# ActiveControl via MRA/Express inschakelen

## Inhoud


[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[Probleem](#)
[Algemene informatie](#)
[Expressway versies voor X12.5](#)
[Expressway versies van X12.5 en hoger](#)
[Oplossing](#)
[Oplossing 1: Beveiligingsprofielen voor beveiligde telefoons voor de endpoints (gemengde CUCM-modus)](#)
[Oplossing 2: SIP Audio voor Jabber](#)
[Oplossing 3: Versleuteld iX-kanaal voor onbeveiligde telefoonbeveiligingsprofielen (CUCM 12.5(1)SU1 of hoger)](#)


## Inleiding

Dit document beschrijft de verschillende opties om het ActiveControl Protocol voor Mobile en Remote Access (MRA)-clients in te schakelen en voor gesprekken van on-prem-endpoints naar Webex Meetings via Expressway. MRA is een implementatieoplossing voor Virtual Private Network-less (VPN) Jabber- en endpointmogelijkheden. Met deze oplossing kunnen eindgebruikers verbinding maken met interne bedrijfsresources van overal ter wereld. Het ActiveControl-protocol is een bedrijfseigen protocol van Cisco dat een rijkere conferencingervaring mogelijk maakt met functies tijdens de uitvoering, zoals vergaderroosters, wijzigingen in de videolay-out, opties voor het muteren en opnemen.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Expressway (MRA- en B2B-gesprekken)

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Achtergrondinformatie

In dit document ligt de nadruk vooral op de MRA-clientverbinding met een Cisco Meeting Server (CMS), maar hetzelfde geldt voor andere platforms of verbindingen, zoals bijvoorbeeld bij verbinding met Webex Meetings. Dezelfde logica kan worden toegepast voor het volgende type gespreksstromen:

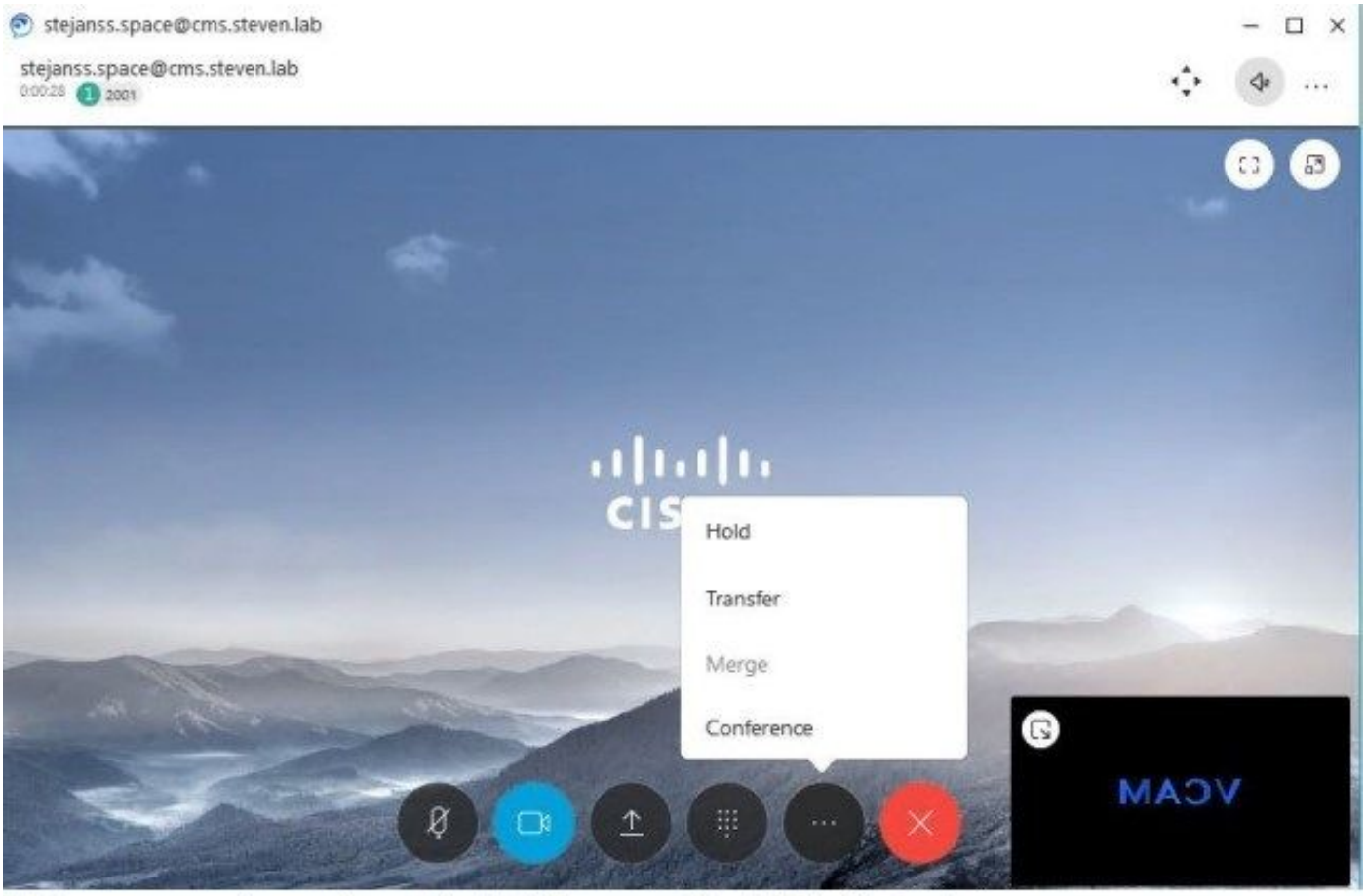
- Endpoint - CUCM - Expressway-C - Expressway-E - Webex Meeting
- MRA Endpoint - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Webex Meeting

> **Opmerking**: de functies van ActiveControl ondersteund door Webex Meetings zijn anders dan die van CMS op dit moment in de tijd en zijn slechts een beperkte subset.

Het Cisco Meeting Server-platform biedt deelnemers aan vergaderingen de mogelijkheid om hun vergaderervaring direct vanaf hun conferencingendpoint via ActiveControl te beheren zonder de noodzaak voor externe toepassingen of operatoren. ActiveControl maakt gebruik van het iX-mediaprotocol in Cisco-apparaten en wordt besproken als deel van SIP-berichtenuitwisseling tijdens een gesprek. Vanaf CMS versie 2.5 zijn de belangrijkste functies die zijn ingeschakeld de volgende (hoewel deze kunnen afhangen van het type eindpunt en de softwareversie die wordt gebruikt):

- Het bekijken van een lijst van alle deelnemers (roosterlijst of deelnemerslijst) die met de vergadering wordt verbonden
- Het muteren of het unmuting van andere deelnemers
- Het toevoegen of het verwijderen van een andere deelnemer van de vergadering
- Opname van een vergadering starten of stoppen
- Een deelnemer belangrijk maken
- Indicator voor de deelnemer die de actieve spreker in de vergadering is
- Indicator voor de deelnemer die momenteel inhoud of presentatie in de vergadering deelt
- Vergrendeling of ontgrendeling van de vergadering

Op de eerste afbeelding ziet u een gebruikersweergave van een Jabber-client die een oproep in een CMS-ruimte zonder ActiveControl heeft geplaatst, terwijl de tweede afbeelding laat zien dat u de meer uitgebreide gebruikersweergave biedt waar Jabber ActiveControl met de CMS-server heeft kunnen onderhandelen.




Jabber user experience when calling to CMS space without ActiveControl


Jabber user experience when calling to CMS space with ActiveControl

ActiveControl is een op XML gebaseerd protocol dat wordt overgedragen met behulp van het iX-protocol dat wordt besproken in het Session Description Protocol (SDP) van de Session Initiation Protocol (SIP)-oproepen. Het is een Cisco-protocol (eXtensible Conference Control Protocol (XCCP)) en alleen in SIP onderhandeld (zodat interworking-oproepen geen ActiveControl hebben) en maakt gebruik van UDP/UDT (UDP-gebaseerd Protocol voor gegevensoverdracht) voor gegevensoverdracht. Beveiligde onderhandeling vindt plaats via Datagram TLS (DTLS), dat als

TLS via UDP-verbinding kan worden bekeken. Hier worden enkele voorbeelden getoond van de verschillen in onderhandeling.

**Niet versleuteld**

m=applicatie xxxxxx UDP/UDT/IX *****
a=ixmap:11 **xcp**

**Versleuteld (optimale inspanning - probeer de versleuteling maar laat de feedback naar de niet-versleutelde verbinding toe)**

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

a=ixmap:2 **xcp**

a=**vingerafdruk**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

**Versleuteld (krachtversleuteling - geen feedback naar ongecodeerde verbinding toestaan)**

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

a=ixmap:2 **xcp**

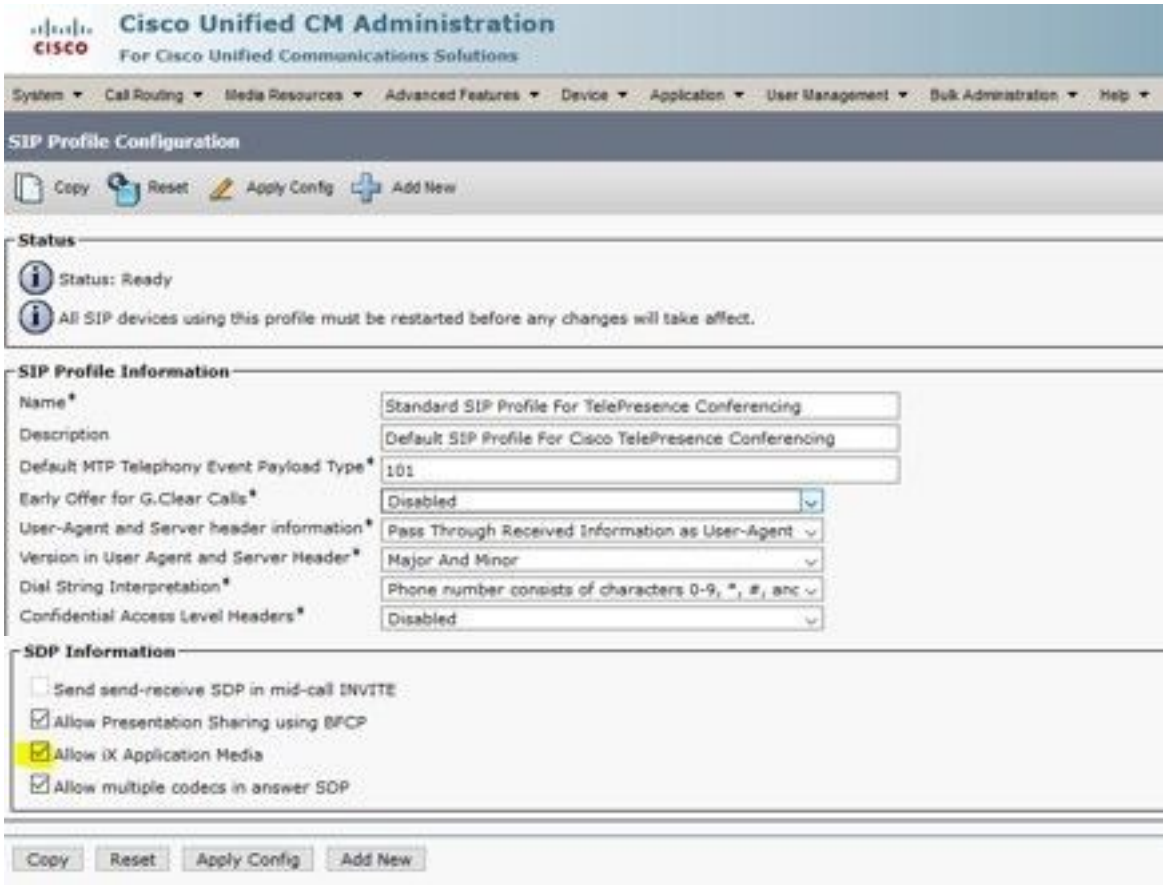
a=**vingerafdruk**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx

Er zijn een aantal minimale softwareversies vereist voor de volledige ondersteuning van ActiveControl zoals hieronder vermeld:

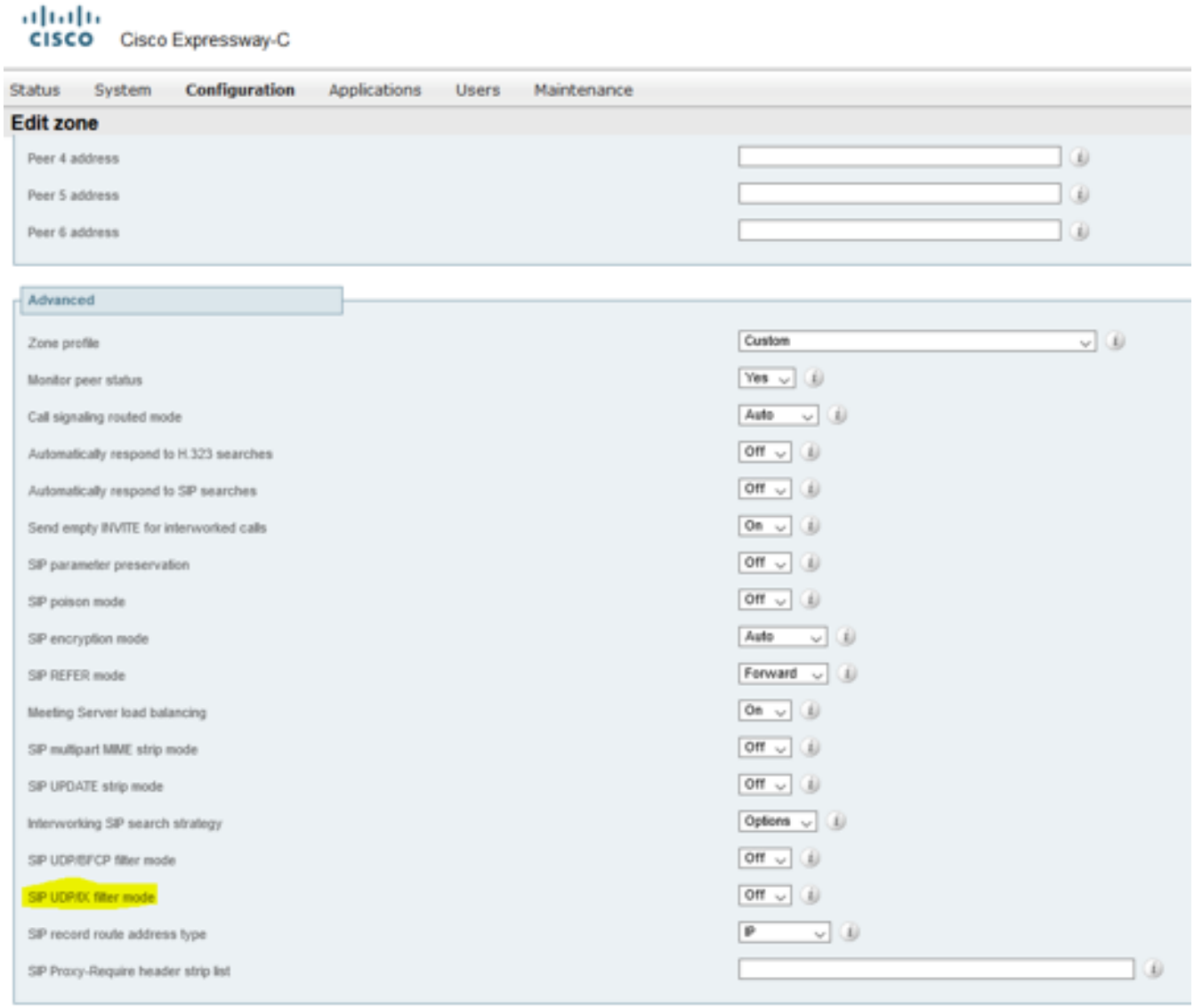
- Jabber, versie 12.5 of hoger (releaseopmerkingen)
- CE-eindpunten 8.3 of hoger, 9.6.2 of hoger, aanbevolen volgens de CMS ActiveControl-handleiding (CE9.3.1 of hoger voor Webex volgens de Webex help link)
- CUCM 10.5 of hoger (voor ondersteuning van Jabber 12.5 ActiveControl) (11.5(1) of hoger voor Webex via de link)
- CMS 2.1 of hoger, 2.5 of hoger aanbevolen volgens de CMS ActiveControl Guide
- Expressway X12.5 of hoger (release notes) om ondersteuning op niet-versleutelde MRA-clients mogelijk te maken

Er zijn een paar configuratieopties die u in overweging kunt nemen:

- Zorg er op CUCM voor dat de relevante SIP-trunks (naar Expressway-C en CMS) zijn geconfigureerd met een SIP-profiel dat het selectievakje 'Toestaan iX-toepassingsmedia' heeft ingeschakeld




- Op CMS is het standaard ingeschakeld vanaf 2.1, maar u kunt het uitschakelen via een compatibiliteitsprofiel waarop u *sipUDT* kunt instellen op false
- Zorg er op Expressway in de Zone-configuratie onder de Geavanceerde instellingen (bij gebruik van een 'Aangepaste' zone profiel) voor dat de *SIP UDP/IX-filtermodus* is ingesteld op 'Uit' als u wilt dat iX kan passeren




# Probleem

## Algemene informatie

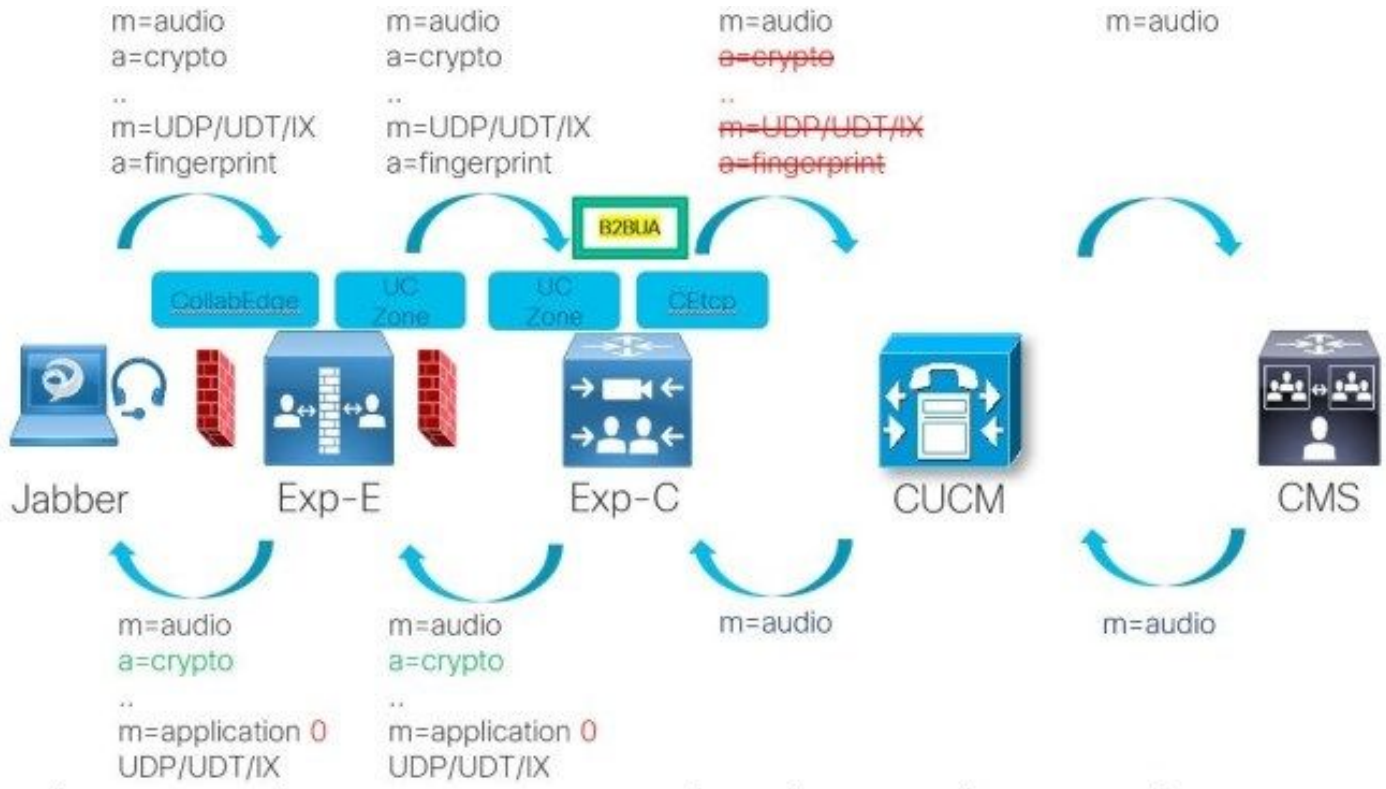
ActiveControl wordt veilig anders onderhandeld dan andere mediakanalen. Voor andere mediakanalen zoals audio en video, wordt de SDP toegevoegd met cryptolijnen die worden gebruikt om aan de verafgelegen partij de encryptiesleutel aan te kondigen die voor dit kanaal moet worden gebruikt. Het Real-time Transport Protocol (RTP)-kanaal kan daarom veilig worden gemaakt en dus worden beschouwd als Secure RTP (SRTP). Voor het iX-kanaal gebruikt het DTLS-protocol om de XCCP-mediastroom te versleutelen, zodat er een ander mechanisme wordt gebruikt.

De Expressway-software sluit het DTLS-protocol niet af. Dit wordt aangegeven onder de sectie *Beperkingen* onder *Niet-ondersteunde functionaliteit* van de sneltoetsen.

- 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.

## Expressway versies voor X12.5

Wanneer een Expressway-versie voor X12.5 wordt uitgevoerd, als er een inkomende verbinding is met een versleuteld iX-kanaal dat wordt doorgegeven via een onveilige TCP-zone, zal de Expressway zowel de cryptolijnen van de normale mediakanalen als het gehele iX-kanaal verwijderen. Dit wordt visueel getoond voor een MRA-client die verbinding maakt met een CMS-ruimte waar u ziet dat de verbinding is beveiligd van de MRA-client naar de Expressway-C, maar vervolgens afhankelijk van het telefoonbeveiligingsprofiel dat is ingesteld op CUCM voor het apparaat, is het niet versleuteld (en verzonden over CEtcp zone) of versleuteld (en verzonden over CEtls zone). Wanneer het wordt ontsleuteld zoals getoond op het beeld, ziet u dat de Expressway-C strips van de crypto lijnen voor alle mediakanalen en zelfs strips van het gehele iX mediakanaal ook omdat het niet kan beëindigen van het DTLS protocol. Dit gebeurt via de back-to-back User Agent (B2BUA) omdat de zone-configuratie voor de CEtcp-zone is ingesteld met mediacodering 'Force unencrypted'. In de tegenovergestelde richting (over de UC-transversale zone met 'Force versleutelde' media-encryptie) wanneer het SDP-antwoord wordt ontvangen, voegt het de crypto-lijnen voor de normale medialijnen toe en zet het de poort voor het iX-kanaal op nul, wat resulteert in geen ActiveControl-onderhandeling. Intern wanneer de clients direct zijn geregistreerd bij CUCM, maakt het zowel voor versleutelde als niet-versleutelde iX-mediakanalen mogelijk, aangezien CUCM zichzelf niet in het mediapad plaatst.



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

Hetzelfde soort logica is van toepassing op de gespreksverbindingen via Expressway naar Webex Meetings. Het vereist dat het volledige pad eind om veilig te eindigen als de Expressway servers (voor X12.5) alleen over de DTLS-verbindingsinfo gaan, maar niet eindigen op het zelf om een nieuwe sessie te starten of om het mediakanaal te versleutelen/decrypteren op de verschillende aanroepbenen.

## Expressway versies van X12.5 en hoger

Bij het uitvoeren van een Expressway versie van X12.5 of hoger, is het gedrag veranderd, omdat het nu over het iX kanaal gaat via de TCP zone verbinding als geforceerde encryptie (UDP/DTLS/UDT/IX) zodat het nog steeds kan onderhandelen over het iX kanaal, maar alleen wanneer het externe eind ook encryptie gebruikt. Het dwingt encryptie af omdat de Expressway de

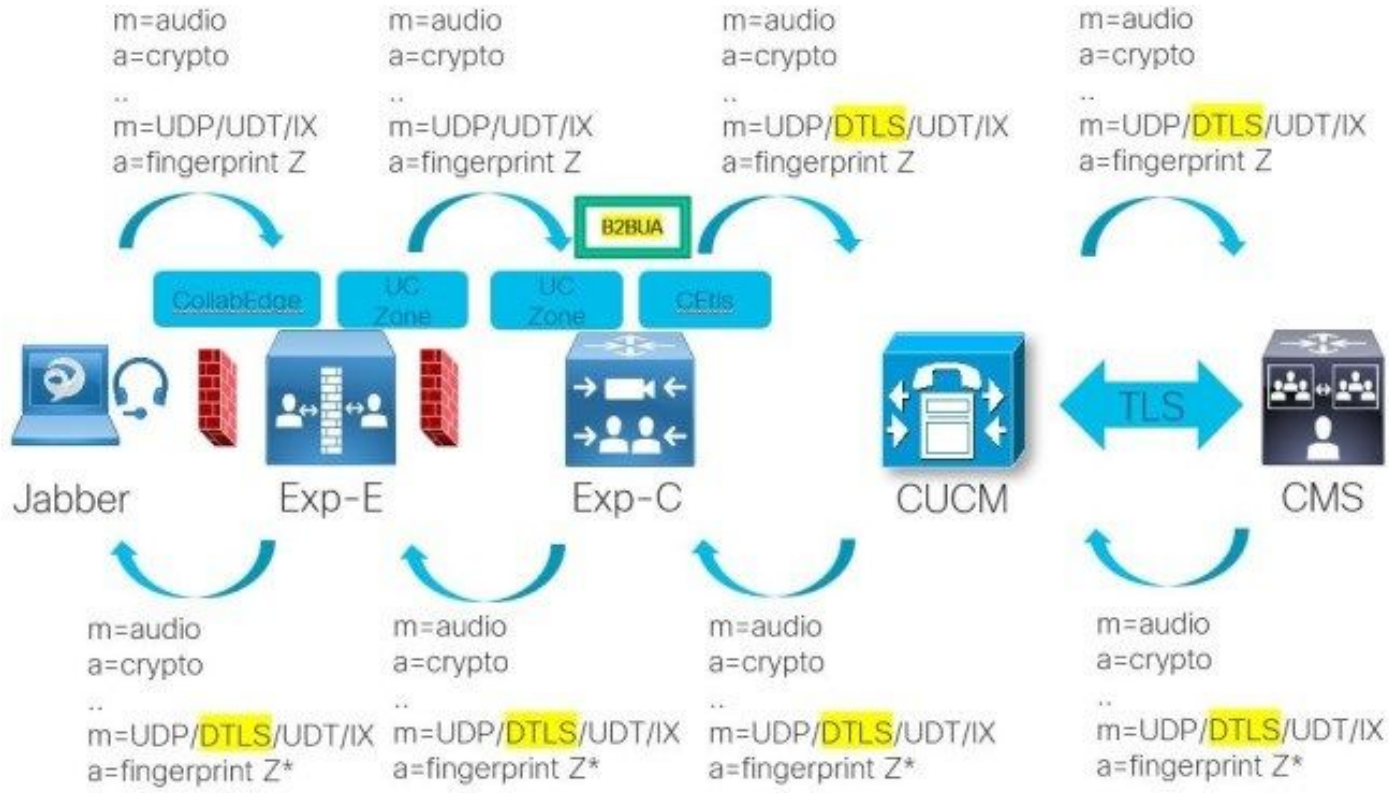
DTLS-sessie niet afsluit en dus alleen werkt op pass-through, zodat het zich op het externe einde baseert om de DTLS-sessie dan te starten/beëindigen. De cryptolijnen worden over de TCP-verbinding gestript voor beveiligingsdoeleinden. Deze gedragsverandering wordt behandeld in de release notities zoals beschreven in de sectie 'MRA: Support for Encrypted iX (for ActiveControl)'. Wat er daarna gebeurt, hangt af van de CUCM-versie zoals dat gedrag veranderde in 12.5(1)SU1 waar het mogelijk maakt om over iX-kanaal te passeren en ook op onveilige inkomende verbindingen. Zelfs als er een beveiligde TLS SIP-trunk naar CMS zou zijn, zou het bij een CUCM-versie lager dan 12.5(1)SU1, het iX-kanaal verwijderen voordat het wordt doorgegeven aan het CMS, wat uiteindelijk zou resulteren in een uitgenummerde poort van CUCM naar 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.

Met een end-to-end beveiligde gesprekssignalering en mediapad kan het iX-kanaal rechtstreeks worden onderhandeld (via verschillende snelheden van Expressway-servers) tussen de (MRA)-client en de conferencingoplossing (CMS of Webex Meeting). De afbeelding toont dezelfde gespreksstroom voor MRA-client die verbinding maakt met een CMS-ruimte, maar nu met een beveiligd telefoonbeveiligingsprofiel geconfigureerd op CUCM en een beveiligde TLS SIP-trunk naar CMS. U kunt zien dat het pad veilig end-to-end is en dat de DTLS-vingerafdrukparameter alleen over het gehele pad wordt doorgegeven.

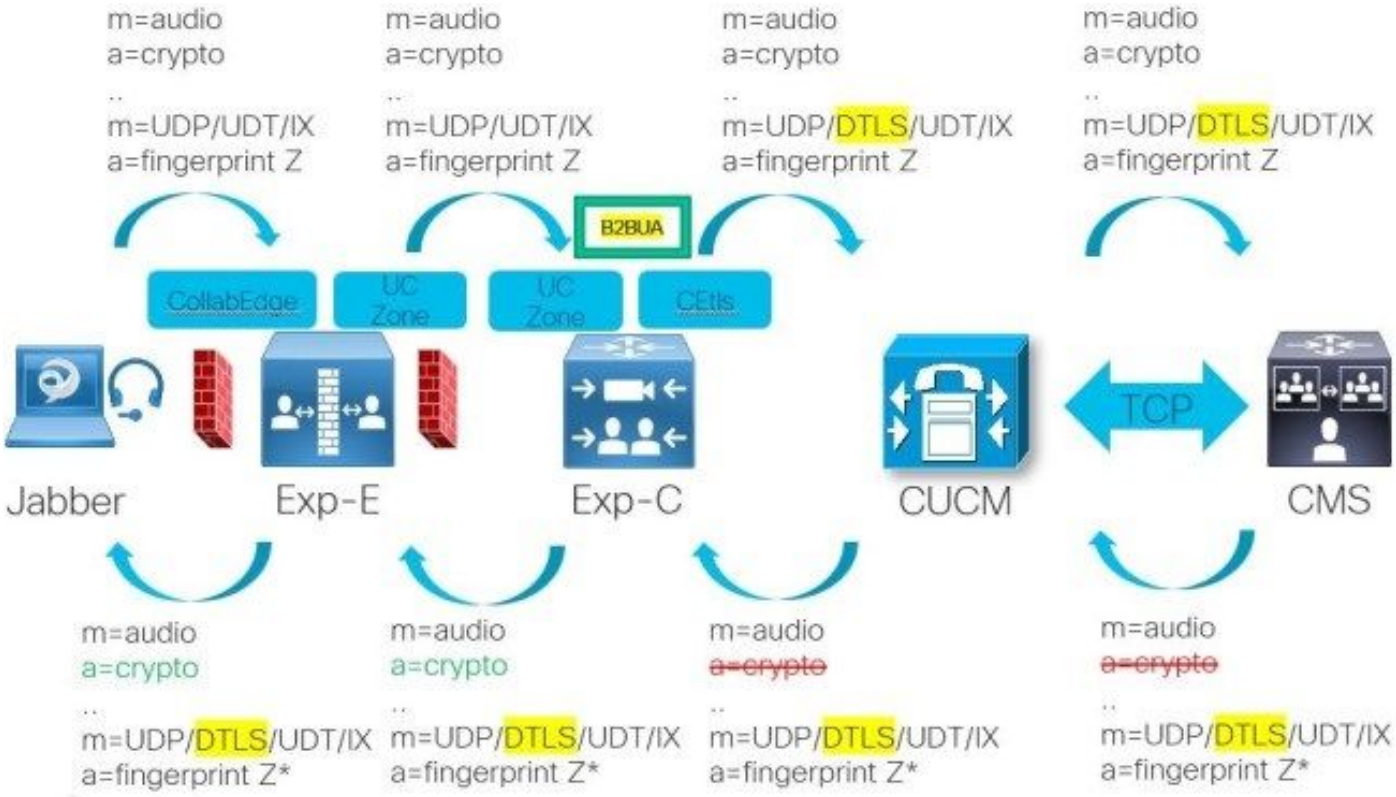



Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

Om een beveiligd beveiligingsprofiel voor een apparaat op te stellen, moet u ervoor zorgen dat de CUCM in een gemengde modus is opgezet en dat dit een omslachtig proces kan zijn (ook wanneer het operationeel is, aangezien hiervoor de functie Certificaatautoriteit Proxy (CAPF) is vereist voor veilige communicatie op het bedrijf). Daarom kunnen hier andere handigere oplossingen worden aangeboden ter ondersteuning van de beschikbaarheid van ActiveControl

over MRA en Expressway in het algemeen, zoals in dit document wordt besproken.

Beveiligde TLS SIP-trunks naar de CMS-server(s) zijn niet vereist omdat CUCM (ervan uitgaande dat de SIP-trunk de optie SRTP ingeschakeld heeft) nog steeds van een inkomende beveiligde SIP-verbinding het iX-kanaal en de cryptolijnen overgaat, maar CMS reageert alleen met encryptie naar het iX-kanaal (wat actieve controle mogelijk maakt) (ervan uitgaande dat **SIP-media-encryptie** is ingesteld op *toegestaan* of *afgedwongen* op CMS onder **Instellingen > Call-instellingen**) maar geen encryptie op de andere mediakanalen heeft per de afbeelding. De Expressway-servers kunnen de cryptolijnen weer toevoegen om dat deel van de verbinding nog te beveiligen (en iX wordt nog steeds direct tussen de eindclients onderhandeld via DTLS), maar dit is niet ideaal vanuit een veiligheidsperspectief en daarom wordt aanbevolen om een beveiligde SIP-trunk naar de conferentiebrug op te zetten. Wanneer **SRTP** niet is ingeschakeld op de SIP-trunk, zal CUCM strips van de crypto-lijnen en beveiligde iX-onderhandeling ook mislukken.



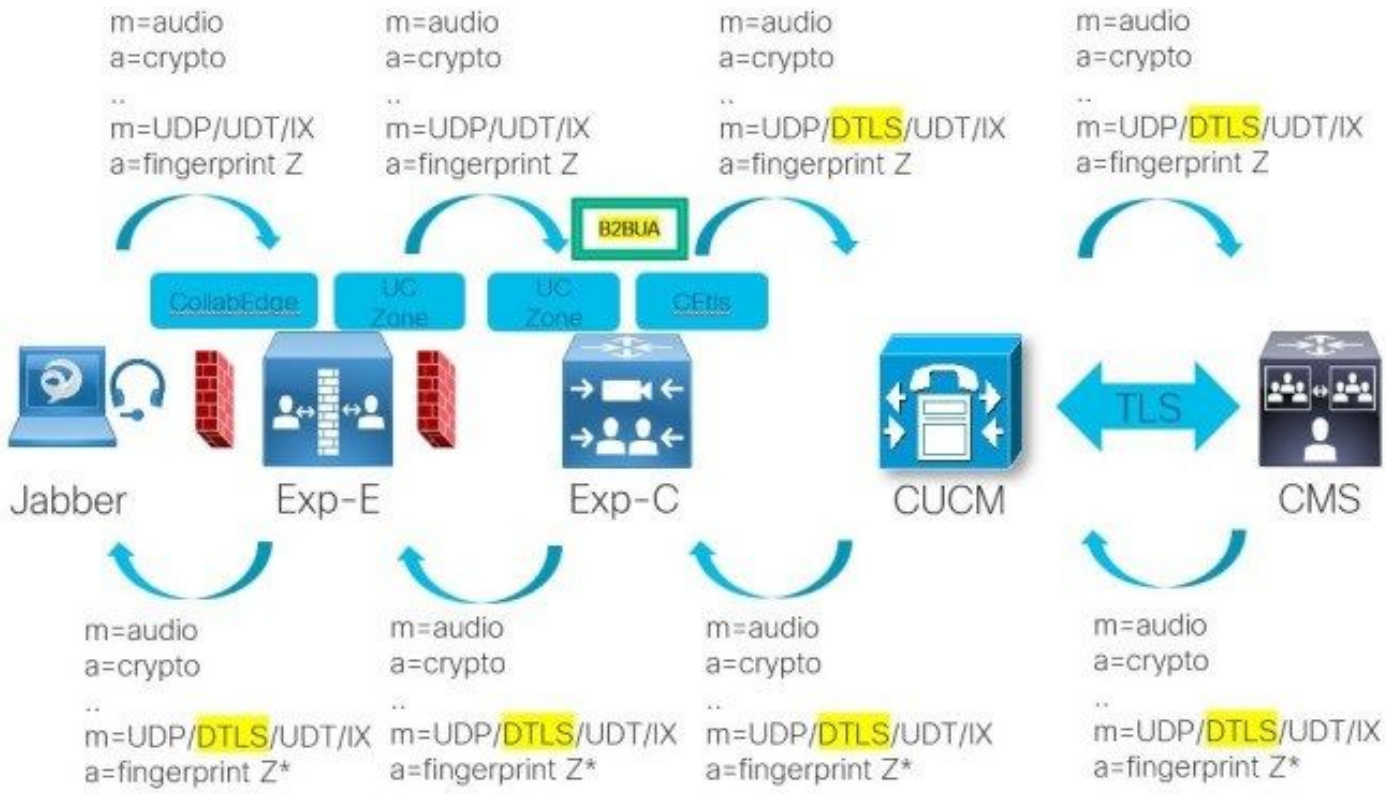

Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

# Oplossing

Er zijn een aantal verschillende opties beschikbaar met verschillende vereisten en verschillende pro en cons. Elk daarvan wordt in een meer gedetailleerde sectie gepresenteerd. De verschillende opties zijn:

1. Beveiligde telefoonbeveiligingsprofielen voor de eindpunten (gemengde CUCM)
2. SIP Waarheid voor Jabber
3. Versleuteld iX-kanaal voor onbeveiligde telefoonbeveiligingsprofielen (CUCM 12.5(1)SU1 of hoger)

## Oplossing 1: Beveiligingsprofielen voor beveiligde telefoons voor de endpoints (gemengde CUCM-modus)




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

**Voorwaarden:**

- CUCM in gemengde modus

**Voor:**

- Werkt op elke CUCM-versie
- Werkt voor alle clientapparaten

**Opmerking:**

- Vereist configuratie van CUCM in gemengde modus (en CAPF-bewerkingen op on-prem endpoints)

Dit is de methode zoals die op de sectie van het Probleem evenals aan het eind wordt verdoezeld waar u ervoor zorgt dat u een van begin tot eind gecodeerde vraag signalering en media weg hebt. Het vereist dat de CUCM in gemengde modus is ingesteld volgens het volgende document.

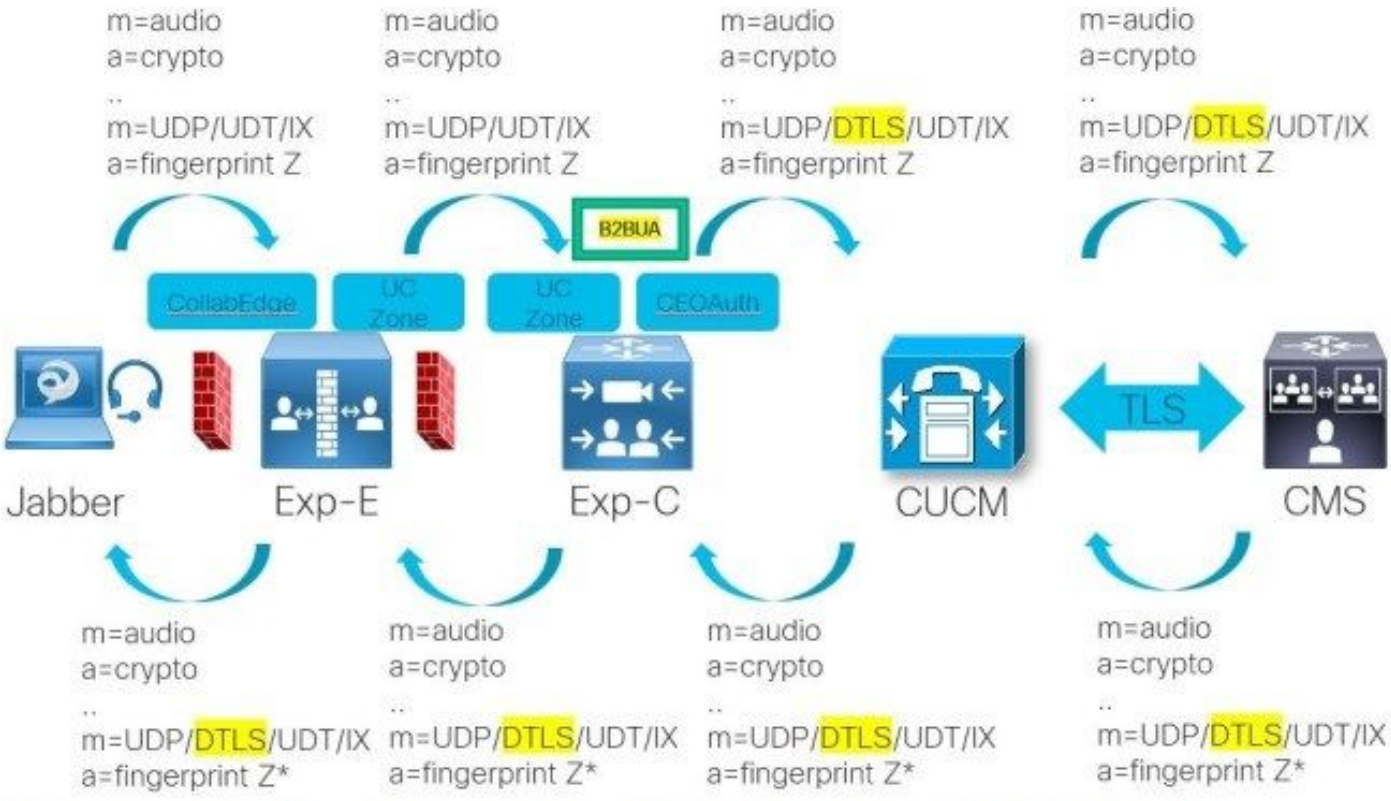
Voor MRA-clients is er geen CAPF-handeling vereist, maar zorg ervoor dat de extra configuratiestappen worden gevolgd met het beveiligde telefoonbeveiligingsprofiel met een naam die overeenkomt met een van de alternatieve onderwerpnamen van het Expressway-C-servercertificaat zoals gemarkeerd in het Collaboration Edge TC-gebaseerde Endpoints Configuration Voorbeeld (dat ook van toepassing is op CE-gebaseerde endpoints en Jabber-clients).

Wanneer u verbinding maakt van een on-prem-eindpunt of Jabber-client met een Webex-vergadering, moet u op de CAPF-handeling uitvoeren om de client veilig te registreren op de CUCM. Dit is nodig om de veilige call flow van begin tot eind te verzekeren, waarbij de Expressway gewoon over de DTLS-onderhandeling kan gaan en niet zelf over kan gaan.

Om de vraag veilig van begin tot eind te maken, zorg er ook voor dat alle relevante SIP-trunks (naar Expressway-C in het geval van een oproep naar Webex Meeting en naar CMS in het geval

van een oproep naar CMS-conferentie) beveiligde SIP-trunks zijn met behulp van TLS met een beveiligd SIP Trunk-beveiligingsprofiel.

## Oplossing 2: SIP Audio voor Jabber



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

**Voorwaarden:**

- Cisco Jabber 12.5 of hoger (release notes)
- CUCM versie 12.5 of hoger (release notes) met *OAuth met Refresh Login Flow* ingeschakeld
- Expressway X12.5.1 of hoger (release notes) met *Autoriseren via OAuth-token en* verversen ingeschakeld

**Voor:**

- Maakt beveiligde registraties mogelijk en eenvoudig schakelen tussen on-prem en off-prem zonder vernieuwing CAPF telkens
- U hoeft CUCM niet in gemengde modus in te stellen

**Opmerking:**

- Alleen van toepassing op Jabber, niet van toepassing op TC/CE-eindpunten

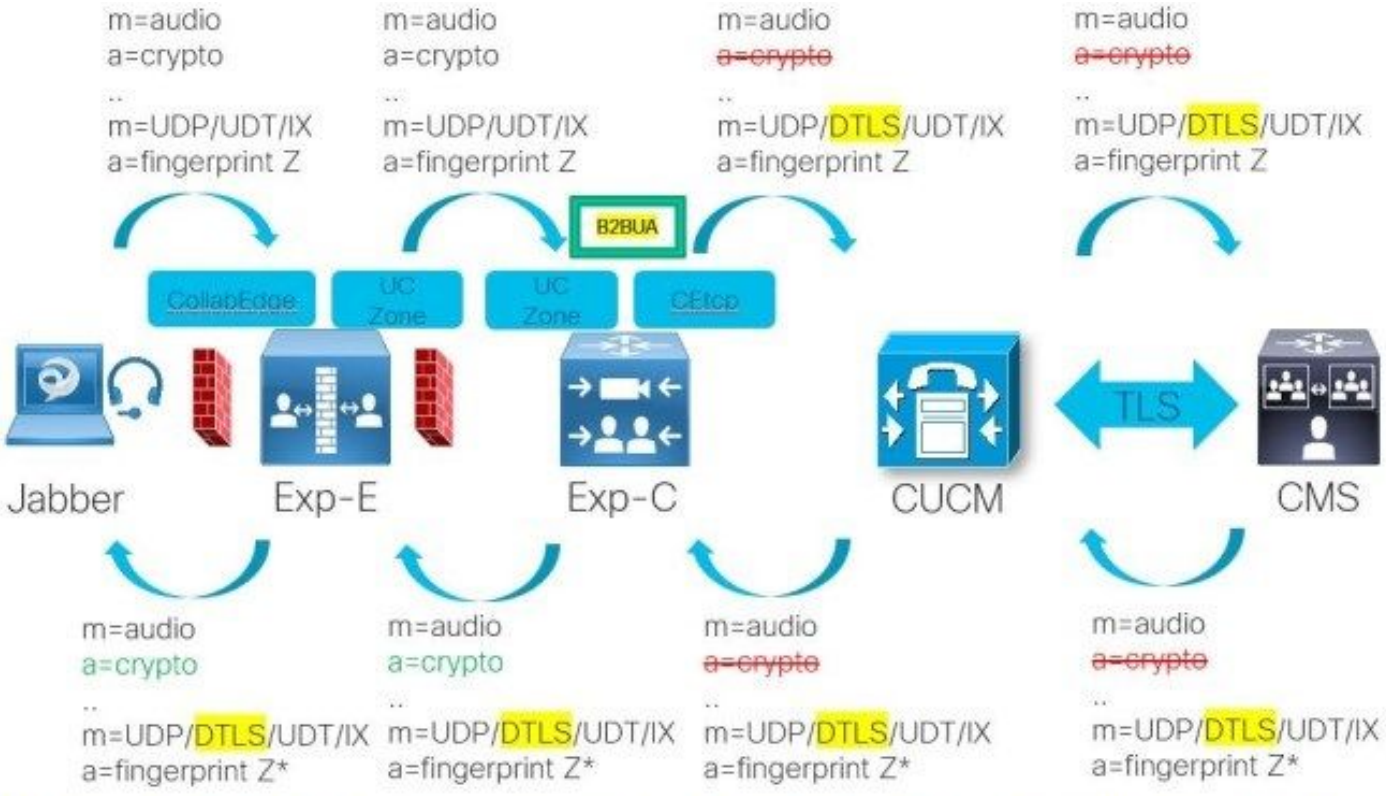
In de SIP OAuth-modus kunt u OAuth refresh tokens gebruiken voor Cisco Jabber-verificatie in beveiligde omgevingen. Het maakt beveiligde signalering en media mogelijk zonder de CAPF-eis van Oplossing 1. De token-validatie tijdens de SIP-registratie is voltooid wanneer op OAuth gebaseerde autorisatie is ingeschakeld op CUCM-cluster en de Jabber-endpoints.

De configuratie op CUCM is gedocumenteerd in de handleiding voor functieconfiguraties en vereist dat u de OAuth met Refresh Login Flow onder Enterprise Parameters al ingeschakeld hebt. Om dit ook mogelijk te maken via MRA, zorg ervoor dat u de CUCM-knooppunten in de Expressway-C-server vernieuwt onder **Configuration > Unified Communications > Unified CM**

**Servers** zodat u onder **Configuration > Zones > Zones** nu ook de automatisch gecreëerde CEOAuth-zones moet zien. Zorg er ook voor dat onder **Configuration > Unified Communications > Configuration** dat **bij OAuth-token** ook **geautoriseerd** is **met Refresh** wordt ingeschakeld.

Met deze configuratie, kunt u een gelijkaardige veilige vraagverbinding van begin tot eind voor zowel signalering als media bereiken en daarom de Expressway enkel overgaand over de onderhandeling DTLS aangezien het dat verkeer zelf niet beëindigt. Dit is te zien op het beeld waar het enige verschil in vergelijking met de vorige oplossing is dat het de CEOAuth-zone op de Expressway-C naar de CUCM gebruikt in tegenstelling tot de CEtls-zone omdat het SIP OAuth gebruikt in plaats van de beveiligde apparaatregistratie via TLS wanneer CUCM werkt in een gemengde modus met een beveiligd telefoonbeveiligingsprofiel, maar los daarvan blijft alles hetzelfde.

## Oplossing 3: Versleuteld iX-kanaal voor onbeveiligde telefoonbeveiligingsprofielen (CUCM 12.5(1)SU1 of hoger)




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

**Voorwaarden:**

- CUCM versie 12.5(1)SU1 of hoger (release notes)
- Expressway X12.5.1 of hoger (release notes)

**Voor:**

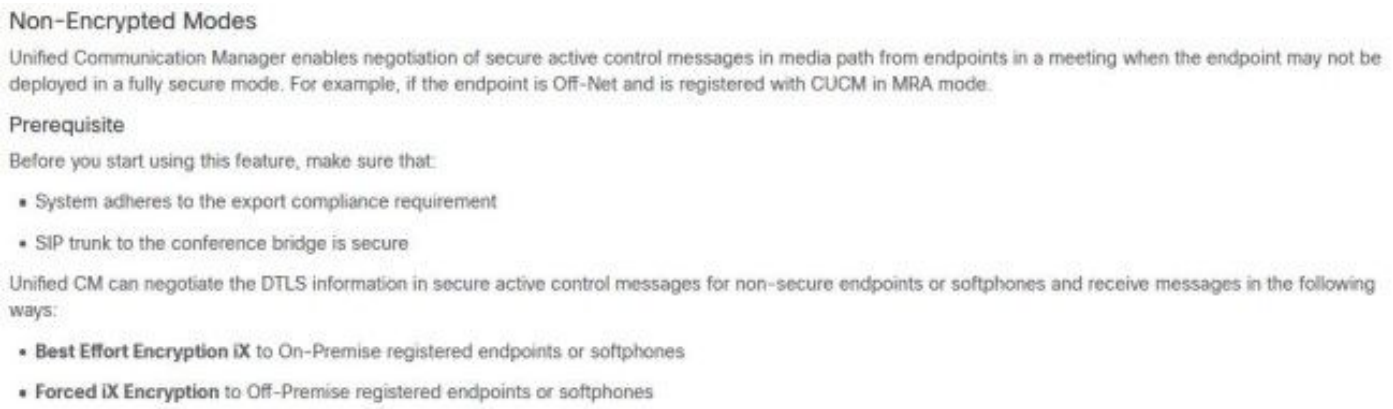
- U hoeft CUCM niet in gemengde modus in te stellen
- Geen noodzaak voor het instellen van beveiligde end-to-end communicatie
- Van toepassing op zowel Jabber- als TC/CE-endpoints

**Opmerking:**

- Upgrade van CUCM vereist
- Alleen CUCM-beperkte versies worden ondersteund

Van CUCM 12.5(1)SU1, ondersteunt het iX-encryptie onderhandeling voor elk SIP-lijnapparaat, zodat het de DTLS-informatie kan onderhandelen in beveiligde ActiveControl-berichten voor niet-beveiligde endpoints of softphones. Het verstuurt iX-encryptie over TCP waardoor telefoons een versleuteld iX-kanaal te beëindigen ondanks een onveilige TCP-verbinding (niet TLS) naar de CUCM.

In de beveiligingsgids van CUCM 12.5(1)SU1 onder de sectie 'Encrypted iX Channel', laat het zien dat voor niet-versleutelde modi met onveilige apparaten, de beste inspanning en geforceerde iX-encryptie kan worden onderhandeld met de voorwaarde dat uw systeem zich houdt aan de export compliance en de SIP-trunk naar uw conferentiebrug veilig is.



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

Op CUCM:

- U moet gebruiken export beperkte CUCM (niet onbeperkt)
- Onder **System > Licensing > Licentiebeheer**, moet u de optie "Export-Controlled Functionality" op toegestaan instellen.
- Uw SIP-trunk moet de optie "**SRTP ingeschakeld**" hebben (ongeacht of de trunk zelf beveiligd of onbeveiligd is)

Bij CMS:

- Uw callbridge moet een licentie met encryptie hebben (zodat u geen callBridgeNoEncryption-licentie hebt)
- Op webadmin onder **Configuration > Call Settings**, moet u de **SIP media encryptie** hebben ingesteld op **toegestaan** (of **vereist**)

In het beeld, kunt u zien dat de verbinding veilig is tot Expressway-C en dan C over SDP naar CUCM zonder de crypto lijnen verzenden maar het omvat nog het iX mediakanaal. Dus de normale media voor audio/video/... is niet beveiligd met cryptolijnen maar het heeft nu wel een beveiligde verbinding voor iX media kanaal, zodat de Expressway de DTLS-verbinding niet hoeft te beëindigen. Daarom kan ActiveControl rechtstreeks tussen de client en de conferentiebrug worden onderhandeld, zelfs met een onveilig beveiligingsprofiel voor de telefoon. In eerdere versies van CUCM zou de stroom anders zijn en ActiveControl wordt niet onderhandeld omdat het niet over het iX-kanaal naar het CMS in de eerste plaats omdat dat deel reeds zou zijn gestript.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.