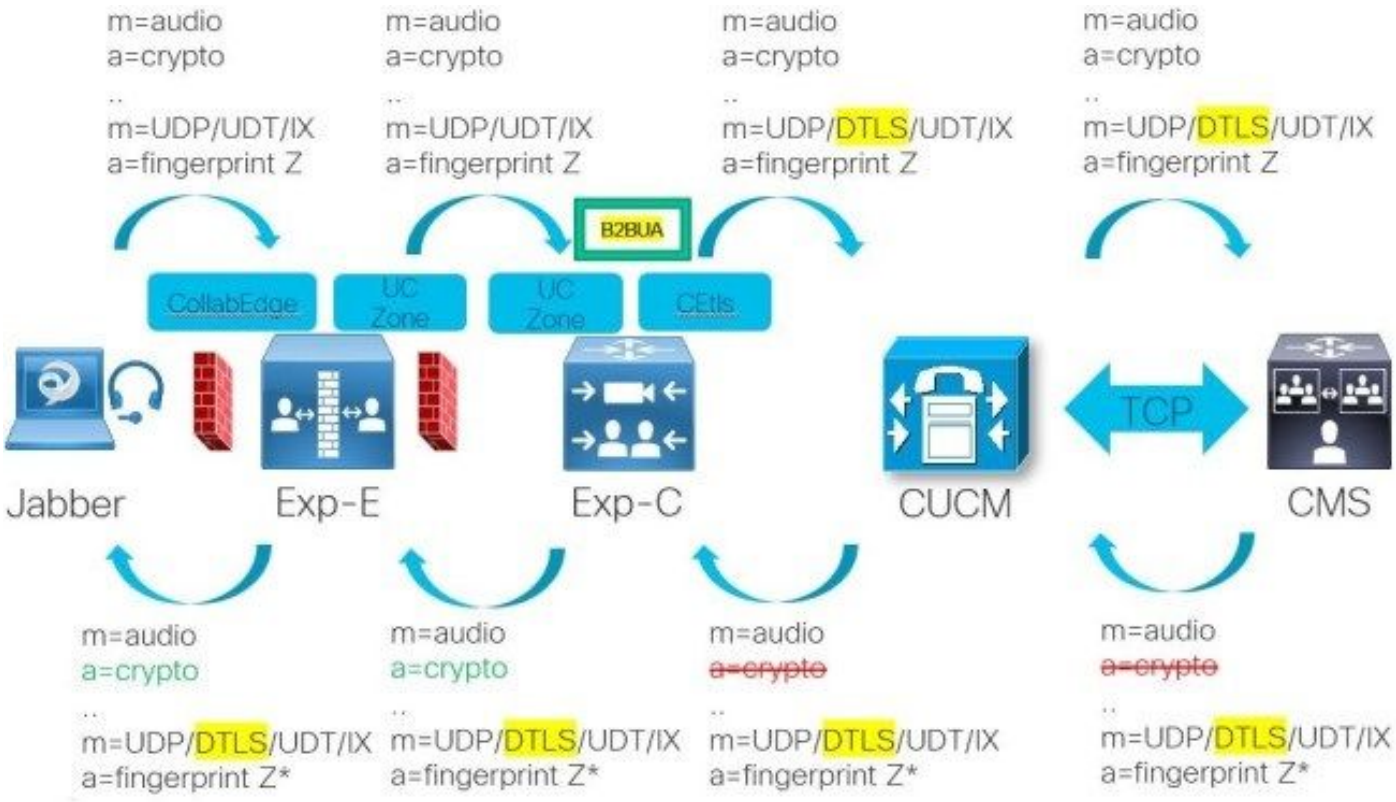


Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

Para configurar un perfil de seguridad de dispositivo seguro, debe asegurarse de que CUCM se configura en modo mixto y esto puede ser un proceso engorroso (también cuando está operativo, ya que requiere Certificate Authority Proxy Function (CAPF) para las comunicaciones seguras en las instalaciones). Por lo tanto, aquí se pueden ofrecer otras soluciones más convenientes para admitir la disponibilidad de ActiveControl sobre MRA y Expressway en general, como se describe

en este documento.

Los enlaces troncales SIP de TLS seguros a los servidores CMS no son necesarios porque CUCM (suponiendo que el enlace troncal SIP tenga la opción SRTP permitido) siempre pasa de una conexión SIP segura entrante al canal iX, así como a las líneas criptográficas, pero CMS solo responde con cifrado al canal iX (permitiendo ActiveControl) (suponiendo que el **cifrado de medios SIP** está configurado en *permitido* o forzado en CMS en Configuración > Configuración de llamada), pero no tiene cifrado en los otros canales multimedia ya que quita las líneas criptográficas de ellos como por la imagen. Los servidores de Expressway pueden agregar las líneas criptográficas nuevamente para asegurar esa parte de la conexión todavía (e iX se negocia directamente entre los clientes finales aún a través de DTLS), pero esto no es ideal desde un punto de vista de seguridad y por lo tanto se recomienda configurar un troncal SIP seguro al puente de conferencia. Cuando **SRTP Allowed** no se verifica en el troncal SIP, CUCM quita las líneas crypto y la negociación segura de iX también falla.



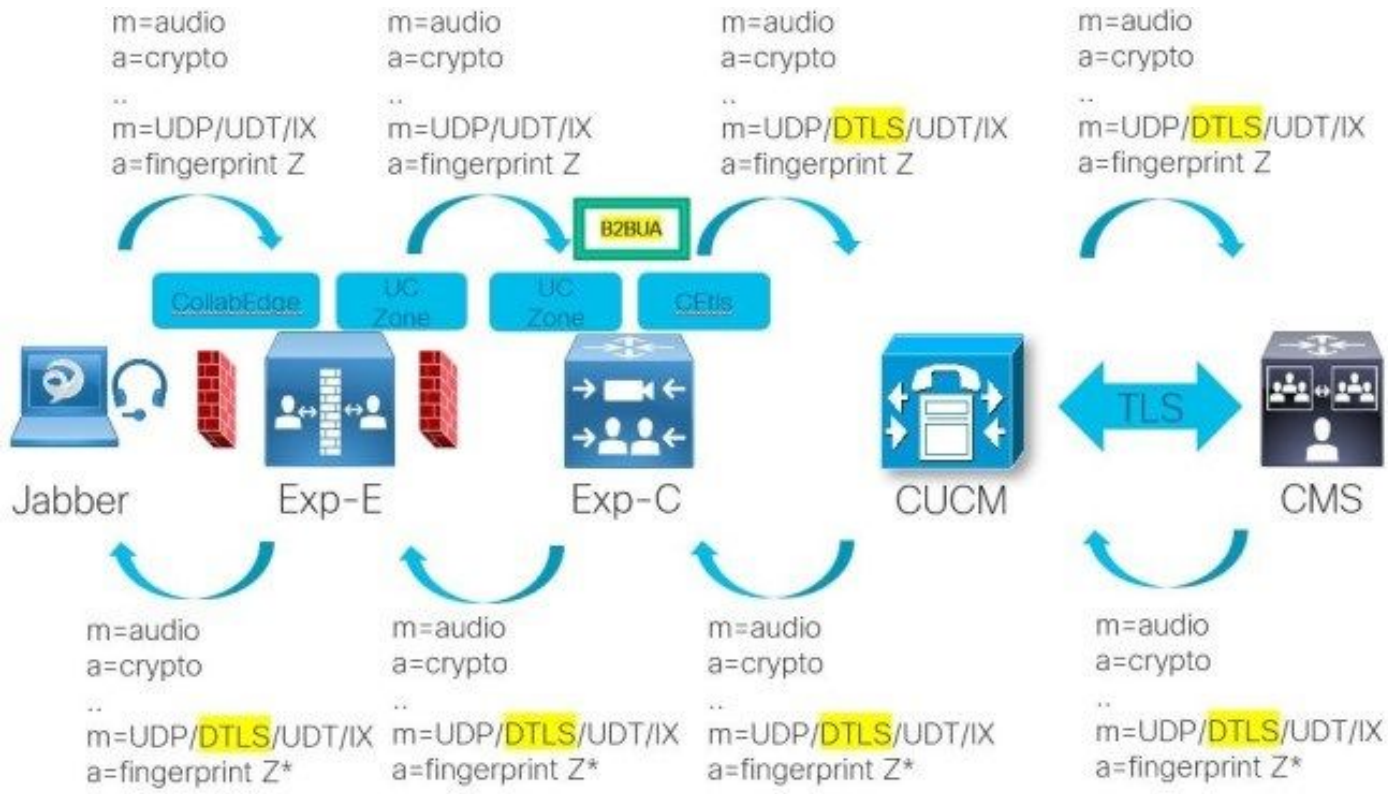
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

Solución

Hay un par de opciones diferentes disponibles con varios requisitos y varios pro y contra. Cada uno de ellos se presenta en una sección más detallada. Las diferentes opciones son:

1. Perfiles de seguridad de teléfonos seguros para los terminales (CUCM de modo mixto)
2. SIP OAuth para Jabber
3. Canal iX cifrado para perfiles de seguridad telefónica no seguros (CUCM 12.5(1)SU1 o superior)

Solución 1: perfiles de seguridad telefónica seguros para los terminales (CUCM de modo mixto)



Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

Requisitos previos:

- CUCM en modo mixto

Pro:

- Funciona en cualquier versión de CUCM
- Funciona para todos los dispositivos cliente

Con:

- Requiere la configuración de CUCM en modo mixto (y operaciones CAPF en terminales en las instalaciones)

Este es el método que se describe en la sección Problema, así como al final, donde se garantiza que tiene una señalización de llamada cifrada de extremo a extremo y una ruta de medios. Requiere que CUCM se configure en modo mixto según el siguiente documento.

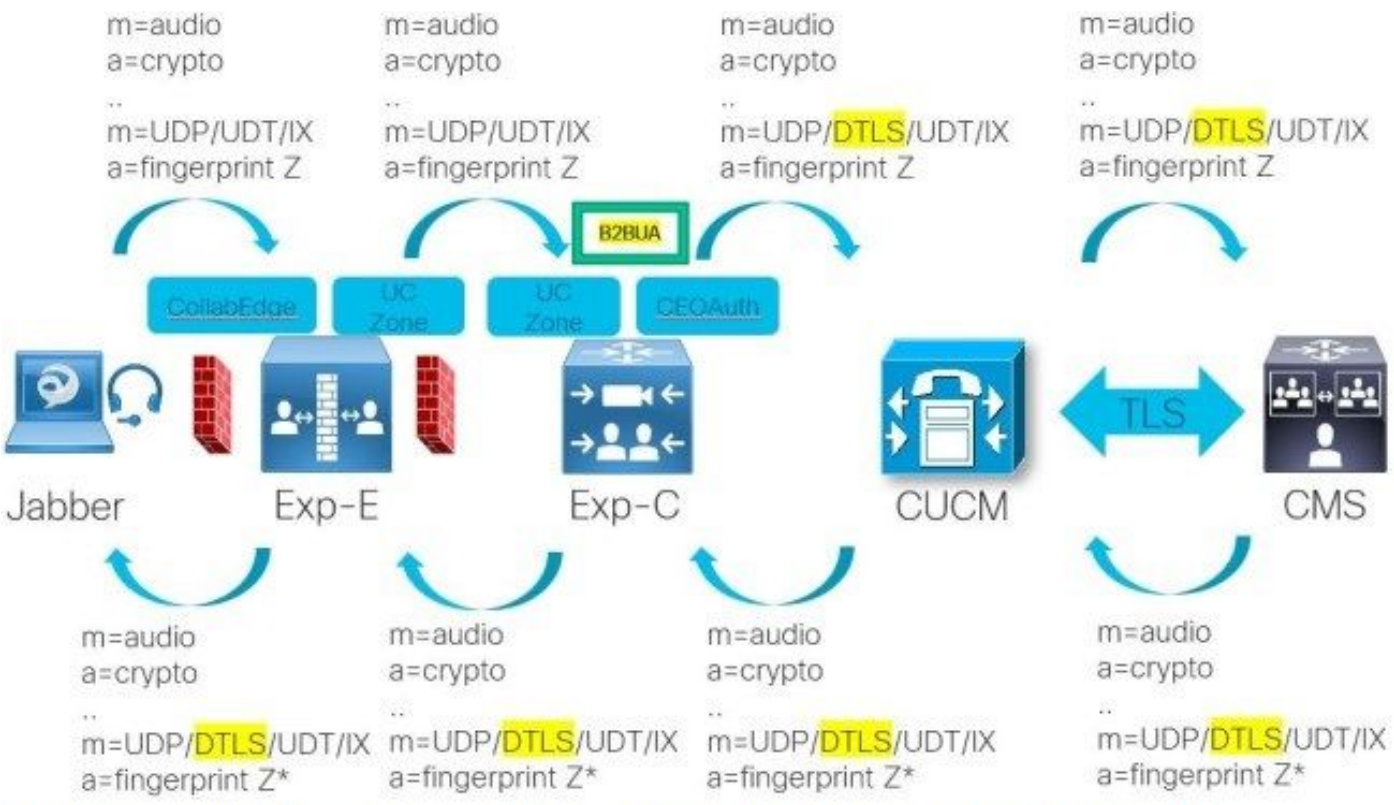
Para los clientes de MRA, no se requiere ninguna operación de CAPF, pero asegúrese de seguir los pasos de configuración adicionales con el perfil de seguridad del teléfono seguro con un nombre que coincida con uno de los nombres alternativos de asunto del certificado de servidor de Expressway-C, como se resalta en el Ejemplo de configuración de terminales basados en TC de Collaboration Edge (que también se aplica para los terminales basados en CE y los clientes Jabber).

Al conectarse desde un terminal en las instalaciones o un cliente Jabber a una reunión Webex, debe realizar la operación CAPF para registrar de forma segura el cliente en CUCM. Esto es necesario para garantizar el flujo de llamadas seguras de extremo a extremo en el que Expressway solo puede pasar por la negociación DTLS y no manejarse en ella misma.

Para que la llamada sea segura de extremo a extremo, asegúrese también de que todos los troncales SIP relevantes (a Expressway-C en caso de llamada a una reunión Webex y a CMS en

caso de llamada a una conferencia CMS) sean troncales SIP seguros mediante TLS con un perfil de seguridad de troncal SIP seguro.

Solución 2: SIP OAuth para Jabber



Media negotiation when using Expressway and CEOAuth SIP trunk with TLS SIP trunk to CMS

Requisitos previos:

- Cisco Jabber 12.5 o superior (notas de la versión)
- CUCM versión 12.5 o superior (notas de la versión) con *OAuth con flujo de inicio de sesión de actualización* habilitado
- Expressway X12.5.1 o superior (notas de la versión) con *autorización por token de OAuth con actualización* habilitada

Pro:

- Permite realizar registros seguros y cambiar fácilmente entre las instalaciones y las instalaciones sin tener que renovar CAPF cada vez.
- No es necesario configurar CUCM en modo mixto

Con:

- Solo aplicable a Jabber, no aplicable a terminales TC/CE

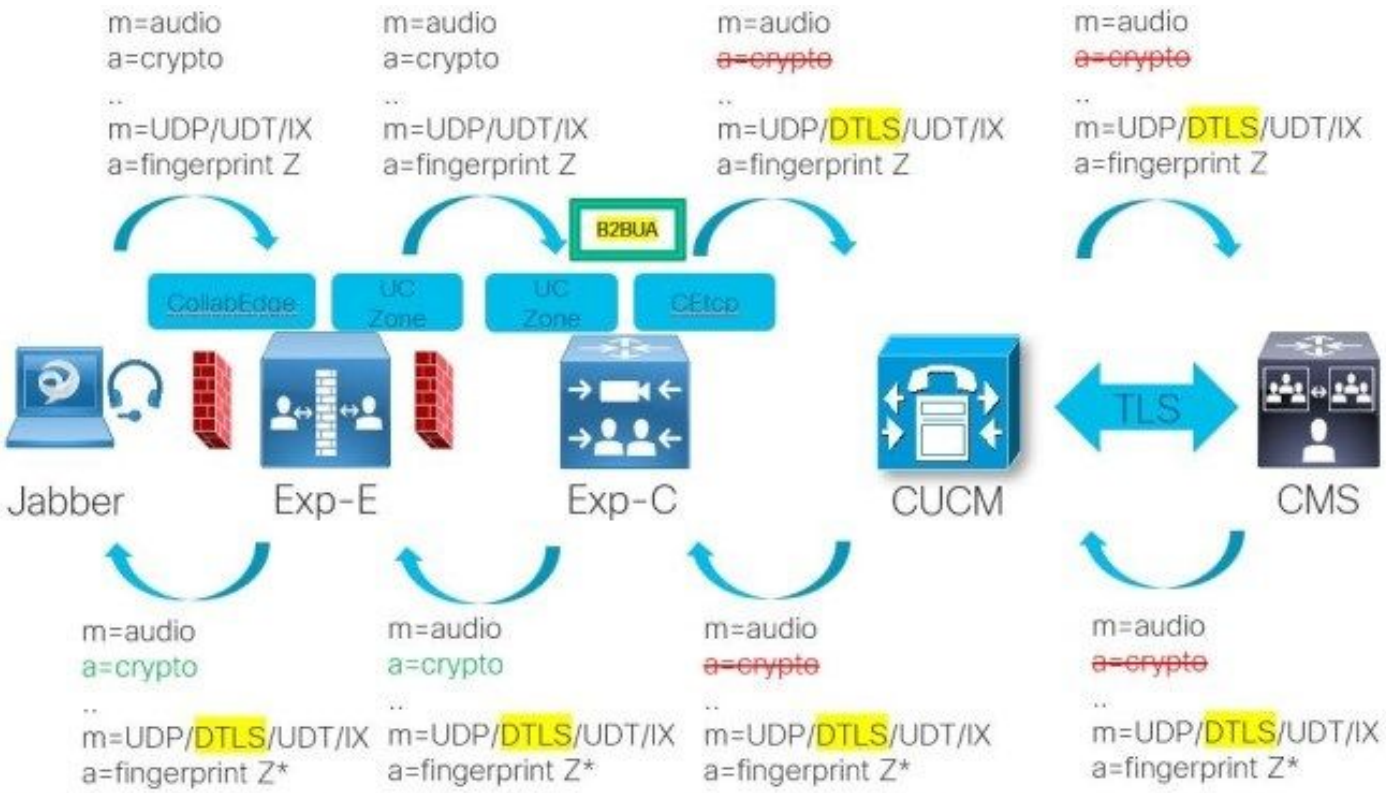
El modo OAuth de SIP permite utilizar tokens de actualización de OAuth para la autenticación de Cisco Jabber en entornos seguros. Permite una señalización y medios seguros sin los requisitos de CAPF de la solución 1. La validación de token durante el registro SIP se completa cuando se habilita la autorización basada en OAuth en el clúster de CUCM y los terminales de Jabber.

La configuración en CUCM se documenta en la guía de configuración de funciones y requiere que ya tenga habilitado OAuth con el flujo de inicio de sesión de actualización en Parámetros empresariales. Para habilitar esto también a través de MRA, asegúrese de actualizar los nodos de

CUCM en el servidor de Expressway-C en **Configuración > Unified Communication > Servidores de Unified CM** de modo que en **Configuración > Zonas > Zonas** ahora también debe ver las zonas de CEOAuth creadas automáticamente. Asegúrese también de que en **Configuration > Unified Communication > Configuration** that **Authorize by OAuth token with refresh** esté habilitado también.

Con esta configuración, puede lograr una conexión de llamada segura de extremo a extremo similar tanto para la señalización como para los medios y, por lo tanto, Expressway solo pasa por la negociación DTLS ya que no finaliza ese tráfico en sí. Esto se observa en la imagen, donde la única diferencia en comparación con la solución anterior es que utiliza la zona CEOAuth en Expressway-C para CUCM en lugar de la zona CEtls porque utiliza SIP OAuth en lugar del registro de dispositivo seguro sobre TLS cuando CUCM funciona en modo mixto con un perfil de seguridad de teléfono seguro, pero aparte de eso, todo sigue igual.

Solución 3: canal iX cifrado para perfiles de seguridad telefónica no seguros (CUCM 12.5(1)SU1 o superior)



Media negotiation when using Expressway on version higher than X12.5 and CEtcp SIP trunk to CUCM running a version of 12.5(1)SU1 or higher and a TLS SIP trunk to CMS

Requisitos previos:

- CUCM versión 12.5(1)SU1 o superior (notas de la versión)
- Expressway X12.5.1 o superior (notas de la versión)

Pro:

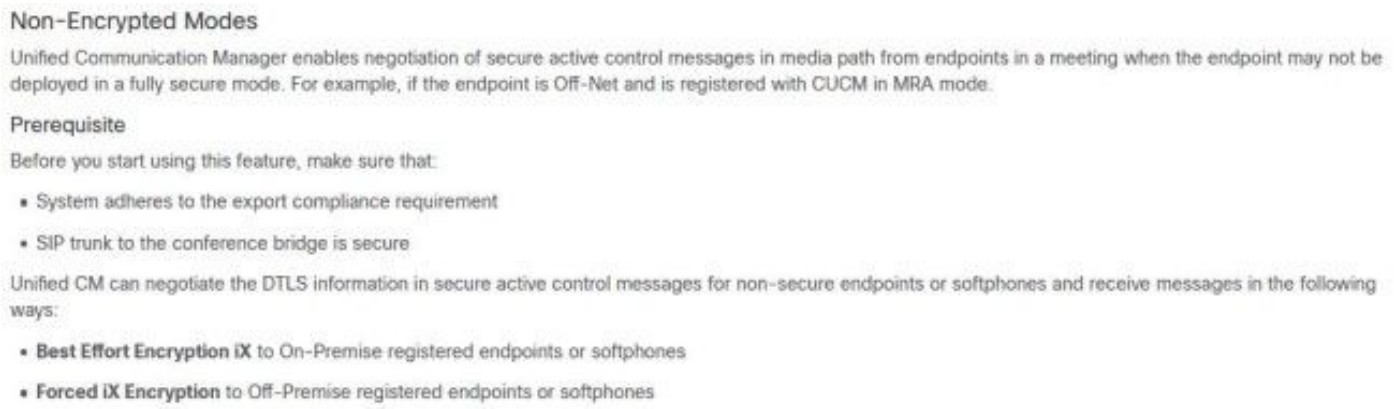
- No es necesario configurar CUCM en modo mixto
- No es necesario configurar comunicaciones seguras de extremo a extremo
- Aplicable a los terminales Jabber y TC/CE

Con:

- Se requiere actualización de CUCM
- Solo se admiten versiones restringidas de CUCM

A partir de CUCM 12.5(1)SU1, admite la negociación de cifrado iX para cualquier dispositivo de línea SIP, de modo que puede negociar la información DTLS en mensajes ActiveControl seguros para terminales o softphones no seguros. Envía cifrado iX mediante TCP en el mejor de los casos, lo que permite que los teléfonos tengan un canal iX cifrado de extremo a extremo a pesar de tener una conexión TCP no segura (no TLS) con CUCM.

En la guía de seguridad de CUCM 12.5(1)SU1 en la sección de "Canal iX cifrado", se muestra que para los modos no cifrados con dispositivos no seguros, se puede negociar el mejor esfuerzo y el cifrado iX forzado con el requisito previo de que el sistema cumpla con la normativa de exportación y que el troncal SIP del puente de conferencia sea seguro.



Non-Encrypted Modes

Unified Communication Manager enables negotiation of secure active control messages in media path from endpoints in a meeting when the endpoint may not be deployed in a fully secure mode. For example, if the endpoint is Off-Net and is registered with CUCM in MRA mode.

Prerequisite

Before you start using this feature, make sure that:

- System adheres to the export compliance requirement
- SIP trunk to the conference bridge is secure

Unified CM can negotiate the DTLS information in secure active control messages for non-secure endpoints or softphones and receive messages in the following ways:

- **Best Effort Encryption iX** to On-Premise registered endpoints or softphones
- **Forced iX Encryption** to Off-Premise registered endpoints or softphones

En CUCM:

- Debe utilizar CUCM con exportación restringida (no sin restricción)
- En **System > Licensing > License Management**, debe tener "Export-Controlled Functionality" (Función de exportación controlada) establecido en allowed (permitida).
- Su troncal SIP debe tener la opción "**SRTP Allowed**" habilitada (independientemente de si el troncal en sí es seguro o no)

En CMS:

- El callbridge debe tener una licencia con cifrado (por lo que no tiene una licencia de callBridgeNoEncryption)
- En webadmin, en **Configuration > Call Settings**, debe haber configurado **SIP media encryption** en **allowed** (o **required**)

En la imagen, puede ver que la conexión es segura hasta que Expressway-C y luego C envía a través del SDP a CUCM sin las líneas criptográficas, pero sí incluye el canal de medios iX. Por lo tanto, los medios normales para audio/vídeo/... no están protegidos con líneas criptográficas, pero tienen una conexión segura para el canal de medios iX ahora, de modo que Expressway no necesita terminar la conexión DTLS. Por lo tanto, ActiveControl se puede negociar directamente entre el cliente y el puente de conferencia, incluso con un perfil de seguridad de teléfono no seguro. En versiones anteriores de CUCM, el flujo sería diferente y ActiveControl no se negocia porque no pasa por el canal iX al CMS en primer lugar, ya que esa parte ya se habría eliminado.

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).