启用对MRA/Expressway的ActiveControl

目录

简介

本文档介绍用于启用移动和远程访问(MRA)客户端的ActiveControl协议以及通过Expressway从内部终端到Webex会议的呼叫的不同选项。MRA是用于虚拟专用无网络(VPN)Jabber和终端功能的部署解决方案。此解决方案允许最终用户从全球任何地方连接到内部企业资源。ActiveControl协议是Cisco专有协议，通过会议记录器、视频布局更改、静音和录制选项等运行时功能，可提供更丰富的会议体验。

先决条件

要求

Cisco 建议您了解以下主题：

- Expressway（MRA和B2B呼叫）

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Expressway X12.5
- 思科会议服务器(CMS)2.9
- Cisco Unified Communications Manager 12.5

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在本文档中，重点介绍与思科会议服务器(CMS)的MRA客户端连接，但其他类型的平台或连接（例如，连接到Webex会议时）也同样如此。同样的逻辑可以应用于以下类型的呼叫流：

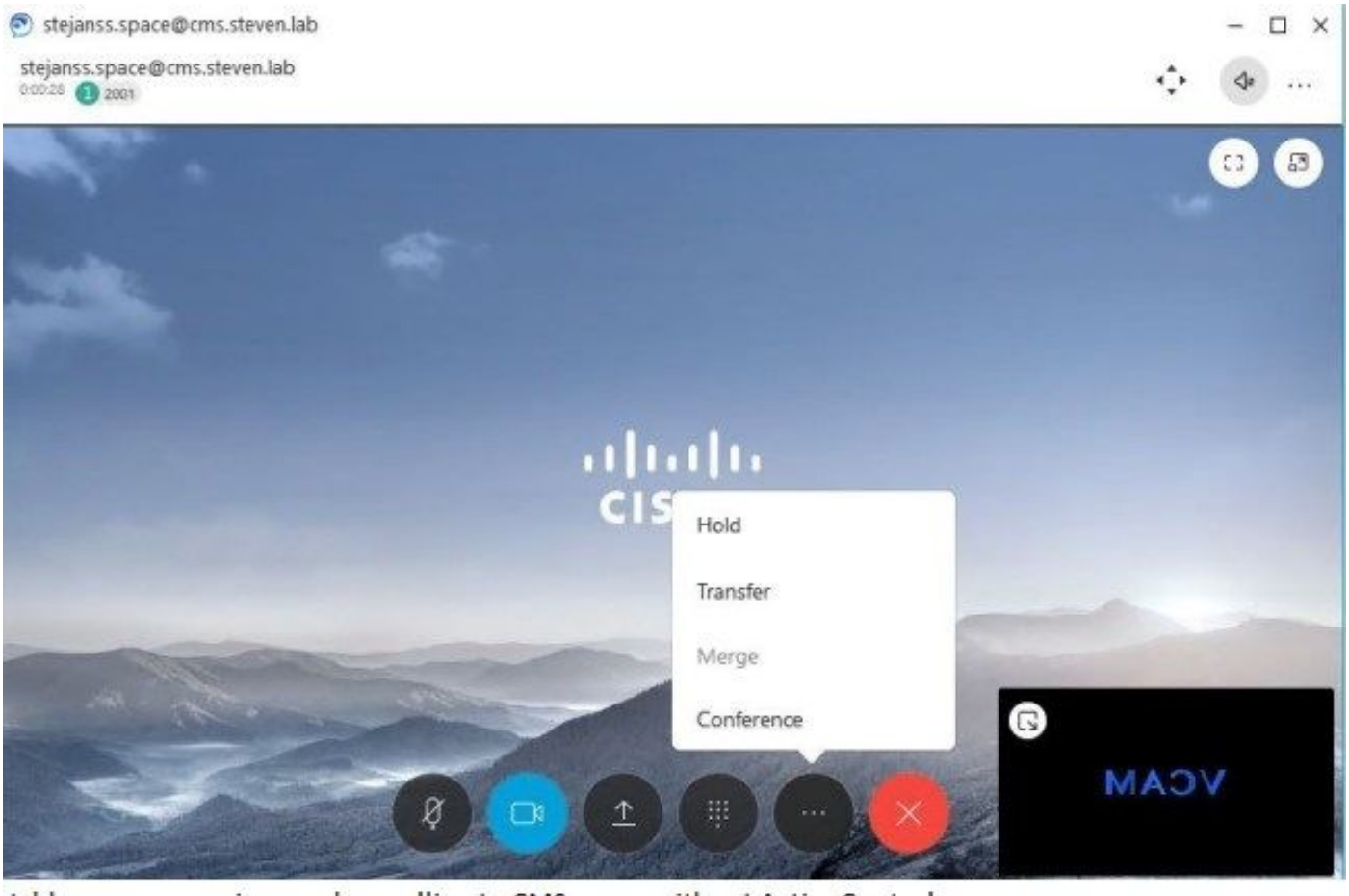
- 终端 — CUCM - Expressway-C - Expressway-E - Webex会议
- MRA终端 — (Expressway-E - Expressway-C)- CUCM - Expressway-C - Expressway-E - Webex会议

注意：Webex会议支持的ActiveControl功能与目前的CMS功能不同，并且仅是有限的子集。

Cisco Meeting Server平台使会议参与者能够通过ActiveControl直接从会议终端控制其会议体验，而无需外部应用或操作员。ActiveControl在思科设备中使用iX媒体协议，并作为呼叫的SIP消息传送的一部分进行协商。自CMS版本2.5起，启用的主要功能如下（尽管它们可能取决于使用的终端类型和软件版本）：

- 查看连接到会议的所有出席者的列表（名单列表或出席者列表）
- 将其他参与者静音或取消静音
- 在会议中添加或删除其他参与者
- 开始或停止会议录制
- 使学员变得重要
- 会议中活动发言者的出席者指示器
- 当前在会议中共享内容或演示文稿的参与者的指示器
- 锁定或解锁会议

在第一个图像上，您会看到来自Jabber客户端的用户视图，该客户端在未使用ActiveControl的情况下向CMS空间发出呼叫，而第二个图像则显示功能更丰富的用户视图，其中Jabber能够与CMS服务器协商ActiveControl。



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl是基于XML的协议，使用会话发起协议(SIP)呼叫的会话描述协议(SDP)中协商的iX协议进行传输。它是思科协议(可扩展会议控制协议(XCCP))，仅在SIP中协商（因此互通呼叫不具有ActiveControl），并且利用UDP/UDT（基于UDP的数据传输协议）进行数据传输。安全协商通过数据报TLS(DTLS)进行，可以将其视为TLS over UDP连接。这里显示了一些协商差异的示例。

未加密

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

已加密（尽力 — 尝试加密，但允许回退到未加密连接）

m=application 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（强制加密 — 不允许回退到未加密的连接）

m=application 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:

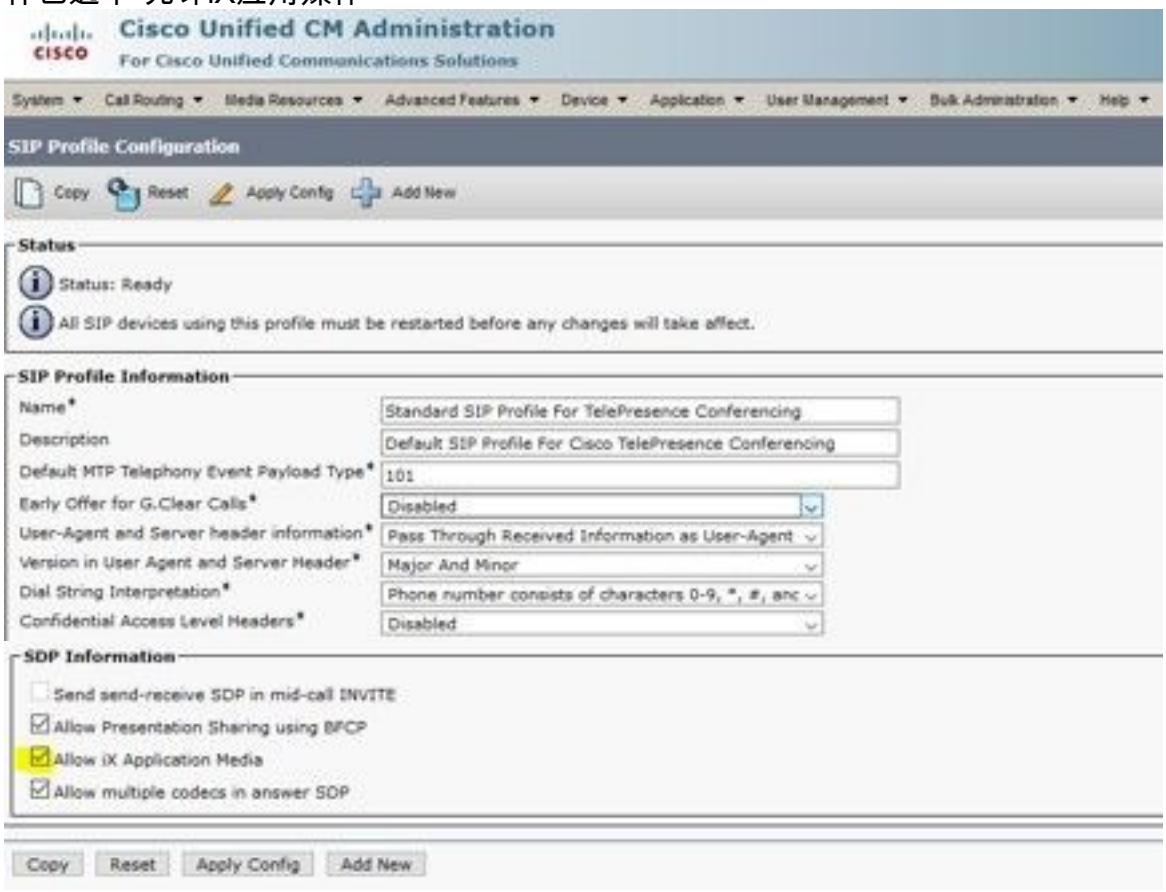
以下是完整ActiveControl支持所需的最低软件版本：

- Jabber 12.5或更高版本(版本说明)
- 根据CMS ActiveControl指南，建议使用CE终端8.3或更高版本、9.6.2或更高版本(根据Webex帮助链接，CE9.3.1或更高版本适用于Webex)

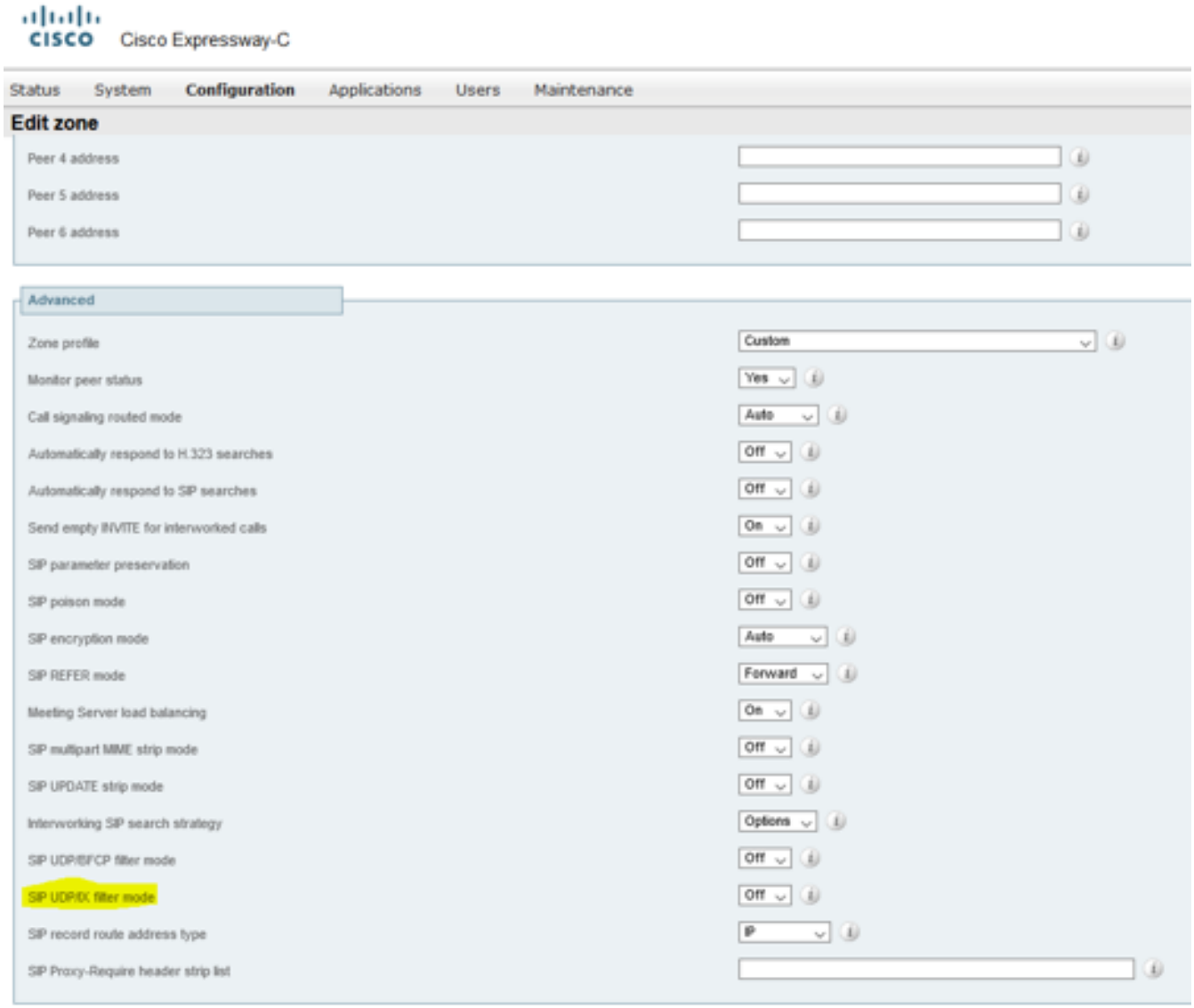
- CUCM 10.5或更高版本（适用于Jabber 12.5 ActiveControl支持）(11.5(1)或更高版本，适用于Webex，根据链路)
- 根据CMS ActiveControl指南，建议使用CMS 2.1或更高版本、2.5或更高版本
- Expressway X12.5或更高版本(版本说明)，以允许对非加密MRA客户端的支持

有几个配置选项需要考虑：

- 在CUCM上，确保为相关SIP中继（到Expressway-C和CMS）配置了SIP配置文件，该配置文件已选中“允许iX应用媒体”



- 在CMS上，从2.1起默认启用该功能，但您可以通过一个compatibilityProfile禁用它，在该配置文件上可以将*sipUDT*设置为false
- 在Expressway上，在Advanced设置下的Zone config中（使用“Custom”区域配置文件时），如果要允许iX通过，请确保将*SIP UDP/IX过滤模式*设置为“Off”



问题

一般信息

ActiveControl的协商方式与其他媒体通道的安全方式不同。对于其他媒体通道（如音频和视频），SDP会附加加密线路，用于向远程方通告要用于此通道的加密密钥。因此，可以将实时传输协议(RTP)通道设置为安全，从而将其视为安全RTP(SRTP)。对于iX信道，它使用DTLS协议加密XCCP媒体流，因此它使用不同的机制。

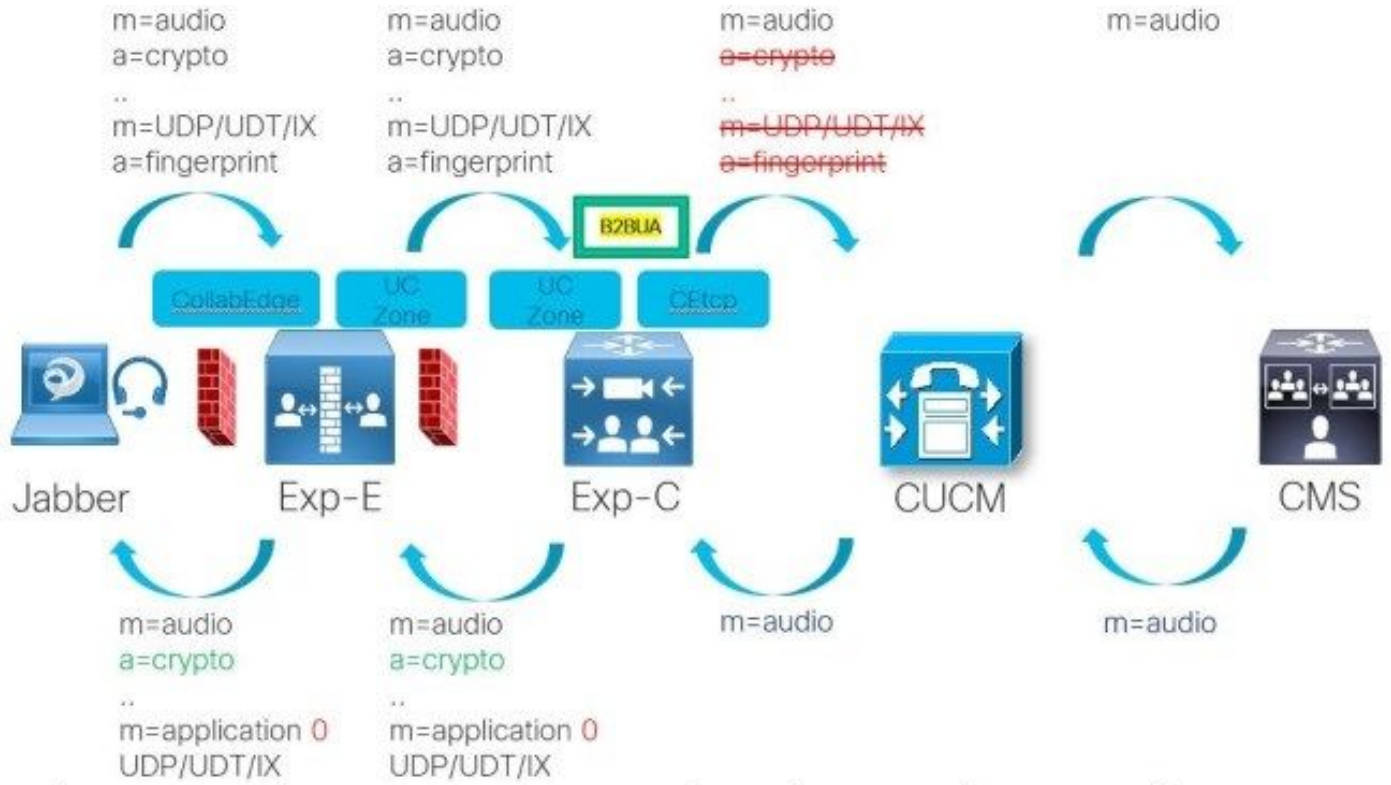
Expressway软件不会终止DTLS协议。*Expressway版本说明不受支持的功能下的限制部分中对此进行了说明。*

- 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版本

当运行X12.5之前的Expressway版本时，如果传入连接带有经过不安全TCP区域的加密iX通道，则Expressway会删除普通媒体通道的加密线路以及整个iX通道。这是针对连接到CMS空间的MRA客户端的视觉显示，在该空间中，您会看到从MRA客户端到Expressway-C的连接是安全的，但随后

根据设备在CUCM上设置的电话安全配置文件，该连接要么是未加密的（并通过CEtcp区域发送），要么是加密的（并通过CEtls区域发送）。如图所示，当未加密时，您会看到Expressway-C解除了所有媒体信道的加密线路，甚至解除了整个iX媒体信道，因为它无法终止DTLS协议。这是通过背对背用户代理(B2BUA)实现的，因为CEtcp区域的区域配置是用媒体加密"强制未加密"设置的。在相反的方向（通过具有"强制加密"媒体加密的UC遍历区域），当收到SDP应答时，它确实会为正常媒体行添加加密行，并将iX信道的端口清零，从而不会导致ActiveControl协商。当客户端直接注册到CUCM时，CUCM内部允许加密和未加密的iX媒体通道，因为CUCM不会将自身置于媒体路径中。



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

同样的逻辑也适用于通过Expressway到Webex会议的呼叫连接。它需要完整的端到端安全路径，因为Expressway服务器（在X12.5之前）仅传递DTLS连接信息，但不会在它自身上终止以启动新会话或加密/解密不同呼叫段上的媒体通道。

X12.5及更高版本的Expressway

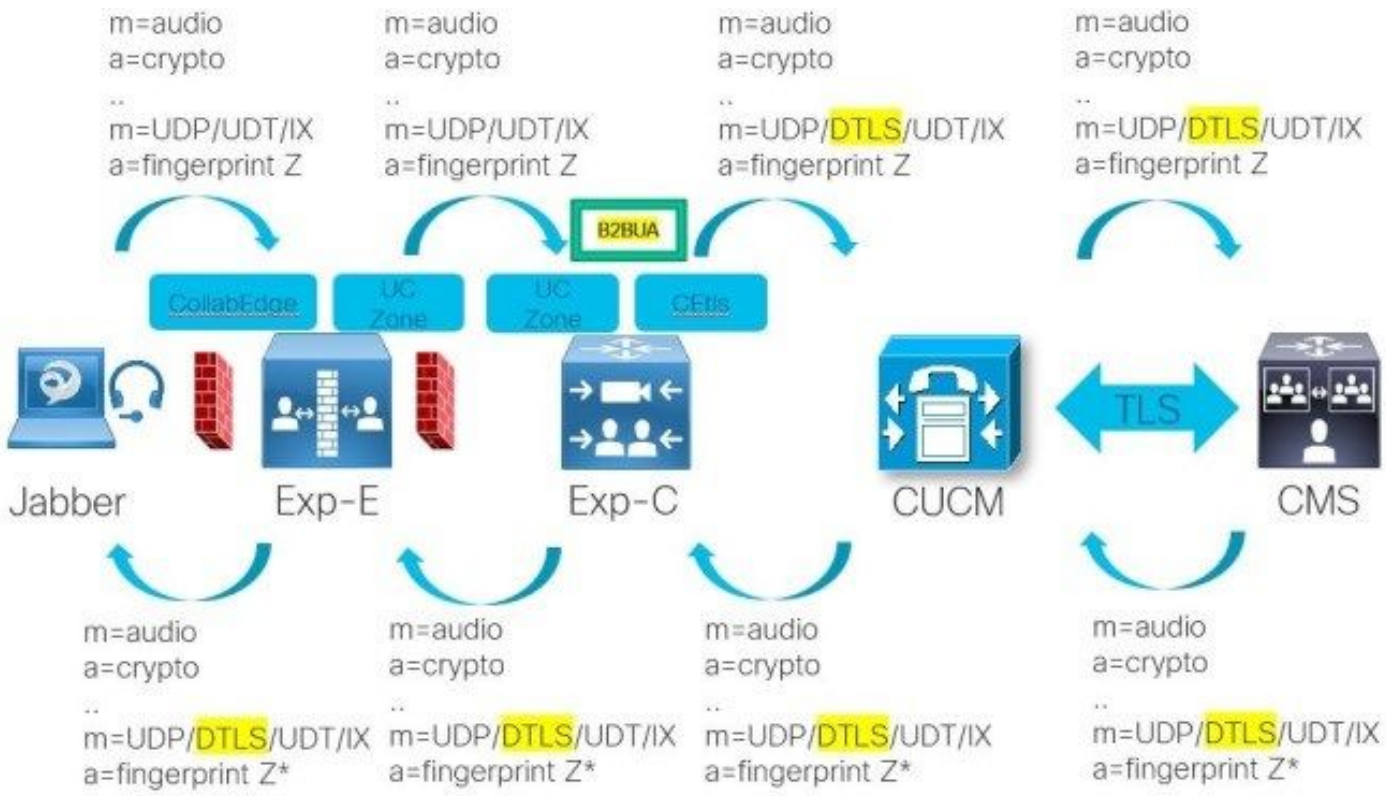
当运行Expressway版本X12.5或更高版本时，行为已更改，因为它现在确实以强制加密(UDP/DTLS/UDT/IX)通过TCP区域连接上的iX通道，以便允许仍协商iX通道，但仅当远程端也使用加密时。因为Expressway不终止DTLS会话，因此它仅对传递起作用，因此它依赖远程端启动/结束DTLS会话。出于安全考虑，加密线路通过TCP连接被删除。根据"MRA：对加密iX的支持（适用于ActiveControl）"部分，此行为更改在发行说明中介绍。此后发生的情况取决于CUCM版本，因为行为在12.5(1)SU1中发生更改，在该版本中，CUCM允许通过iX信道和不安全的传入连接。即使存在到CMS的安全TLS SIP中继，当运行低于12.5(1)SU1的CUCM版本时，它会在将iX通道传递到CMS之前将其剥离，从而最终导致从CUCM到Expressway-C的零输出端口。

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.

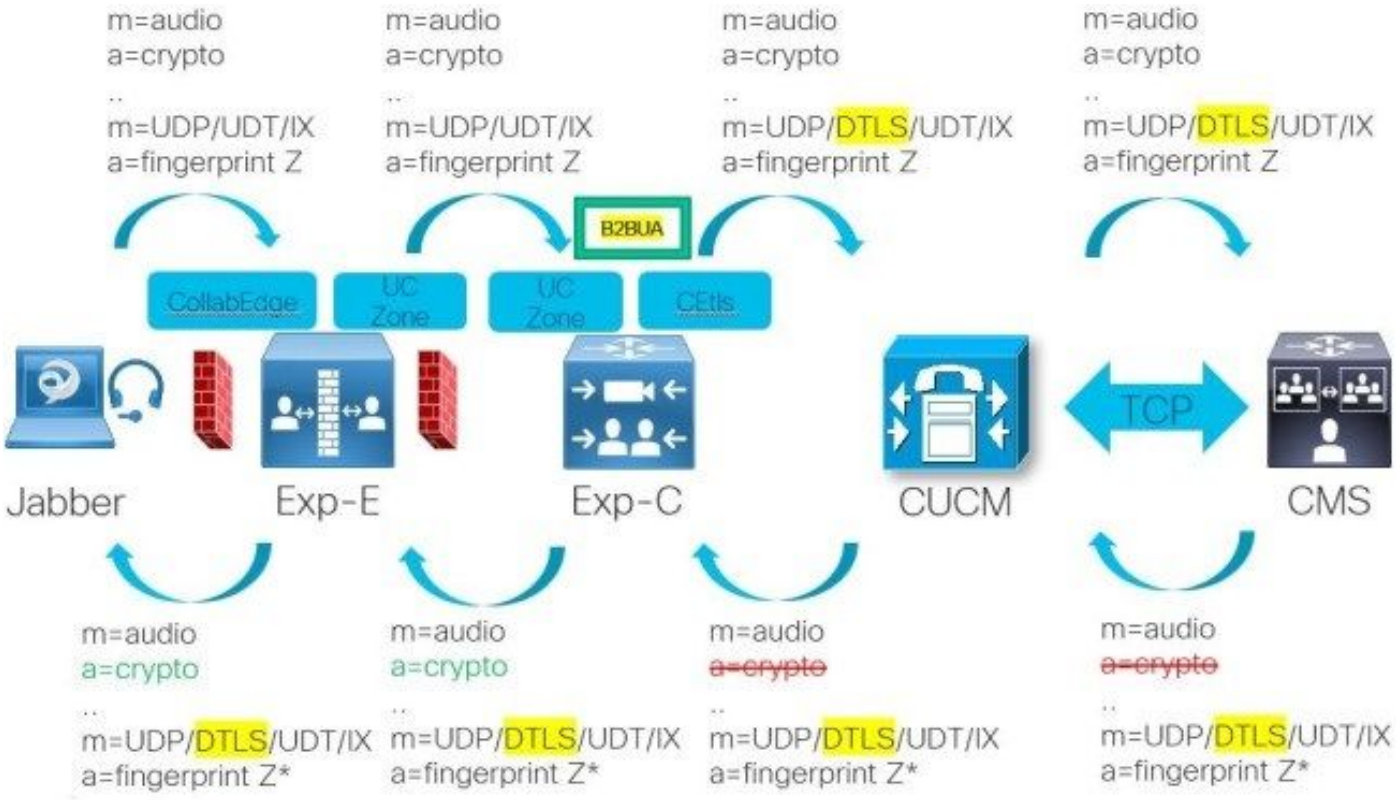
通过端到端安全呼叫信令和媒体路径，iX通道可以在(MRA)客户端和会议解决方案（CMS或Webex会议）之间直接协商（通过不同的Expressway服务器跃点传递）。该图显示了连接到CMS空间的MRA客户端的相同呼叫流，但现在已在CUCM上配置了安全电话安全配置文件，并提供了到CMS的安全TLS SIP中继。您可以看到路径是端到端安全的，并且DTLS指纹参数只是沿整个路径传递。



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

要设置安全设备安全配置文件，您需要确保CUCM设置为混合模式，这可能是一个繁琐的过程(当操作时也会如此，因为它确实需要证书颁发机构代理功能(CAPF)来实现安全的内部通信)。因此，此处可以提供其他更方便的解决方案来支持对MRA和Expressway的ActiveControl的可用性（一般如本文档所述）。

不需要到CMS服务器的安全TLS SIP中继，因为CUCM(假设SIP中继具有SRTP Allowed选项)始终会从传入的安全SIP连接传递到iX信道以及加密线路，但CMS仅回复到iX信道（允许ActiveControl）(假设**SIP媒体加密在CMS上设置**为*allowed*或*enforced* on CMS上)，但不会加密其他媒体信道，因为它会删除加密线路从他们那里照出来。Expressway服务器可以再次添加加密线路以保护该部分连接（并且仍通过DTLS直接在终端客户端之间协商iX），但是从安全角度来看，这并不理想，因此建议设置到会议网桥的安全SIP中继。在SIP中继上未选中**SRTP Allowed**时，CUCM会解开加密线路，并且安全iX协商也会失败。



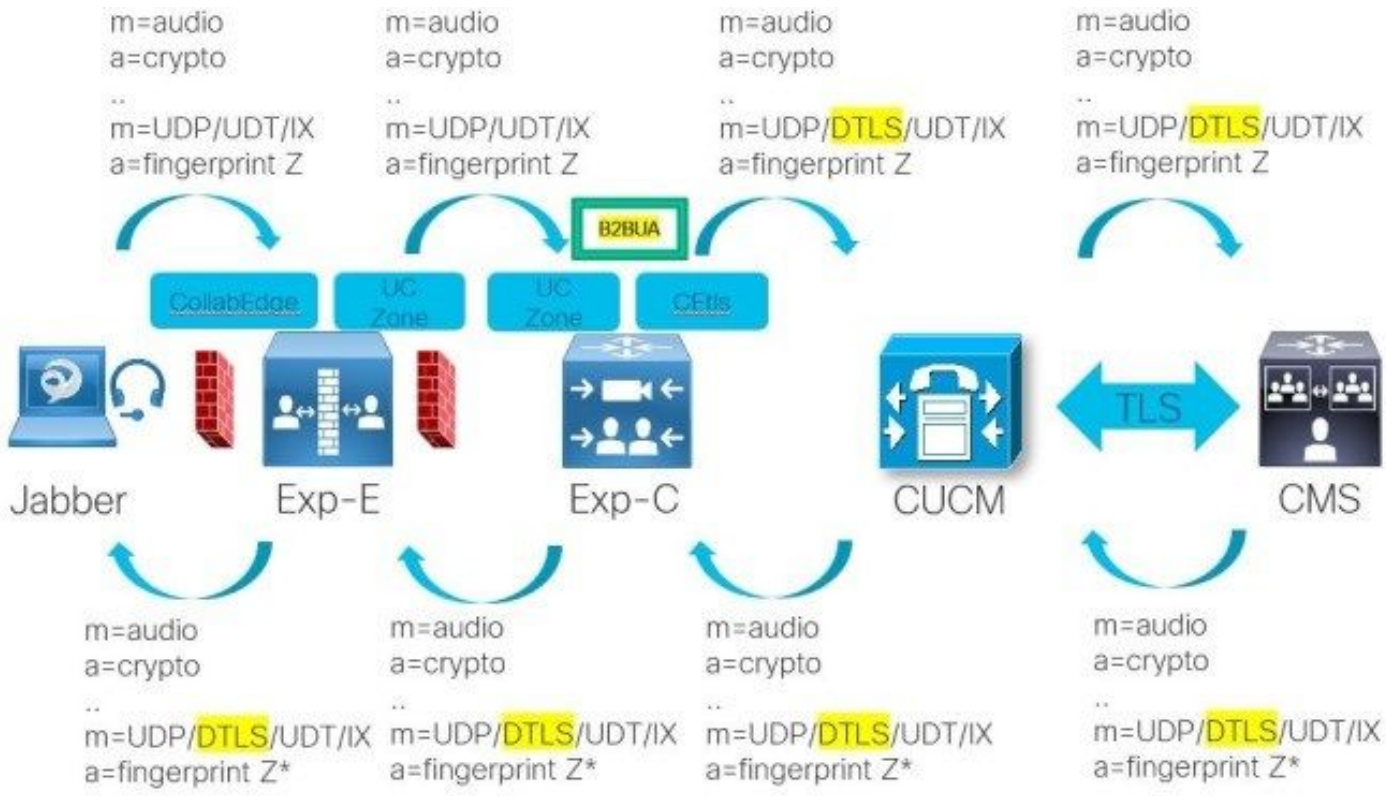
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

解决方案

有多种不同的选项可供选择，包括各种要求和各种优缺点。每个步骤都将在更详细的章节中介绍。不同的选项包括：

1. 终端的安全电话安全配置文件（混合模式CUCM）
2. 用于Jabber的SIP OAuth
3. 用于不安全电话安全配置文件的加密iX通道(CUCM 12.5(1)SU1或更高版本)

解决方案1：终端的安全电话安全配置文件（混合模式CUCM）



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

先决条件:

- 混合模式下的CUCM

专业：

- 适用于任何CUCM版本
- 适用于所有客户端设备

Con:

- 需要在混合模式下配置CUCM（以及本地终端上的CAPF操作）

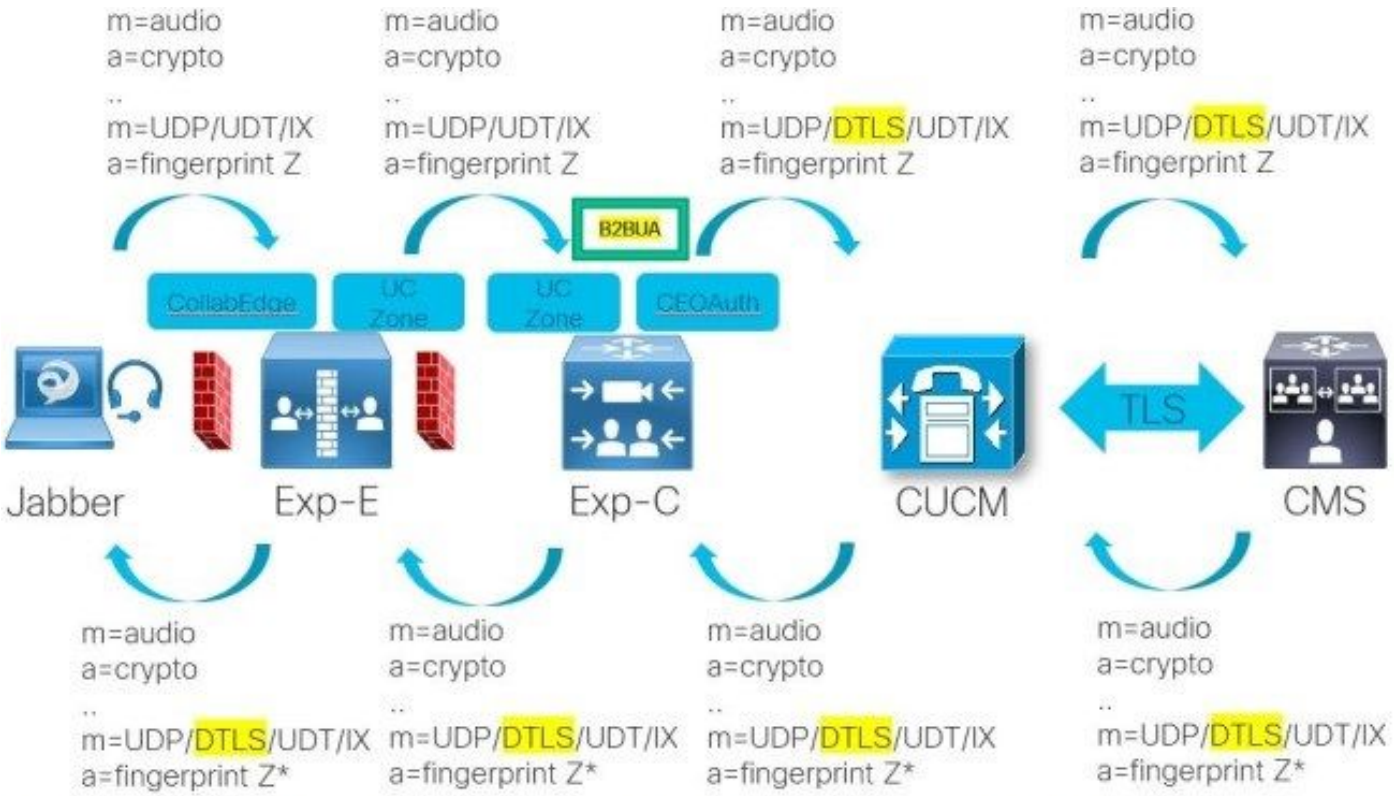
这是问题部分以及您确保具有端到端加密呼叫信令和媒体路径的末尾所介绍的方法。它要求按照以下文档在混合模式下设置CUCM。

对于MRA客户端，不需要CAPF操作，但请确保按照安全电话安全配置文件执行额外的配置步骤，该配置文件的名称与Collaboration Edge TC-based Endpoints Configuration Example（也适用于基于CE的终端和Jabber客户端）中突出显示的Expressway-C服务器证书的主题备用名称之一相匹配。

从内部终端或Jabber客户端连接到Webex会议时，您需要对CAPF操作执行操作，以安全地向CUCM注册客户端。这是确保端到端安全呼叫流所必需的，其中Expressway只需通过DTLS协商，而不用自行处理。

为了使呼叫端到端安全，请确保所有相关SIP中继（在呼叫到Webex会议时到Expressway-C，在呼叫到CMS会议时到CMS）都是安全的SIP中继，使用带有安全SIP中继安全配置文件的TLS。

解决方案2：用于Jabber的SIP OAuth



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

先决条件:

- Cisco Jabber 12.5或更高版本(版本说明)
- CUCM 12.5版或更高版本(发行说明)，启*用OAuth并刷新登录流*量
- Expressway X12.5.1或更高版本(版本说明),通过*OAuth令牌授权，启用刷*新

专业：

- 允许安全注册，并可在内部和外部之间轻松切换，而无需每次续订CAPF
- 无需在混合模式下设置CUCM

Con:

- 仅适用于Jabber，不适用于TC/CE终端

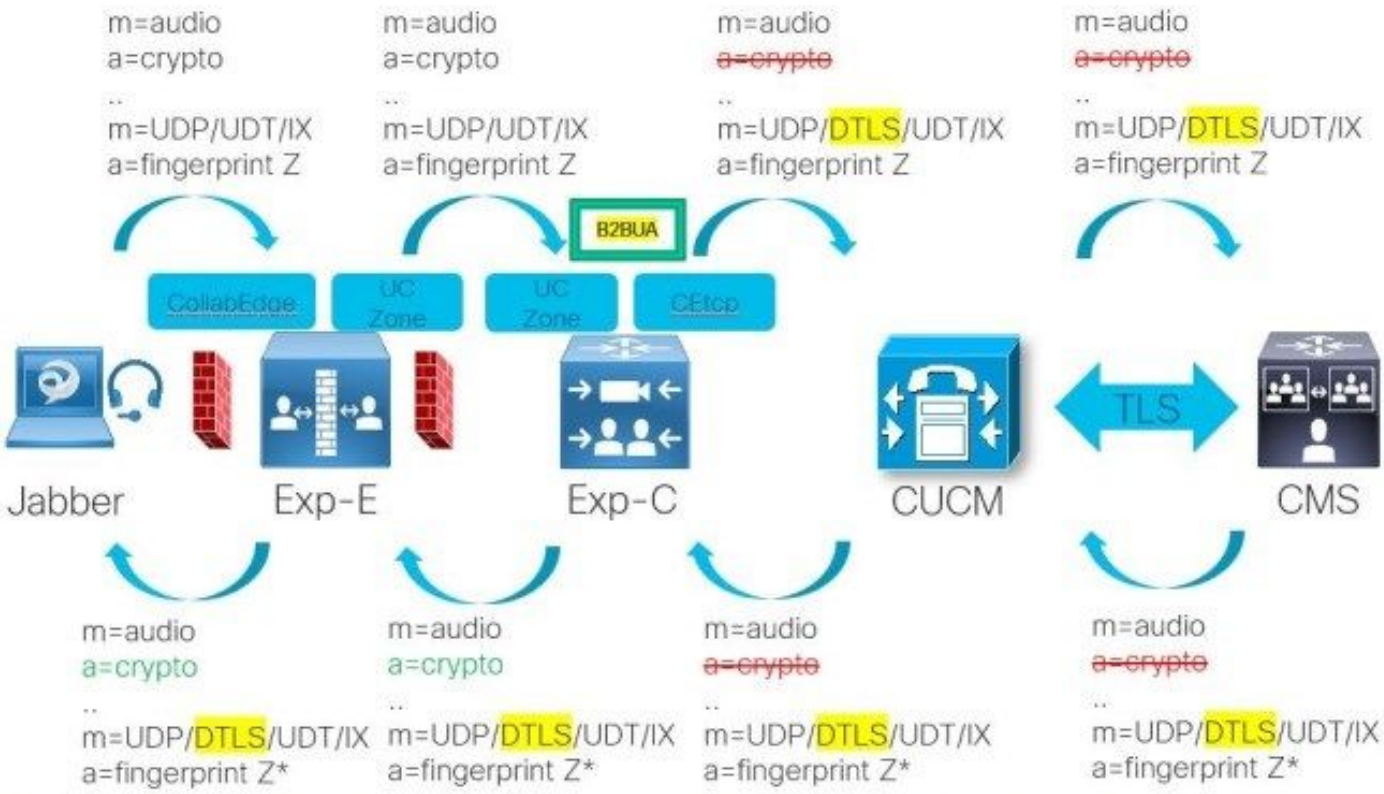
SIP OAuth模式允许您在安全环境中使用OAuth刷新令牌进行Cisco Jabber身份验证。它允许使用安全信令和媒体，而无需解决方案1的CAPF要求。在CUCM集群和Jabber终端上启用基于OAuth的授权时，完成SIP注册过程中的令牌验证。

CUCM上的配置记录在功能配置指南中，并要求您已在Enterprise Parameters下启用OAuth with Refresh Login Flow。要通过MRA启用此功能，请确保在Expressway-C服务器中的**Configuration > Unified Communication > Unified CM Servers**下刷新CUCM节点，以便在**Configuration > Zones > Zones**下您现在还必须看到自动创建的CEOAuth区域。同时确保**Configuration > Unified Communication > Configuration**下也启用了**Authorize by OAuth token with refresh**。

通过此配置，您可以为信令和媒体实现类似的端到端安全呼叫连接，因此Expressway仅通过DTLS协商，因为它不会终止该流量本身。这显示在图像上，与之前的解决方案相比，唯一的区别是，它使用Expressway-C上与CUCM之间的CEOAuth区域，与CEtls区域相对，因为它使用SIP OAuth，而不是TLS上的安全设备注册，当CUCM在具有安全电话安全配置文件的混合模式中运行时，除了此以外，所有内容都保持不变。

解决方案3：用于不安全电话安全配置文件的加密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

先决条件:

- CUCM 12.5(1)SU1或更高版本(版本说明)
- Expressway X12.5.1或更高版本(版本说明)

专业：

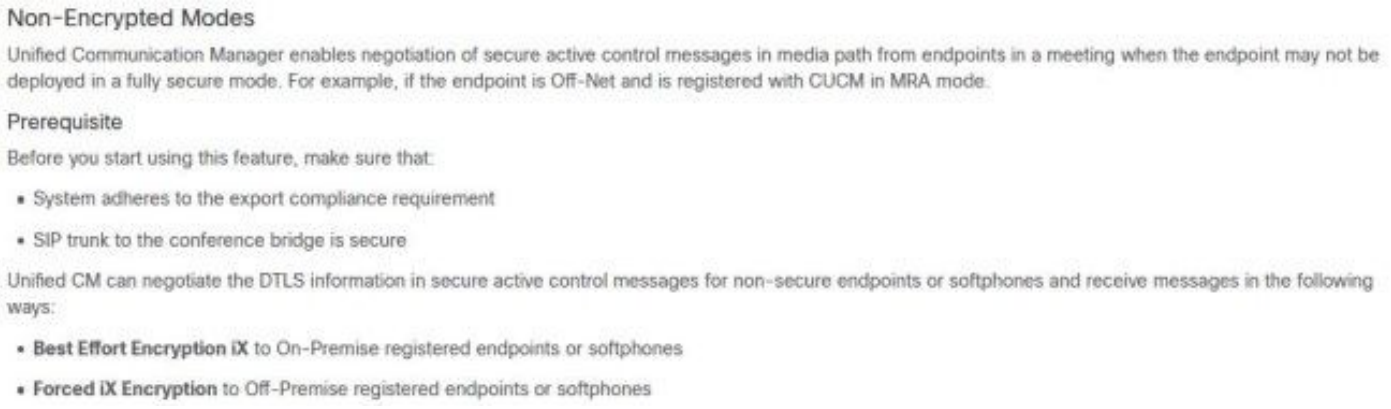
- 无需在混合模式下设置CUCM
- 无需设置安全的端到端通信
- 适用于Jabber和TC/CE终端

Con:

- 需要升级CUCM
- 仅支持CUCM受限版本

从CUCM 12.5(1)SU1，它支持任何SIP线路设备的iX加密协商，因此它可以在非安全终端或软件电话的安全ActiveControl消息中协商DTLS信息。它通过TCP发送Best Effort iX加密，使电话在与CUCM的不安全TCP连接（非TLS）的情况下端到端拥有加密的iX通道。

在CUCM 12.5(1)SU1的“加密iX通道”部分的安全指南中，它显示对于使用不安全设备的非加密模式，可以在系统遵守导出合规性且到会议网桥的SIP中继安全的前提下协商尽力而为和强制iX加密。



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

在CUCM上：

- 必须使用导出受限制的CUCM（非不受限制）
- 在**System > Licensing > License Management**下，必须将“Export-Controlled Functionality”设置为“allowed”。
- 您的SIP中继必须启用“**SRTP Allowed**”选项（无论中继本身是否安全都不管）

在CMS上：

- 您的callbridge必须具有带加密的许可证（因此您没有callBridgeNoEncryption许可证）
- 在webadmin上，在**Configuration > Call Settings**下，您必须将**SIP media encryption**设置为**allowed**(或**required**)

在图像中，您可以看到连接是安全的，直到Expressway-C和C通过SDP发送到CUCM而没有加密线路，但是仍然包含iX媒体信道。因此，音频/视频/..的普通媒体没有加密线路保护，但是它现在有用于iX媒体通道的安全连接，因此Expressway不需要终止DTLS连接。因此，即使使用不安全的电话安全配置文件，ActiveControl也可以在客户端和会议网桥之间直接协商。在CUCM的早期版本中，流量会有所不同，并且不会协商ActiveControl，因为最初它不会通过iX信道传递到CMS，因为该部分已经剥离。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。