Ativar AtiveControl sobre MRA/Expressway

Contents

Introduction

Este documento descreve as diferentes opções para ativar o protocolo AtiveControl para clientes de acesso remoto e móvel (MRA) e para chamadas de endpoints locais para reuniões Webex via Expressway. O MRA é uma solução de implantação para o Jabber sem rede privada virtual (VPN) e recurso de endpoint. Essa solução permite que os usuários finais se conectem aos recursos internos da empresa de qualquer lugar do mundo. O protocolo AtiveControl é um protocolo proprietário da Cisco que permite uma experiência de conferência mais rica com recursos de tempo de execução, como listas de reuniões, alterações de layout de vídeo, opções de cancelamento de áudio e gravação.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Expressway (chamadas MRA e B2B)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Neste documento, o foco principal está na conexão do cliente MRA a um Cisco Meeting Server (CMS), mas o mesmo se aplica a outros tipos de plataformas ou conexões, como, por exemplo, ao conectar-se a Webex Meetings. A mesma lógica pode ser aplicada para os seguintes tipos de fluxos de chamada:

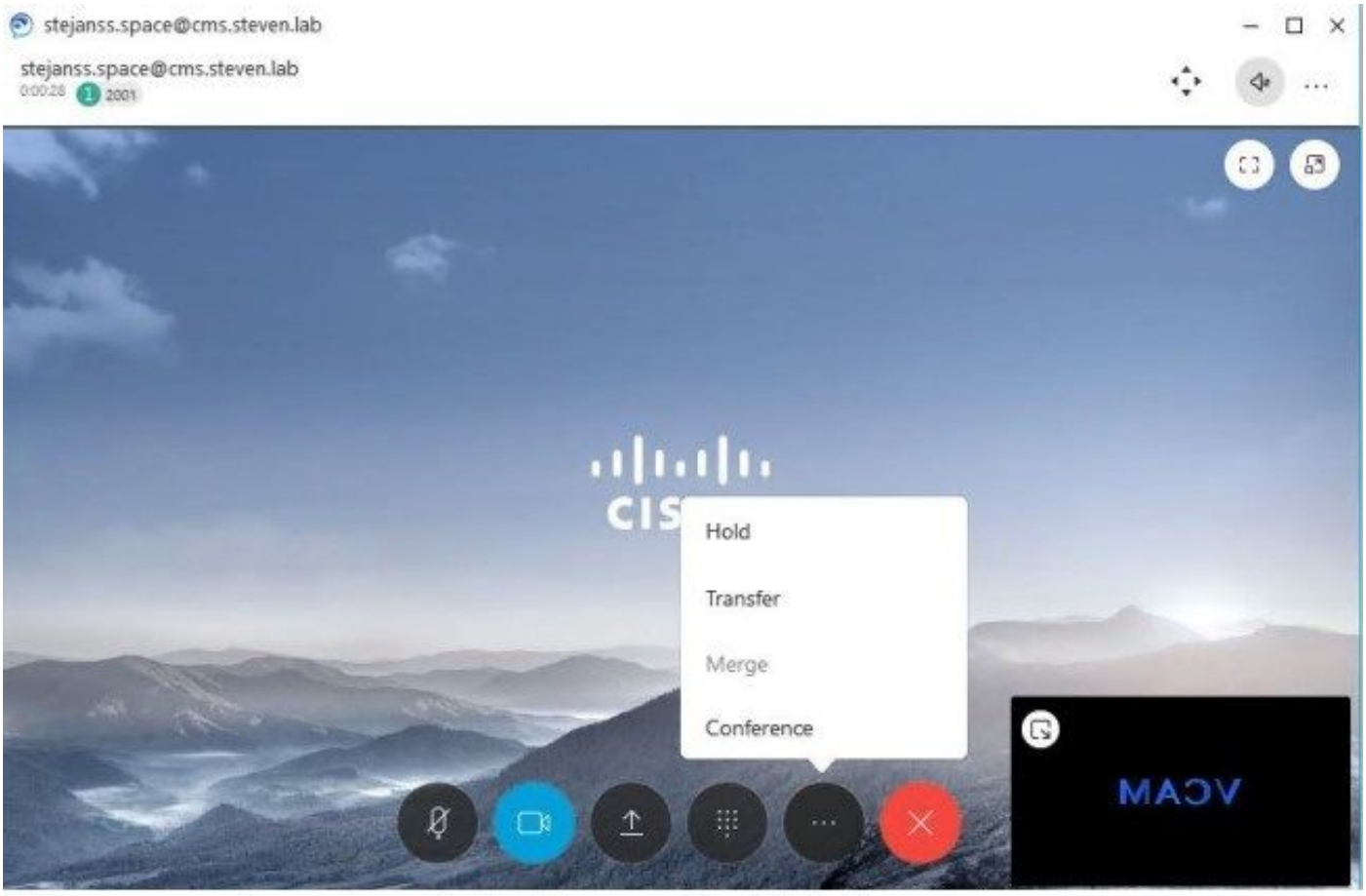
- Endpoint - CUCM - Expressway-C - Expressway-E - Webex Meeting
- Ponto de extremidade MRA - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Webex Meeting

  Observação: os recursos do AtiveControl suportados pelo Webex Meetings são diferentes dos do CMS no momento e são apenas um subconjunto limitado.

A plataforma Cisco Meeting Server oferece aos participantes da reunião a capacidade de controlar a experiência de reunião diretamente do endpoint de conferência por meio do AtiveControl, sem a necessidade de aplicativos ou operadores externos. O AtiveControl utiliza o protocolo de mídia iX em dispositivos Cisco e é negociado como parte do sistema de mensagens SIP de uma chamada. A partir da versão 2.5 do CMS, os principais recursos ativados são os seguintes (embora possam depender do tipo de endpoint e da versão de software em uso):

- Exibindo uma lista de todos os participantes (lista de participação ou lista de participantes) conectados à reunião
- Cancelando ou restaurando o áudio de outros participantes
- Adicionar ou remover outro participante da reunião
- Iniciando ou interrompendo a gravação de uma reunião
- Tornar um participante importante
- Indicador para o participante que é o locutor ativo na reunião
- Indicador do participante que está compartilhando conteúdo ou apresentação na reunião no momento
- Bloqueando ou desbloqueando a reunião

Na primeira imagem, você vê uma visualização de usuário de um cliente Jabber que fez uma chamada em um espaço do CMS sem AtiveControl, enquanto a segunda imagem mostra a visualização de usuário mais rica em recursos, onde o Jabber foi capaz de negociar o AtiveControl com o servidor do CMS.



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

O AtiveControl é um protocolo baseado em XML que é transferido usando o protocolo iX que é negociado no Session Description Protocol (SDP) das chamadas do Session Initiation Protocol (SIP). É um protocolo da Cisco (eXtensible Conference Control Protocol (XCCP)) e negociado apenas no SIP (de modo que as chamadas interconectadas não tenham AtiveControl) e aproveita o UDP/UDT (Data Transfer Protocol baseado em UDP) para transferência de dados. A negociação segura acontece por meio do Datagram TLS (DTLS), que pode ser visto como TLS

em conexão UDP. Alguns exemplos são mostrados aqui para as diferenças na negociação.

Não criptografado

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

Criptografado (melhor esforço - tente a criptografia, mas permita o fallback para a conexão não criptografada)

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:

Criptografado (forçar criptografia - não permitir fallback para conexão não criptografada)

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

a=ixmap:2 **xccp**

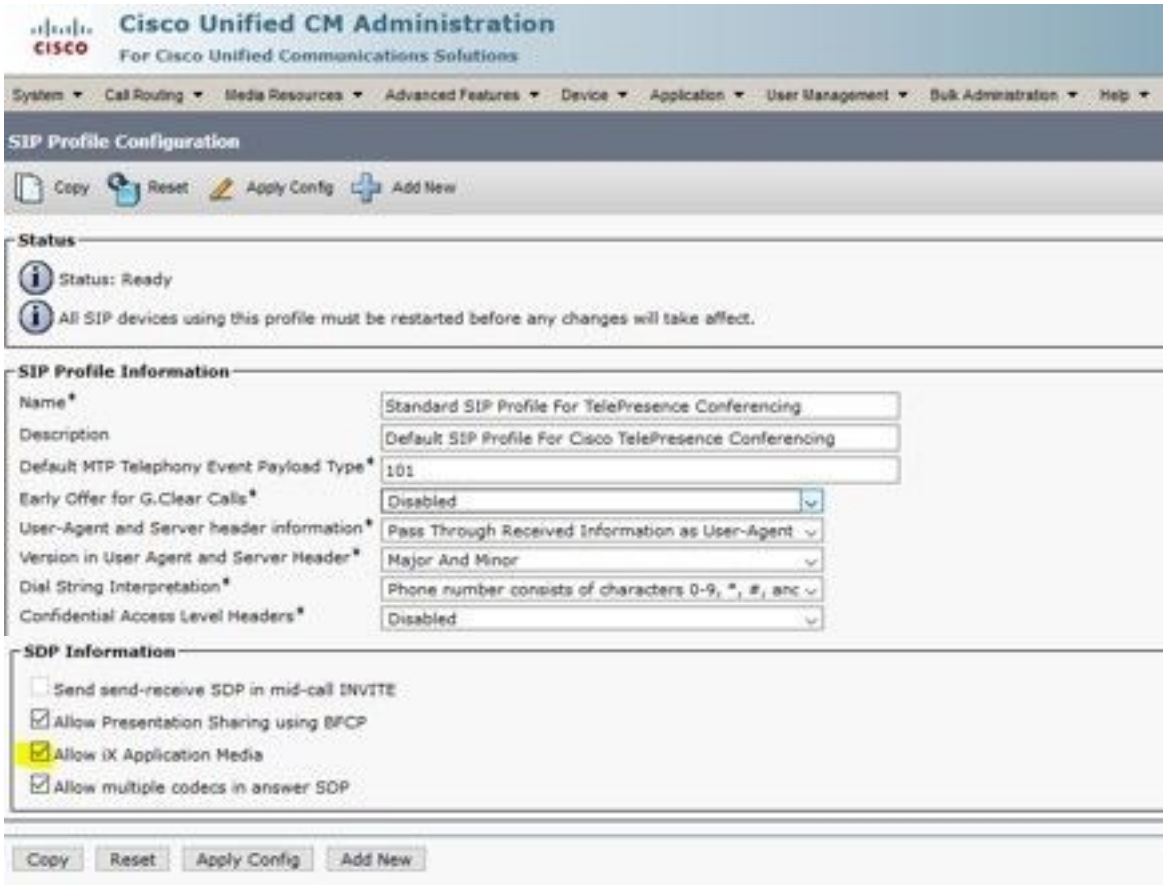
a=**fingerprint**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

Há algumas versões mínimas de software necessárias para suporte total ao AtiveControl, conforme listado:

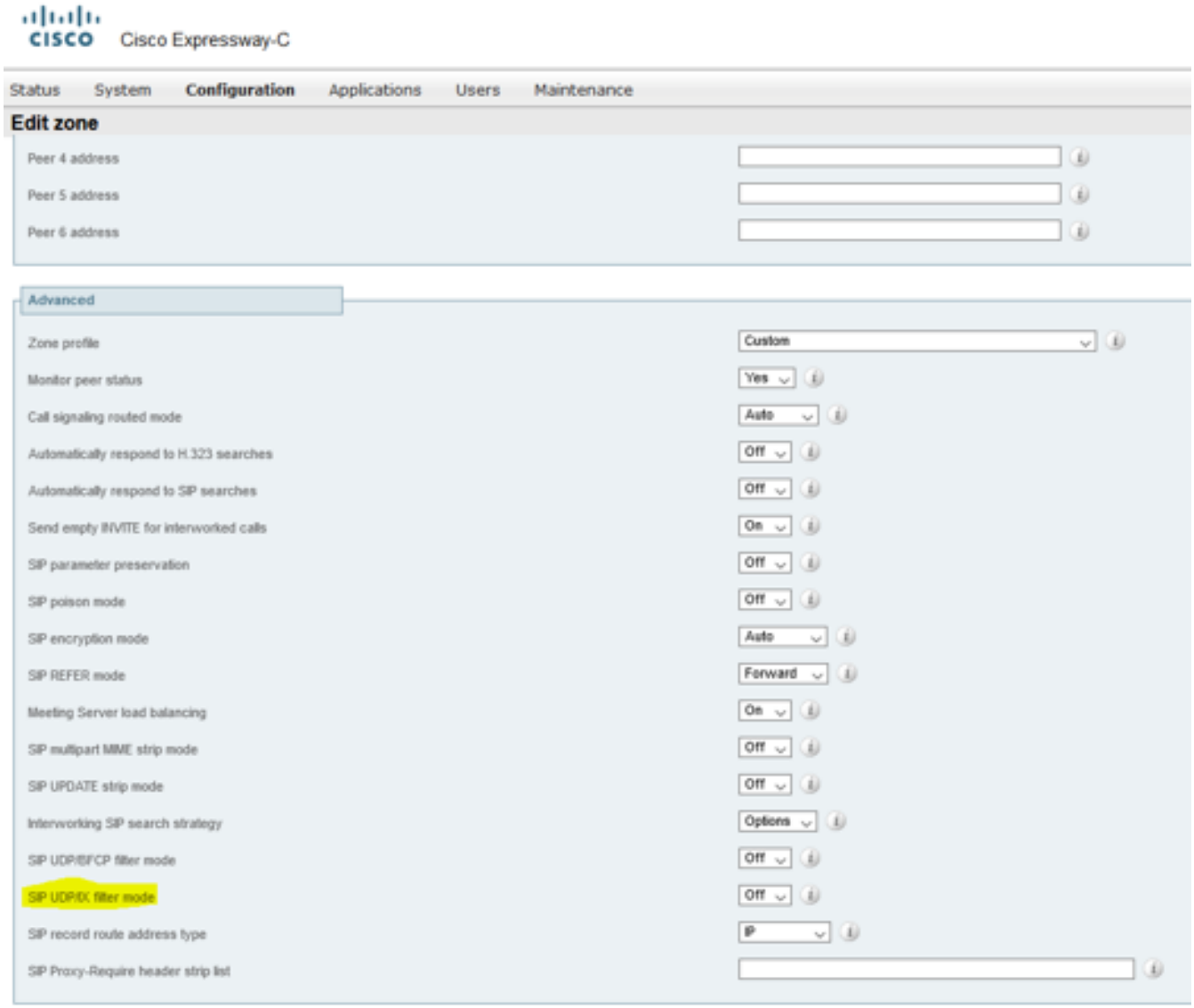
- Jabber versão 12.5 ou posterior (notas de versão)
- Endpoints CE 8.3 ou posterior, 9.6.2 ou posterior recomendados de acordo com o guia CMS AtiveControl (CE9.3.1 ou posterior para Webex de acordo com o link de ajuda do Webex)
- CUCM 10.5 ou posterior (para suporte ao AtiveControl do Jabber 12.5) (11.5(1) ou posterior para Webex conforme o link)
- CMS 2.1 ou posterior, 2.5 ou posterior recomendado de acordo com o guia AtiveControl do CMS
- Expressway X12.5 ou posterior (notas de versão) para permitir suporte em clientes MRA não criptografados

Há algumas opções de configuração a serem consideradas:

- No CUCM, certifique-se de que os troncos SIP relevantes (para Expressway-C e CMS) estejam configurados com um perfil SIP que tenha a opção "Permitir mídia de aplicativo iX" marcada



- No CMS, ele é habilitado por padrão a partir da versão 2.1, mas você pode desabilitá-lo através de um compatibilityProfile no qual você pode definir *sipUDT* como falso
- No Expressway na configuração da zona nas configurações avançadas (ao usar um perfil de zona 'Personalizado'), certifique-se de que o *modo de filtro SIP UDP/IX* esteja definido como 'Desligado' se desejar permitir que o iX passe



Problema

Informações gerais

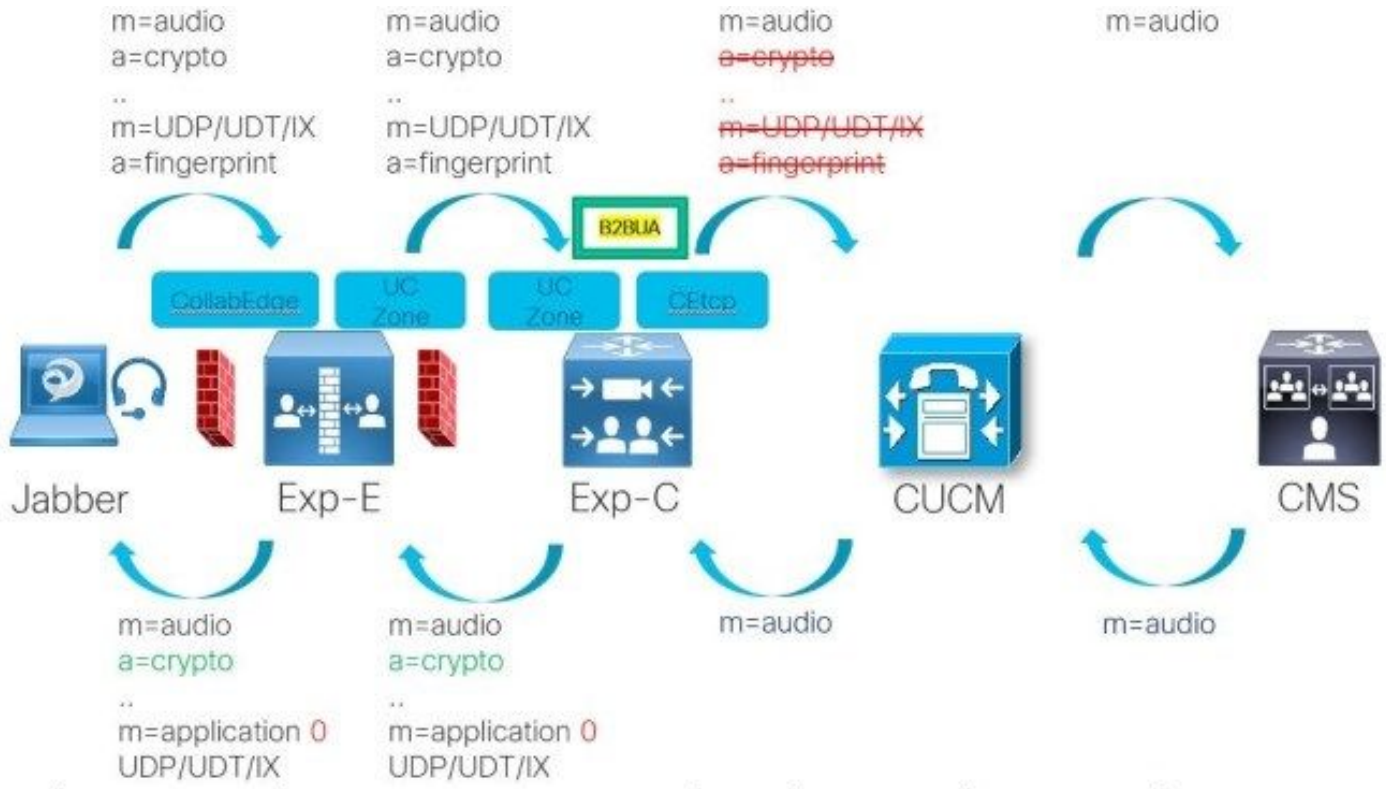
O AtiveControl está sendo negociado de forma segura, diferente de outros canais de mídia. Para outros canais de mídia como áudio e vídeo, por exemplo, o SDP é anexado com linhas de criptografia que são usadas para anunciar ao participante remoto a chave de criptografia a ser usada para esse canal. O canal RTP (Real-time Transport Protocol) pode, portanto, se tornar seguro e, portanto, ser considerado como SRTP (Secure RTP). Para o canal iX, ele usa o protocolo DTLS para criptografar o fluxo de mídia XCCP para que ele use um mecanismo diferente.

O software Expressway não termina o protocolo DTLS. Isso é indicado na seção *Limitações* em *Funcionalidade sem suporte* das *notas de versão do 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.

Versões do Expressway anteriores a X12.5

Ao executar uma versão do Expressway antes de X12.5, se houver uma conexão de entrada com um canal iX criptografado que passa por uma zona TCP não segura, o Expressway retira as linhas de criptografia dos canais de mídia normais, bem como todo o canal iX. Isso é mostrado visualmente para um cliente MRA que se conecta a um espaço CMS onde você vê que a conexão é segura do cliente MRA para o Expressway-C, mas, em seguida, dependendo do perfil de segurança do telefone configurado no CUCM para o dispositivo, ele é não criptografado (e enviado pela zona CEtcp) ou criptografado (e enviado pela zona CEtls). Quando ele é descriptografado, como mostrado na imagem, você vê que o Expressway-C retira as linhas de criptografia de todos os canais de mídia e até mesmo retira todo o canal de mídia iX também porque ele não pode terminar o protocolo DTLS. Isso acontece por meio do agente de usuário back-to-back (B2BUA) porque a configuração de zona para a zona CEtcp está configurada com a criptografia de mídia 'Force unencrypted'. Na direção oposta (sobre a zona de passagem de UC com criptografia de mídia 'Force encrypted') quando a resposta SDP é recebida, ela adiciona as linhas de criptografia para as linhas de mídia normais e zera a porta para o canal iX, resultando em nenhuma negociação AtiveControl. Internamente, quando os clientes são registrados diretamente no CUCM, ele permite canais de mídia iX criptografados e não criptografados, já que o CUCM não está se colocando no caminho de mídia.



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

O mesmo tipo de lógica se aplica às conexões de chamada no Expressway para Webex Meetings. Ele requer que o caminho completo seja seguro de ponta a ponta, pois os servidores Expressway (antes de X12.5) apenas passam as informações de conexão DTLS, mas não terminam neles mesmos para iniciar uma nova sessão ou para criptografar/descriptografar o canal de mídia nos diferentes segmentos de chamada.

Versões do Expressway do X12.5 e posterior

Ao executar uma versão do Expressway do X12.5 ou superior, o comportamento mudou como agora ele passa sobre o canal iX sobre a conexão da zona TCP como criptografia forçada (UDP/DTLS/UDT/IX) para que ele permita ainda negociar o canal iX, mas somente quando a extremidade remota usa criptografia também. Impõe a criptografia porque o Expressway não

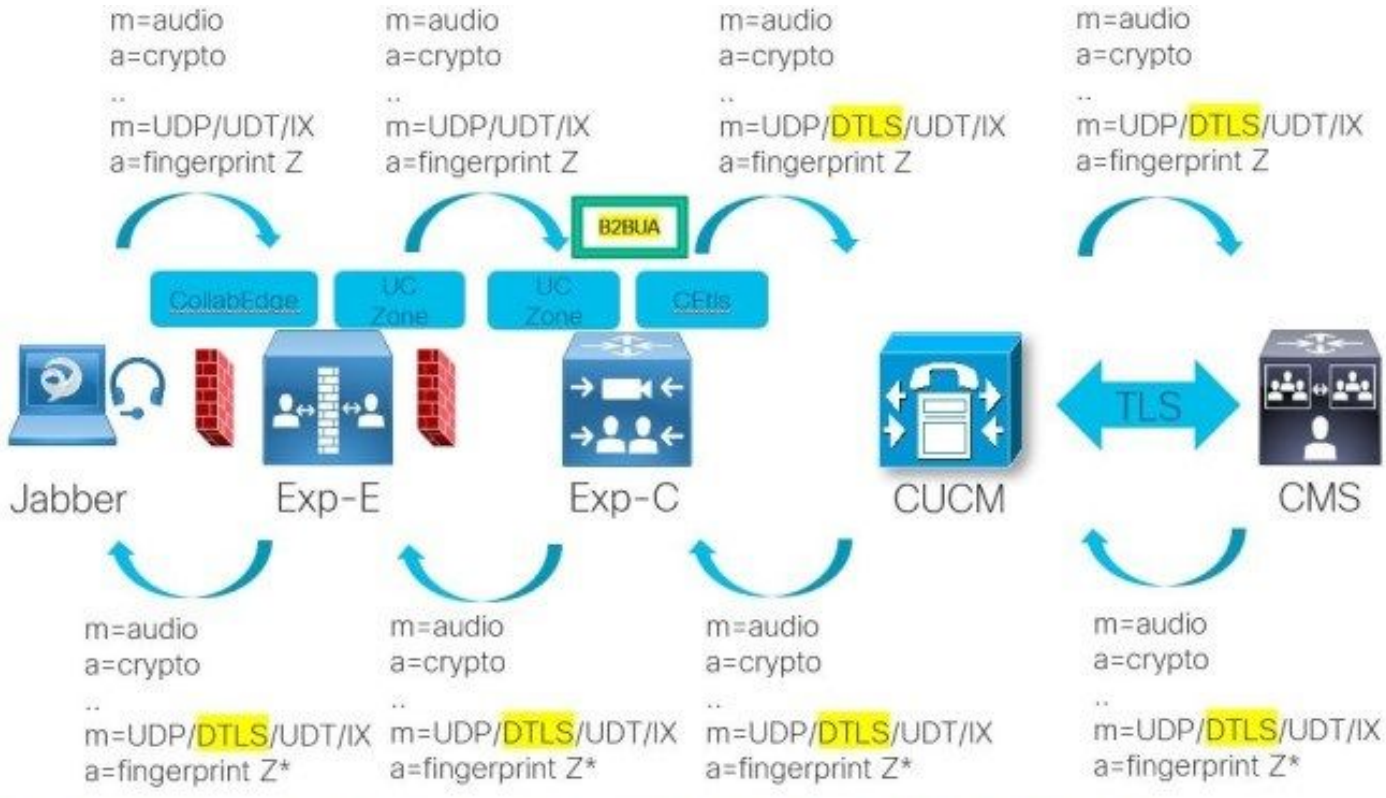
termina a sessão DTLS e, portanto, atua apenas na passagem, de modo que ele depende da extremidade remota para iniciar/terminar a sessão DTLS. As linhas de criptografia são removidas através da conexão TCP para fins de segurança. Essa mudança de comportamento é abordada nas notas de versão conforme a seção de 'MRA: Suporte para iX criptografado (para AtiveControl)'. O que acontece depois disso, depende da versão do CUCM, já que esse comportamento mudou no 12.5(1)SU1, onde permite passar pelo canal iX, bem como em conexões de entrada não seguras. Mesmo quando houvesse um tronco SIP TLS seguro para o CMS, ao executar a versão do CUCM inferior a 12.5(1)SU1, ele removeria o canal iX antes de passá-lo para o CMS, resultando eventualmente em uma porta de saída zero do CUCM para o 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.

Com uma sinalização de chamada segura de ponta a ponta e um caminho de mídia, o canal iX pode ser negociado diretamente (transmitido por saltos diferentes de servidores Expressway) entre o cliente (MRA) e a solução de conferência (CMS ou Webex Meeting). A imagem mostra o mesmo fluxo de chamada para o cliente MRA que se conecta a um espaço CMS, mas agora com um perfil de segurança de telefone seguro configurado no CUCM e um tronco SIP TLS seguro para o CMS. Você pode ver que o caminho é seguro de ponta a ponta e que o parâmetro de impressão digital DTLS acaba de passar por todo o caminho.

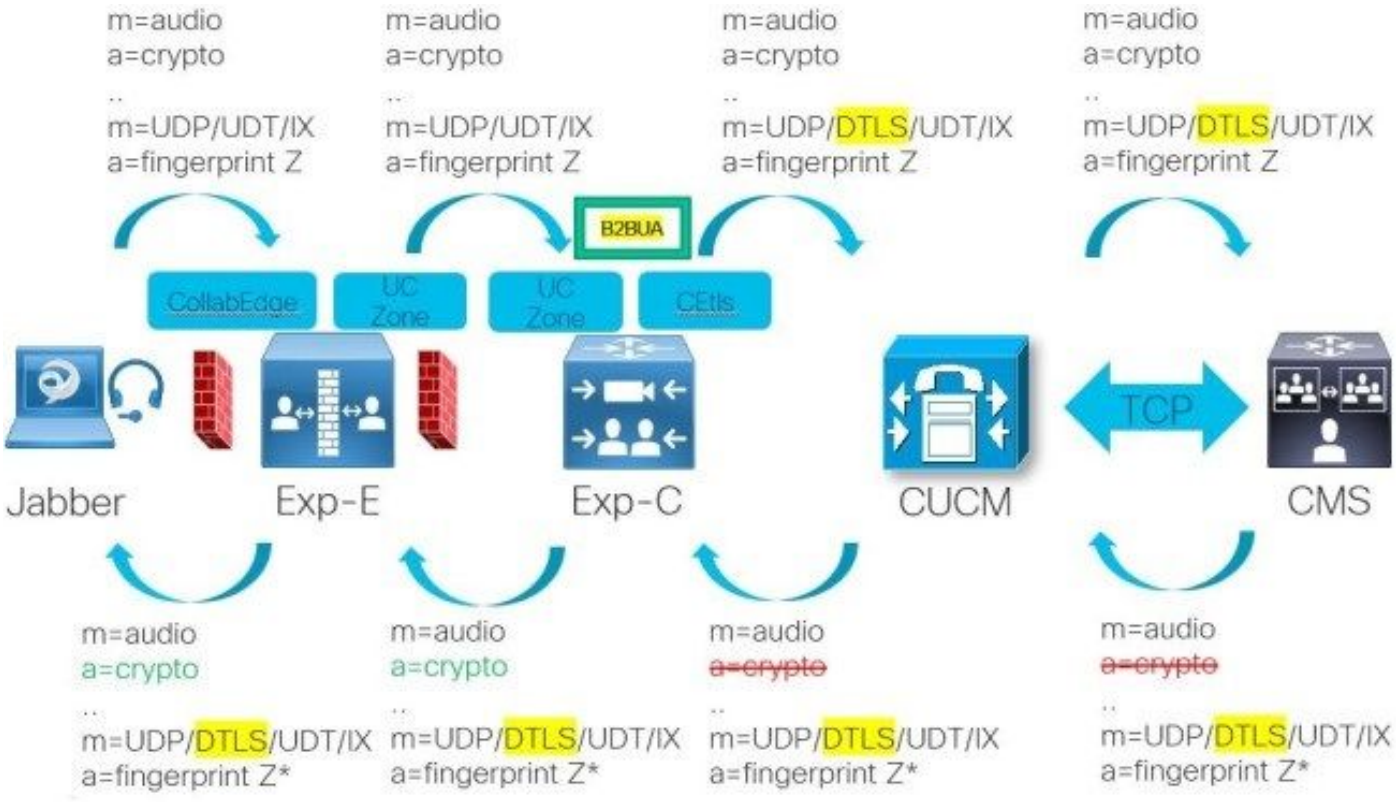


Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

Para configurar um perfil de segurança de dispositivo seguro, você precisaria garantir que o CUCM seja configurado em um modo misto e isso pode ser um processo incômodo (também quando operacional, pois requer a Certificate Authority Proxy Function (CAPF) para comunicações locais seguras). Portanto, outras soluções mais convenientes podem ser

oferecidas aqui para oferecer suporte à disponibilidade do AtiveControl sobre MRA e Expressway em geral, conforme abordado neste documento.

Troncos SIP TLS seguros para o(s) servidor(es) CMS não são necessários porque o CUCM (supondo que o tronco SIP tenha a opção de SRTP Permitido habilitado) sempre passa de uma conexão SIP segura de entrada para o canal iX, bem como as linhas de criptografia, mas o CMS só responde com criptografia para o canal iX (permitindo AtiveControl) (supondo que a **criptografia de mídia SIP** esteja definida como **permitido** ou imposto no CMS em Configurações > Configurações de chamada), mas não tem criptografia nos outros canais de mídia como ele se desencapta remova as linhas de criptografia delas de acordo com a imagem. Os servidores Expressway podem adicionar as linhas de criptografia novamente para proteger essa parte da conexão ainda (e o iX é negociado diretamente entre os clientes finais ainda através do DTLS), mas isso não é ideal do ponto de vista da segurança e, portanto, é recomendável configurar um tronco SIP seguro para a ponte de conferência. Quando **SRTP permitido** não é verificado no tronco SIP, o CUCM retira as linhas de criptografia e a negociação iX segura também falha.



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

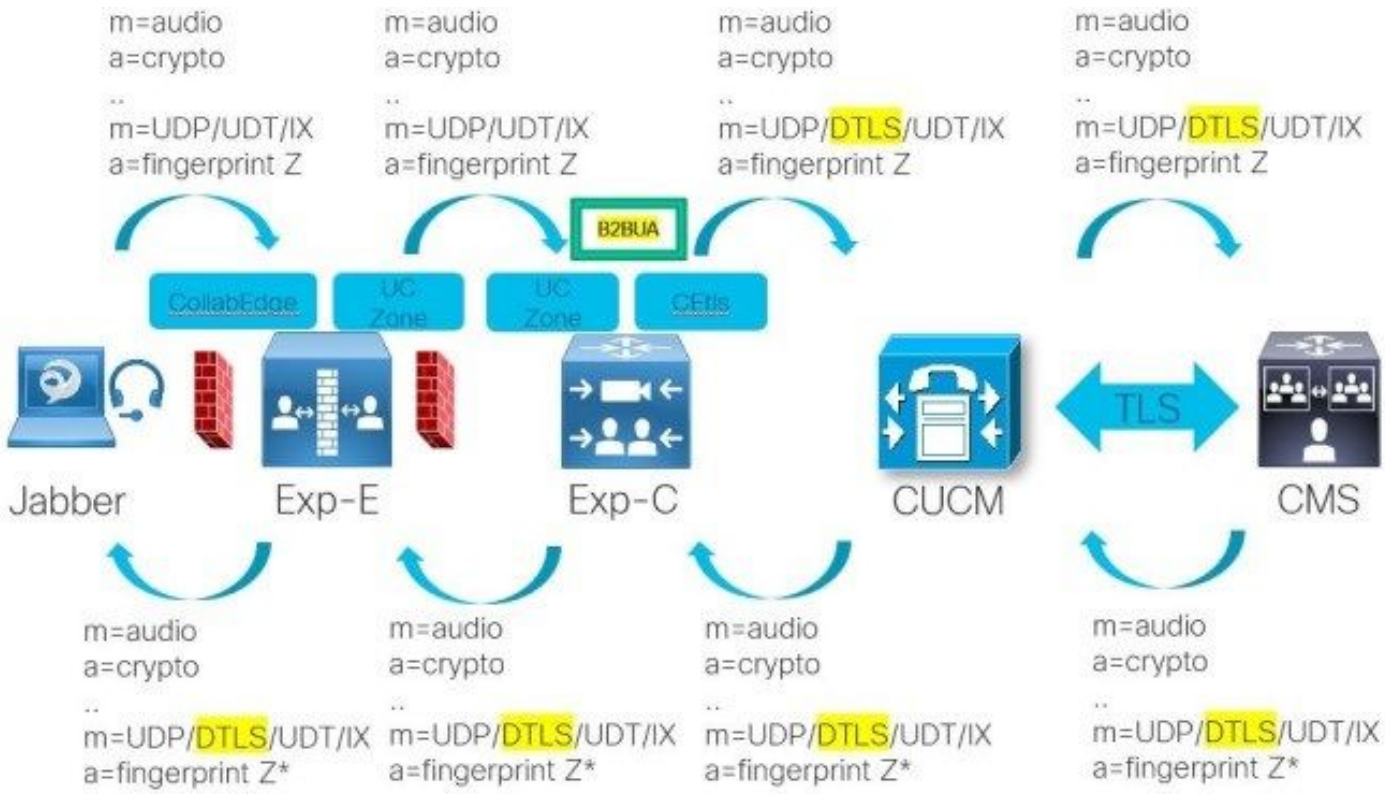
Solução

Há algumas opções diferentes disponíveis com vários requisitos e vários prós e contras. Cada um deles é apresentado em uma seção mais detalhada. As diferentes opções são:

1. Perfis de segurança de telefone seguros para os endpoints (CUCM de modo misto)
2. SIP OAuth para Jabber
3. Canal iX criptografado para perfis de segurança de telefone não seguros (CUCM 12.5(1)SU1 ou superior)

Solução 1: perfis de segurança telefônica seguros para os endpoints (CUCM de

modo misto)



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

Pré-requisitos:

- CUCM em modo misto

Profissional:

- Funciona em qualquer versão do CUCM
- Funciona para todos os dispositivos cliente

Cont.:

- Requer configuração do CUCM em modo misto (e operações CAPF em endpoints locais)

Esse é o método, como abordado na seção Problema, bem como no final, onde você garante que tenha uma sinalização de chamada criptografada de ponta a ponta e um caminho de mídia. Ele exige que o CUCM seja configurado no modo misto conforme o documento a seguir.

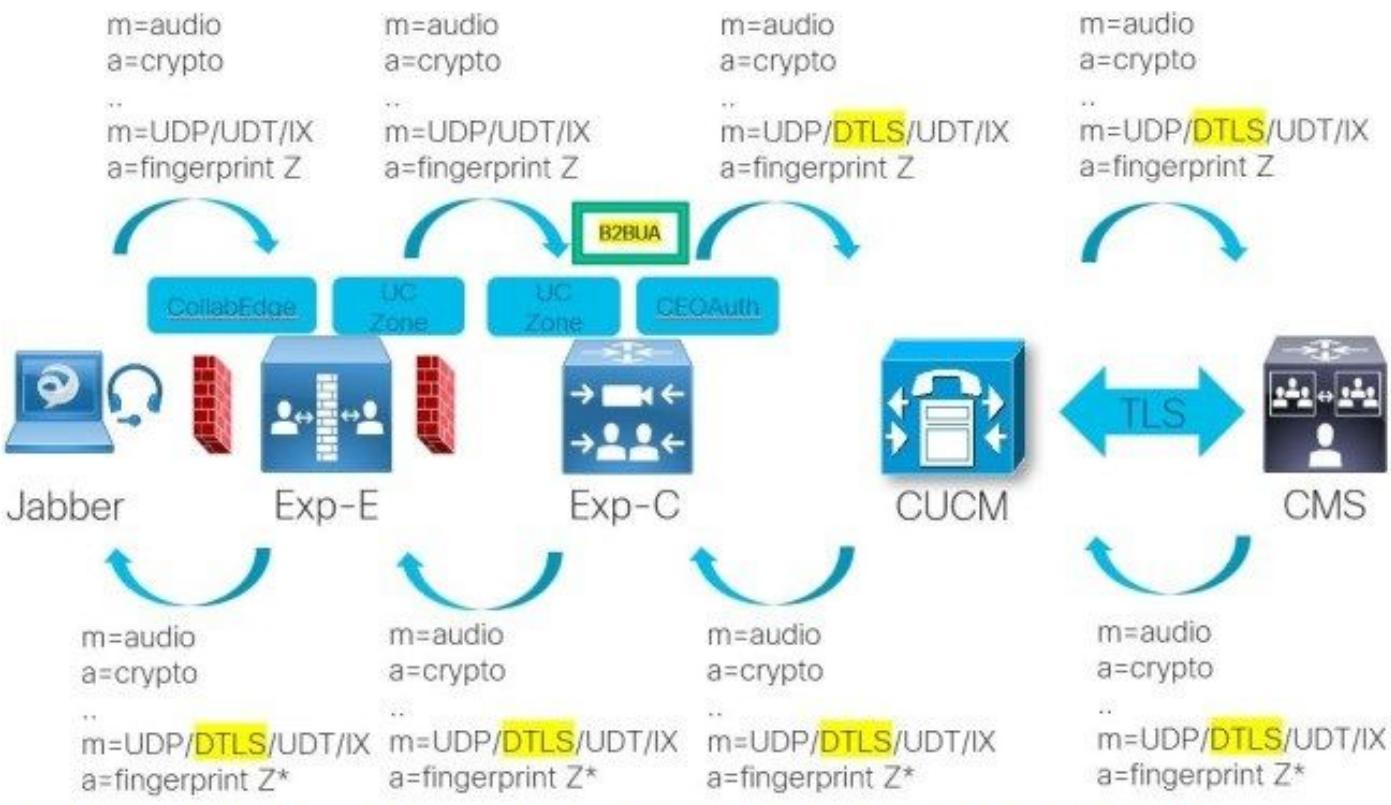
Para clientes MRA, não há operação CAPF necessária, mas certifique-se de seguir as etapas de configuração extra com o perfil de segurança do telefone seguro com um nome que corresponda a um dos nomes alternativos do assunto do certificado do servidor Expressway-C, conforme destacado no Exemplo de configuração de endpoints baseados em TC do Collaboration Edge (que também se aplica a endpoints baseados em CE e clientes Jabber).

Ao conectar-se de um endpoint local ou cliente Jabber a uma reunião do Webex, você precisa executar a operação CAPF para registrar com segurança o cliente no CUCM. Isso é necessário para garantir o fluxo de chamada seguro de ponta a ponta, onde o Expressway pode simplesmente passar sobre a negociação DTLS e não lidar com ela mesma.

Para tornar a chamada segura de ponta a ponta, certifique-se também de que todos os troncos SIP relevantes (para Expressway-C em caso de chamada para Webex Meeting e para CMS em

caso de chamada para conferência CMS) sejam troncos SIP seguros usando TLS com um perfil de segurança de tronco SIP seguro.

Solução 2: SIP OAuth para Jabber



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

Pré-requisitos:

- Cisco Jabber 12.5 ou superior (notas de versão)
- CUCM versão 12.5 ou superior (notas de versão) com *OAuth com Atualizar fluxo de login* habilitado
- Expressway X12.5.1 ou superior (notas de versão) com *Autorização por token OAuth com atualização* habilitada

Profissional:

- Permite registros seguros e fácil alternância entre o local e o local sem renovação de CAPF todas as vezes
- Não há necessidade de configurar o CUCM no modo misto

Cont.:

- Aplicável somente ao Jabber, não aplicável aos terminais TC/CE

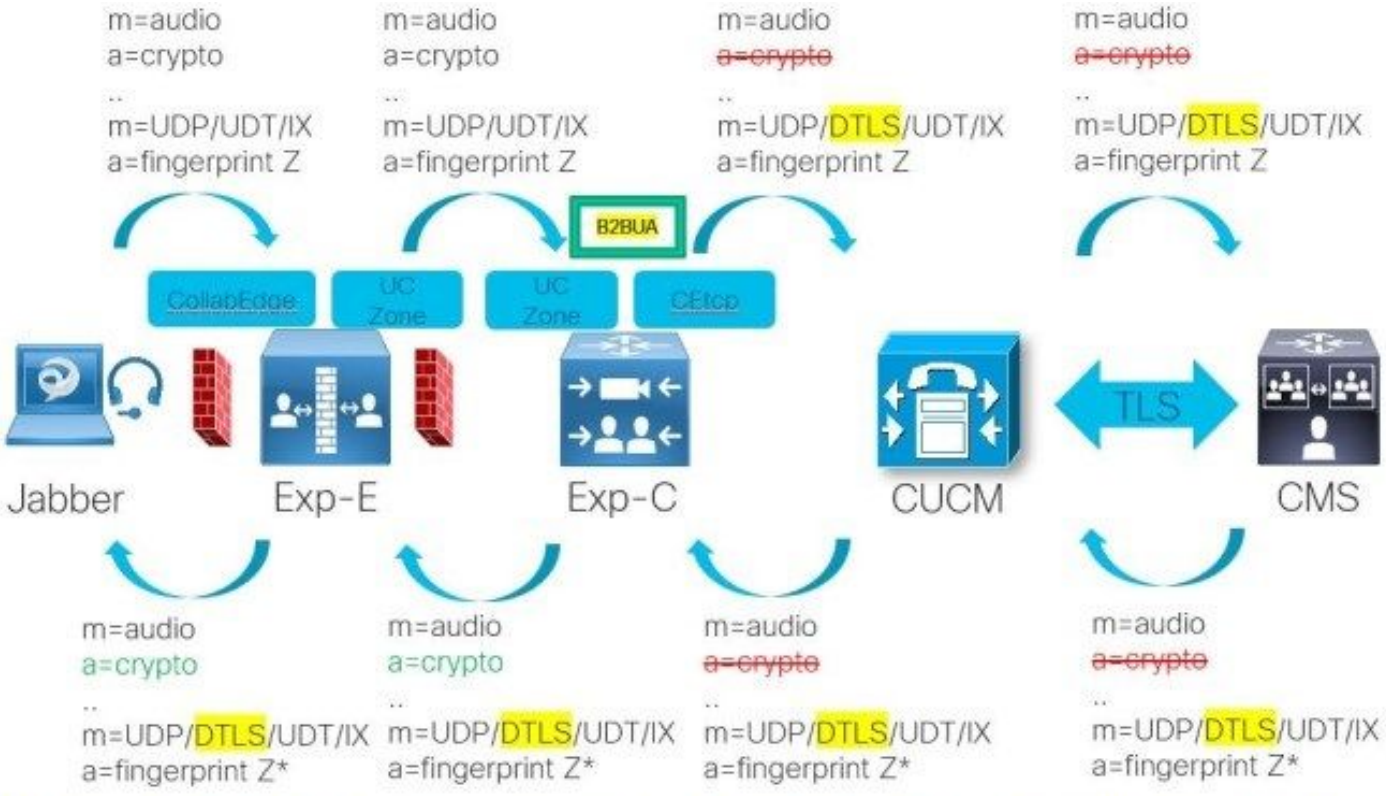
O modo OAuth do SIP permite que você use tokens de atualização OAuth para autenticação do Cisco Jabber em ambientes seguros. Ele permite sinalização e mídia seguras sem o requisito CAPF da Solução 1. A validação do token durante o registro SIP é concluída quando a autorização baseada em OAuth é habilitada no cluster CUCM e nos endpoints Jabber.

A configuração no CUCM está documentada no guia de configuração do recurso e requer que você tenha o OAuth com Atualizar fluxo de logon em Parâmetros corporativos já habilitado. Para habilitar isso também em MRA, certifique-se de atualizar os nós de CUCM no servidor

Expressway-C em **Configuration > Unified Communication > Unified CM Servers** para que em **Configuration > Zones > Zones** você agora deve ver as zonas CEOAuth criadas automaticamente também. Verifique também se em **Configuration > Unified Communication > Configuration** que **Authorize by OAuth token with refresh** também está habilitado.

Com essa configuração, você pode obter uma conexão de chamada segura de ponta a ponta semelhante para sinalização e mídia e, portanto, o Expressway apenas passa pela negociação DTLS, pois não termina o próprio tráfego. Isso é visto na imagem onde a única diferença em comparação à solução anterior é que ele usa a zona CEOAuth no Expressway-C para o CUCM em oposição à zona CEtls porque ele usa o SIP OAuth em vez do registro de dispositivo seguro sobre TLS quando o CUCM opera em um modo misto com um perfil de segurança de telefone seguro, mas além disso, tudo permanece o mesmo.

Solução 3: canal iX criptografado para perfis de segurança de telefone não seguros (CUCM 12.5(1)SU1 ou superior)



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

Pré-requisitos:

- CUCM versão 12.5(1)SU1 ou superior (notas de versão)
- Expressway X12.5.1 ou superior (notas de versão)

Profissional:

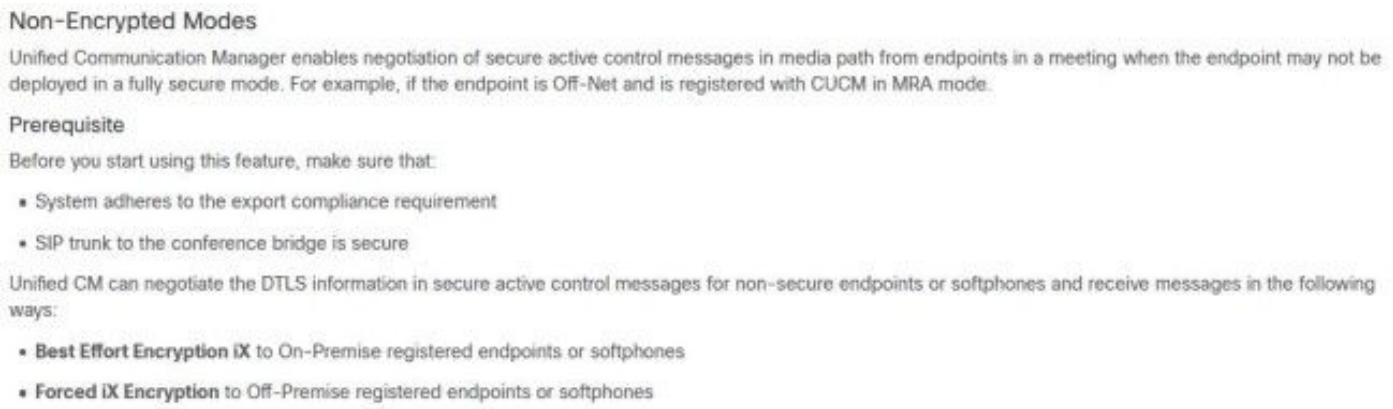
- Não há necessidade de configurar o CUCM no modo misto
- Não há necessidade de configurar comunicações seguras de ponta a ponta
- Aplicável a endpoints Jabber e TC/CE

Cont.:

- Atualização do CUCM necessária
- Somente versões restritas do CUCM são suportadas

A partir do CUCM 12.5(1)SU1, ele oferece suporte à negociação de criptografia iX para qualquer dispositivo de linha SIP para que possa negociar as informações DTLS em mensagens AtiveControl seguras para terminais ou softphones não seguros. Ele envia criptografia iX de melhor esforço sobre TCP, permitindo que os telefones tenham um canal iX criptografado de ponta a ponta, apesar de uma conexão TCP não segura (não TLS) com o CUCM.

No guia de segurança do CUCM 12.5(1)SU1, na seção de "Canal iX criptografado", ele mostra que para modos não criptografados com dispositivos não seguros, o melhor esforço e a criptografia iX forçada podem ser negociados com o pré-requisito de que seu sistema adere à conformidade de exportação e o tronco SIP para sua ponte de conferência é seguro.



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

No CUCM:

- Você deve usar o CUCM de exportação restrita (não irrestrita)
- Em **System > Licensing > License Management**, você deve ter a "Export-Controlled Functionality" (Funcionalidade controlada por exportação) definida como permitida.
- Seu tronco SIP deve ter a opção "**SRTP permitido**" habilitada (independentemente de o próprio tronco ser seguro ou não)

No CMS:

- Seu callbridge deve ter uma licença com criptografia (para que você não tenha a licença callBridgeNoEncryption)
- Em webadmin em **Configuration > Call Settings**, você deve ter definido a **criptografia de mídia SIP** como **allowed** (ou **required**)

Na imagem, você pode ver que a conexão é segura até que o Expressway-C e C envie pelo SDP para o CUCM sem as linhas de criptografia, mas inclui o canal de mídia iX ainda. Portanto, a mídia normal para áudio/vídeo/.. não é protegida com linhas de criptografia, mas tem uma conexão segura para o canal de mídia iX agora, de modo que o Expressway não precisa encerrar a conexão DTLS. Portanto, o AtiveControl pode ser negociado diretamente entre o cliente e a ponte de conferência, mesmo com um perfil de segurança de telefone não seguro. Em versões anteriores do CUCM, o fluxo seria diferente e o AtiveControl não é negociado porque não passa o canal iX para o CMS em primeiro lugar, pois essa parte já teria sido retirada.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.