啟用對MRA/Expressway的ActiveControl

目錄

簡介

本文檔介紹用於為移動和遠端訪問(MRA)客戶端啟用ActiveControl協定以及通過Expressway從本地終端到Webex Meetings的呼叫的不同選項。MRA是用於虛擬專用無網路(VPN)Jabber和終端功能的部署解決方案。此解決方案允許終端使用者從全球任何地方連線到內部企業資源。ActiveControl協定是Cisco專有協定，它通過會議記錄器、影片佈局更改、靜音和錄製選項等運行時功能提供更豐富的會議體驗。

必要條件

需求

思科建議您瞭解以下主題：

- Expressway（MRA和B2B呼叫）

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Expressway X12.5
- 思科會議伺服器(CMS)2.9
- 思科整合通訊管理員12.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

在本文檔中，主要關注的是與Cisco Meeting Server(CMS)的MRA客戶端連線，但同樣適用於其他型別的平台或連線，例如連線到Webex Meetings時。相同的邏輯可以應用於以下型別的呼叫流：

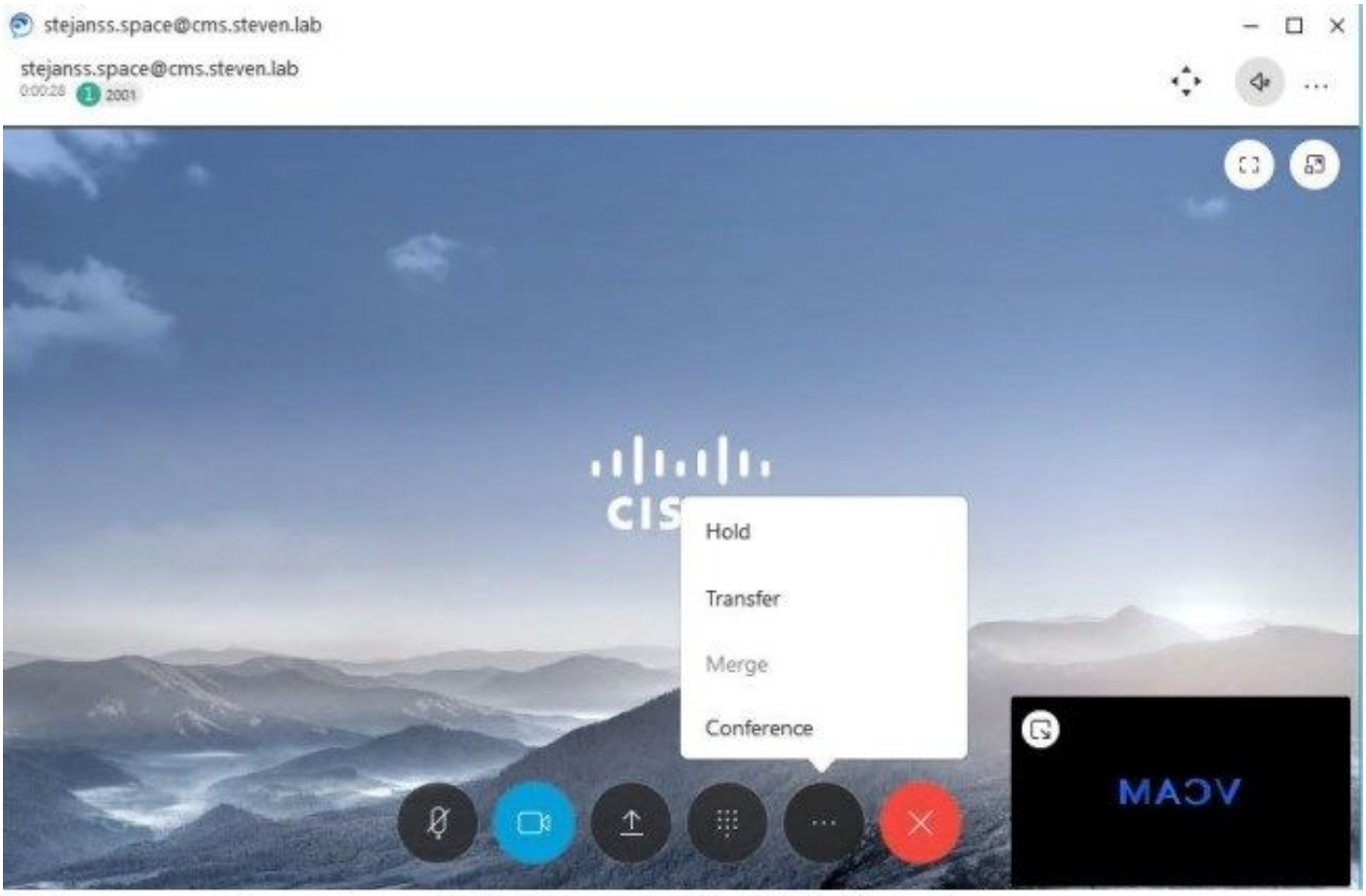
- 終端 — CUCM - Expressway-C - Expressway-E - Webex Meeting
- MRA端點 — (Expressway-E - Expressway-C)- CUCM - Expressway-C - Expressway-E - Webex Meeting

註:Webex Meetings支援的ActiveControl的功能與目前的CMS功能不同，並且僅是一個有限的子集。

思科會議伺服器平台使會議參與者能夠通過ActiveControl直接從其會議終端控制其會議體驗，而無需外部應用程式或操作員。ActiveControl在思科裝置中利用iX媒體協定，並作為呼叫的SIP消息的一部分進行協商。自CMS版本2.5起，啟用的主要功能如下（儘管它們可能取決於使用的終端型別和軟體版本）：

- 檢視連線到會議的所有參與者（名冊清單或參與者清單）的清單
- 使其他參與者靜音或取消靜音
- 在會議中新增或刪除其他參與者
- 開始或停止會議錄製
- 使參與者成為重要參與者
- 會議中活動發言人的與會者的指示器
- 當前在會議中共用內容或簡報的參與者的指示器
- 鎖定或解鎖會議

在第一個影象中，您會看到來自Jabber客戶端的使用者檢視，該使用者檢視將呼叫置入沒有ActiveControl的CMS空間，而第二個影象則顯示功能更豐富的使用者檢視，其中Jabber能夠與CMS伺服器協商ActiveControl。



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl是一種基於XML的協定，它使用在會話發起協定(SIP)呼叫的會話描述協定(SDP)中協商的iX協定進行傳輸。它是思科協定(可擴展會議控制協定(XCCP))並且僅在SIP中協商（因此互通呼叫不具有ActiveControl），並且利用UDP/UDT（基於UDP的資料傳輸協定）進行資料傳輸。安全協商通過資料包TLS(DTLS)進行，可以將其視為TLS over UDP連線。這裡顯示了一些協商差異的示例。

未加密

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

已加密（盡最大努力 — 嘗試加密，但允許回退到未加密的連線）

m=應用程式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:xx:xx:

已加密（強制加密 — 不允許回退到未加密的連線）

m=應用程式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:xx:xx:

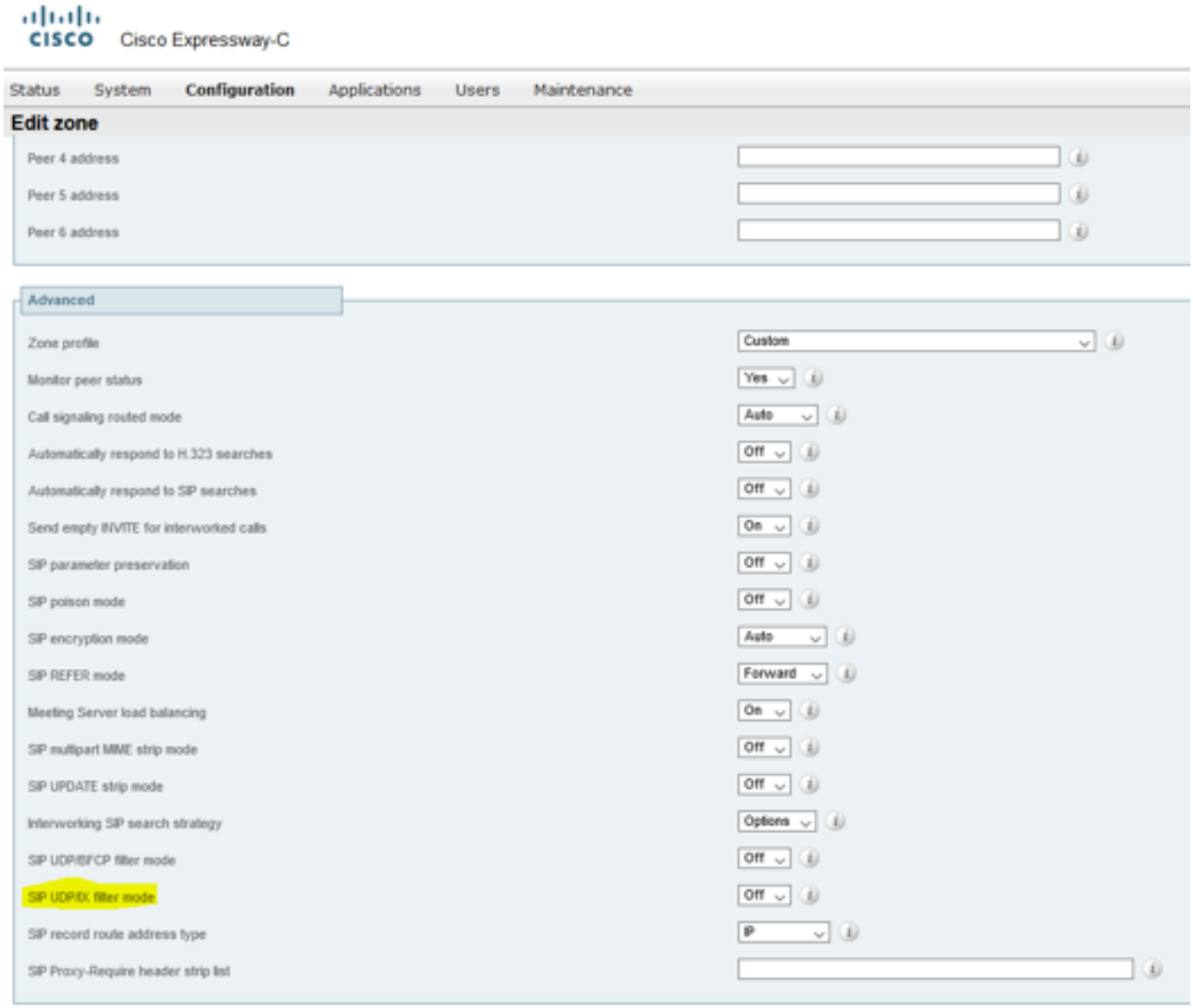
以下是完整ActiveControl支援所需的最低軟體版本：

- Jabber 12.5或更高版本(發行說明)
- 根據CMS ActiveControl指南，建議使用CE終端8.3或更高版本、9.6.2或更高版本(根據Webex幫助連結，適用於Webex的CE9.3.1或更高版本)
- CUCM 10.5或更高版本（適用於Jabber 12.5 ActiveControl支援）(11.5(1)或更高版本，適用於Webex(根據鏈路)
- 根據CMS ActiveControl指南，建議使用CMS 2.1或更高版本、2.5或更高版本
- Expressway X12.5或更高版本(發行說明)，以允許對非加密MRA客戶端提供支援

有幾個配置選項需要考慮：

- 在CUCM上，確保相關SIP中繼（到Expressway-C和CMS）配置有SIP配置檔案，該配置檔案已選中「允許iX應用媒體」

- 在CMS上，從2.1起預設啟用該功能，但您可以通過相容性配置檔案將其禁用，在該配置檔案上可以將*sipUDT*設定為false
- 在Expressway上，在Advanced設定下的Zone config中（使用「Custom」區域配置檔案時），如果要允許iX通過，請確保將*SIP UDP/IX過濾模式*設定為「Off」



問題

一般資訊

ActiveControl的協商方式與其他媒體通道不同。例如，對於音訊和影片等其他媒體通道，SDP附加了加密行，這些行用於向遠端方通告要用於此通道的加密金鑰。因此，即時傳輸通訊協定(RTP)通道可以設定為安全，因此被視為安全RTP(SRTP)。對於iX通道，它使用DTLS協定來加密XCCP媒體流，因此它使用不同的機制。

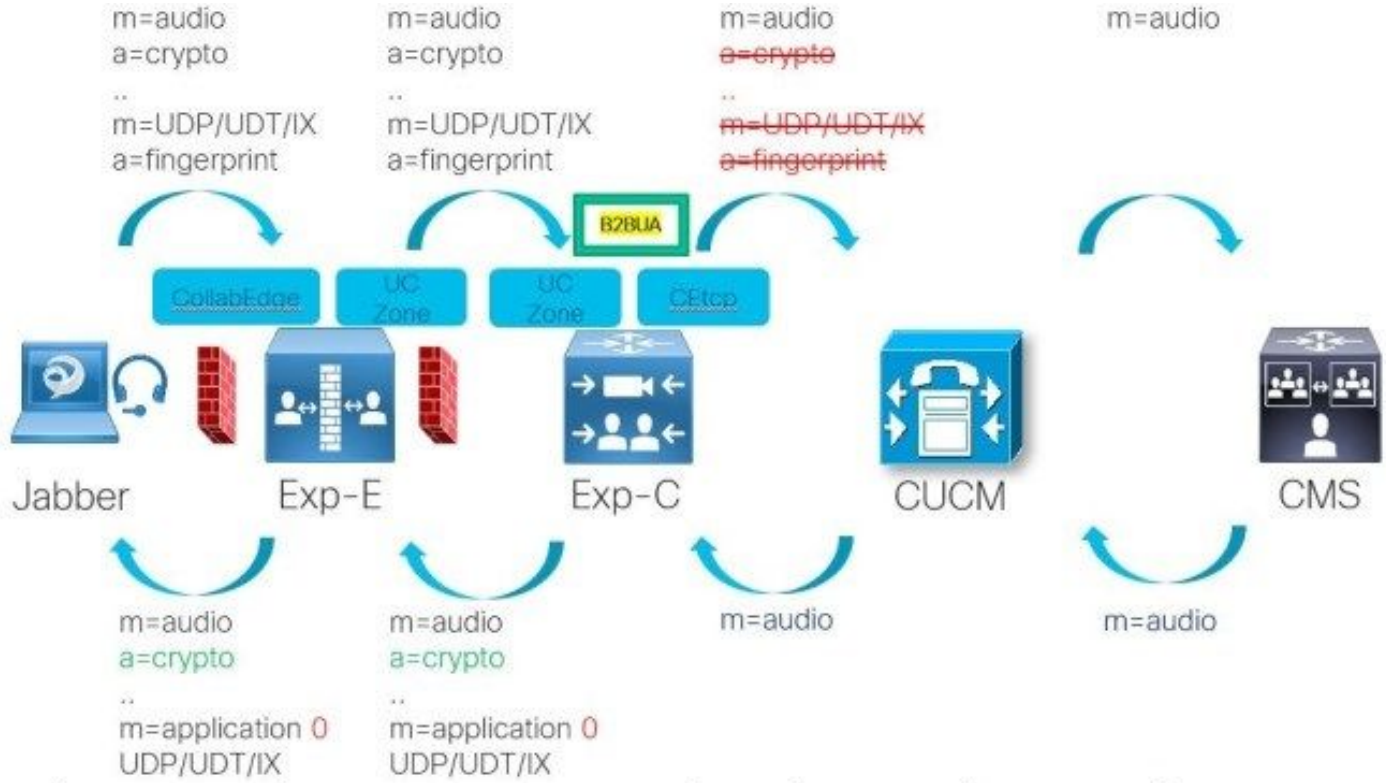
Expressway軟體不會終止DTLS協定。在Expressway發行說明*不支援的功能*下的*限制*部分中指出了

這一點。

- 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.

X12.5之前的Expressway

當運行X12.5之前的Expressway版本時，如果傳入連線帶有經過加密的iX通道，且通過不安全的TCP區域傳遞，則Expressway將刪除普通媒體通道的加密線路以及整個iX通道。對於連線到CMS空間的MRA客戶端，此處會以視覺方式顯示連線是安全的，從MRA客戶端到Expressway-C的連線是安全的，但隨後根據裝置在CUCM上設定的電話安全配置檔案，它要麼是未加密的（並通過CEtcp區域傳送），要麼是加密的（並通過CEtls區域傳送）。如圖所示，未加密時，您會看到Expressway-C剝離了所有媒體通道的加密線路，甚至剝離了整個iX媒體通道，因為它無法終止DTLS協定。這是通過背對背使用者代理(B2BUA)實現的，因為CEtcp區域的區域配置是用介質加密「強制未加密」設定的。在相反的方向（在具有「強制加密」媒體加密的UC遍歷區域上），當收到SDP回覆時，它確實會為正常媒體行新增加密行，並將iX通道的埠清零，導致無ActiveControl協商。當客戶端直接註冊到CUCM時，CUCM內部允許加密和未加密的iX媒體通道，因為CUCM不會將其自身置於媒體路徑中。



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

通過Expressway到Webex Meetings的呼叫連線也適用同樣的邏輯。它要求完整的路徑是端到端安全的，因為Expressway伺服器（在X12.5之前）僅傳遞DTLS連線資訊，但不會在它自身上終止以啟動新會話或加密/解密不同呼叫段上的媒體通道。

Expressway X12.5及更高版本

運行Expressway版本X12.5或更高版本時，行為已更改，因為它現在確實以強制加密(UDP/DTLS/UDT/IX)通過TCP區域連線通過iX通道，以便允許仍協商iX通道，但僅當遠端也使用加密時。它實施加密是因為Expressway不終止DTLS會話，因此只對傳遞執行操作，因此它依賴於遠端終端啟動/結束DTLS會話。出於安全考慮，會透過TCP連線刪除密碼編譯線路。此行為變化在「

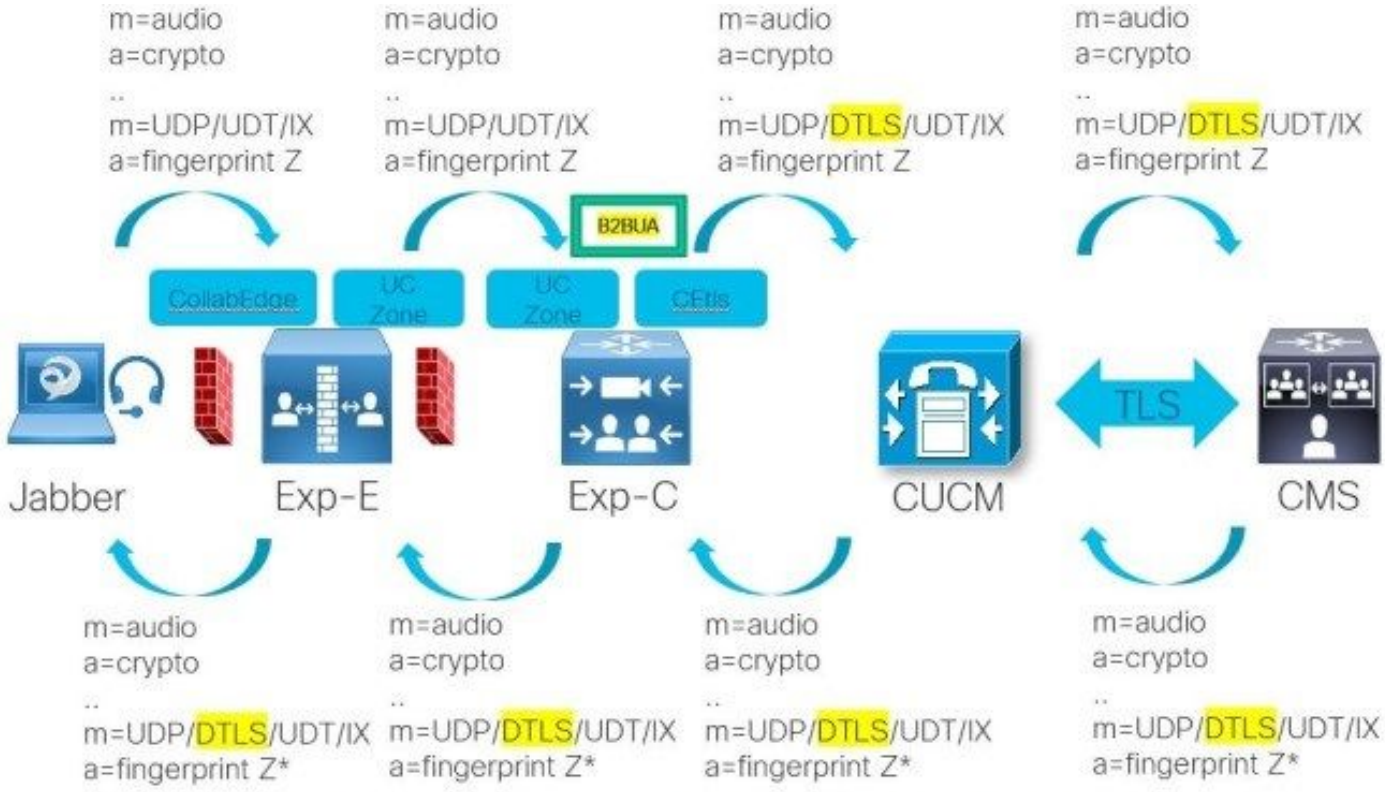
MRA：支援加密iX（適用於ActiveControl）」一節中的版本說明中介紹。此後發生的情況取決於CUCM版本，因為在12.5(1)SU1中行為發生了變化，允許通過iX通道以及不安全的傳入連線。即使存在到CMS的安全TLS SIP中繼，當運行低於12.5(1)SU1的CUCM版本時，它也會在將iX通道傳遞到CMS之前將其剝離，從而最終導致從CUCM到Expressway-C的埠歸零。

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.

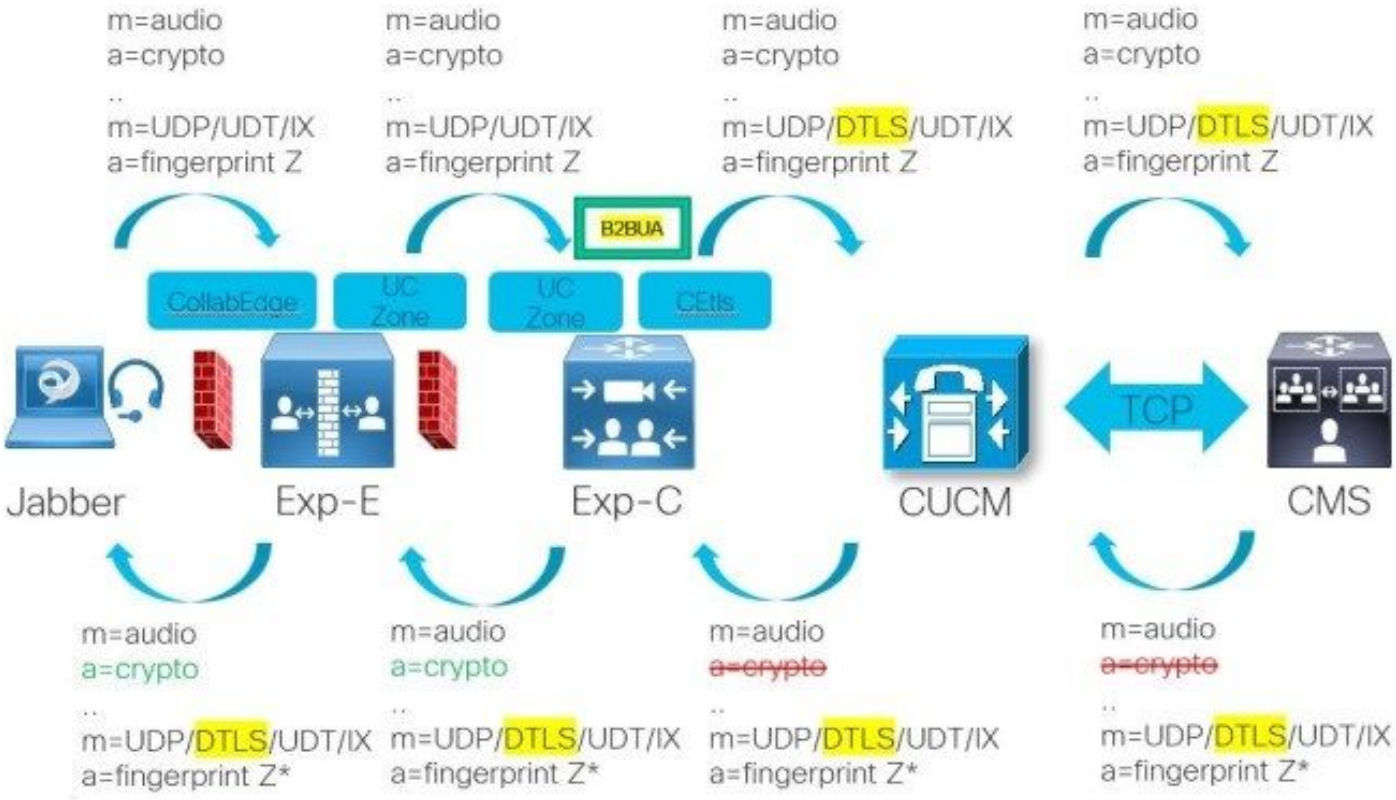
藉助端到端安全呼叫信令和媒體路徑，iX通道可以在(MRA)客戶端和會議解決方案（CMS或Webex會議）之間直接協商（通過不同的Expressway伺服器躍點）。該圖顯示了連線到CMS空間的MRA客戶端的相同呼叫流，但現在在CUCM上配置了安全電話安全配置檔案以及到CMS的安全TLS SIP中繼。您可以看到路徑是端到端安全的，並且DTLS指紋引數只是在整個路徑中傳遞。



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

為了設定安全裝置安全配置檔案，您需要確保CUCM設定為混合模式，這可能是一個繁瑣的過程(當操作時也會如此，因為它確實需要證書頒發機構代理功能(CAPF)來實現安全的內部通訊)。因此，此處也可以提供其他更方便的解決方案來支援對MRA和Expressway的ActiveControl的可用性，如本文檔所述。

不需要到CMS伺服器的安全TLS SIP中繼，因為CUCM(假設SIP中繼具有SRTP Allowed選項)始終從傳入安全SIP連線傳遞iX通道以及加密線路，但CMS僅通過加密回覆iX通道（允許ActiveControl）(假設**SIP媒體加密在**Settings > Call Settings *下設定為allowed*或*enforced*CMS上)，但是在其他媒體通道上沒有加密，因為它刪除了加密線路照圖從他們身上取出。Expressway伺服器可以再次新增加密線路以保護該部分的連線（並且仍通過DTLS直接在終端客戶端之間協商iX），但從安全形度來看這不是理想的，因此建議設定到會議網橋的安全SIP中繼。在SIP中繼上未選中**SRTP Allowed**時，CUCM剝離加密線路並安全iX協商也失敗。



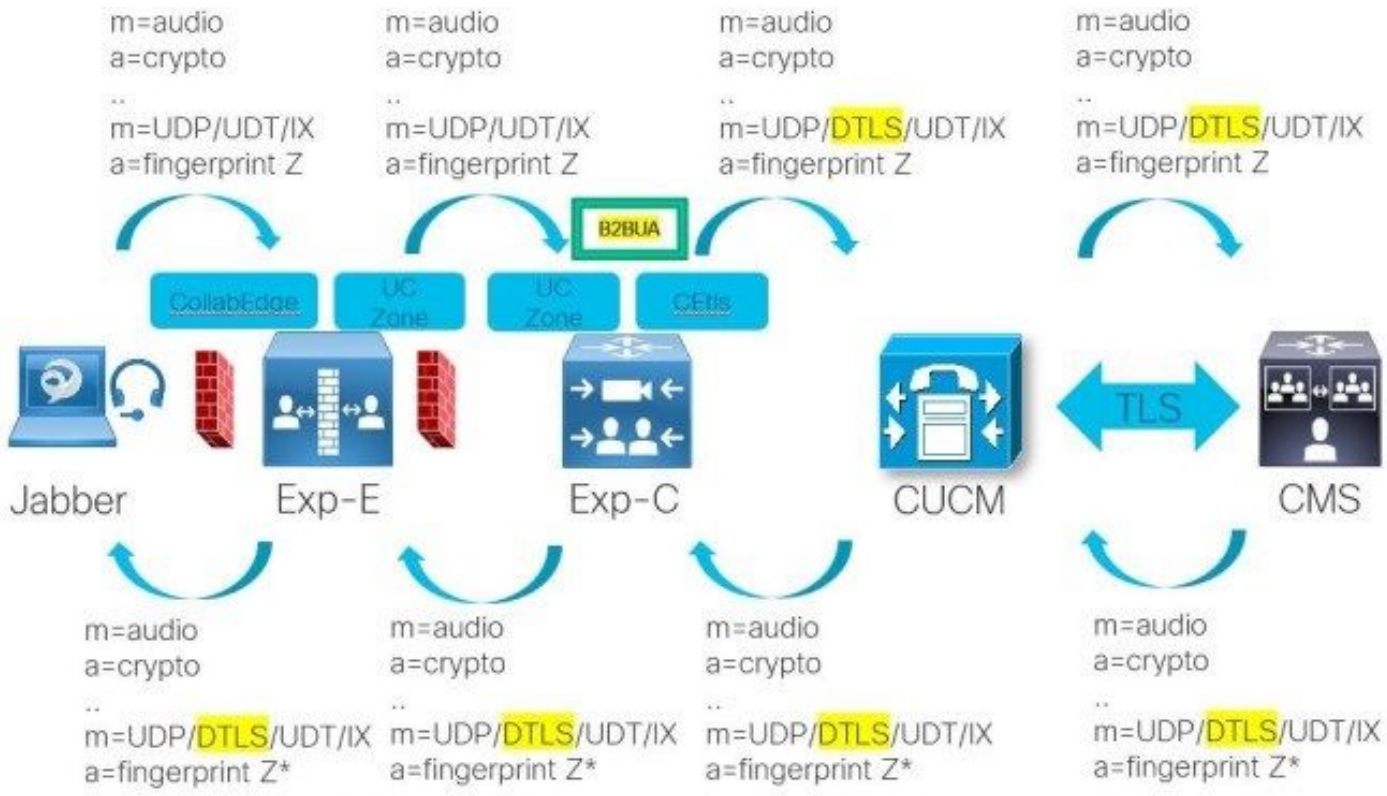
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

解決方案

有幾種不同的選項可供選擇，它們有不同的要求以及各種優缺點。每個部分都在一個更詳細的章節中介紹。不同的選項包括：

1. 終端的安全電話安全配置檔案（混合模式CUCM）
2. Jabber版SIP OAuth
3. 用於不安全電話安全配置檔案的加密iX通道(CUCM 12.5(1)SU1或更高版本)

解決方案1：終端的安全電話安全配置檔案（混合模式CUCM）



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

必要條件:

- 混合模式下的CUCM

專業：

- 適用於任何CUCM版本
- 適用於所有客戶端裝置

Con:

- 需要在混合模式下配置CUCM（以及本地終端上的CAPF操作）

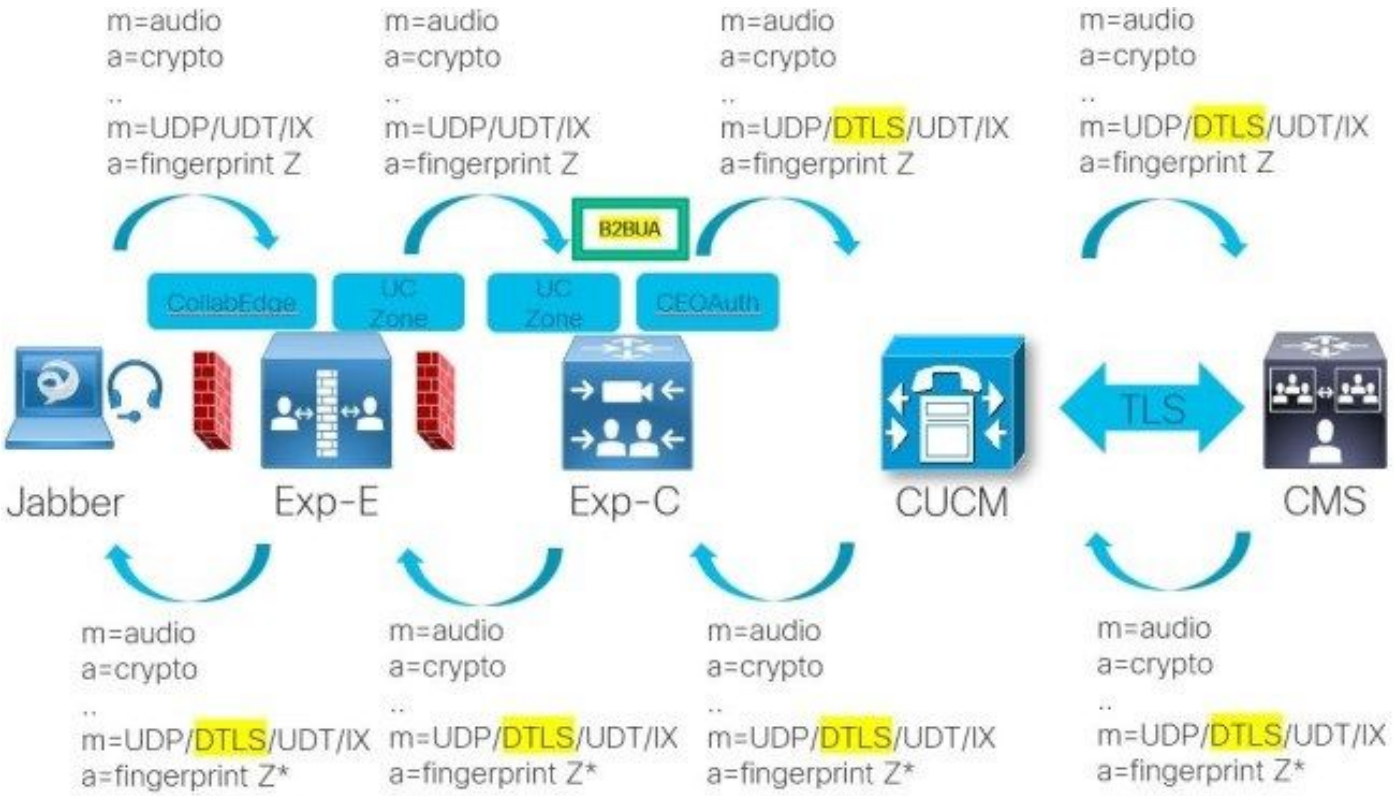
這是「問題」部分以及結尾部分介紹的方法，可以確保您具有端到端加密的呼叫信令和媒體路徑。根據以下文檔，它要求以混合模式設定CUCM。

對於MRA客戶端，不需要CAPF操作，但應確保使用安全電話安全配置檔案執行額外的配置步驟，該配置檔案的名稱與Collaboration Edge TC型終端配置示例中突出顯示的Expressway-C伺服器證書的主題替代名稱之一相匹配（也適用於基於CE的終端和Jabber客戶端）。

從內部終端或Jabber客戶端連線到Webex會議時，您需要對CAPF操作執行操作，以便安全地將客戶端註冊到CUCM。這是確保端對端安全呼叫流程所必需的，其中Expressway只需通過DTLS協商，而不在其上處理。

為了使呼叫端到端安全，請確保所有相關的SIP中繼（在呼叫Webex會議時到Expressway-C，在呼叫CMS會議時到CMS）都是使用具有安全SIP中繼安全配置檔案的TLS的安全SIP中繼。

解決方案2：適用於Jabber的SIP OAuth



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

必要條件:

- Cisco Jabber 12.5或更高版本(發行說明)
- CUCM 12.5版或更高版本(發行說明),*啟用刷新登入流*的OAuth
- Expressway X12.5.1或更高版本(發行說明),*啟用刷新的Authorize by OAuth權*杖

專業：

- 允許安全註冊，並且無需每次續訂CAPF即可輕鬆在內部和外部之間切換
- 無需在混合模式下設定CUCM

Con:

- 僅適用於Jabber，不適用於TC/CE終端

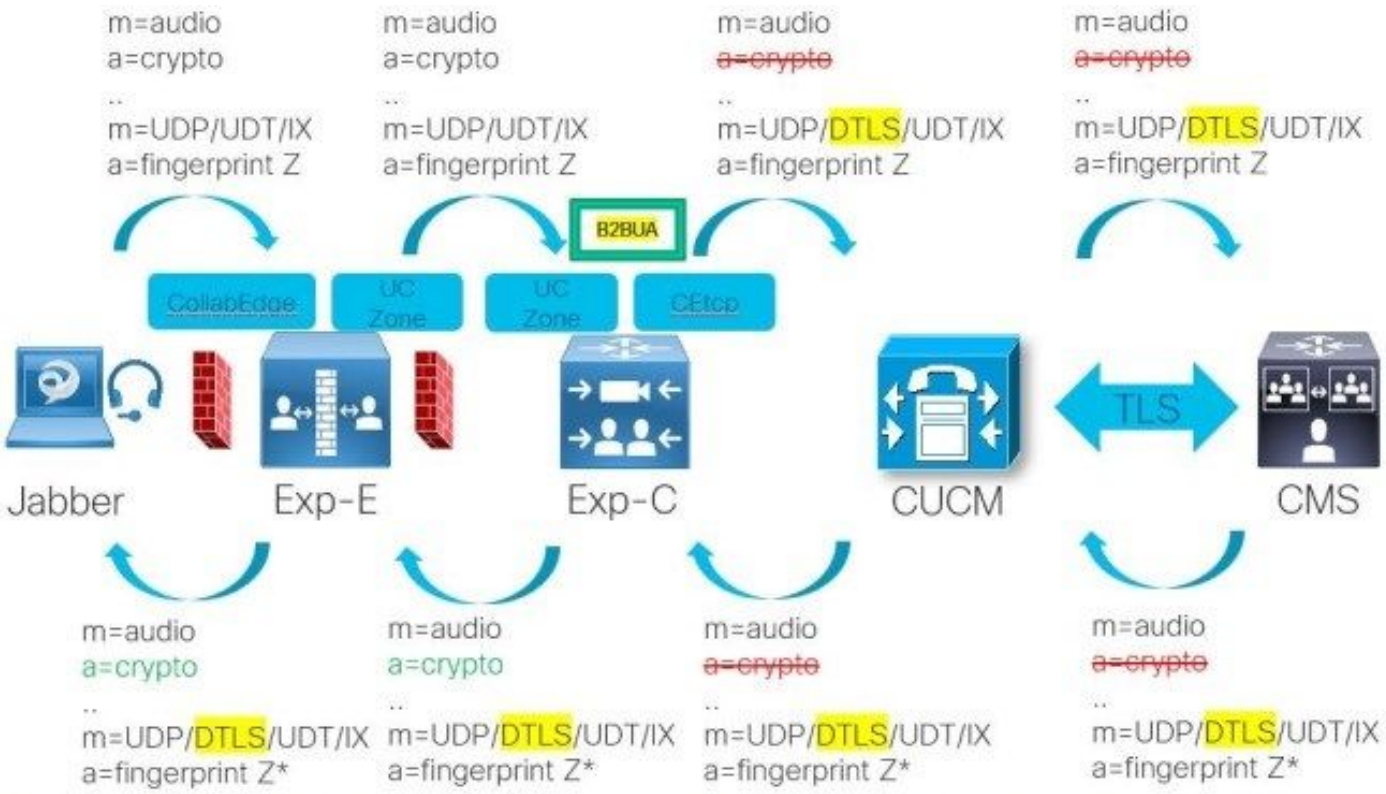
SIP OAuth模式允許您在安全環境中使用OAuth刷新令牌進行Cisco Jabber身份驗證。它允許使用安全信令和介質，而無解決方案1的CAPF要求。在CUCM群集和Jabber終端上啟用基於OAuth的授權時，完成SIP註冊期間的令牌驗證。

CUCM上的配置記錄在功能配置指南中，並要求您已在Enterprise Parameters下啟用OAuth with Refresh Login Flow。若要在MRA上啟用此功能，請確保在**Configuration > Unified Communication > Unified CM Servers**下刷新Expressway-C伺服器中的CUCM節點，以便在**Configuration > Zones > Zones**下，您現在還必須看到自動建立的CEOAuth區域。同時確保在**Configuration > Unified Communication > Configuration**下啟用了**Authorize by OAuth token with refresh**。

通過此配置，您可以為信令和媒體實現類似的端到端安全呼叫連線，因此Expressway只需通過DTLS協商，因為它不會終止該流量本身。與先前的解決方案相比，唯一的區別在於它使用Expressway-C上的CEOAuth區域來連線CUCM，而不是使用CEtls區域，因為當CUCM在具有安全電話安全配置檔案的混合模式下運行時，它會使用SIP OAuth而不是TLS上的安全裝置註冊，但除此之外，一切都保持不變。

解決方案3：用於不安全電話安全配置檔案的加密iX通道(CUCM 12.5(1)SU1或更高版

本)



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

必要條件:

- CUCM 12.5(1)SU1或更高版本(發行說明)
- Expressway X12.5.1或更高版本(發行說明)

專業：

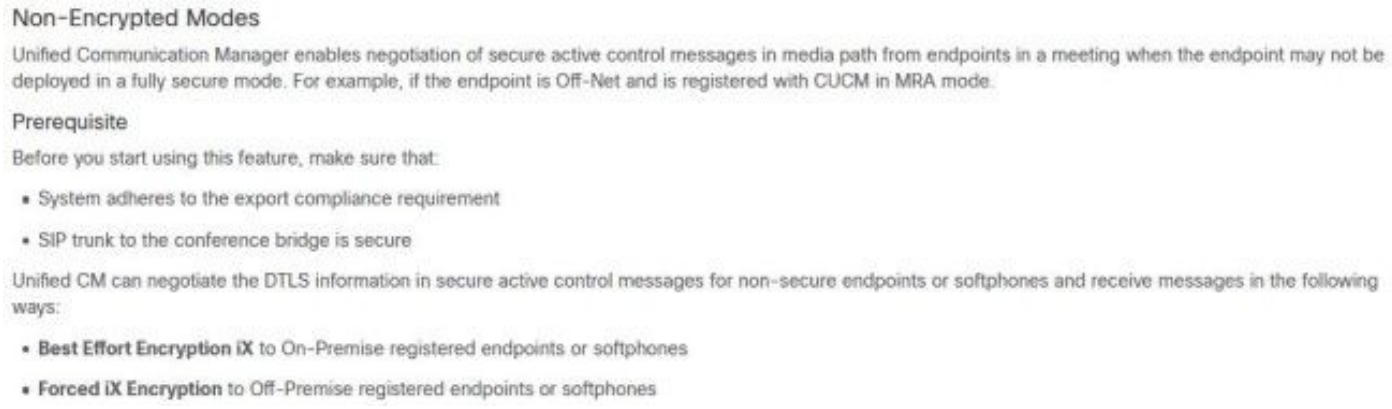
- 無需在混合模式下設定CUCM
- 無需設定安全的端到端通訊
- 適用於Jabber和TC/CE終端

Con:

- 需要升級CUCM
- 僅支援CUCM受限版本

從CUCM 12.5(1)SU1開始，它支援任何SIP線路裝置的iX加密協商，以便可以協商非安全終端或軟體電話的安全ActiveControl消息中的DTLS資訊。它通過TCP傳送盡最大努力的iX加密，允許電話端對端具有加密的iX通道，儘管與CUCM的TCP連線（非TLS）不安全。

在CUCM 12.5(1)SU1的安全指南的「加密iX通道」一節中，它顯示，對於使用不安全裝置的非加密模式，可以在系統遵守匯出合規性且到會議網橋的SIP中繼安全的前提下協商盡力而為和強制iX加密。



在CUCM上：

- 必須使用匯出受限制的CUCM（非受限）
- 在**System > Licensing > License Management**下，必須將「Export-Controlled Functionality」設定為「allowed」。
- 您的SIP中繼必須啟用「**SRTP Allowed**」選項（無論中繼本身是否安全或不安全）

在CMS上：

- 您的callbridge必須具有加密許可證（因此您沒有callBridgeNoEncryption許可證）
- 在Webadmin上的**Configuration > Call Settings**下，必須將**SIP media encryption**設定為**allowed**(或**必需**)

在圖中，您可以看到連線是安全的，直到Expressway-C和C在不使用加密線路的情況下將SDP傳送到CUCM，但它仍然包含iX媒體通道。因此，音訊/影片/..的普通媒體沒有加密線路保護，但它現在確實有用於iX媒體通道的安全連線，因此Expressway不需要終止DTLS連線。因此，即使使用不安全的電話安全配置檔案，ActiveControl也可以在客戶端和會議網橋之間直接協商。在CUCM的早期版本中，流量會有所不同，並且不會協商ActiveControl，因為首先它不會通過iX通道傳遞到CMS，因為該部分已經剝離。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。