Abilita ActiveControl su MRA/Expressway

Sommario

Introduzione

In questo documento vengono descritte le diverse opzioni per abilitare il protocollo ActiveControl per i client Mobile e Remote Access (MRA) e per le chiamate dagli endpoint locali a Webex Meetings tramite Expressway. MRA è una soluzione di installazione per Jabber e funzionalità endpoint VPN (Virtual Private Network-less). Questa soluzione consente agli utenti finali di connettersi alle risorse aziendali interne da qualsiasi parte del mondo. Il protocollo ActiveControl è un protocollo proprietario di Cisco che consente di sfruttare al meglio le funzionalità di conferenza in fase di esecuzione, ad esempio gli elenchi delle riunioni, le modifiche al layout video, le opzioni di disattivazione dell'audio e di registrazione.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Expressway (chiamate MRA e B2B)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In questo documento l'attenzione principale è posta sulla connessione del client MRA a un Cisco Meeting Server (CMS), ma lo stesso vale per altri tipi di piattaforme o connessioni, come ad esempio quando ci si connette a Webex Meetings. È possibile applicare la stessa logica per i seguenti tipi di flussi di chiamata:

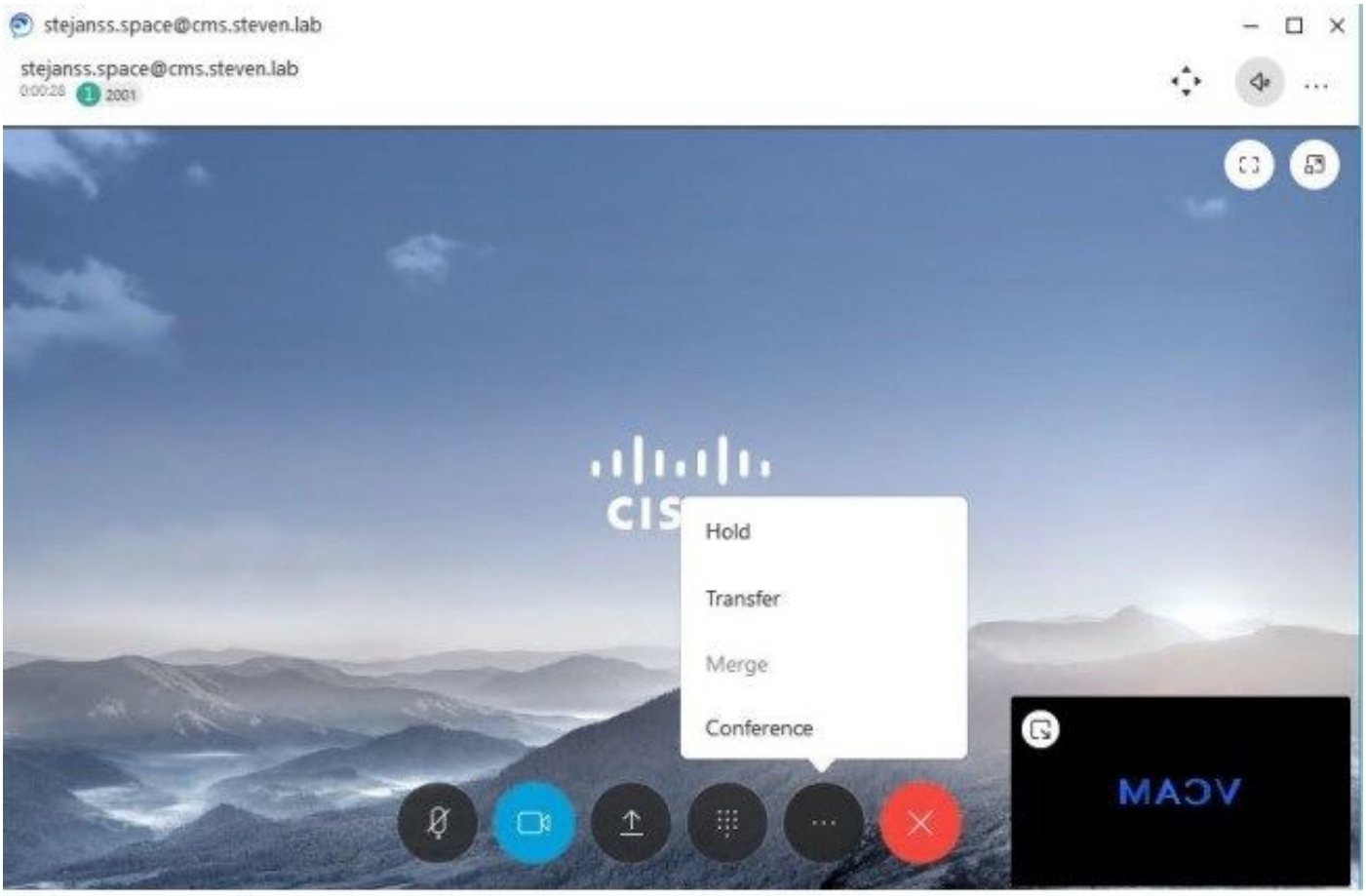
- Endpoint - CUCM - Expressway-C - Expressway-E - Webex Meeting
- Endpoint MRA - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Webex Meeting

  Nota: le funzionalità di ActiveControl supportate da Webex Meetings sono diverse da quelle di CMS in questo momento e sono solo un sottoinsieme limitato.

La piattaforma Cisco Meeting Server offre ai partecipanti la possibilità di controllare l'esperienza di una riunione direttamente dall'endpoint di conferenza tramite ActiveControl senza la necessità di applicazioni o operatori esterni. ActiveControl utilizza il protocollo multimediale iX nei dispositivi Cisco e viene negoziato come parte dei messaggi SIP di una chiamata. A partire dalla versione 2.5 di CMS, le principali funzionalità abilitate sono le seguenti (sebbene possano dipendere dal tipo di endpoint e dalla versione software in uso):

- Visualizzazione di un elenco di tutti i partecipanti (elenco dei partecipanti o elenco dei partecipanti) connessi al meeting
- Disattivazione o riattivazione dell'audio di altri partecipanti
- Aggiunta o rimozione di un altro partecipante dalla riunione
- Avvio o interruzione della registrazione di una riunione
- Rendere un partecipante importante
- Indicatore per il partecipante che è il relatore attivo della riunione
- Indicatore per il partecipante che sta attualmente condividendo il contenuto o la presentazione nella riunione
- Blocco o sblocco della riunione

Nella prima immagine è visualizzata una visualizzazione utente da un client Jabber che ha effettuato una chiamata in uno spazio CMS senza ActiveControl, mentre nella seconda immagine è illustrata la visualizzazione utente più ricca di funzionalità in cui Jabber è stato in grado di negoziare ActiveControl con il server CMS.



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl è un protocollo basato su XML che viene trasferito utilizzando il protocollo iX che viene negoziato nel SDP (Session Description Protocol) delle chiamate SIP (Session Initiation Protocol). È un protocollo Cisco (eXtensible Conference Control Protocol (XCCP)) e negoziato solo in SIP (quindi le chiamate interconnesse non dispongono di ActiveControl) e utilizza UDP/UDT (UDP-based Data Transfer Protocol) per il trasferimento dei dati. La negoziazione sicura avviene tramite il protocollo DTLS (Datagram TLS), che può essere considerato come TLS

su una connessione UDP. Di seguito sono riportati alcuni esempi delle differenze nelle negoziazioni.

Non crittografato

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

Crittografia (tentativo di crittografia, ma possibilità di fallback a connessioni non crittografate)

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

a=ixmap:2 **xccp**

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

Crittografia (imposizione della crittografia - non consentire il fallback a connessioni non crittografate)

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

a=ixmap:2 **xccp**

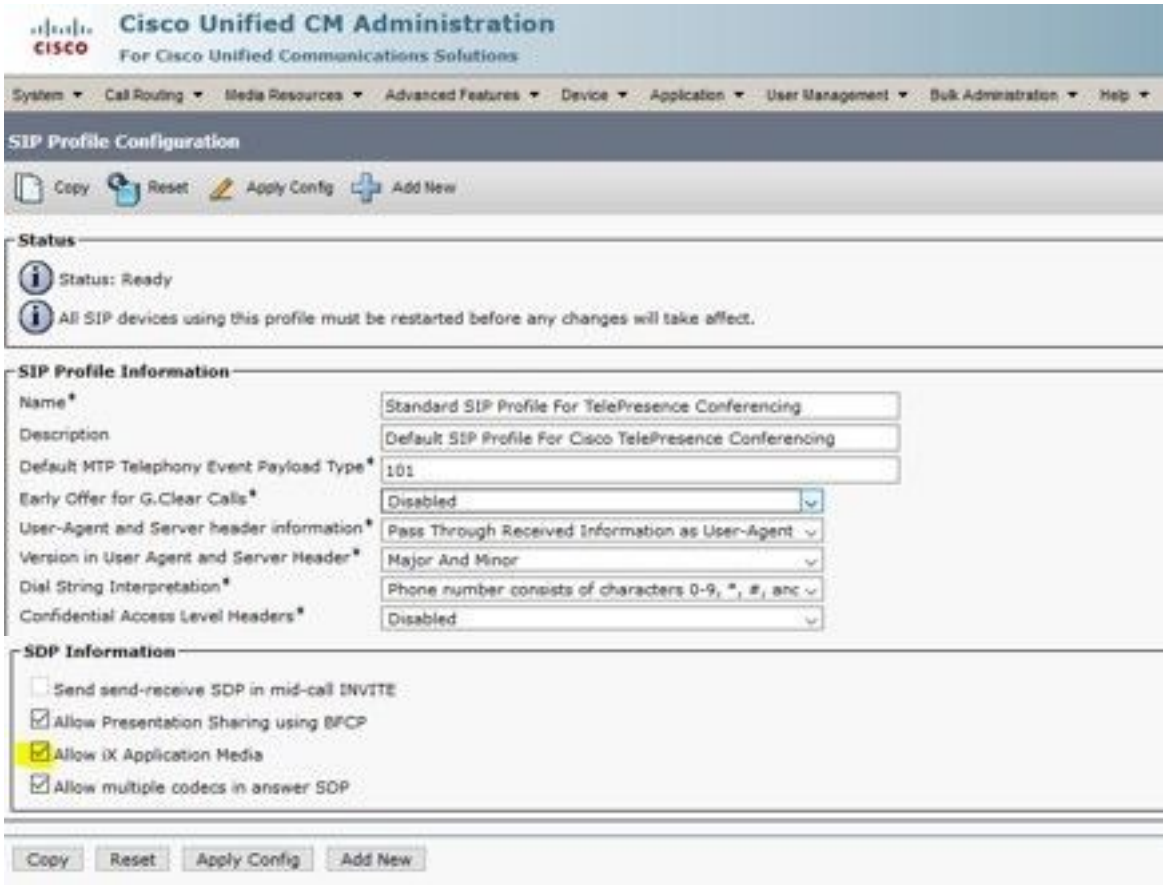
a=**fingerprint**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

Per il supporto completo di ActiveControl sono necessarie almeno alcune versioni software:

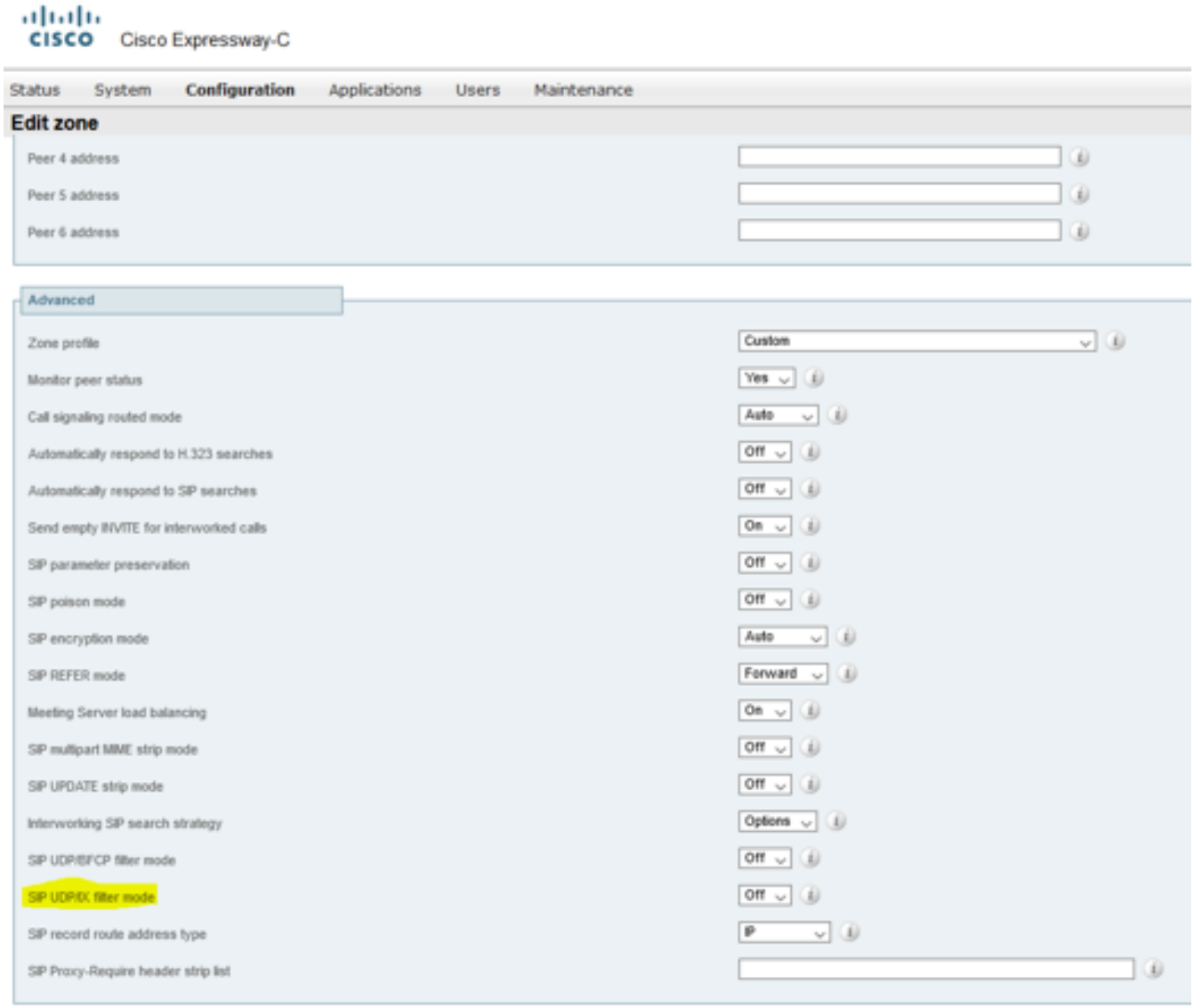
- Jabber versione 12.5 o successiva (note di rilascio)
- Endpoint CE 8.3 o successivi, 9.6.2 o successivi consigliati in base alla guida CMS Active Control (CE9.3.1 o successivi per Webex in base al collegamento alla guida di Webex)
- CUCM 10.5 o versioni successive (per il supporto ActiveControl di Jabber 12.5) (11.5(1) o versioni successive per Webex come da collegamento)
- CMS 2.1 o versione successiva, 2.5 o versione successiva consigliata in base alla guida CMS ActiveControl
- Expressway X12.5 o versioni successive (note di rilascio) per consentire il supporto di client MRA non crittografati

Èpossibile prendere in considerazione alcune opzioni di configurazione:

- In CUCM verificare che i trunk SIP rilevanti (a Expressway-C e CMS) siano configurati con un profilo SIP con l'opzione 'Consenti supporto applicazione iX' selezionata



- Sul CMS è abilitato per impostazione predefinita a partire dalla 2.1, ma è possibile disabilitarlo tramite un compatibilityProfile su cui è possibile impostare *sipUDT* su false
- In Expressway nella configurazione di zona in Impostazioni avanzate (quando si utilizza un profilo di zona personalizzato), verificare che la *modalità filtro SIP UDP/IX* sia impostata su 'Off' se si desidera consentire il passaggio di iX



Problema

Informazioni generali

ActiveControl è stato negoziato in modo diverso rispetto ad altri canali multimediali. Per altri canali multimediali come audio e video, ad esempio, l'SDP viene aggiunto con linee crittografiche che vengono utilizzate per annunciare alla parte remota la chiave di crittografia da utilizzare per questo canale. Il canale Real-time Transport Protocol (RTP) può quindi essere reso sicuro e considerato come Secure RTP (SRTP). Per il canale iX, utilizza il protocollo DTLS per crittografare il flusso multimediale XCCP in modo da utilizzare un meccanismo diverso.

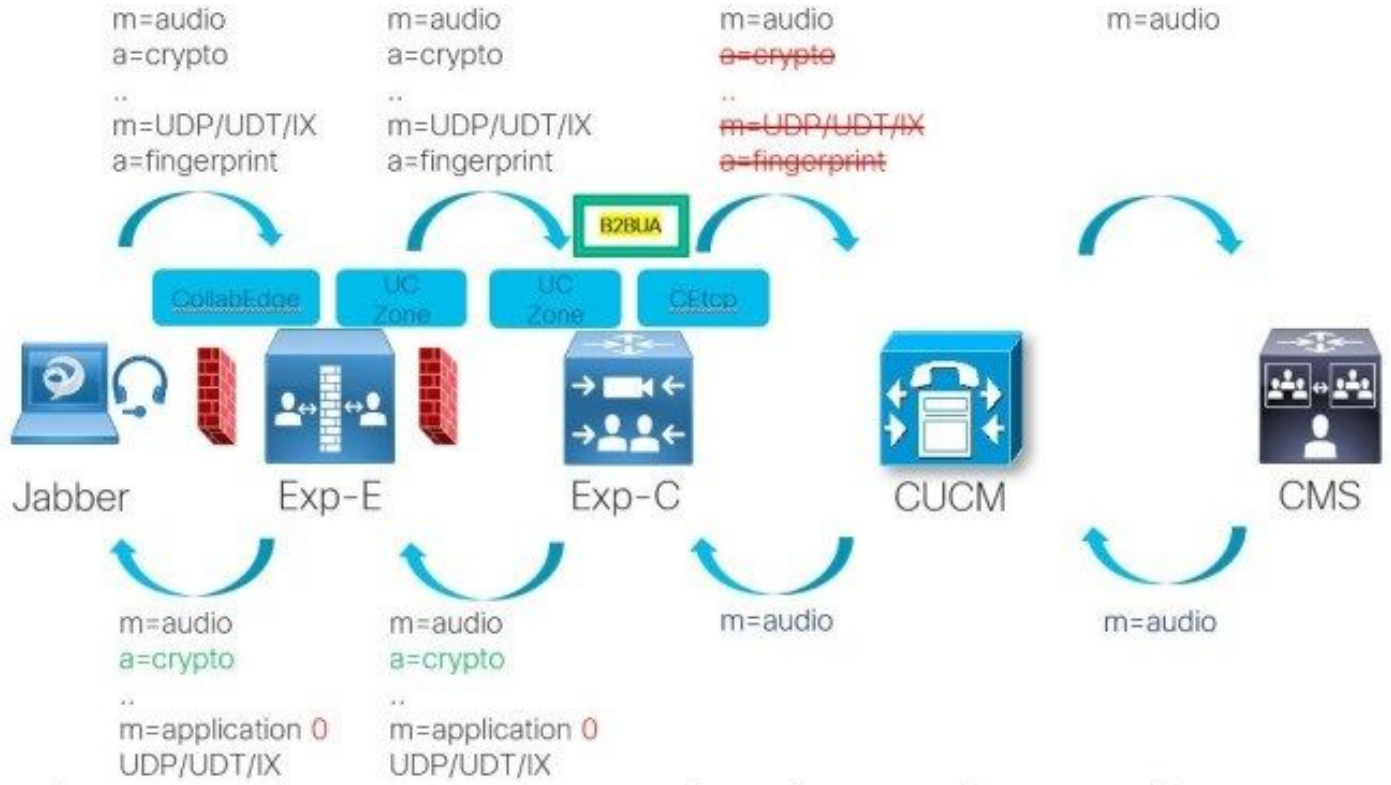
Il software Expressway non termina il protocollo DTLS. Questa condizione è indicata nella sezione *Limitazioni* in *Funzionalità non supportate* delle note di rilascio di Expressway.

- 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.

Versioni di Expressway prima di X12.5

Quando si esegue una versione di Expressway precedente a X12.5, se è presente una

connessione in entrata con un canale iX crittografato che viene trasmesso attraverso una zona TCP non protetta, Expressway rimuove sia le linee crittografiche dei normali canali multimediali che l'intero canale iX. Questo viene mostrato visivamente per un client MRA che si connette a uno spazio CMS dove si vede che la connessione è sicura dal client MRA a Expressway-C ma poi a seconda del profilo di sicurezza telefonica impostato su CUCM per il dispositivo, è non crittografato (e inviato sulla zona CEtcp) o criptato (e inviato sulla zona CEtls). Quando non è crittografato, come mostrato nell'immagine, si vede che Expressway-C rimuove le linee crittografiche per tutti i canali multimediali e addirittura rimuove l'intero canale iX, anche perché non può terminare il protocollo DTLS. Questo avviene tramite l'agente utente back-to-back (B2BUA), in quanto la configurazione della zona CEtcp è configurata con la crittografia dei supporti 'Force unencrypted'. Nella direzione opposta (sulla zona di attraversamento UC con crittografia dei supporti 'Force encrypted') quando si riceve la risposta SDP, le linee crittografiche per le linee multimediali normali vengono aggiunte e la porta del canale iX viene azzerata, evitando la negoziazione ActiveControl. Internamente, quando i client sono registrati direttamente in CUCM, consente sia i canali multimediali iX crittografati che non crittografati, in quanto CUCM non si inserisce nel percorso multimediale.



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

Lo stesso tipo di logica si applica alle connessioni di chiamata da Expressway a Webex Meetings. Richiede che il percorso completo sia end-to-end sicuro, in quanto i server Expressway (prima di X12.5) passano solo attraverso le informazioni di connessione DTLS, ma non terminano su di esso per avviare una nuova sessione o per crittografare/decrittografare il canale multimediale sulle diverse tratte di chiamata.

Versioni Expressway di X12.5 e successive

Quando si esegue una versione Expressway di X12.5 o successiva, il comportamento è cambiato in quanto ora passa sul canale iX tramite la connessione della zona TCP come crittografia forzata (UDP/DTLS/UDT/IX) in modo da consentire la negoziazione del canale iX, ma solo quando anche l'estremità remota utilizza la crittografia. Impone la crittografia perché Expressway non termina la sessione DTLS e pertanto agisce solo su pass-through, pertanto si basa sull'estremità remota per

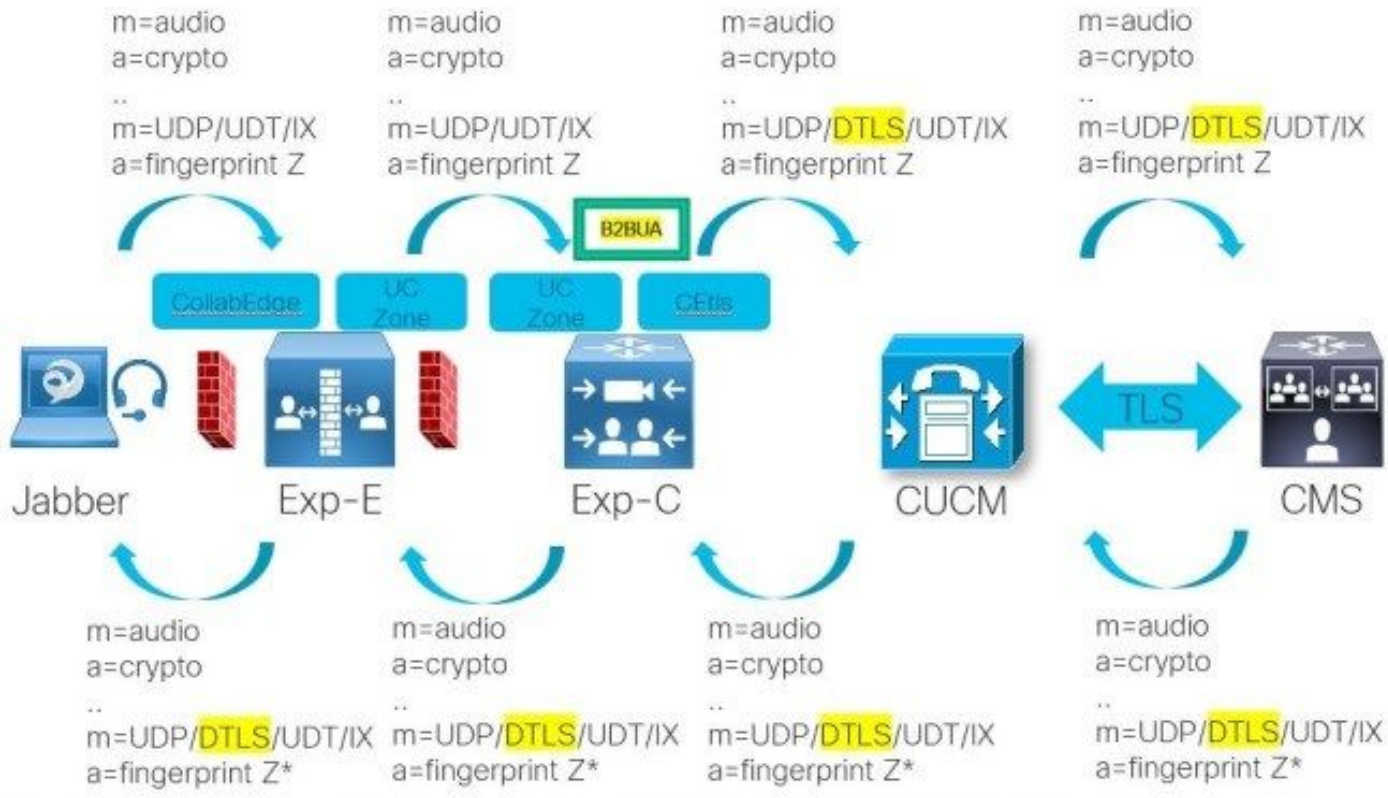
avviare/terminare la sessione DTLS. Le linee crittografiche vengono eliminate tramite la connessione TCP per motivi di sicurezza. Questo cambiamento di comportamento è descritto nelle note sulla versione nella sezione "MRA: Supporto per iX crittografati (per ActiveControl)". Ciò che accade dopo, dipende dalla versione CUCM come tale comportamento è cambiato in 12.5(1)SU1 dove permette di passare su canale iX e su connessioni in ingresso non sicure. Anche quando ci sarebbe un trunk SIP TLS sicuro su CMS, quando si esegue CUCM versione inferiore a 12.5(1)SU1, avrebbe spogliato il canale iX prima di passarlo al CMS e quindi alla fine si avrebbe una porta azzerata da 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.

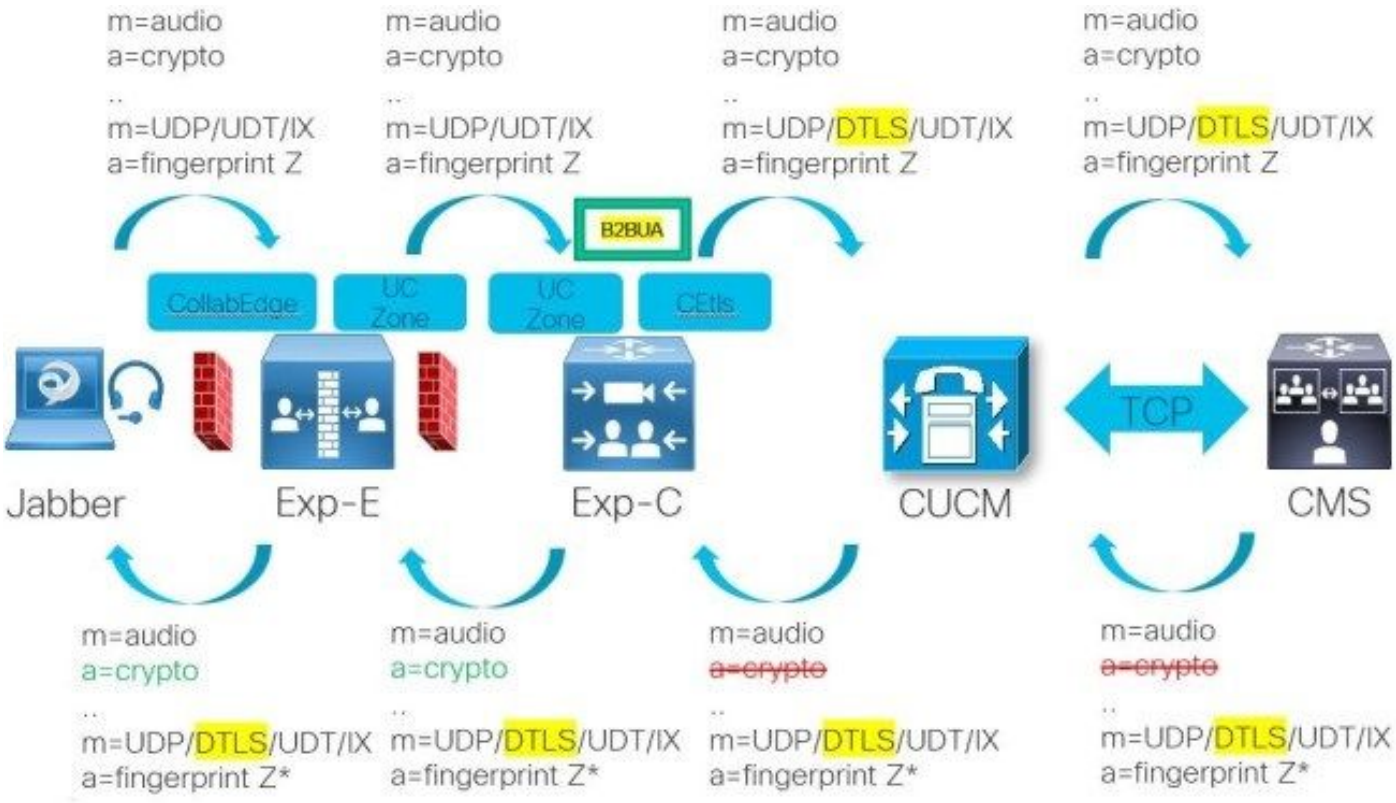
Con un percorso multimediale e una segnalazione di chiamata end-to-end sicura, il canale iX può essere negoziato direttamente (passato attraverso diversi hop di server Expressway) tra il client (MRA) e la soluzione di conferenza (CMS o Webex Meeting). Nell'immagine è illustrato lo stesso flusso di chiamate per il client MRA che si connette a uno spazio CMS, ma ora con un profilo di sicurezza telefono protetto configurato su CUCM e un trunk SIP TLS sicuro su CMS. È possibile verificare che il percorso sia completamente sicuro e che il parametro DTLS fingerprint venga passato sull'intero percorso.



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

Per impostare un profilo di sicurezza del dispositivo protetto, è necessario verificare che il CUCM sia configurato in modalità mista e che ciò possa risultare complesso, anche quando è operativo in quanto richiede la funzione CAPF (Certificate Authority Proxy Function) per comunicazioni locali protette. Pertanto, è possibile offrire altre soluzioni più convenienti per supportare la disponibilità di ActiveControl su MRA ed Expressway in generale, come descritto in questo documento.

I trunk SIP TLS sicuri verso i server CMS non sono richiesti perché CUCM (presumendo che il trunk SIP abbia l'opzione SRTP consentito abilitata) passa sempre da una connessione SIP protetta in entrata sul canale iX e sulle linee crittografiche, ma CMS risponde solo con crittografia al canale iX (consentendo ActiveControl) (presumendo che la **crittografia dei supporti SIP** sia impostata su *consentito* o *imposto* su CMS in **Impostazioni > Impostazioni chiamata**) ma non ha crittografia sugli altri canali multimediali in quanto rimuove le linee crittografiche da essi in base all'immagine. I server Expressway possono aggiungere di nuovo le linee crittografiche per proteggere ancora quella parte della connessione (e iX viene negoziato direttamente tra i client finali ancora tramite DTLS), ma questo non è ideale dal punto di vista della sicurezza ed è quindi consigliabile configurare un trunk SIP sicuro per il bridge di conferenze. Quando **SRTP Allowed** non è selezionato sul trunk SIP, CUCM rimuove le linee crittografiche e la negoziazione iX sicura ha esito negativo.



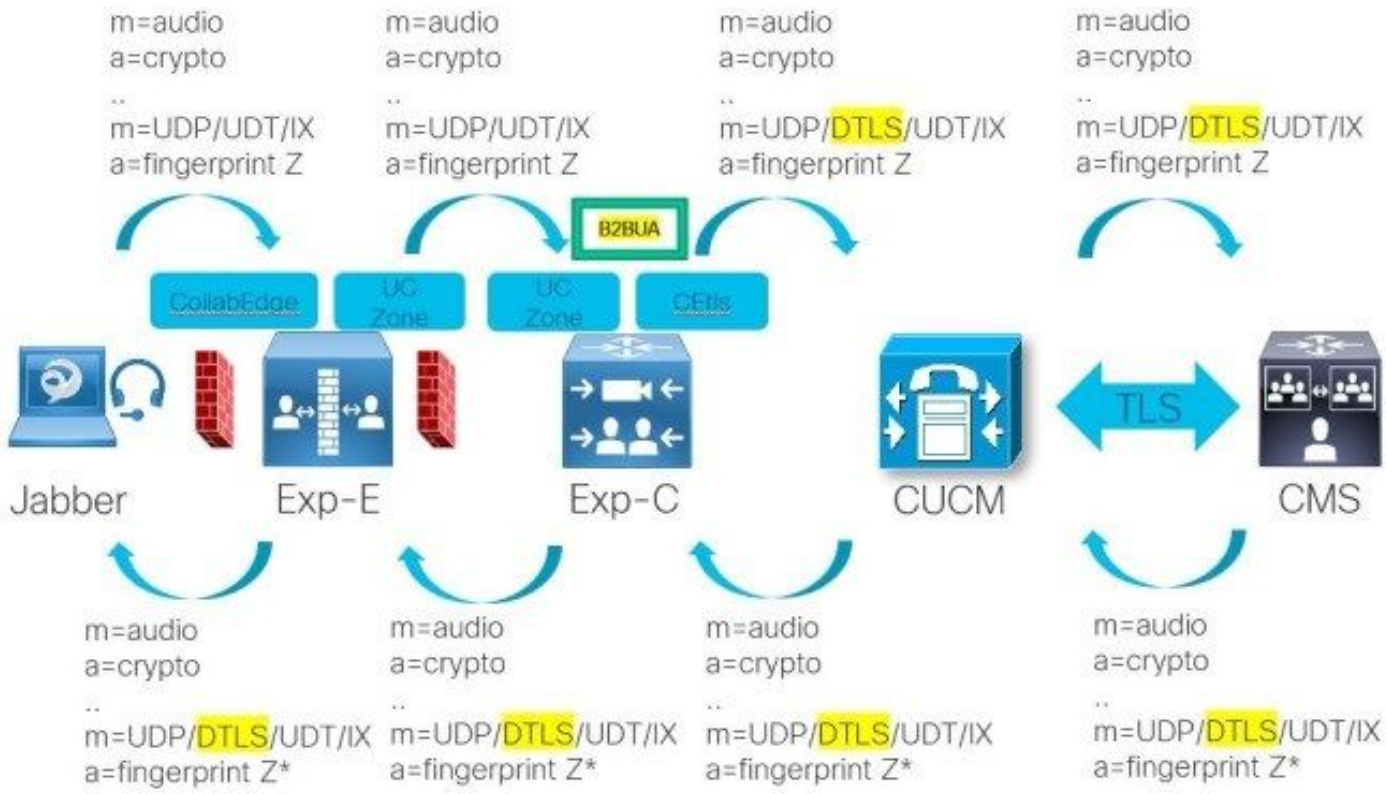
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

Soluzione

Ci sono un paio di opzioni diverse disponibili con vari requisiti e vari pro e contro. Ognuno di essi è presentato in una sezione più dettagliata. Le diverse opzioni sono:

1. Profili di sicurezza telefono protetto per gli endpoint (CUCM in modalità mista)
2. SIP OAuth per Jabber
3. Canale iX crittografato per profili di sicurezza telefono non protetto (CUCM 12.5(1)SU1 o superiore)

Soluzione 1: profili di protezione telefono sicuro per gli endpoint (CUCM in modalità mista)



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

Prerequisiti:

- CUCM in modalità mista

Pro:

- Compatibile con qualsiasi versione CUCM
- Compatibile con tutti i dispositivi client

Con:

- Richiede la configurazione di CUCM in modalità mista (e le operazioni CAPF sugli endpoint locali)

Questo è il metodo descritto anche nella sezione Problema e si trova alla fine del percorso, in cui è possibile assicurarsi di disporre di una segnalazione di chiamata e di un percorso multimediale crittografati end-to-end. È necessario impostare CUCM in modalità mista come indicato nel documento seguente.

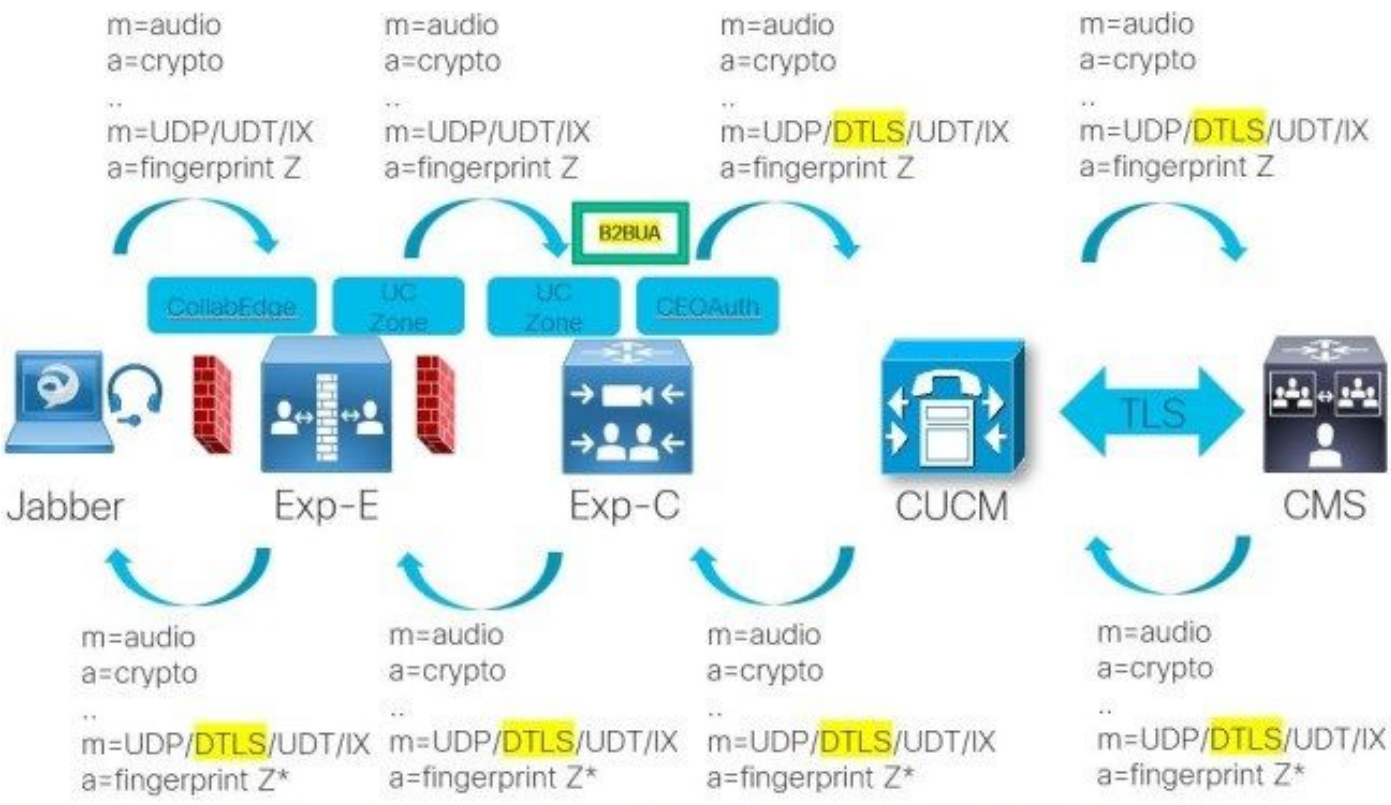
Per i client MRA non è richiesta alcuna operazione CAPF, ma assicurarsi di seguire i passaggi di configurazione aggiuntivi con il profilo di sicurezza per il telefono protetto con un nome che corrisponda a uno dei nomi alternativi soggetto del certificato del server Expressway-C, come evidenziato nell'esempio di configurazione degli endpoint basati su TC di Collaboration Edge (applicabile anche agli endpoint basati su CE e ai client Jabber).

Quando ci si connette da un endpoint locale o da un client Jabber a un Webex Meeting, è necessario eseguire l'operazione CAPF per registrare in modo sicuro il client su CUCM. Ciò è necessario per garantire il flusso di chiamate protette end-to-end in cui Expressway può solo passare la negoziazione DTLS e non gestirla direttamente.

Per rendere sicura la chiamata end-to-end, accertarsi inoltre che tutti i trunk SIP rilevanti (a Expressway-C in caso di chiamata a Webex Meeting e a CMS in caso di chiamata a una

conferenza CMS) siano trunk SIP sicuri che utilizzino TLS con un profilo di sicurezza trunk SIP sicuro.

Soluzione 2: SIP OAuth per Jabber



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

Prerequisiti:

- Cisco Jabber 12.5 o versione successiva (note di rilascio)
- CUCM versione 12.5 o successiva (note di rilascio) con *OAuth con flusso di accesso per l'aggiornamento* abilitato
- Expressway X12.5.1 o versione successiva (note di rilascio) con *token Authorize by OAuth con aggiornamento* abilitato

Pro:

- Consente registrazioni sicure e una facile commutazione tra locali e locali senza necessità di rinnovare ogni volta il file CAPF
- Non è necessario impostare CUCM in modalità mista

Con:

- Applicabile solo a Jabber, non applicabile agli endpoint TC/CE

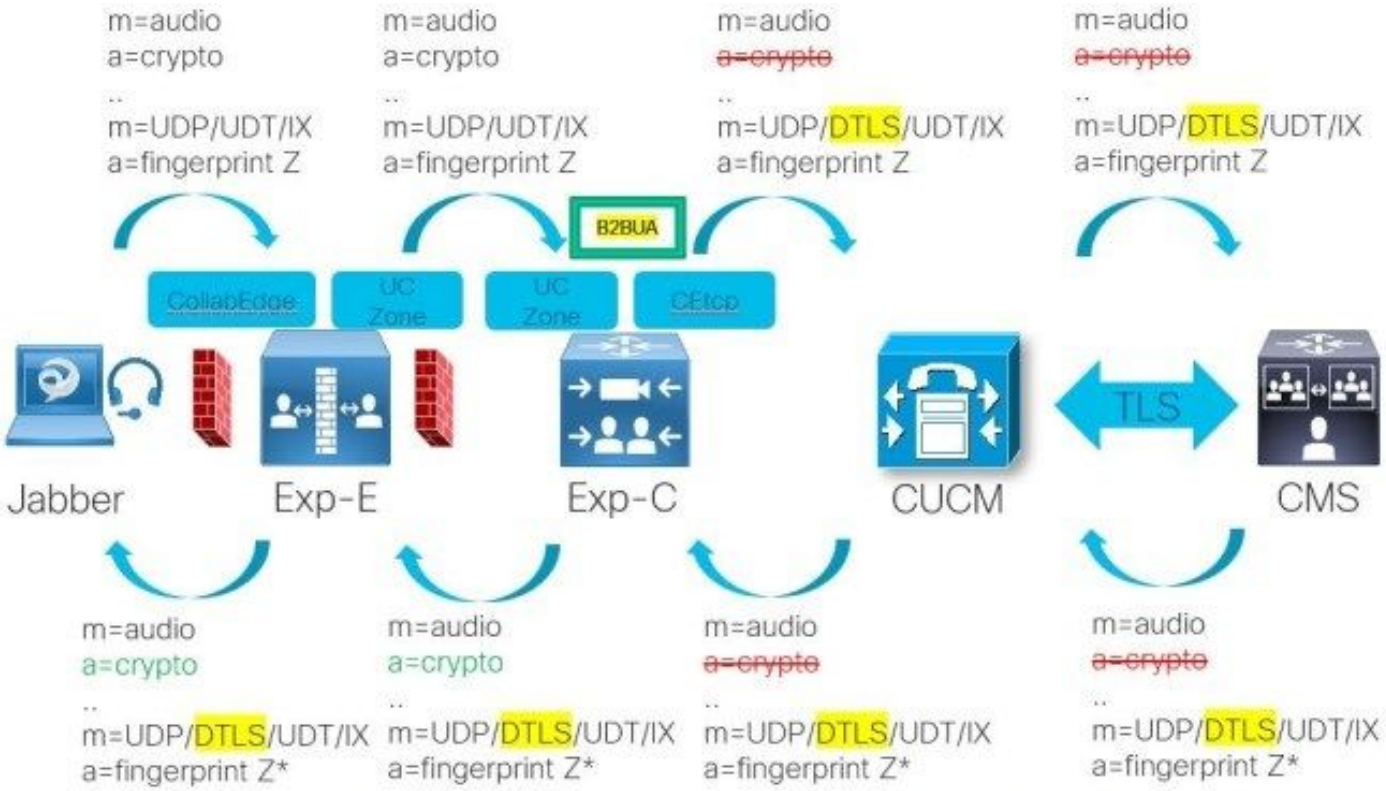
La modalità SIP OAuth consente di utilizzare i token di aggiornamento OAuth per l'autenticazione Cisco Jabber in ambienti protetti. Garantisce una segnalazione e supporti sicuri senza il requisito CAPF della soluzione 1. La convalida del token durante la registrazione SIP viene completata quando l'autorizzazione basata su OAuth è abilitata sul cluster CUCM e sugli endpoint Jabber.

La configurazione in CUCM è documentata nella guida alla configurazione delle funzionalità e richiede che sia già abilitata la funzionalità OAuth con Flusso di login per l'aggiornamento in Parametri aziendali. Per abilitare questa funzionalità anche su MRA, assicurarsi di aggiornare i

nodi CUCM nel server Expressway-C in **Configurazione > Comunicazione unificata > Server CM unificati in** modo che in **Configurazione > Zone > Zone** sia ora necessario visualizzare anche le zone CEOAuth create automaticamente. Verificare inoltre che in **Configurazione > Comunicazione unificata > Configurazione** sia attivata anche l'opzione **Autorizza tramite token OAuth con aggiornamento**.

Con questa configurazione, è possibile ottenere una connessione di chiamata sicura end-to-end simile sia per la segnalazione che per i supporti, quindi Expressway sta passando la negoziazione DTLS poiché non termina il traffico in sé. Questo è visto sull'immagine dove l'unica differenza rispetto alla soluzione precedente è che utilizza la zona CEOAuth su Expressway-C per CUCM rispetto alla zona CEtls perché utilizza SIP OAuth piuttosto che la registrazione del dispositivo sicuro su TLS quando CUCM opera in modalità mista con un profilo di sicurezza del telefono sicuro, ma a parte questo, tutto rimane lo stesso.

Soluzione 3: canale iX crittografato per profili di sicurezza telefono non protetti (CUCM 12.5(1)SU1 o superiore)



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

Prerequisiti:

- CUCM versione 12.5(1)SU1 o superiore (note di rilascio)
- Expressway X12.5.1 o versione successiva (note di rilascio)

Pro:

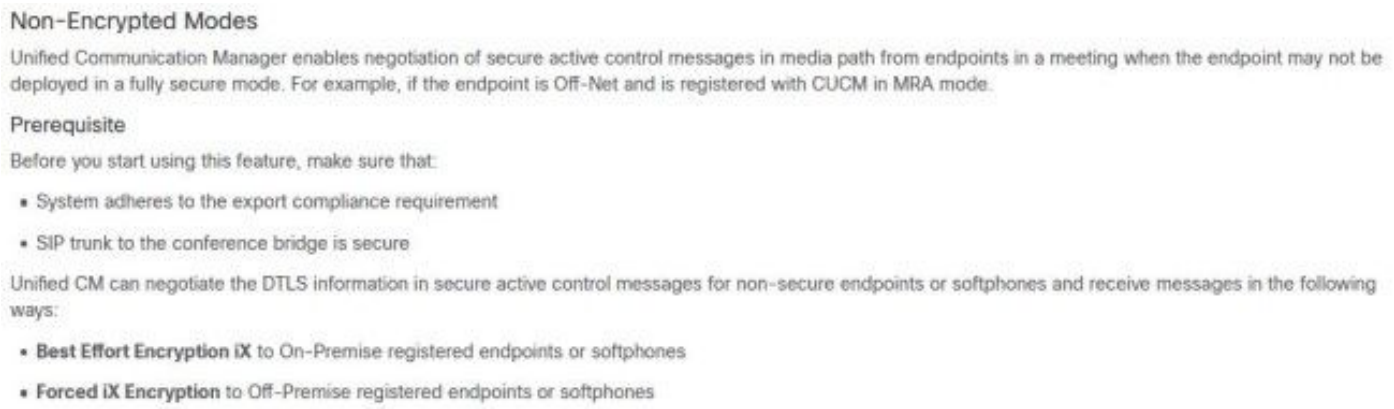
- Non è necessario impostare CUCM in modalità mista
- Nessuna necessità di comunicazioni end-to-end sicure
- Applicabile agli endpoint Jabber e TC/CE

Con:

- Aggiornamento di CUCM richiesto
- Sono supportate solo le versioni con restrizioni CUCM

Da CUCM 12.5(1)SU1, supporta la negoziazione della crittografia iX per qualsiasi dispositivo di linea SIP in modo da poter negoziare le informazioni DTLS nei messaggi ActiveControl sicuri per endpoint o softphone non protetti. Invia la massima crittografia iX su TCP consentendo ai telefoni di avere un canale iX criptato end-to-end nonostante una connessione TCP non sicura (non TLS) al CUCM.

Nella guida alla sicurezza di CUCM 12.5(1)SU1 nella sezione 'Encrypted iX Channel', viene mostrato che per le modalità non crittografate con dispositivi non sicuri, è possibile negoziare il massimo sforzo e la crittografia iX forzata con il prerequisito che il sistema rispetti la conformità alle normative di esportazione e che il trunk SIP sul bridge di conferenza sia sicuro.



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

Per CUCM:

- Ènecessario utilizzare Esporta CUCM con restrizioni (non senza restrizioni)
- In **Sistema > Licenze > Gestione licenze**, "Funzionalità sottoposta a controllo per l'esportazione" deve essere impostato su consentito.
- Sul trunk SIP deve essere abilitata l'opzione "**SRTP consentito**" (indipendentemente dal fatto che il trunk sia sicuro o non sicuro)

CMS:

- Il callbridge deve disporre di una licenza con crittografia (pertanto non si dispone della licenza callBridgeNoEncryption)
- In webadmin in **Configurazione > Impostazioni chiamata**, è necessario aver impostato la **crittografia dei supporti SIP** su **consentita** (o **richiesta**)

Nell'immagine, è possibile vedere che la connessione è sicura fino a quando Expressway-C e poi C invia l'SDP a CUCM senza le linee crittografiche, ma include ancora il canale multimediale iX. Quindi il supporto normale per audio/video/... non è protetto con linee crittografiche, ma dispone ora di una connessione protetta per il canale multimediale iX in modo che Expressway non debba terminare la connessione DTLS. Pertanto, ActiveControl può essere negoziato direttamente tra il client e il bridge di conferenze, anche con un profilo di protezione telefono non protetto. Nelle versioni precedenti di CUCM, il flusso sarebbe diverso e ActiveControl non viene negoziato perché non passa il canale iX al CMS in primo luogo perché la parte sarebbe già stata rimossa.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).