Activer ActiveControl sur MRA/Expressway

Table des matières

Introduction

Ce document décrit les différentes options pour activer le protocole ActiveControl pour les clients Mobile and Remote Access (MRA) et pour les appels des terminaux sur site aux réunions Webex via Expressway. MRA est une solution de déploiement pour la fonctionnalité Jabber et les terminaux VPN (Virtual Private Network-less). Cette solution permet aux utilisateurs finaux de se connecter aux ressources internes de l'entreprise où qu'ils se trouvent dans le monde. Le protocole ActiveControl est un protocole propriétaire de Cisco qui offre une expérience de conférence plus riche grâce à des fonctionnalités d'exécution telles que les listes de présence, les modifications de la présentation vidéo, le mode silencieux et les options d'enregistrement.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expressway (appels MRA et B2B)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Expressway X12.5
- Serveur de réunion Cisco (CMS) 2.9
- Cisco Unified Communications Manager 12.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Dans ce document, l'accent est mis sur la connexion du client MRA à un serveur de réunion Cisco (CMS), mais la même chose s'applique à d'autres types de plates-formes ou de connexions comme par exemple lors de la connexion à des réunions Webex. La même logique peut être appliquée aux types de flux d'appels suivants :

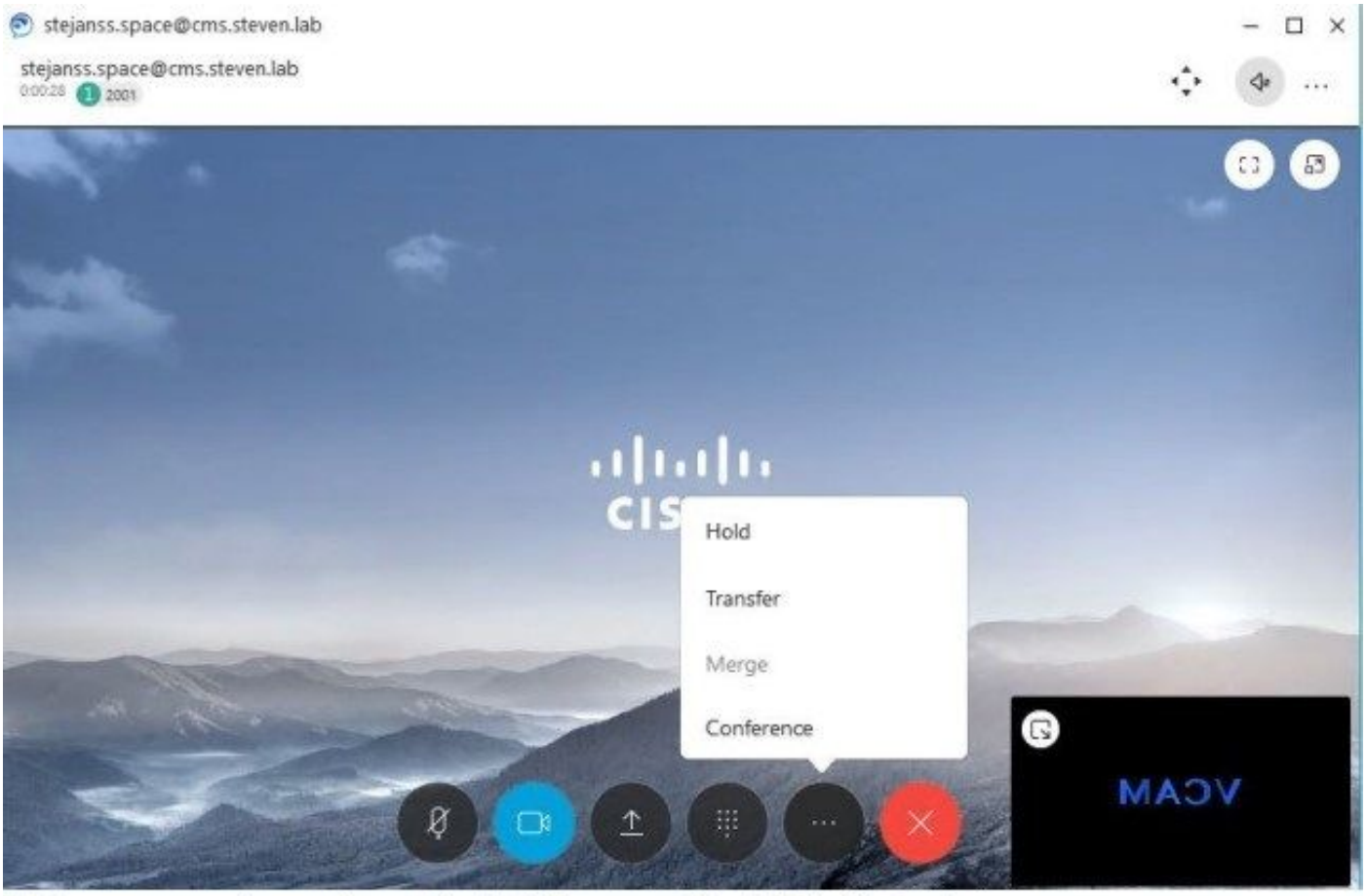
- Terminaux - CUCM - Expressway-C - Expressway-E - Webex Meeting
- Terminal MRA - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Webex Meeting

  Remarque : les fonctionnalités d'ActiveControl prises en charge par Webex Meetings sont différentes de celles de CMS à l'heure actuelle et ne constituent qu'un sous-ensemble limité.

La plate-forme Cisco Meeting Server offre aux participants la possibilité de contrôler leur expérience de réunion directement depuis leur terminal de conférence via ActiveControl, sans qu'il soit nécessaire de recourir à des applications ou opérateurs externes. ActiveControl utilise le protocole multimédia iX dans les périphériques Cisco et est négocié dans le cadre de la messagerie SIP d'un appel. Depuis la version 2.5 de CMS, les principales fonctionnalités activées sont les suivantes (bien qu'elles puissent dépendre du type de terminal et de la version logicielle utilisée) :

- Affichage de la liste de tous les participants (liste de participants ou liste de participants) connectés à la téléconférence
- Mise en sourdine ou désactivation des autres participants
- Ajout ou suppression d'un autre participant à la téléconférence
- Démarrage ou arrêt de l'enregistrement d'une téléconférence
- Rendre un participant important
- Indicateur pour le participant qui est l'intervenant actif dans la téléconférence
- Indicateur pour le participant qui partage actuellement du contenu ou une présentation dans la téléconférence
- Verrouillage ou déverrouillage de la téléconférence

Sur la première image, vous voyez une vue utilisateur d'un client Jabber qui a passé un appel dans un espace CMS sans ActiveControl tandis que la seconde image vous montre la vue utilisateur plus riche en fonctionnalités où Jabber a pu négocier ActiveControl avec le serveur CMS.



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl est un protocole XML qui est transféré à l'aide du protocole iX négocié dans le protocole SDP (Session Description Protocol) des appels SIP (Session Initiation Protocol). Il s'agit d'un protocole Cisco (XCCP (eXtensible Conference Control Protocol) négocié uniquement dans SIP (les appels interconnectés n'ont donc pas ActiveControl) et qui exploite le protocole UDP/UDT (UDP-based Data Transfer Protocol) pour le transfert de données. La négociation sécurisée se fait par le biais de Datagram TLS (DTLS) qui peut être considéré comme TLS sur une connexion

UDP. Quelques exemples sont montrés ici pour les différences dans la négociation.

Non Chiffré

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

Chiffré (meilleur effort - essayez le chiffrement mais autorisez le retour à une connexion non chiffrée)

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

a=ixmap:2 **xccp**

a=**empreinte digitale**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

Chiffré (forcer le chiffrement - ne pas autoriser le retour à une connexion non chiffrée)

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

a=ixmap:2 **xccp**

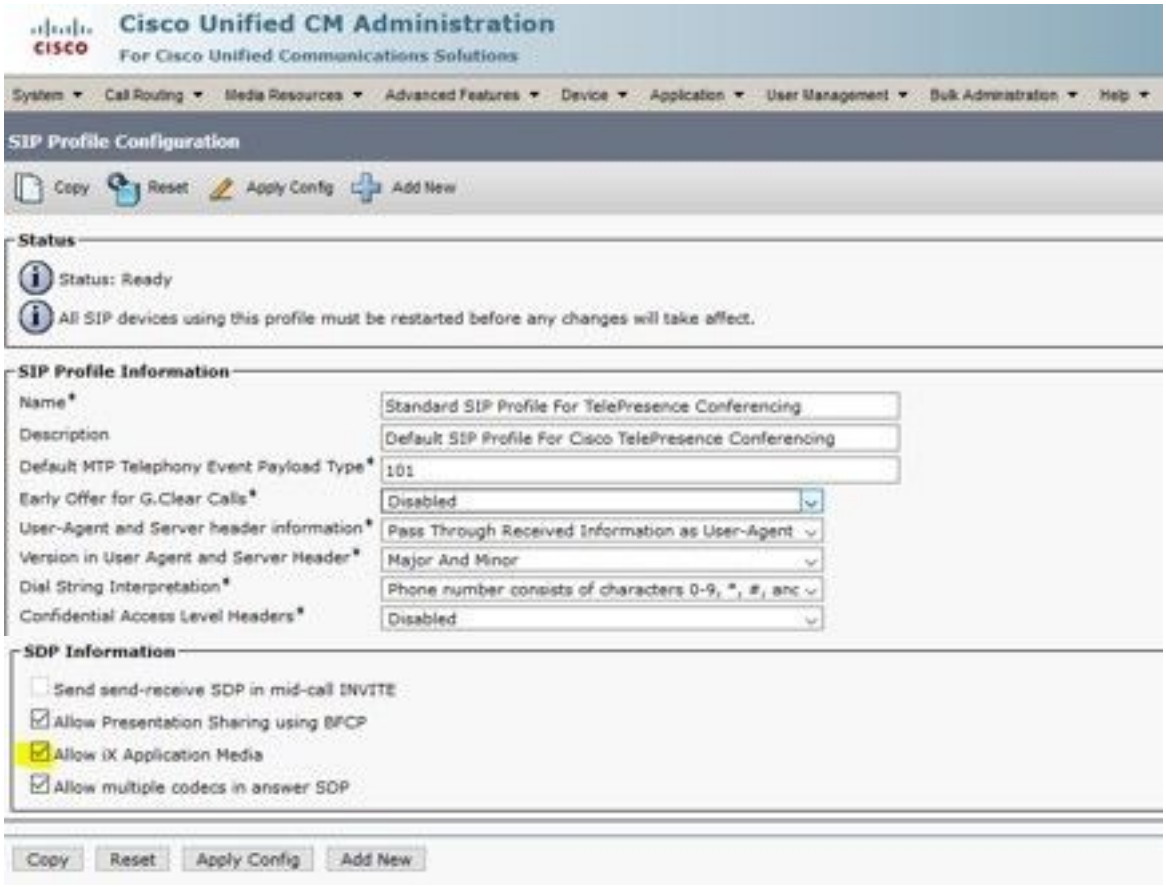
a=**empreinte digitale**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

Certaines versions logicielles minimales sont requises pour la prise en charge complète d'ActiveControl, comme indiqué ci-dessous :

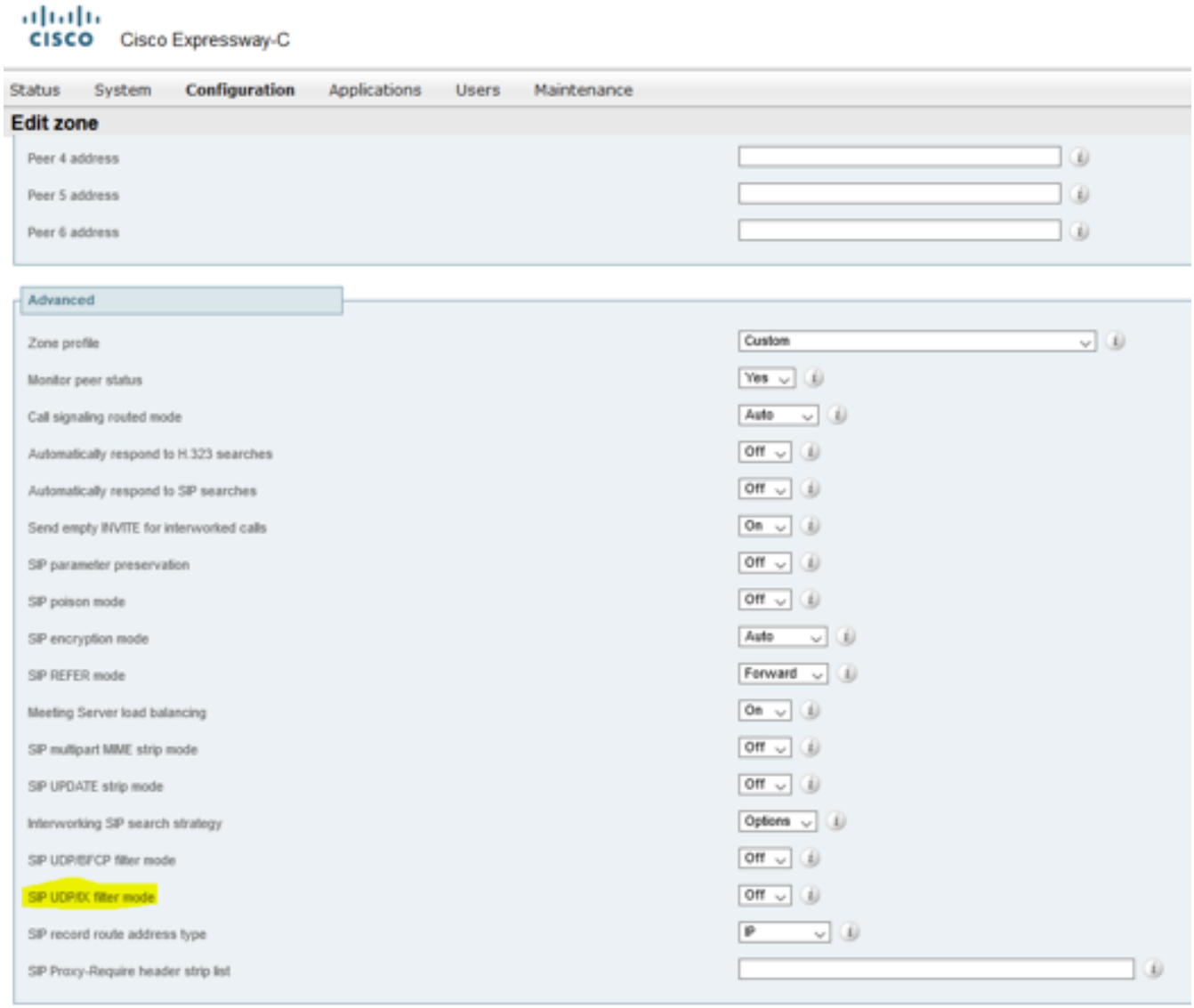
- Jabber version 12.5 ou ultérieure (notes de version)
- Terminaux CE 8.3 ou version ultérieure, 9.6.2 ou version ultérieure recommandés conformément au guide ActiveControl de CMS (CE9.3.1 ou version ultérieure pour Webex conformément au lien d'aide Webex)
- CUCM 10.5 ou version ultérieure (pour la prise en charge d'ActiveControl Jabber 12.5) (11.5(1) ou version ultérieure pour Webex selon le lien)
- CMS version 2.1 ou ultérieure, version 2.5 ou ultérieure recommandée conformément au guide ActiveControl de CMS
- Expressway X12.5 ou version ultérieure (notes de version) pour prendre en charge les clients MRA non chiffrés

Il existe quelques options de configuration à prendre en compte :

- Sur CUCM, assurez-vous que les liaisons SIP appropriées (vers Expressway-C et CMS) sont configurées avec un profil SIP dont l'option « Allow iX Application Media » est cochée



- Sur CMS, il est activé par défaut à partir de la version 2.1, mais vous pouvez le désactiver via un compatibilityProfile sur lequel vous pouvez définir *sipUDT* à false
- Sur Expressway dans la configuration de zone sous les paramètres avancés (lors de l'utilisation d'un profil de zone « Personnalisé »), assurez-vous que le *mode de filtre SIP UDP/IX* est défini sur « Désactivé » si vous voulez permettre à iX de passer



Problème

Informations générales

ActiveControl est négocié de manière sécurisée différemment des autres canaux multimédias. Pour d'autres canaux multimédias comme l'audio et la vidéo, par exemple, le SDP est ajouté avec des lignes de chiffrement qui sont utilisées pour annoncer à la partie distante la clé de chiffrement à utiliser pour ce canal. Le canal RTP (Real-time Transport Protocol) peut donc être sécurisé et considéré comme SRTP (Secure RTP). Pour le canal iX, il utilise le protocole DTLS pour chiffrer le flux multimédia XCCP afin d'utiliser un mécanisme différent.

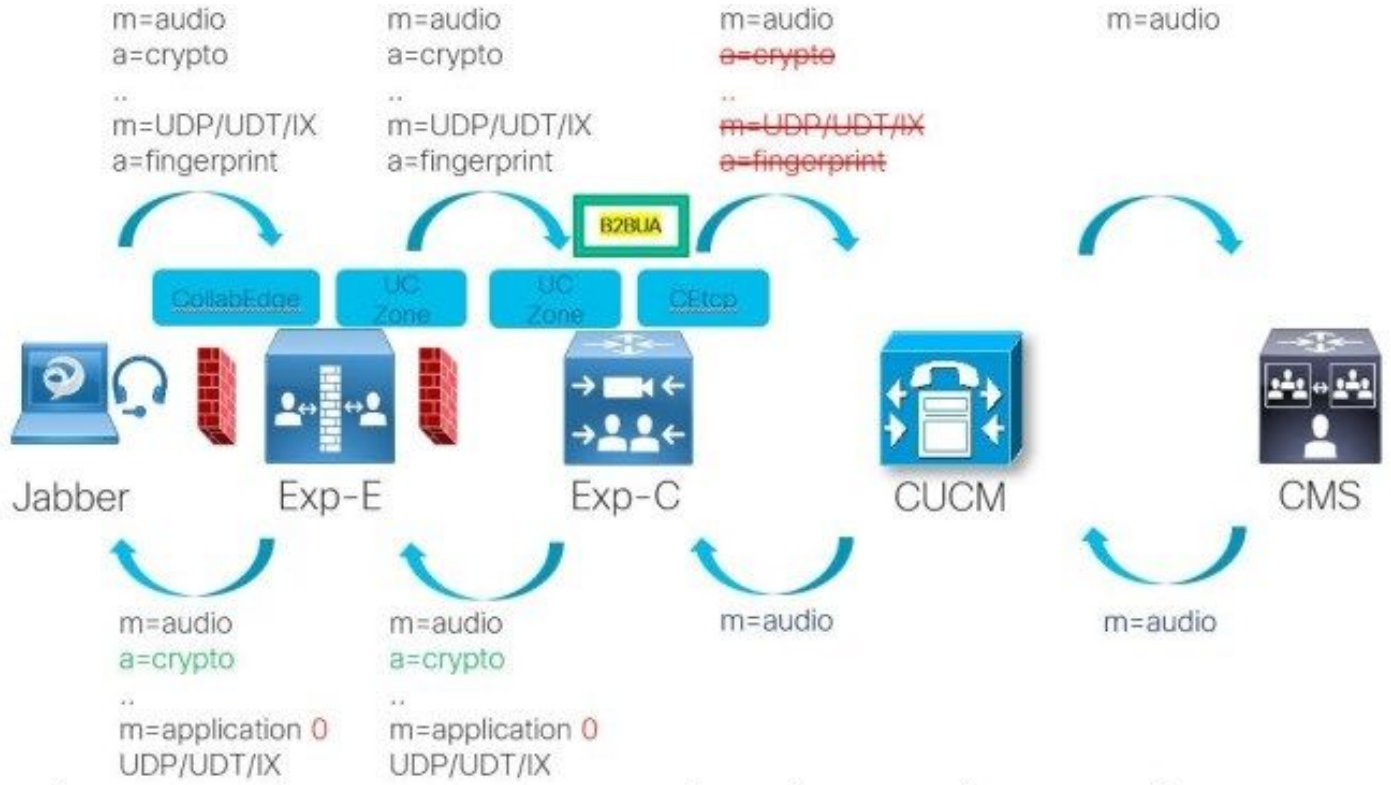
Le logiciel Expressway ne met pas fin au protocole DTLS. Ceci est indiqué dans la section *Limitations* sous *Fonctionnalité non prise en charge* des notes de version d'Expressway.

- 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.

Versions d'Expressway antérieures à X12.5

Lors de l'exécution d'une version d'Expressway antérieure à X12.5, s'il y a une connexion entrante

avec un canal iX chiffré qui passe le long d'une zone TCP non sécurisée, l'Expressway supprime les lignes de chiffrement des canaux média normaux ainsi que le canal iX entier. Ceci est visuellement montré pour un client MRA qui se connecte à un espace CMS où vous voyez que la connexion est sécurisée du client MRA à l'Expressway-C mais ensuite selon le profil de sécurité du téléphone configuré sur CUCM pour le périphérique, il est soit non chiffré (et envoyé sur la zone CEtcp) ou chiffré (et envoyé sur la zone CEtls). Lorsqu'il n'est pas chiffré, comme illustré sur l'image, vous voyez que l'Expressway-C supprime les lignes de chiffrement de tous les canaux multimédias et même la totalité du canal multimédia iX, car il ne peut pas mettre fin au protocole DTLS. Cela se produit via l'agent utilisateur back-to-back (B2BUA), car la configuration de zone pour la zone CEtcp est configurée avec le chiffrement de support « Force unencryption ». Dans la direction opposée (sur la zone de traversée UC avec chiffrement de support « Forcer crypté ») lorsque la réponse SDP est reçue, elle ajoute les lignes de cryptage pour les lignes de support normales et met à zéro le port pour le canal iX, ce qui n'entraîne aucune négociation ActiveControl. En interne, lorsque les clients sont directement enregistrés auprès de CUCM, il permet à la fois les canaux multimédia iX chiffrés et non chiffrés, car CUCM ne se place pas dans le chemin multimédia.



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

Le même type de logique s'applique aux connexions d'appel entre Expressway et Webex Meetings. Il nécessite que le chemin complet soit sécurisé de bout en bout, car les serveurs Expressway (avant X12.5) ne passent que sur les informations de connexion DTLS, mais ne se terminent pas sur eux-mêmes pour démarrer une nouvelle session ou pour chiffrer/déchiffrer le canal média sur les différentes branches d'appel.

Versions Expressway de X12.5 et ultérieures

Lors de l'exécution d'une version Expressway de X12.5 ou supérieure, le comportement a changé car maintenant il passe sur le canal iX sur la connexion de zone TCP en tant que chiffrement forcé (UDP/DTLS/UDT/IX) afin de lui permettre de toujours négocier le canal iX mais seulement quand l'extrémité distante utilise le chiffrement aussi. Il applique le chiffrement parce que l'Expressway ne termine pas la session DTLS et n'agit donc que sur le pass-through, de sorte qu'il s'appuie sur

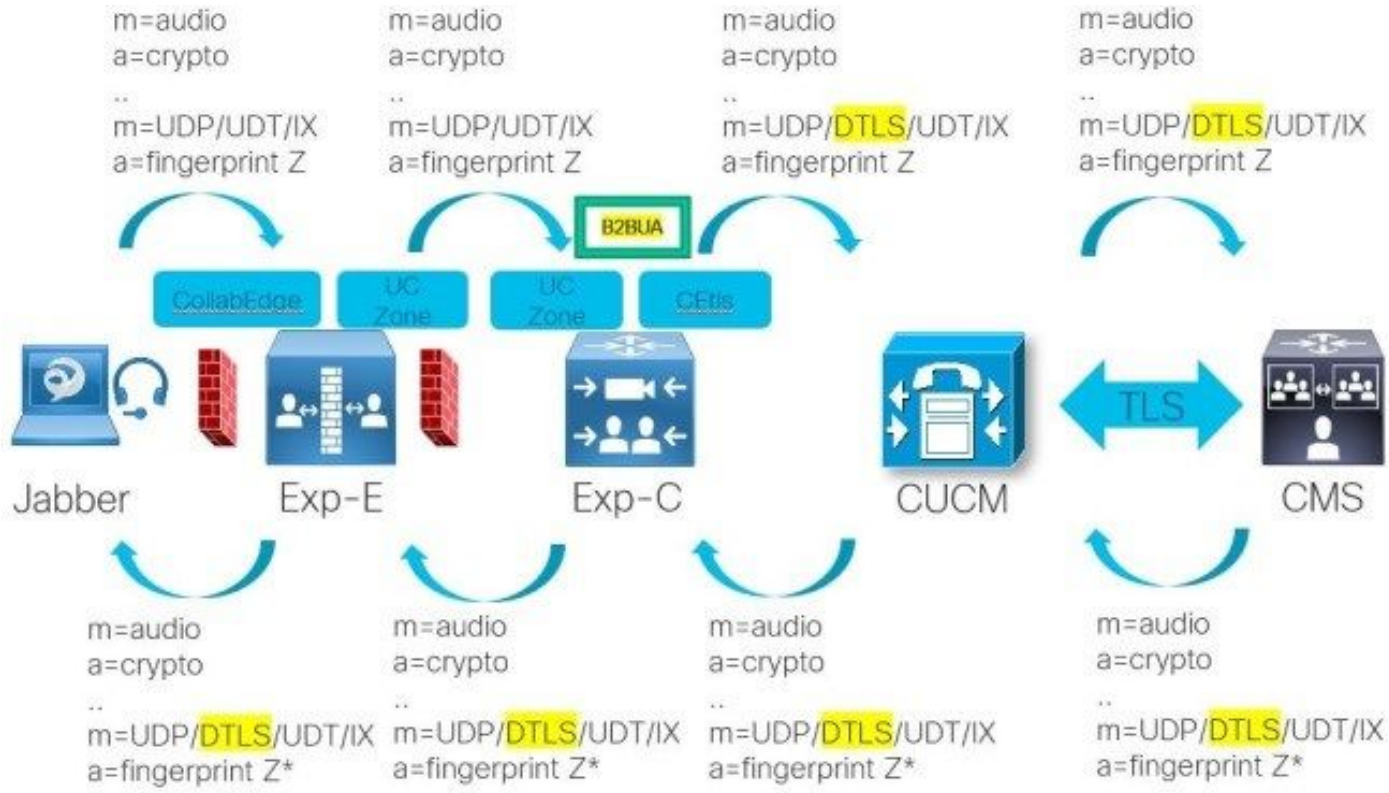
l'extrémité distante pour démarrer/terminer la session DTLS. Les lignes de chiffrement sont supprimées via la connexion TCP à des fins de sécurité. Ce changement de comportement est traité dans les notes de version, conformément à la section « MRA : Prise en charge d'Encrypted iX (pour ActiveControl) ». Ce qui se passe ensuite dépend de la version de CUCM car ce comportement a changé dans 12.5(1)SU1 où il permet de passer sur le canal iX ainsi que sur les connexions entrantes non sécurisées. Même lorsqu'il y aurait une liaison SIP TLS sécurisée vers CMS, lorsqu'une version de CUCM inférieure à 12.5(1)SU1 est exécutée, elle éliminerait le canal iX avant de le transmettre au CMS, ce qui aboutirait finalement à un port de mise à zéro de CUCM vers 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.

Grâce à une signalisation d'appel et un chemin multimédia sécurisés de bout en bout, le canal iX peut être négocié directement (via différents tronçons de serveurs Expressway) entre le client (MRA) et la solution de conférence (CMS ou Webex Meeting). L'image montre le même flux d'appels pour le client MRA se connectant à un espace CMS, mais avec désormais un profil de sécurité téléphonique sécurisé configuré sur CUCM et une liaison SIP TLS sécurisée vers CMS. Vous pouvez voir que le chemin est sécurisé de bout en bout et que le paramètre d'empreinte DTLS est simplement transmis sur l'ensemble du chemin.

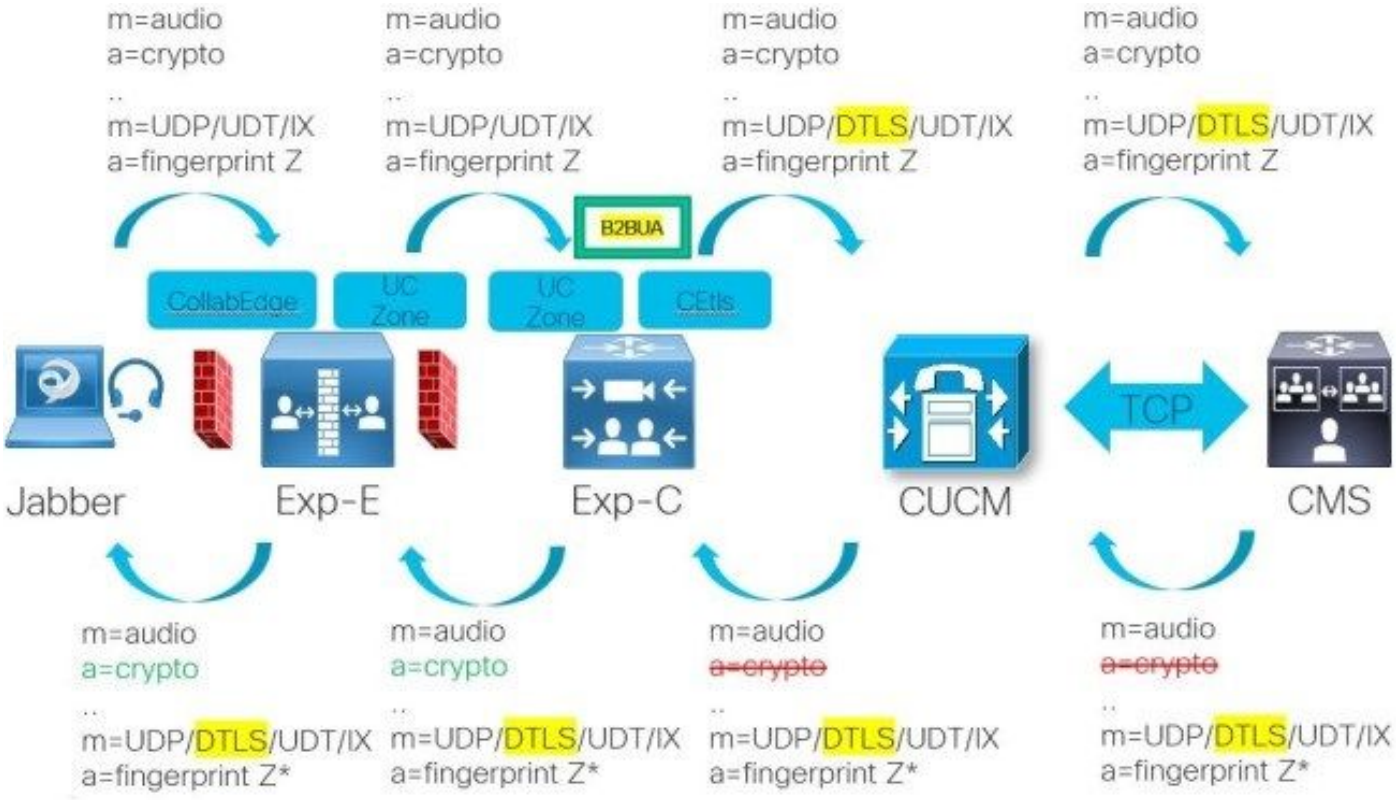


Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

Afin de configurer un profil de sécurité de périphérique sécurisé, vous devez vous assurer que le CUCM est configuré en mode mixte et cela peut être un processus fastidieux (également lorsqu'il est opérationnel car il nécessite la fonction Proxy de l'autorité de certification (CAPF) pour les communications sur site sécurisées). Par conséquent, d'autres solutions plus pratiques peuvent être proposées ici pour prendre en charge la disponibilité d'ActiveControl sur MRA et Expressway

en général, comme indiqué dans ce document.

Les liaisons SIP TLS sécurisées vers le(s) serveur(s) CMS ne sont pas requises car CUCM (en supposant que la liaison SIP ait l'option SRTP autorisé activée) passe toujours d'une connexion SIP sécurisée entrante au canal iX ainsi qu'aux lignes de chiffrement, mais CMS ne répond qu'en cryptant le canal iX (en prenant en compte ActiveControl) (en supposant que le **cryptage de support SIP** est *autorisé* ou *appliqué* sur CMS sous **Paramètres > Paramètres d'appel**) mais n'a pas de cryptage sur les autres canaux de support car il supprime les lignes de chiffrement selon l'image. Les serveurs Expressway peuvent ajouter à nouveau les lignes de cryptage pour sécuriser cette partie de la connexion (et iX est négocié directement entre les clients finaux toujours via DTLS) mais ce n'est pas idéal du point de vue de la sécurité et il est donc recommandé de configurer une liaison SIP sécurisée vers le pont de conférence. Lorsque **SRTP autorisé** n'est pas coché sur la ligne principale SIP, CUCM retire les lignes de chiffrement et la négociation iX sécurisée échoue également.



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

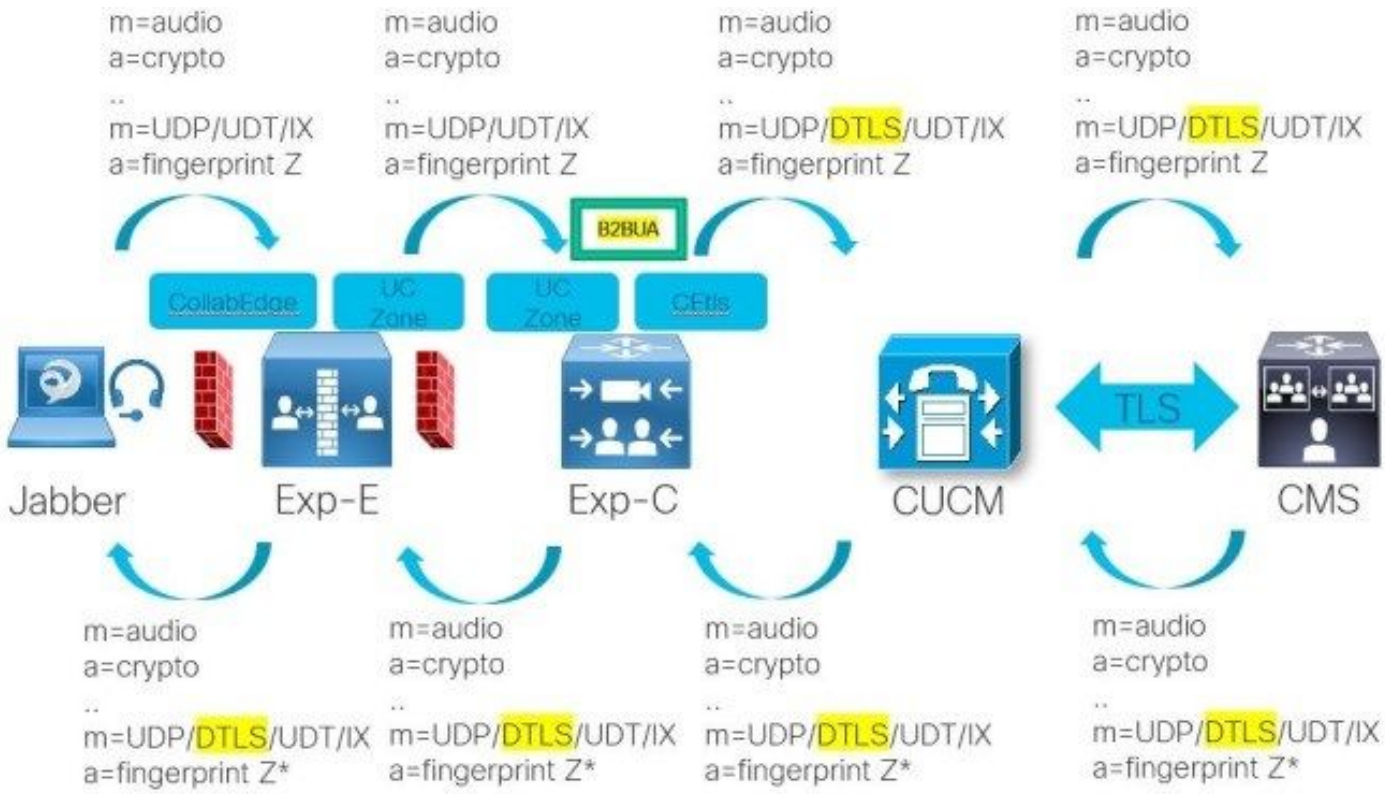
Solution

Il y a quelques options différentes disponibles avec diverses exigences et divers avantages et inconvénients. Chacun d'entre eux est présenté dans une section plus détaillée. Les différentes options sont les suivantes :

1. Profils de sécurité téléphonique sécurisés pour les terminaux (CUCM en mode mixte)
2. SIP OAuth pour Jabber
3. Canal iX crypté pour profils de sécurité téléphonique non sécurisés (CUCM 12.5(1)SU1 ou supérieur)

Solution 1 : profils de sécurité téléphonique sécurisés pour les terminaux (CUCM en

mode mixte)



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

Conditions préalables:

- CUCM en mode mixte

Professionnel :

- Fonctionne avec n'importe quelle version CUCM
- Fonctionne pour tous les périphériques clients

Inconvénients :

- Nécessite la configuration de CUCM en mode mixte (et les opérations CAPF sur les terminaux sur site)

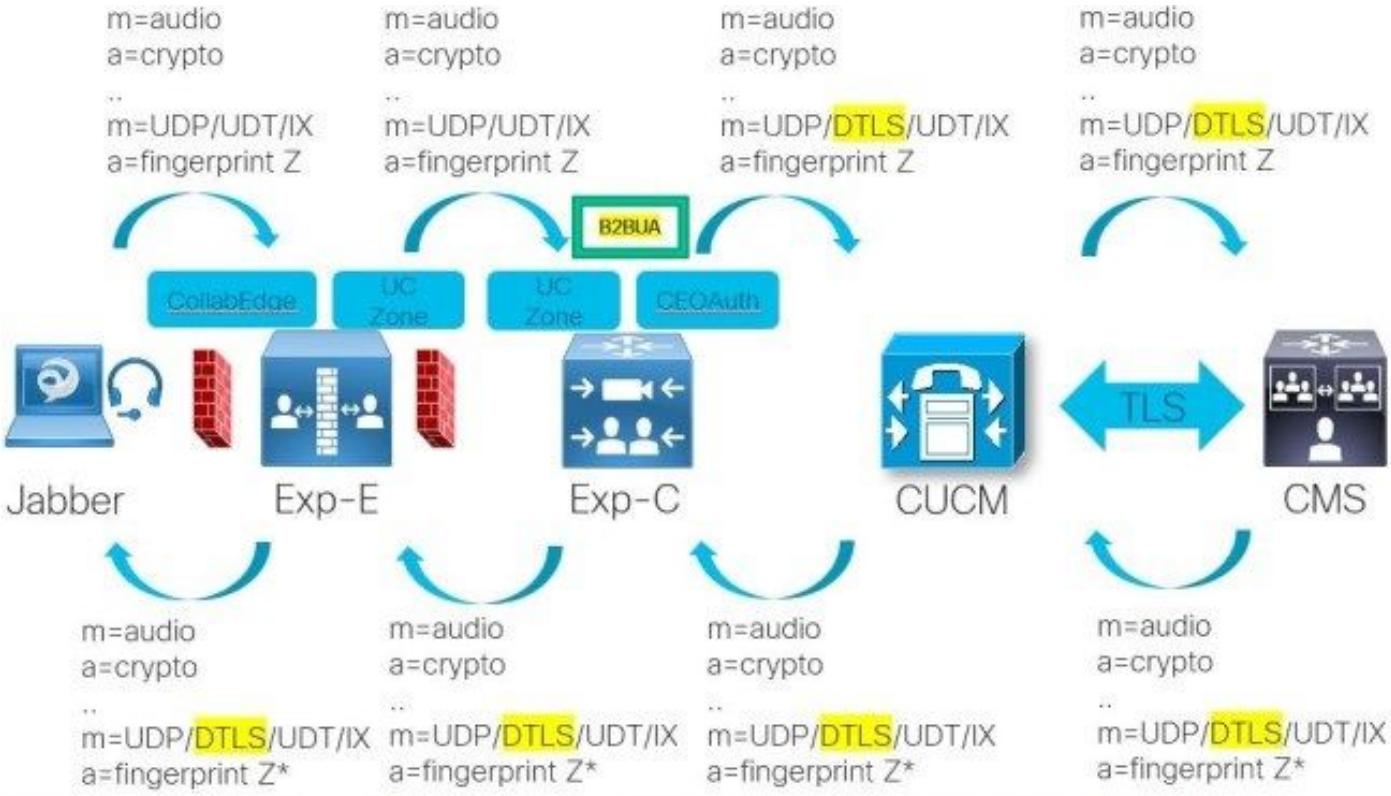
Il s'agit de la méthode décrite dans la section Problème, ainsi qu'à la fin, où vous vous assurez que vous disposez d'un chemin d'accès média et d'une signalisation d'appel chiffrée de bout en bout. Il nécessite que le CUCM soit configuré en mode mixte comme indiqué dans le document suivant.

Pour les clients MRA, aucune opération CAPF n'est requise, mais assurez-vous de suivre les étapes de configuration supplémentaires avec le profil de sécurité du téléphone sécurisé avec un nom qui correspond à l'un des noms de substitution de sujet du certificat du serveur Expressway-C, comme indiqué dans l'exemple de configuration des terminaux basés sur Collaboration Edge TC (qui s'applique également aux terminaux basés sur CE et aux clients Jabber).

Lorsque vous vous connectez d'un terminal local ou d'un client Jabber à une réunion Webex, vous devez effectuer l'opération CAPF pour enregistrer le client en toute sécurité sur le CUCM. Cela est nécessaire pour assurer le flux d'appels sécurisé de bout en bout où l'Expressway peut simplement passer la négociation DTLS et ne pas la gérer elle-même.

Afin de sécuriser l'appel de bout en bout, assurez-vous également que toutes les lignes SIP pertinentes (vers Expressway-C en cas d'appel vers Webex Meeting et vers CMS en cas d'appel vers une conférence CMS) sont des lignes SIP sécurisées utilisant TLS avec un profil de sécurité de ligne SIP sécurisé.

Solution 2 : SIP OAuth pour Jabber



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

Conditions préalables:

- Cisco Jabber 12.5 ou version ultérieure (notes de version)
- CUCM version 12.5 ou ultérieure (notes de version) avec *OAuth avec le flux de connexion d'actualisation* activé
- Expressway X12.5.1 ou version ultérieure (notes de version) avec *jeton Authorize by OAuth avec actualisation* activée

Professionnel :

- Permet des enregistrements sécurisés et une commutation aisée entre les locaux et les locaux hors site sans renouveler le CAPF à chaque fois.
- Pas besoin de configurer CUCM en mode mixte

Inconvénients :

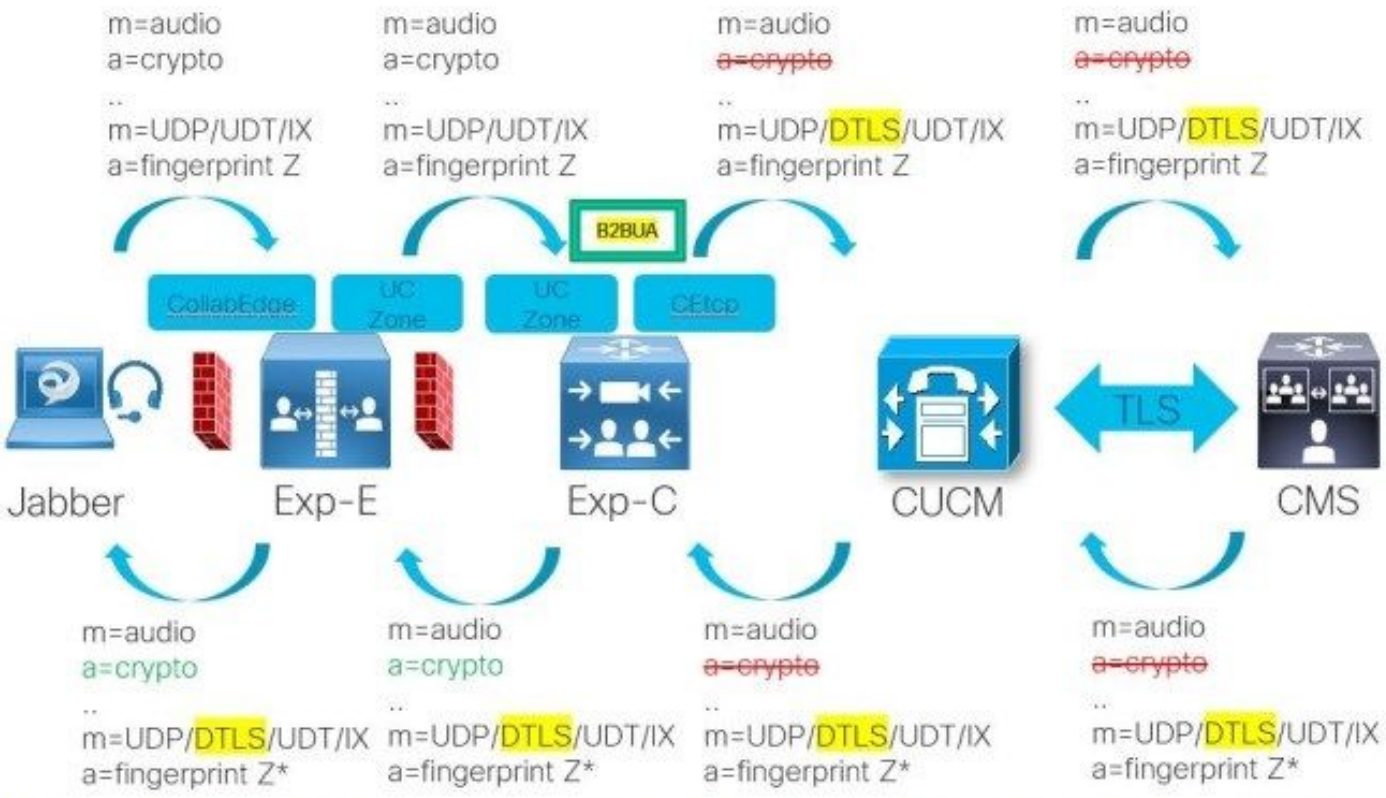
- Uniquement applicable à Jabber, non applicable aux terminaux TC/CE

Le mode SIP OAuth vous permet d'utiliser des jetons d'actualisation OAuth pour l'authentification Cisco Jabber dans des environnements sécurisés. Il permet une signalisation et un support sécurisés sans l'exigence CAPF de la Solution 1. La validation du jeton lors de l'enregistrement SIP est terminée lorsque l'autorisation basée sur OAuth est activée sur le cluster CUCM et les terminaux Jabber.

La configuration sur CUCM est documentée dans le guide de configuration de fonctionnalité et nécessite que vous ayez le flux de connexion OAuth avec actualisation sous les paramètres d'entreprise déjà activé. Afin d'activer cela aussi sur MRA, assurez-vous d'actualiser les noeuds CUCM dans le serveur Expressway-C sous **Configuration > Unified Communication > Unified CM Servers** afin que sous **Configuration > Zones > Zones** vous puissiez maintenant voir aussi les zones CEOAuth créées automatiquement. Assurez-vous également que sous **Configuration > Unified Communication > Configuration** that **Authorize by OAuth token with refresh** est également activé.

Avec cette configuration, vous pouvez obtenir une connexion d'appel sécurisée de bout en bout similaire pour la signalisation et les supports et par conséquent l'Expressway ne fait que passer sur la négociation DTLS car il ne termine pas ce trafic lui-même. Ceci est vu sur l'image où la seule différence par rapport à la solution précédente est qu'il utilise la zone CEOAuth sur l'Expressway-C vers le CUCM par opposition à la zone CEtls parce qu'il utilise SIP OAuth plutôt que l'enregistrement de périphérique sécurisé sur TLS quand CUCM fonctionne dans un mode mixte avec un profil de sécurité téléphonique sécurisé, mais à part cela, tout reste le même.

Solution 3 : canal iX crypté pour les profils de sécurité téléphonique non sécurisés (CUCM 12.5(1)SU1 ou supérieur)



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

Conditions préalables:

- CUCM version 12.5(1)SU1 ou ultérieure (notes de version)
- Expressway X12.5.1 ou version ultérieure (notes de version)

Professionnel :

- Pas besoin de configurer CUCM en mode mixte
- Pas besoin de configurer des communications sécurisées de bout en bout

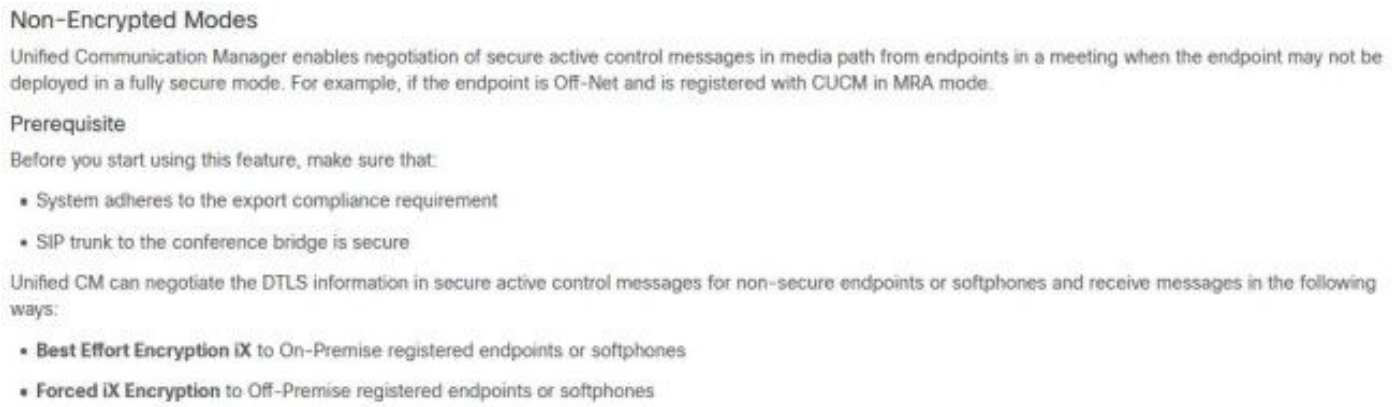
- Applicable aux terminaux Jabber et TC/CE

Inconvénients :

- Mise à niveau de CUCM requise
- Seules les versions limitées CUCM sont prises en charge

Àpartir de CUCM 12.5(1)SU1, il prend en charge la négociation de cryptage iX pour tout périphérique de ligne SIP afin de pouvoir négocier les informations DTLS dans les messages ActiveControl sécurisés pour les terminaux ou les téléphones logiciels non sécurisés. Il envoie le cryptage iX au mieux sur TCP, permettant aux téléphones d'avoir un canal iX crypté de bout en bout malgré une connexion TCP non sécurisée (pas TLS) au CUCM.

Dans le guide de sécurité de CUCM 12.5(1)SU1 sous la section « Encrypted iX Channel », il montre que pour les modes non cryptés avec des périphériques non sécurisés, le meilleur effort et le cryptage iX forcé peuvent être négociés avec la condition préalable que votre système adhère à la conformité d'exportation et que la ligne principale SIP vers votre pont de conférence est sécurisée.



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

Sur CUCM :

- Vous devez utiliser l'exportation restreinte CUCM (non illimitée)
- Sous **System > Licensing > License Management**, vous devez avoir « Export-Controlled Functioning » défini sur allowed.
- L'option **SRTP Allowed** doit être activée sur votre ligne SIP (que la ligne elle-même soit sécurisée ou non)

Sur CMS :

- Votre pont d'appels doit disposer d'une licence de cryptage (vous n'avez donc pas de licence callBridgeNoEncryption)
- Sur webadmin sous **Configuration > Call Settings**, vous devez avoir défini le **cryptage de support SIP** sur **allowed** (or **required**)

Sur l’image, vous pouvez voir que la connexion est sécurisée jusqu’à ce que l’Expressway-C, puis C, envoie le SDP à CUCM sans les lignes de cryptage, mais qu’il inclut toujours le canal média iX. Ainsi, le média normal pour l’audio/la vidéo/... n’est pas sécurisé avec des lignes de cryptage, mais il a une connexion sécurisée pour le canal média iX maintenant de sorte que l’Expressway n’a pas besoin de terminer la connexion DTLS. Par conséquent, ActiveControl peut être négocié directement entre le client et le pont de conférence, même avec un profil de sécurité téléphonique non sécurisé. Dans les versions précédentes de CUCM, le flux serait différent et ActiveControl n'est pas négocié parce qu'il ne passe pas sur le canal iX au CMS en premier lieu, car cette partie aurait déjà été supprimée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.