MRA/Expressway上でActiveControlを有効にする

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[問題](#)
[General info](#)
[X12.5より前のExpresswayバージョン](#)
[X12.5以降のExpresswayバージョン](#)
[解決方法](#)
[解決策1：エンドポイントのセキュアな電話セキュリティプロファイル（混合モードCUCM）](#)
[解決策2:SIP OAuth for Jabber](#)
[解決策3：セキュアでない電話セキュリティプロファイル用の暗号化されたiXチャネル(CUCM 12.5(1)SU1以降)](#)

概要

このドキュメントでは、モバイルおよびリモートアクセス(MRA)クライアントと、オンプレミスのエンドポイントからExpressway経由でWebex Meetingsへのコールに対してActiveControlプロトコルを有効にするさまざまなオプションについて説明します。MRAは、Virtual Private Network-less(VPN)Jabberおよびエンドポイント機能の導入ソリューションです。このソリューションでは、エンドユーザが世界のどこからでも内部エンタープライズ リソースに接続できます。ActiveControlプロトコルはシスコ独自のプロトコルで、会議の名簿、ビデオレイアウトの変更、ミュート、録音オプションなどのランタイム機能により、より充実した会議エクスペリエンスを実現します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Expressway（MRAおよびB2Bコール）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Expressway X12.5
- Cisco Meeting Server(CMS)2.9

- Cisco Unified Communications Manager 12.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、主にCisco Meeting Server(CMS)へのMRAクライアント接続に重点を置いていますが、同じことが他のタイプのプラットフォームや接続（Webex Meetingsへの接続時など）にも当てはまります。次のタイプのコールフローにも同じロジックを適用できます。

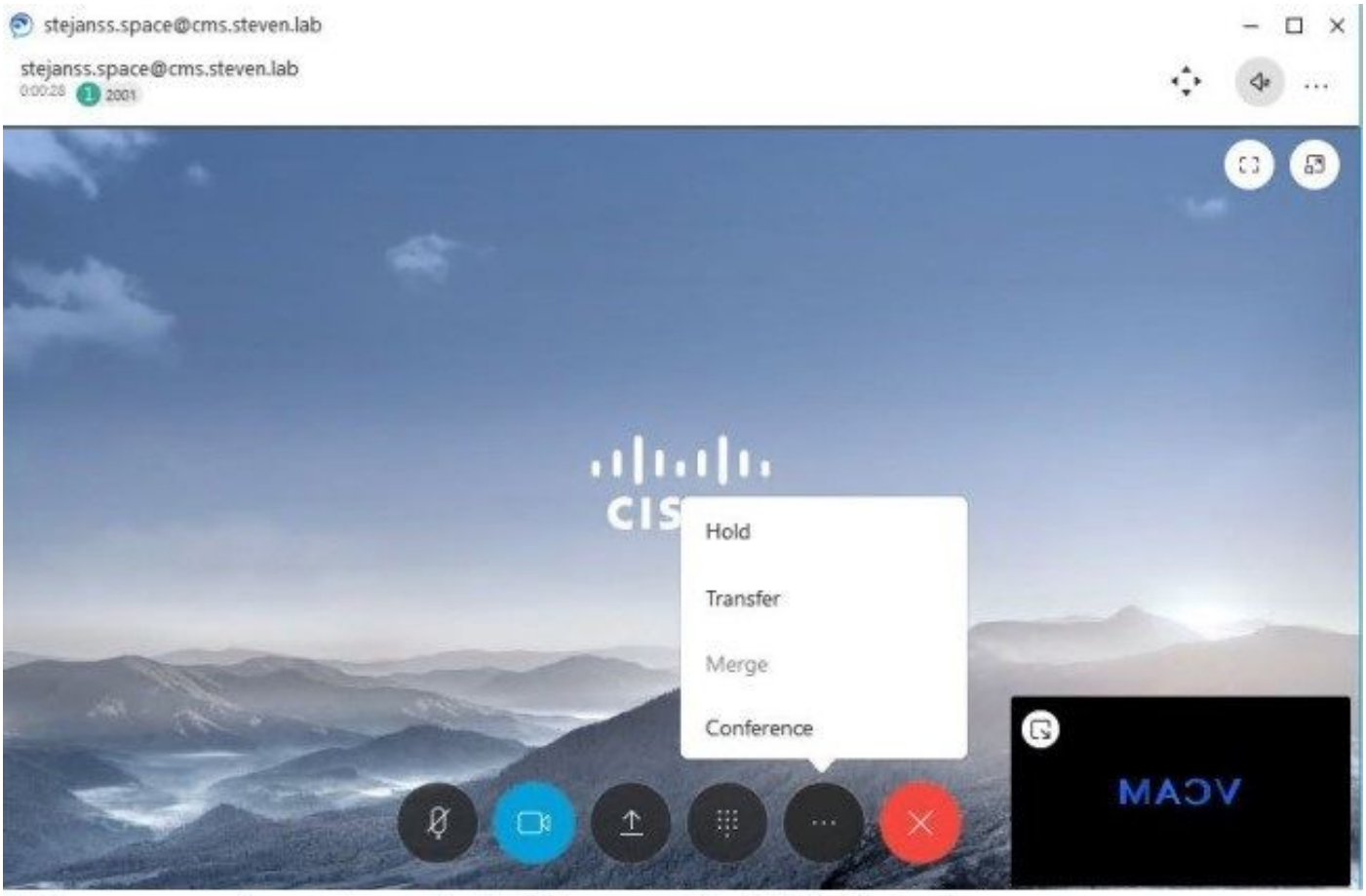
- エンドポイント – CUCM - Expressway-C - Expressway-E - Webex Meeting
- MRAエンドポイント – (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Webex Meeting

注:Webex MeetingsでサポートされているActiveControlの機能は、現時点のCMSの機能とは異なり、一部に限定されています。

Cisco Meeting Serverプラットフォームを使用すると、会議の参加者は、ActiveControlを通じて会議エンドポイントから直接、会議エクスペリエンスを制御できます。外部のアプリケーションやオペレータは必要ありません。ActiveControlは、シスコデバイスでiXメディアプロトコルを使用し、コールのSIPメッセージングの一部としてネゴシエートされます。CMSバージョン2.5の時点で有効になっている主な機能は次のとおりです（使用しているエンドポイントのタイプとソフトウェアバージョンによって異なる場合があります）。

- 会議に接続されたすべての参加者のリスト（名簿または参加者リスト）を表示する
- 他の参加者のミュートまたはミュート解除
- 会議への別の参加者の追加または削除
- 会議の記録の開始または停止
- 参加者を重要にする
- 会議のアクティブスピーカーである参加者のインジケータ
- 会議でコンテンツまたはプレゼンテーションを現在共有している参加者のインジケータ
- 会議のロックまたはロック解除

最初の図では、JabberクライアントからActiveControlを使用せずにCMSスペースにコールを発信したユーザビューが表示されています。2番目の図では、JabberがCMSサーバとActiveControlをネゴシエートできた、より機能の豊富なユーザビューが表示されています。



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControlはXMLベースのプロトコルで、Session Initiation Protocol(SIP)コールのSession Description Protocol(SDP)でネゴシエートされるiXプロトコルを使用して転送されます。これはシスコのプロトコル(eXtensible Conference Control Protocol(XCCP))であり、SIPのみでネゴシエートされ（インターワーキングコールにはActiveControlがないため）、データ転送にUDP/UDT（UDPベースのデータ転送プロトコル）を利用します。セキュアなネゴシエーションは、UDP接続を介したTLSと見なされるDatagram TLS(DTLS)を介して行われます。ネゴシエーシ

ョンの違いに関するサンプルを次に示します。

非暗号化

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

暗号化（ベストエフォート：暗号化を試みますが、暗号化されていない接続にフォールバックできます）

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:

暗号化（強制暗号化 – 暗号化されていない接続へのフォールバックを許可しない）

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

a=ixmap:2 **xccp**

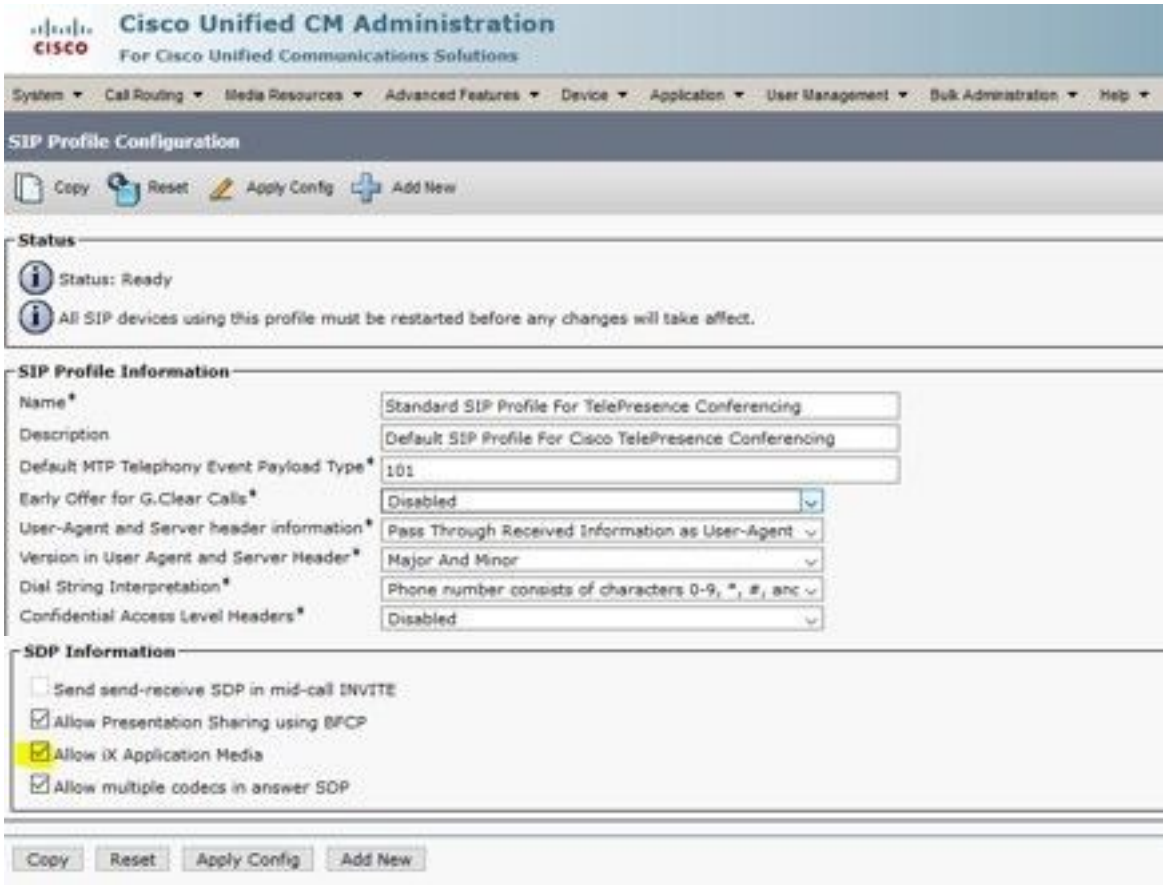
a=**fingerprint**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

ActiveControlを完全にサポートするには、次に示すいくつかの最小ソフトウェアバージョンが必要です。

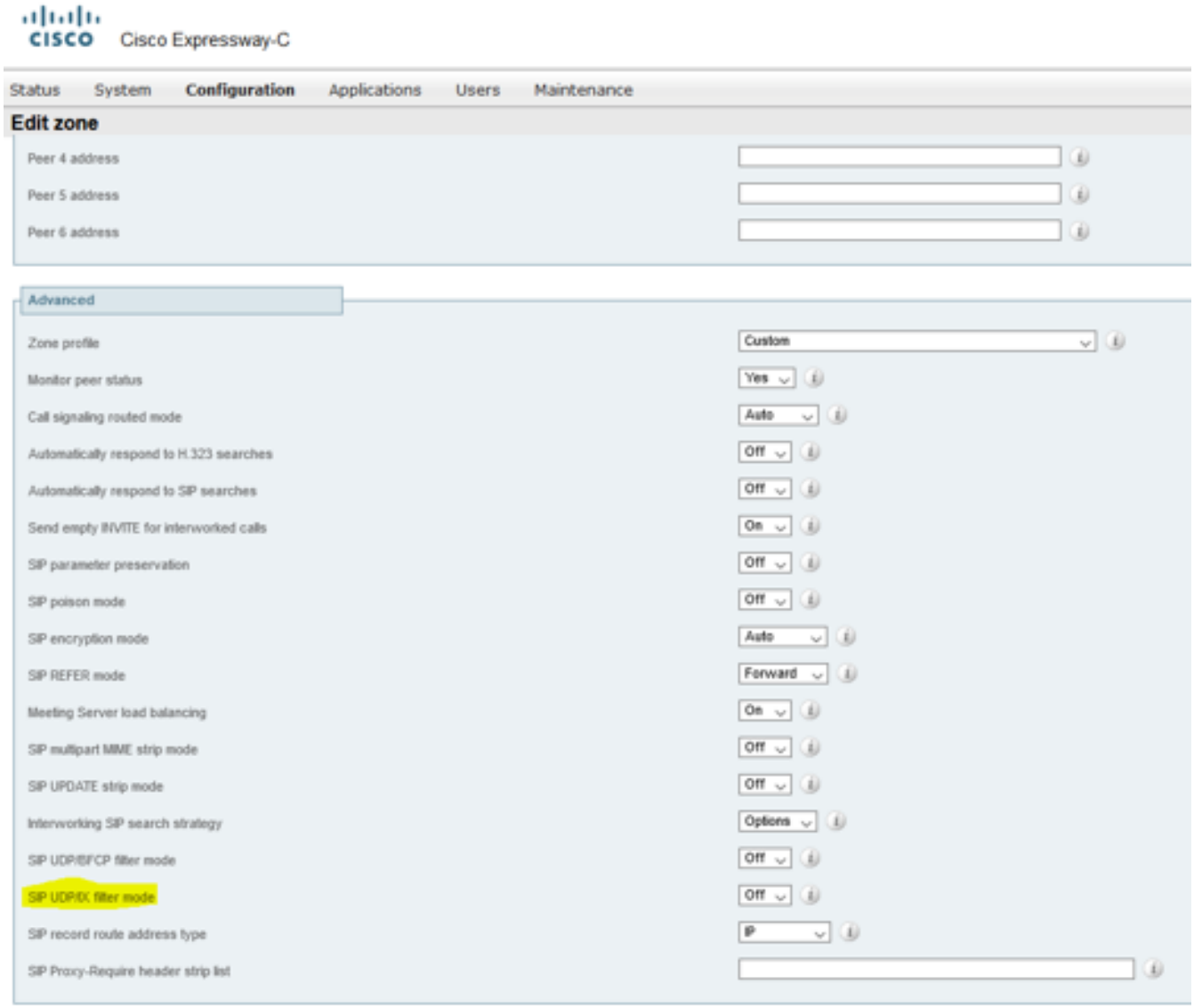
- Jabberバージョン12.5以降(リリースノート)
- CMS ActiveControlガイドに従い、CEエンドポイント8.3以降、9.6.2以降を推奨(Webexヘルプリンクに従い、Webex用のCE9.3.1以降)
- CUCM 10.5以降（Jabber 12.5 ActiveControlのサポート用）(リンクによるWebexの場合は11.5(1)以降)
- CMS ActiveControlガイドに従い、CMS 2.1以降、2.5以降を推奨
- 暗号化されていないMRAクライアントでのサポートを可能にするExpressway X12.5以降(リリースノート)

考慮すべき設定オプションがいくつかあります。

- CUCMで、関連するSIPトランク（Expressway-CおよびCMSへの）が、[iXアプリケーションメディアの許可(Allow iX Application Media)]がオンになっているSIPプロファイルで設定されていることを確認します



- CMSでは、デフォルトで2.1以降で有効になっていますが、*sipUDT*をfalseに設定できるcompatibilityProfileを使用して無効にすることができます
- Expresswayの[Advanced]設定の[Zone]設定で（[Custom]ゾーンプロファイルを使用している場合）、iXの通過を許可する場合は、[SIP UDP/IX filter mode] が[Off]に設定されていることを確認します



問題

General info

ActiveControlは、他のメディアチャネルとは異なる方法で安全にネゴシエートされます。たとえば、音声やビデオなどの他のメディアチャネルの場合、SDPには、このチャネルに使用する暗号キーをリモートパーティにアナウンスするために使用される暗号回線が付加されます。そのため、Real-time Transport Protocol(RTP)チャネルをセキュアにできるため、セキュアRTP(SRTP)と見なすことができます。iXチャネルでは、DTLSプロトコルを使用してXCCPメディアストリームを暗号化するため、別のメカニズムを使用します。

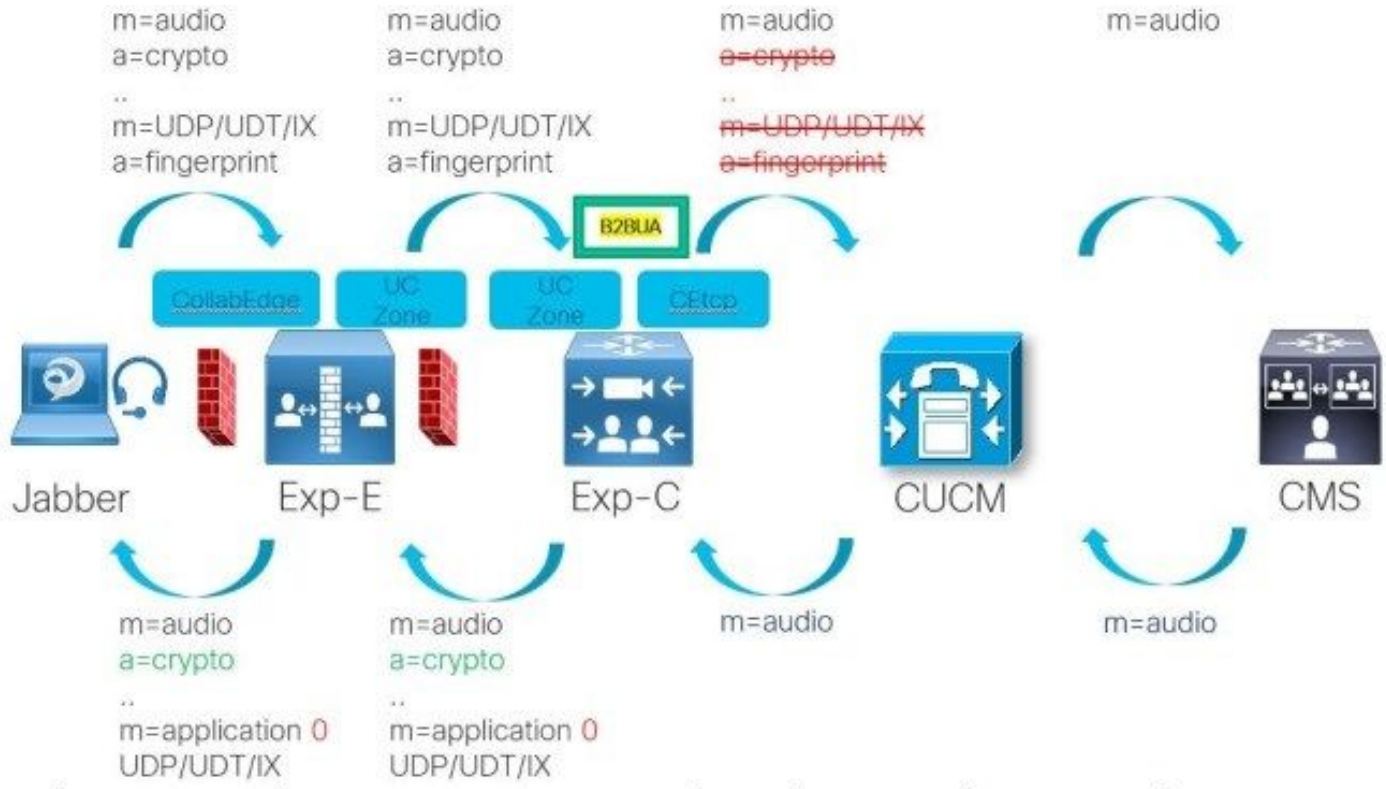
ExpresswayソフトウェアはDTLSプロトコルを終了しません。これは、Expresswayリリースノートの「*サポートされていない機能*」にある「*制限事項*」の項で説明されています。

- 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より前のExpresswayバージョン

X12.5より前のバージョンのExpresswayを実行している場合に、暗号化されたiXチャネルを使用

した着信接続がセキュアでないTCPゾーンを通過すると、Expresswayは通常のメディアチャネルの暗号行とiXチャネル全体の両方を削除します。これは、MRAクライアントからExpressway-Cへの接続が安全であることを確認できるCMSスペースに接続するMRAクライアントに対して表示されますが、デバイスのCUCMに設定されている電話セキュリティプロファイルに応じて、暗号化されていない（CEtcpゾーンを介して送信される）または暗号化されている（CEtlsゾーンを介して送信される）のどちらかになります。図に示すように暗号化が解除されている場合、Expressway-CではDTLSプロトコルを終端できないため、すべてのメディアチャネルの暗号行が削除され、iXメディアチャネル全体も削除されます。これは、Back-To-Back User Agent(B2BUA)を介して発生します。これは、CEtcpゾーンのゾーン設定がメディア暗号化「Force unencrypted」で設定されているためです。逆方向（「Force encrypted」メディア暗号化を使用したUCトラバーサルゾーン上）でSDP応答を受信すると、通常のメディア回線用の暗号行が追加され、iXチャネル用のポートがゼロになり、ActiveControlネゴシエーションは行われません。内部的には、クライアントがCUCMに直接登録されると、CUCMは自身をメディアパスに配置しないため、暗号化されたiXメディアチャネルと暗号化されていないiXメディアチャネルの両方が許可されます。



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

同じ種類のロジックが、Expresswayを介したWebex Meetingsへのコール接続にも適用されます。Expresswayサーバ（X12.5より前）はDTLS接続情報を渡すだけで、新しいセッションを開始したり、異なるコールレッグでメディアチャネルを暗号化/復号化したりするために自分自身で終端しないため、完全なパスはエンドツーエンドで安全である必要があります。

X12.5以降のExpresswayバージョン

ExpresswayバージョンのX12.5以降を実行している場合、強制暗号化(UDP/DTLS/UDT/IX)としてTCPゾーン接続を介してiXチャネルを通過する動作が変更されています。これは、iXチャネルのネゴシエーションを引き続き許可し、リモートエンドが暗号化を使用する場合にのみ許可するためです。ExpresswayはDTLSセッションを終了させないため、暗号化を強制します。そのため、Expresswayはパススルーでのみ動作し、DTLSセッションの開始/終了はリモートエンドに依存します。セキュリティ上の目的で、TCP接続を介して暗号行が取り除かれます。この動作の変更については、「MRA：暗号化iXのサポート（ActiveControlの場合）」の項に従ってリリースノート

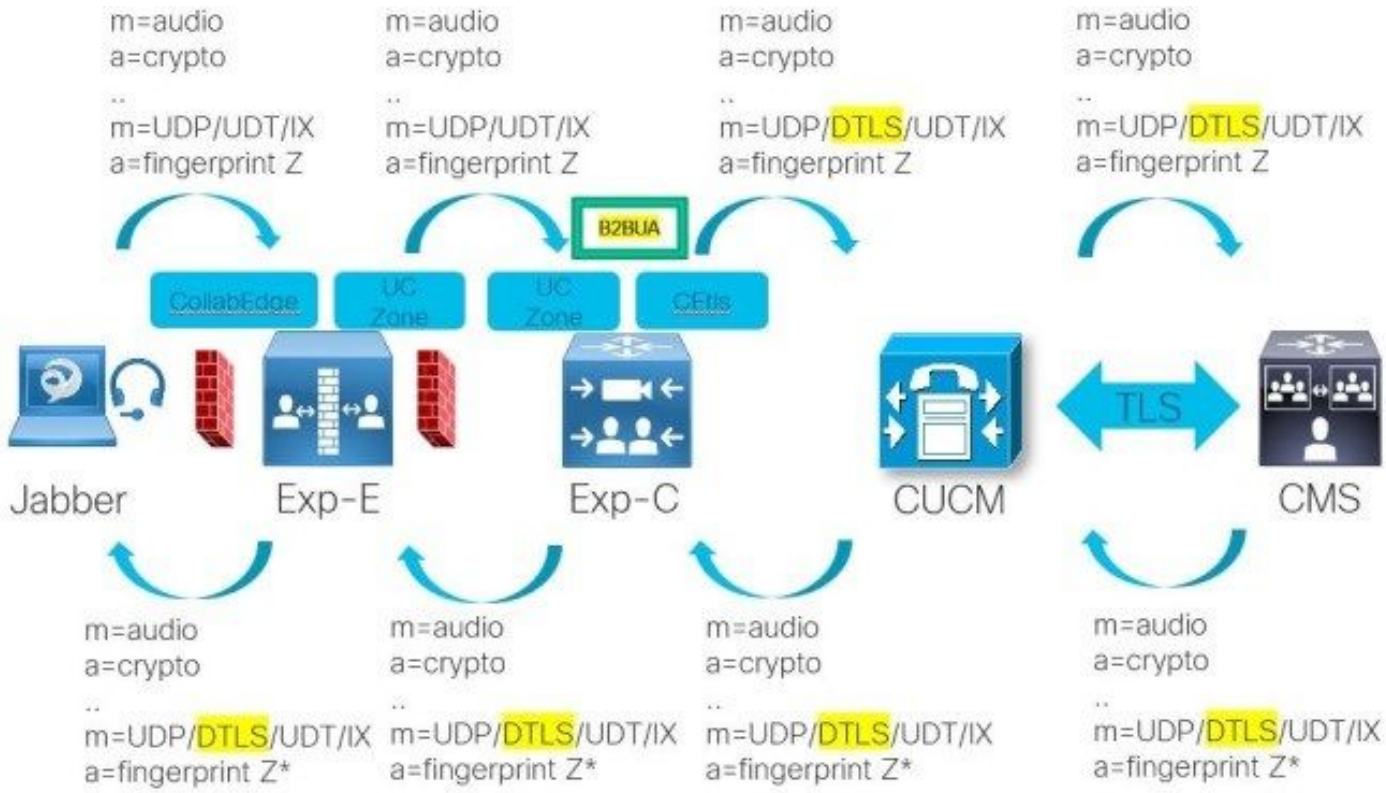
に記載されています。その後の動作は、12.5(1)SU1で変更されたCUCMのバージョンによって異なります。このバージョンでは、iXチャネルを介したパススルーと、セキュアでない着信接続が許可されています。CMSへのセキュアなTLS SIPトランクが存在する場合でも、12.5(1)SU1よりも低いバージョンのCUCMを実行している場合は、iXチャネルをCMSに渡す前に取り除くため、結果的にCUCMからExpressway-Cへのポートがゼロになります。

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.

エンドツーエンドのセキュアコールシグナリングとメディアパスを使用すると、iXチャネルは(MRA)クライアントと会議ソリューション（CMSまたはWebex Meeting）間で直接ネゴシエート（Expresswayサーバの異なるホップ経由で渡される）できます。次の図は、CMSスペースに接続しているMRAクライアントの同じコールフローを示していますが、現在はCUCMに設定されたセキュアな電話セキュリティプロファイルとCMSへのセキュアなTLS SIPトランクを使用しています。パスがエンドツーエンドでセキュアであり、DTLSフィンガープリントパラメータがパス全体に渡されたことがわかります。

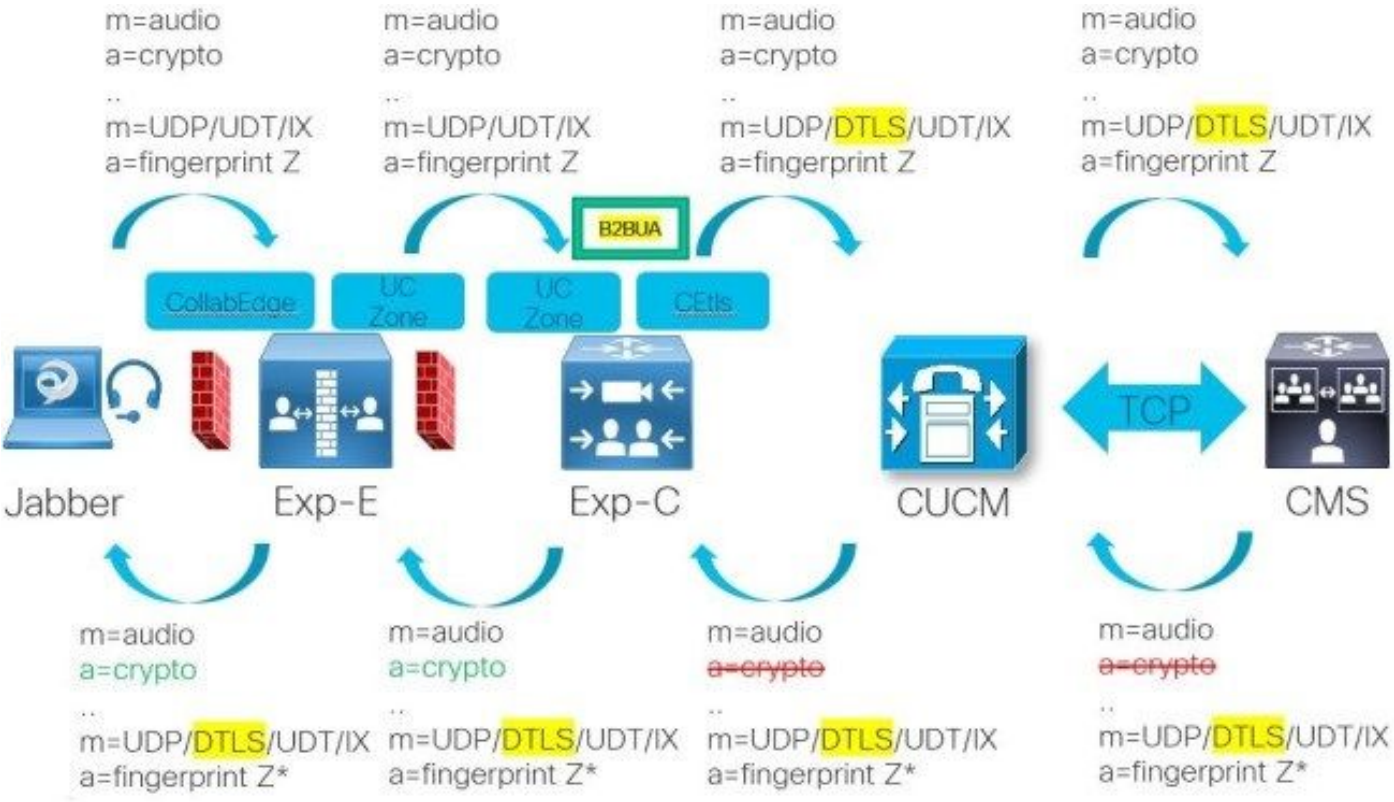


Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

セキュアなデバイスセキュリティプロファイルを設定するには、CUCMが混合モードで設定されていることを確認する必要があります。このプロセスは煩雑になる可能性があります(また、セキュアなオンプレミス通信のためにCertificate Authority Proxy Function(CAPF)が必要であるため、動作している場合も同様です)。したがって、このドキュメントで説明するように、MRAおよびExpressway全体でのActiveControlのアベイラビリティをサポートするために、他のより便利なソリューションをここで提供できます。

CUCM（SIPトランクで[SRTP Allowed]オプションが有効になっていると仮定）は常に着信セキュアSIP接続からiXチャネルおよび暗号化回線を引き継ぐが、CMSは暗号化を使用してiXチャネ

ルに応答するだけ（ActiveControlを許可）で(**SIPメディア暗号化が** *許可または強制が*[設定(**Settings)]**でCMSに設定されている設定されていると設定のCMSに設定に設定設定に設定に設定設定されているされているに設定されているに設定設定に設定されているに設定設定に設定設定されているされているに設定に設定に設定に設定設定設定されているイメージに従ってクリプトラインを除去するようにチャネルを設定します。Expresswayサーバは、接続のその部分を保護するために再び暗号回線を追加できますが（iXはDTLSを介してエンドクライアント間で直接ネゴシエートされます）、セキュリティの観点からは理想的ではありません。そのため、会議ブリッジへのセキュアSIPトランクを設定することをお勧めします。SIPトランクで**SRTP Allowed**にチェックマークが付いていない場合、CUCMは暗号回線を除去し、セキュアiXネゴシエーションも失敗します。



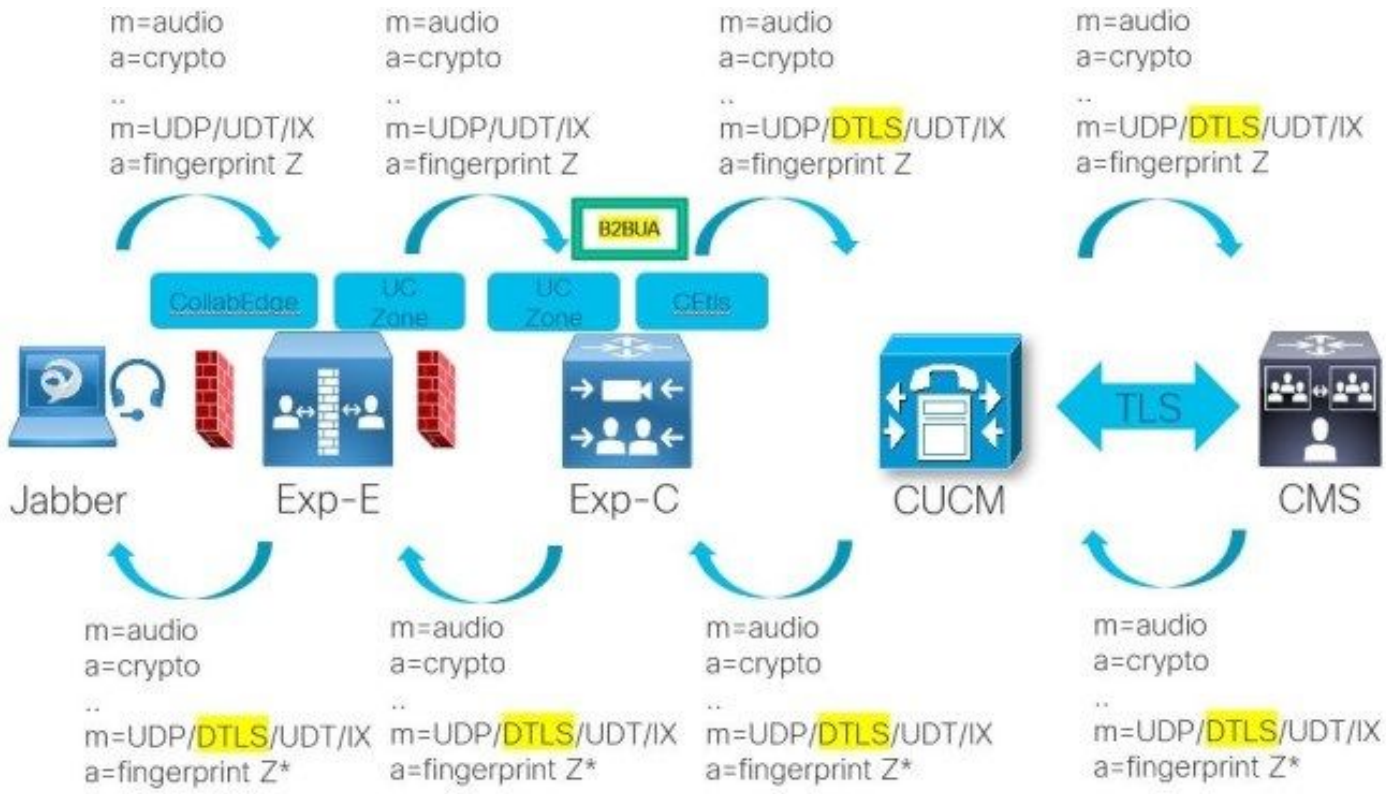
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

解決方法

さまざまな要件とさまざまな長所と短所で利用可能な異なるオプションがいくつかあります。これらはそれぞれ、より詳細なセクションで説明されています。次のオプションがあります。

1. エンドポイントのセキュアな電話セキュリティプロファイル（混合モードCUCM）
2. SIP OAuth for Jabber
3. セキュアでない電話セキュリティプロファイル用の暗号化されたiXチャネル(CUCM 12.5(1)SU1以降)

解決策1：エンドポイントのセキュアな電話セキュリティプロファイル（混合モードCUCM）



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

前提条件

- 混合モードのCUCM

Pro:

- 任意のCUCMバージョンで動作
- すべてのクライアントデバイスに対応

Con:

- 混合モードでのCUCMの設定（およびオンプレミスのエンドポイントでのCAPF操作）が必要

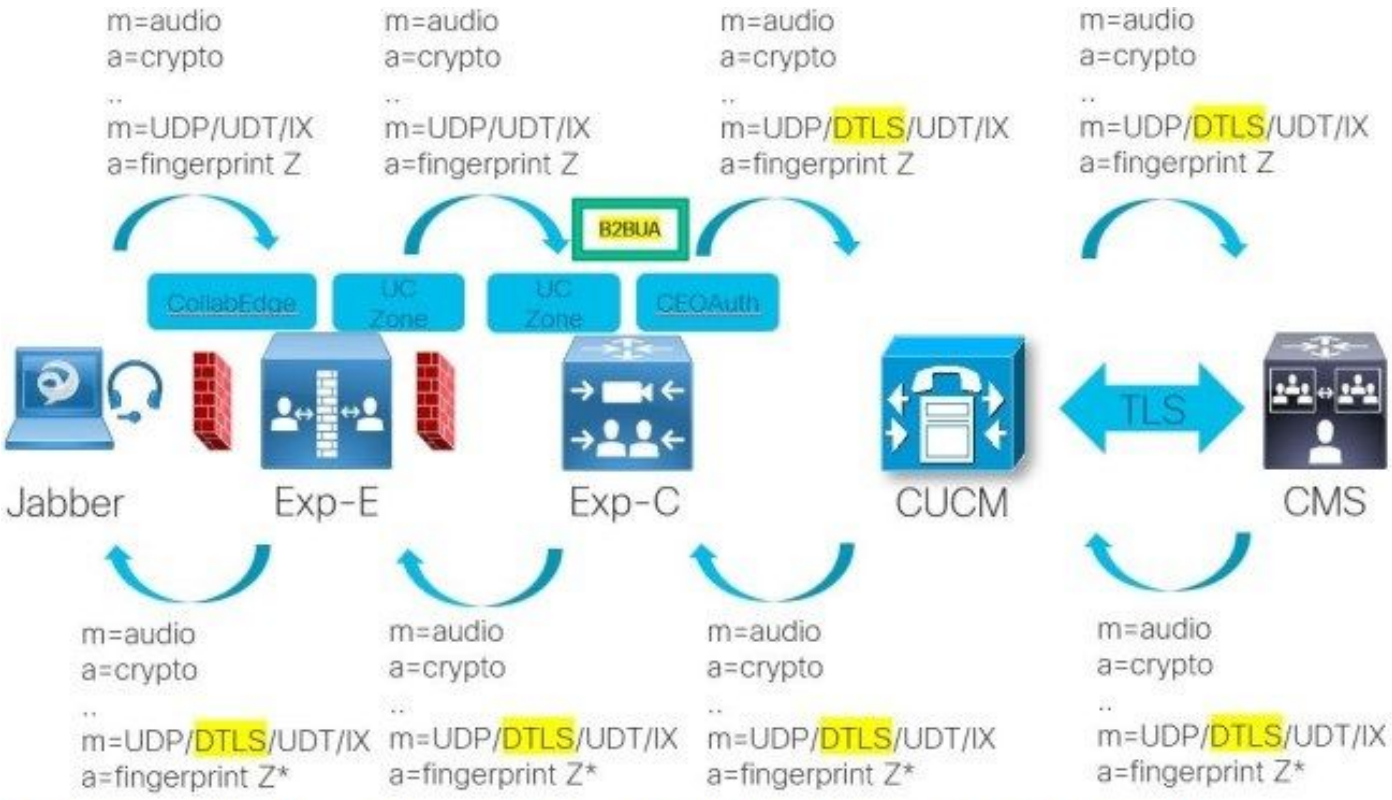
これは、「問題」セクションで説明した方法であり、エンドツーエンドの暗号化されたコールシグナリングとメディアパスがあることを確認する最後の方法でもあります。次のドキュメントに従って、CUCMを混合モードで設定する必要があります。

MRAクライアントの場合はCAPF操作は必要ありませんが、「Collaboration Edge TCベースのエンドポイントの設定例」（CEベースのエンドポイントとJabberクライアントにも適用）で強調表示されているように、Expressway-Cサーバ証明書のサブジェクト代替名の1つと一致する名前を持つセキュア電話セキュリティプロファイルを使用して、追加の設定手順を実行する必要があります。

オンプレミスのエンドポイントまたはJabberクライアントからWebex会議に接続する場合は、CAPF操作を実行して、クライアントをCUCMに安全に登録する必要があります。これは、ExpresswayがDTLSネゴシエーションを通過でき、Expressway自体では処理できない、エンドツーエンドのセキュアコールフローを確保するために必要です。

コールをエンドツーエンドでセキュアにするには、関連するすべてのSIPトランク（Webex Meetingへのコールの場合はExpressway-Cに、CMS会議へのコールの場合はCMSに）が、セキュアSIPトランクセキュリティプロファイルを使用したTLSを使用してセキュアSIPトランクであることを確認します。

解決策2:SIP OAuth for Jabber



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

前提条件

- Cisco Jabber 12.5以降(リリースノート)
- CUCMバージョン12.5以降(リリースノート)、*OAuthとRefresh Login Flow*を有効にした状態
- Expressway X12.5.1以降(リリースノート)、[Authorize by OAuth token with refresh] が有効になっている場合

Pro:

- セキュアな登録が可能で、毎回CAPFを更新することなく、オンプレミスとオフプレミスを簡単に切り替えることができます。
- 混合モードでCUCMを設定する必要がない

Con:

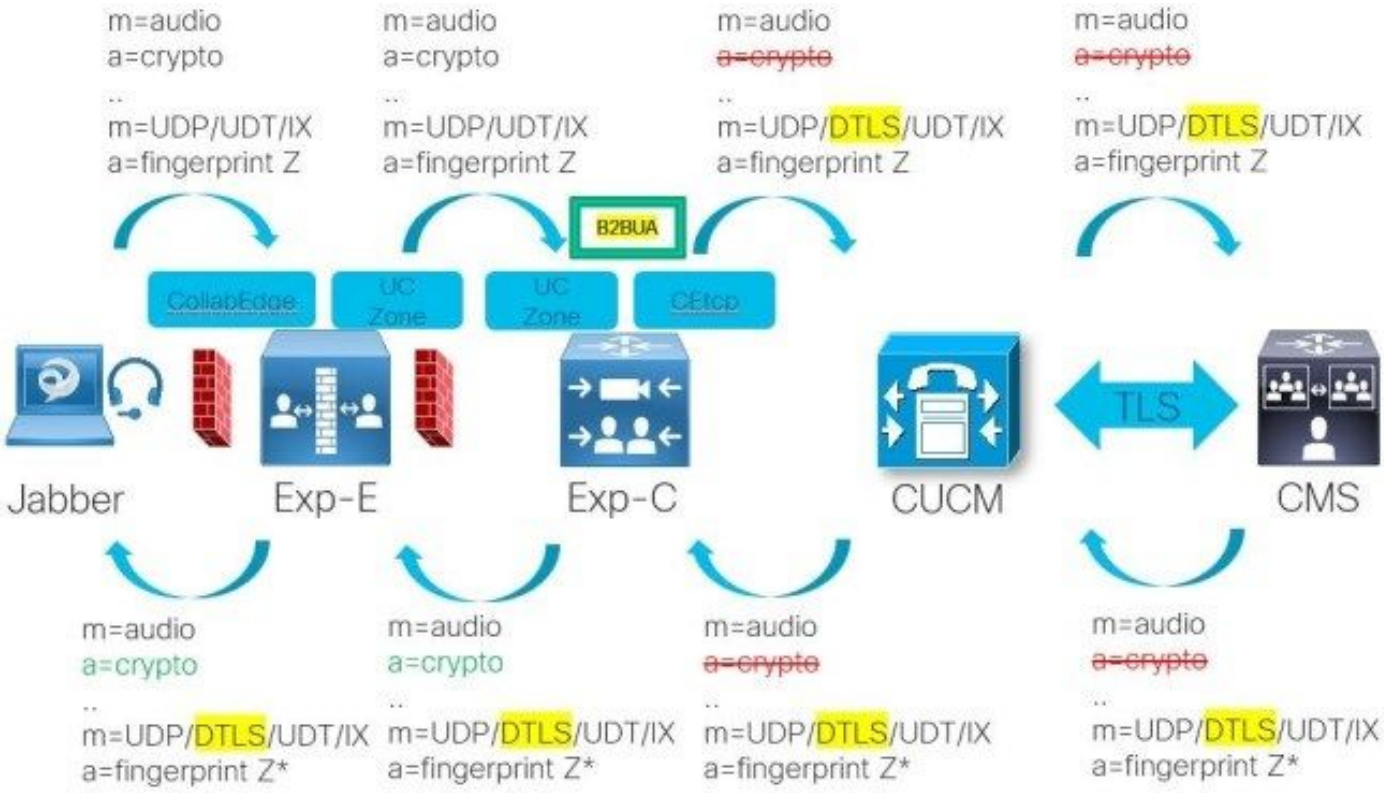
- Jabberにのみ適用され、TC/CEエンドポイントには適用されない

SIP OAuthモードでは、セキュアな環境でCisco Jabber認証にOAuth更新トークンを使用できます。ソリューション1のCAPF要件なしで、セキュアなシグナリングとメディアが可能になります。SIP登録時のトークン検証は、OAuthベースの認証がCUCMクラスタおよびJabberエンドポイントで有効にされたときに完了します。

CUCMの設定は機能設定ガイドに記載されており、[Enterprise Parameters]で[Refresh Login Flow]が有効になっているOAuthが必要です。これをMRAでも有効にするには、[Configuration] > [Unified Communication] > [Unified CM Servers] でExpressway-CサーバのCUCMノードを更新し、[Configuration] > [Zones] > [Zones] で自動作成されたCEOAuthゾーンも表示されるようにします。[Configuration] > [Unified Communication] > [Configuration] で、[Authorize by OAuth token with refresh] も有効になっていることを確認します。

この設定を使用すると、シグナリングとメディアの両方に対して同様のエンドツーエンドのセキュアコール接続を実現できます。したがって、Expresswayはトラフィック自体を終端しないため、DTLSネゴシエーションを通過するだけです。これは、前のソリューションと比較した唯一の違いは、CUCMがセキュア電話セキュリティプロファイルを使用して混合モードで動作する場合、TLS経由のセキュアデバイス登録ではなくSIP OAuthを使用するため、CEtlsゾーンではなく、Expressway-C上のCEOAuthゾーンをCUCMに使用するという点です。ただし、それ以外は同じです。

解決策3：セキュアでない電話セキュリティプロファイル用の暗号化されたiXチャネル(CUCM 12.5(1)SU1以降)



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

前提条件

- CUCMバージョン12.5(1)SU1以降(リリースノート)
- Expressway X12.5.1以降(リリースノート)

Pro:

- 混合モードでCUCMを設定する必要がない
- セキュアなエンドツーエンド通信を設定する必要がない
- JabberとTC/CEの両方のエンドポイントに適用可能

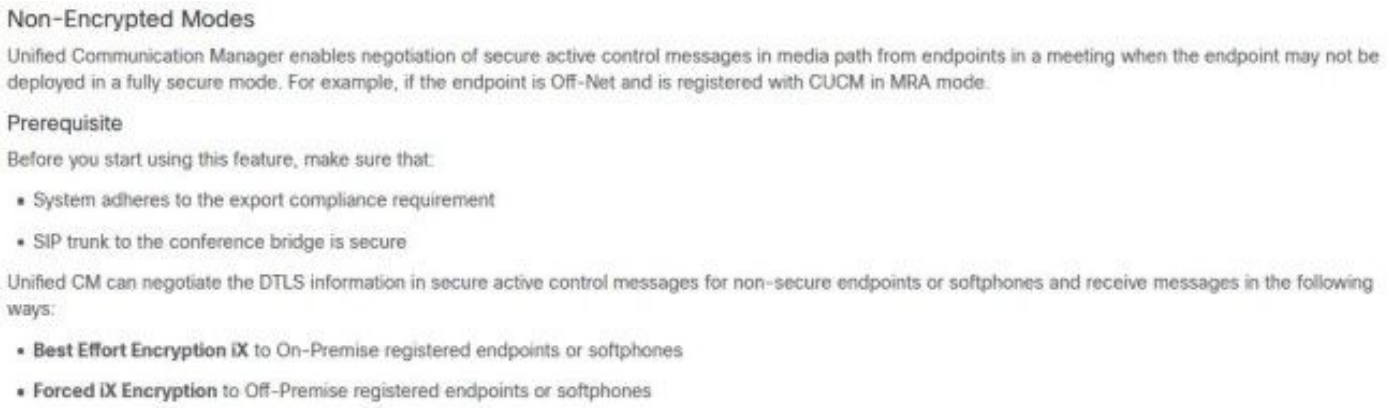
Con:

- CUCMのアップグレードが必要
- CUCM制限バージョンのみがサポートされます

CUCM 12.5(1)SU1以降では、任意のSIP回線デバイスのiX暗号化ネゴシエーションをサポートしているため、非セキュアなエンドポイントまたはソフトフォンのセキュアなActiveControlメッセージでDTLS情報をネゴシエートできます。CUCMへの（TLSではない）セキュアでないTCP接続

に関係なく、電話機がエンドツーエンドで暗号化されたiXチャネルを持つことができるように、TCP経由でベストエフォートiX暗号化を送信します。

「暗号化されたiXチャネル」セクションのCUCM 12.5(1)SU1のセキュリティガイドでは、暗号化されていないデバイスを使用する非暗号化モードでは、システムが輸出規制に準拠し、会議ブリッジへのSIPトランクが安全であることを前提に、ベストエフォートと強制的なiX暗号化をネゴシエートできることを示しています。



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

CUCM上：

- 輸出規制対象のCUCM（制限なし）を使用する必要があります。
- [System] > [Licensing] > [License Management] で、[Export-Controlled Functionality]を[allowed]に設定する必要があります。
- SIPトランクでは、[SRTP Allowed] オプションを有効にする必要があります（トランク自体がセキュアか非セキュアかに関係なく）

CMS上：

- callbridgeには暗号化付きのライセンスが必要です（callBridgeNoEncryptionライセンスは必要ありません）
- webadminの[Configuration] > [Call Settings] で、[SIP media encryption] を[allowed](または[required])に設定する必要があります

この図では、Expressway-CとCがSDPを介して暗号回線なしでCUCMに送信するまで接続がセキュアであることがわかります。ただし、iXメディアチャネルは依然として含まれています。したがって、audio/video/..の通常のメディアは暗号化回線で保護されていませんが、ExpresswayがDTLS接続を終了する必要がないように、iXメディアチャネル用のセキュアな接続が現在あります。したがって、セキュアでない電話セキュリティプロファイルを使用している場合でも、クライアントと会議ブリッジ間で直接ActiveControlをネゴシエートできます。以前のバージョンのCUCMでは、フローが異なり、ActiveControlはネゴシエートされません。これは、その部分がすでに取り除かれていたため、最初にiXチャネルを介してCMSに渡されないためです。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。