Enable ActiveControl over MRA/Expressway

Contents

Introduction

This document describes the different options to enable the ActiveControl protocol for Mobile and Remote Access (MRA) clients and for calls from on-prem endpoints to Webex Meetings via Expressway. MRA is a deployment solution for Virtual Private Network-less (VPN) Jabber and endpoint capability. This solution allows end users to connect to internal enterprise resources from anywhere in the world. The ActiveControl protocol is a Cisco proprietary protocol that allows for a richer conferencing experience with run-time features like meeting rosters, video layout changes, muting and recording options.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Expressway (MRA and B2B calls)

Components Used

The information in this document is based on these software and hardware versions:

- 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. If your network is

live, ensure that you understand the potential impact of any command.

Background Information

In this document the main focus is on the MRA client connection to a Cisco Meeting Server (CMS) but the same applies for other type of platforms or connections like for example when connecting to Webex Meetings. The same logic can be applied for following type of call flows:

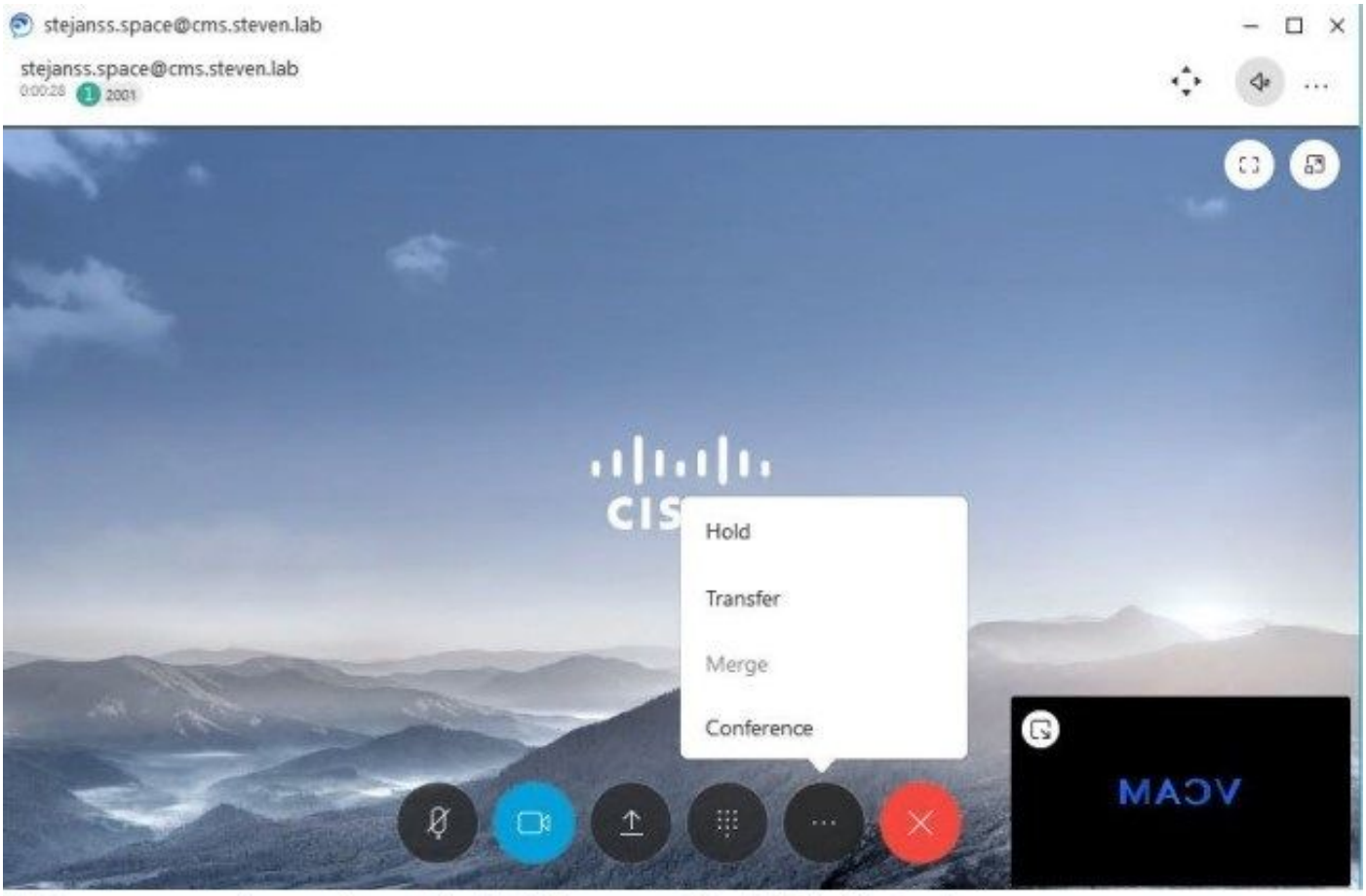
- Endpoint - CUCM - Expressway-C - Expressway-E - Webex Meeting
- MRA Endpoint - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - Webex Meeting

> **Note**: The features of ActiveControl supported by Webex Meetings are different than the ones from CMS at this moment in time and are only a limited subset.

The Cisco Meeting Server platform offers meeting participants the ability to control their meeting experience directly from their conferencing endpoint through ActiveControl without the need for external applications or operators. ActiveControl utilizes the iX media protocol in Cisco devices and is negotiated as part of SIP messaging of a call. As of CMS version 2.5, the main features enabled are the following ones (although they can depend on the endpoint type and software version in use):

- Viewing a list of all participants (roster list or participant list) connected to the meeting
- Muting or unmuting other participants
- Adding or removing another participant from the meeting
- Starting or stopping recording of a meeting
- Making a participant important
- Indicator for the participant who is the active speaker in the meeting
- Indicator for the participant who is currently sharing content or presentation in the meeting
- Locking or unlocking of the meeting

On the first image you see a user view from a Jabber client that placed a call into a CMS space without ActiveControl while the second image shows you the more feature rich user view where Jabber has been able to negotiate ActiveControl with the CMS server.



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl is a XML based protocol that is transferred using the iX protocol which is negotiated in the Session Description Protocol (SDP) of the Session Initiation Protocol (SIP) calls. It is a Cisco protocol (eXtensible Conference Control Protocol (XCCP)) and negotiated in SIP only (so interworked calls do not have ActiveControl) and leverages UDP/UDT (UDP-based Data Transfer Protocol) for data transfer. Secure negotiation happens through Datagram TLS (DTLS) which can be looked at as TLS over UDP connection. Some samples are shown here for the differences in

negotiation.

Unencrypted

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

Encrypted (best effort - try encryption but allow fallback to unencrypted connection)

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:

Encrypted (force encryption - do not allow fallback to unencrypted connection)

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

a=ixmap:2 **xccp**

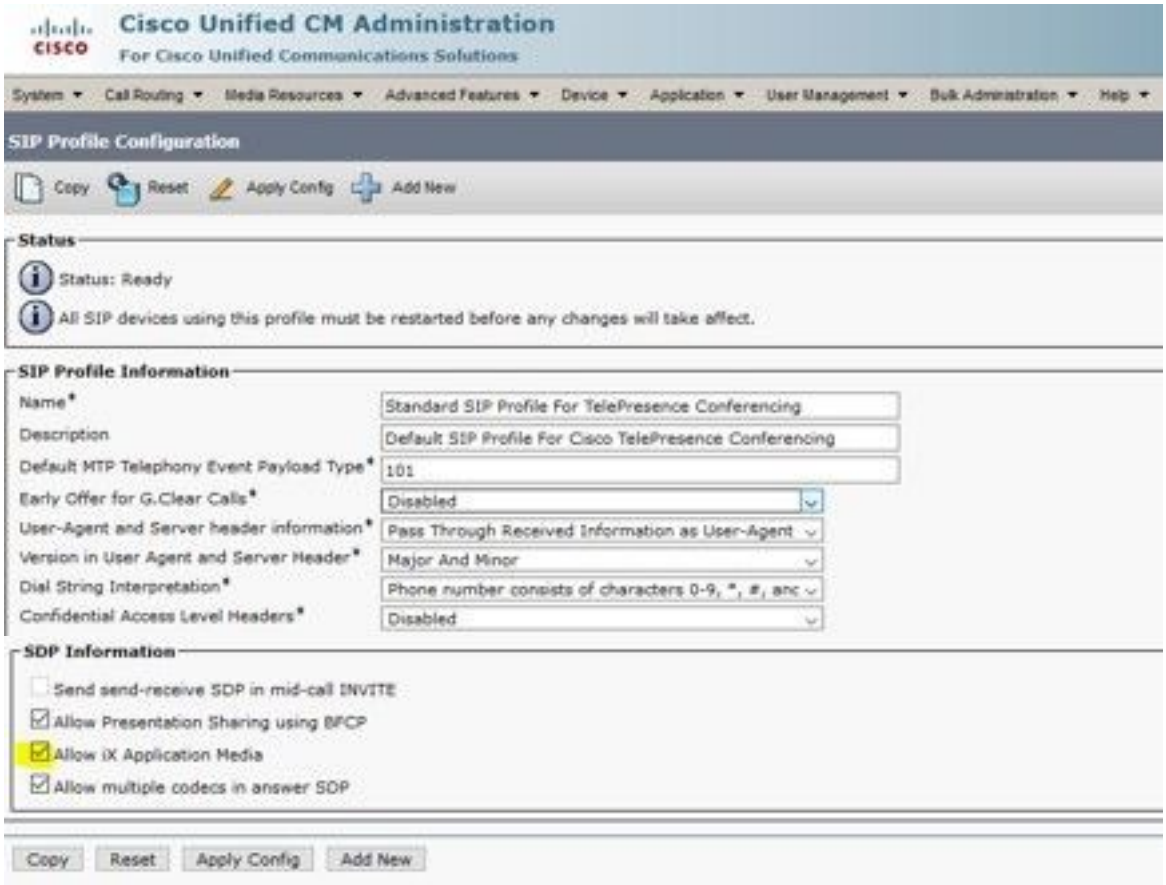
a=**fingerprint**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

There are some minimum software versions required for full ActiveControl support as listed:

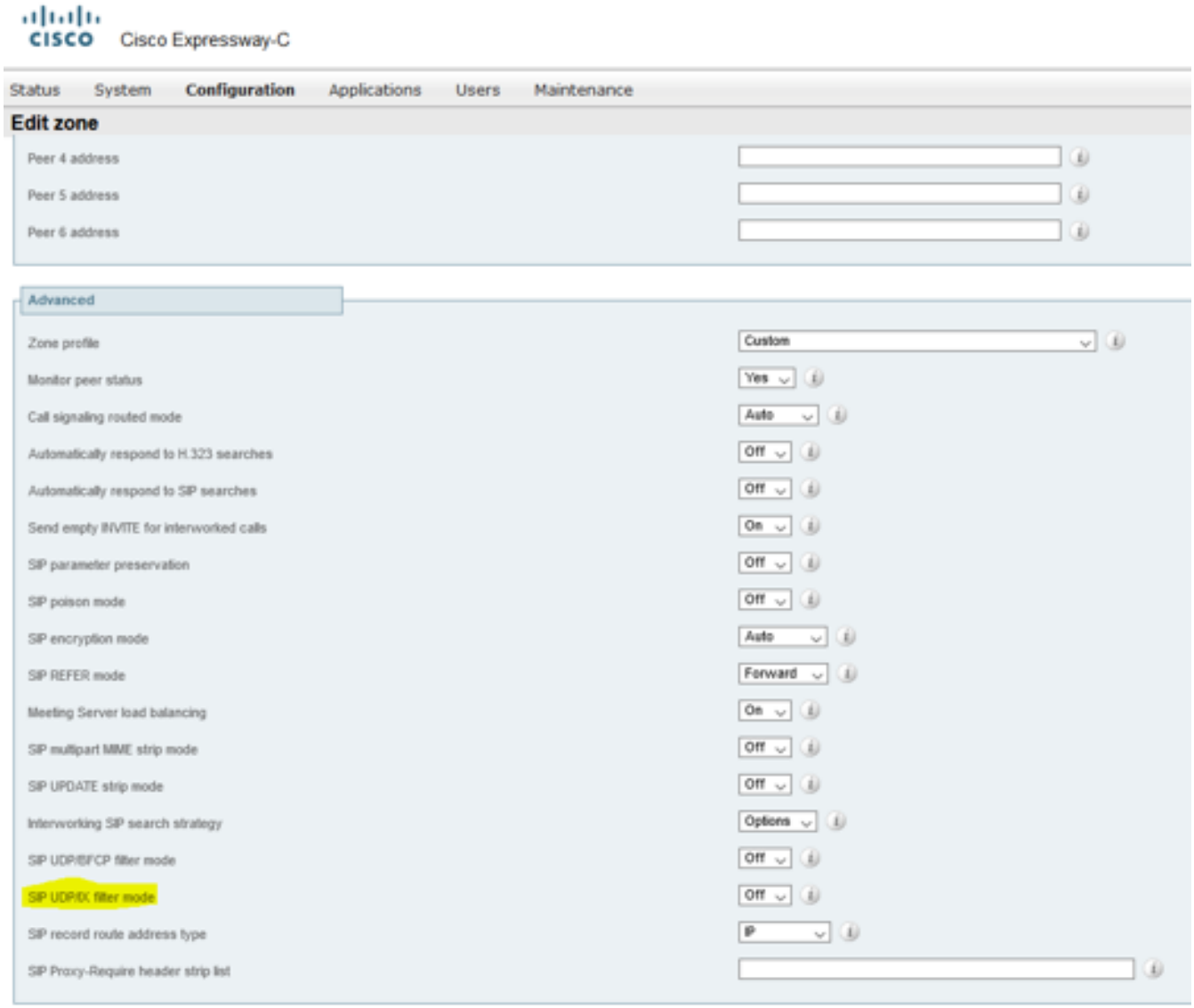
- Jabber version 12.5 or later (release notes)
- CE endpoints 8.3 or later, 9.6.2 or later recommended as per CMS ActiveControl guide (CE9.3.1 or later for Webex as per the Webex help link)
- CUCM 10.5 or later (for Jabber 12.5 ActiveControl support) (11.5(1) or later for Webex as per the link)
- CMS 2.1 or later, 2.5 or later recommended as per CMS ActiveControl guide
- Expressway X12.5 or later (release notes) to allow for support on non-encrypted MRA clients

There are a few configuration options to take into consideration:

- On CUCM ensure that the relevant SIP trunks (to Expressway-C and CMS) are configured with a SIP Profile which has the 'Allow iX Application Media' checked



- On CMS it is enabled by default from 2.1 onwards, but you can disable it via a compatibilityProfile on which you can set *sipUDT* to false
- On Expressway on the Zone config under the Advanced settings (when using a 'Custom' zone profile), ensure that *SIP UDP/IX filter mode* is set to 'Off' if you want to allow iX to pass



Problem

General info

ActiveControl is being negotiated securely differently than other media channels. For other media channels like audio and video for example, the SDP gets appended with crypto lines that are used to announce to the remote party the encryption key to be used for this channel. The Real-time Transport Protocol (RTP) channel can therefore be made secure and thus considered as Secure RTP (SRTP). For the iX channel, it uses DTLS protocol to encrypt the XCCP media stream so it uses a different mechanism.

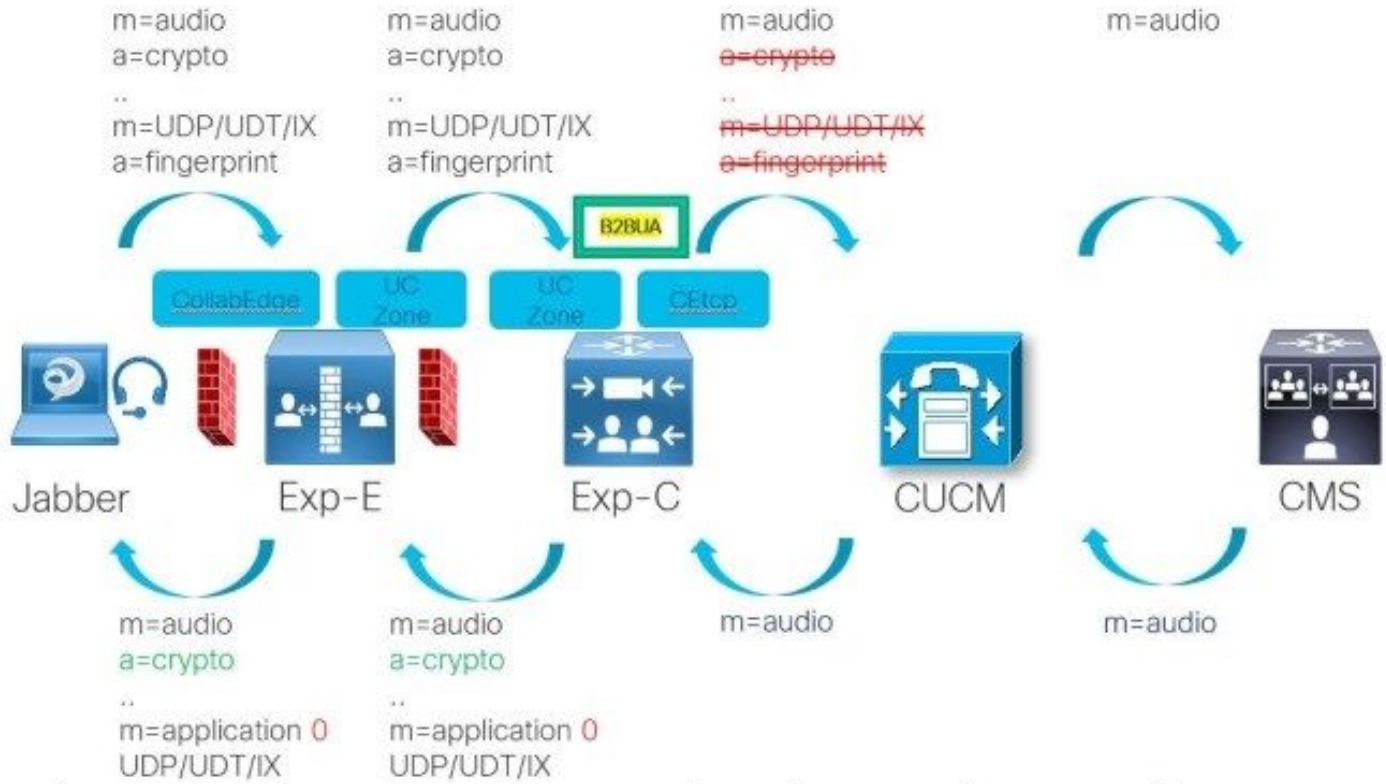
The Expressway software does not terminate the DTLS protocol. This is indicated under the *Limitations* section under *Unsupported Functionality* of the Expressway release notes.

- 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.

Expressway versions before X12.5

When running an Expressway version before X12.5, if there is an incoming connection with an

encrypted iX channel that gets passed along an unsecure TCP zone, the Expressway strips both the crypto lines of the normal media channels as well as the entire iX channel. This is visually shown for a MRA client that connects to a CMS space where you see that the connection is secure from the MRA client to the Expressway-C but then depending on the phone security profile set up on CUCM for the device, it either is unencrypted (and sent over CEtcp zone) or encrypted (and sent over CEtls zone). When it is unencrypted as shown on the image, you see that the Expressway-C strips off the crypto lines for all media channels and even strips off the entire iX media channel as well because it cannot terminate the DTLS protocol. This happens via the Back-To-Back User Agent (B2BUA) because the zone config for the CEtcp zone is set up with media encryption 'Force unencrypted'. In the opposite direction (over the UC traversal zone with 'Force encrypted' media encryption) when the SDP reply is received, it does add in the crypto lines for the normal media lines and zeroes out the port for the iX channel resulting in no ActiveControl negotiation. Internally when the clients are directly registered to CUCM, it allows both for encrypted and unencrypted iX media channels as CUCM is not putting itself in the media path.



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

The same kind of logic applies for the call connections over Expressway to Webex Meetings. It requires the full path to be end to end secure as the Expressway servers (before X12.5) only pass over the DTLS connection info but don't terminate on it themselves to start up a new session or to encrypt/decrypt the media channel on the different call legs.

Expressway versions of X12.5 and later

When running an Expressway version of X12.5 or higher, the behavior has changed as now it does pass over the iX channel over the TCP zone connection as forced encryption (UDP/DTLS/UDT/IX) in order for it to allow to still negotiate the iX channel but only when the remote end uses encryption as well. It enforces encryption because the Expressway does not terminate the DTLS session and thus only acts on pass-through so it relies on the remote end to start/end the DTLS session then. The crypto lines are stripped out though over the TCP connection for security purposes. This change of behavior is covered in the release notes as per the section of 'MRA: Support for Encrypted iX (for ActiveControl)'. What happens after that,

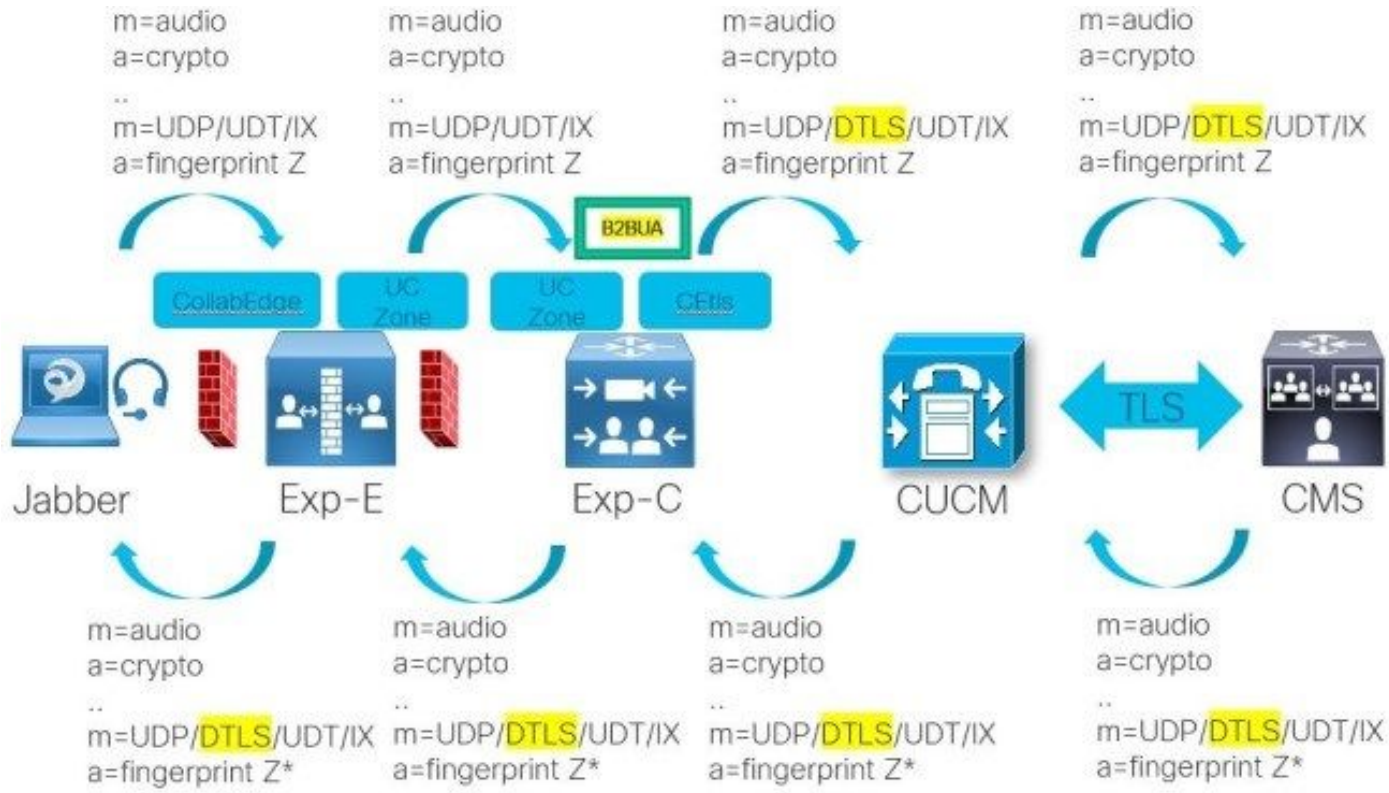
depends on the CUCM version as that behavior changed in 12.5(1)SU1 where it allows to pass over iX channel as well on unsecure incoming connections. Even when there would be a secure TLS SIP trunk over to CMS, when running CUCM version lower than 12.5(1)SU1, it would strip off the iX channel before passing it over to the CMS thus eventually resulting in a zeroed out port from CUCM to 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.

With an end to end secure call signaling and media path, the iX channel can be negotiated directly (passed via different hops of Expressway servers) between the (MRA) client and the conferencing solution (CMS or Webex Meeting). The image shows the same call flow for MRA client connecting to a CMS space but now with a secure phone security profile configured on CUCM and a secure TLS SIP trunk to CMS. You can see that the path is end to end secure and that the DTLS fingerprint parameter is just passed over along the entire path.

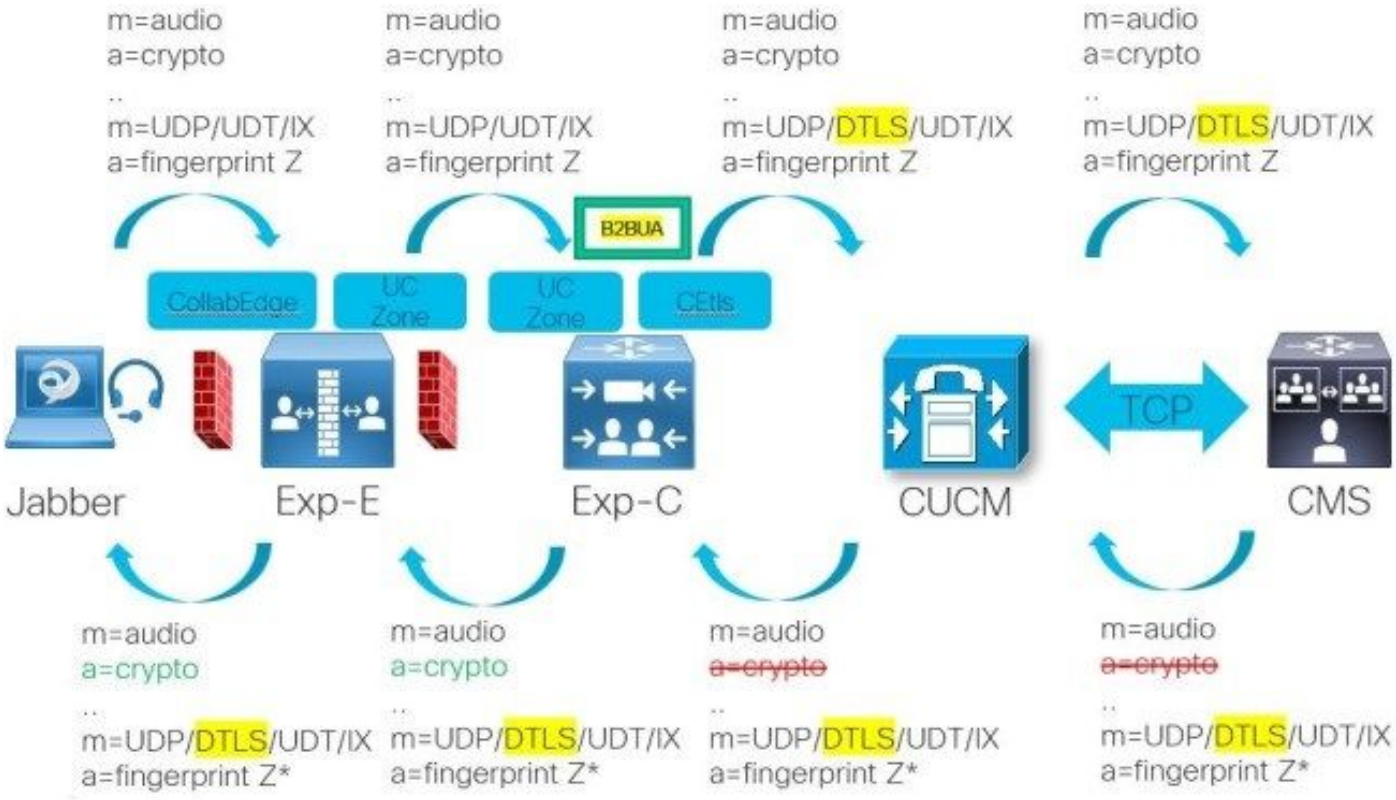


Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

In order to set up a secure device security profile, you would need to ensure that the CUCM is set up in a mixed mode and this can be a cumbersome process (also when operational as it does require Certificate Authority Proxy Function (CAPF) for secure on-prem communications). Therefore, other more convenient solutions can be offered here to support the availability for ActiveControl over MRA and Expressway in general as covered in this document.

Secure TLS SIP trunks to the CMS server(s) are not required because CUCM (assuming the SIP trunk has the option of **SRTP Allowed** enabled) always still passes over from an incoming secure SIP connection the iX channel as well as the crypto lines but CMS only replies back with encryption to the iX channel (allowing for ActiveControl) (assuming **SIP media encryption** is set

to *allowed* or *enforced* on CMS under **Settings > Call Settings**) but does not have encryption on the other media channels as it strips off the crypto lines from them as per the image. The Expressway servers can add in the crypto lines again for securing that part of the connection still (and iX is negotiated directly between the end clients still through DTLS) but this is not ideal from a security point of view and thus it is recommended to set up a secure SIP trunk to the conference bridge. When **SRTP Allowed** is not checked on the SIP trunk, CUCM strips off the crypto lines and secure iX negotiation fails as well.



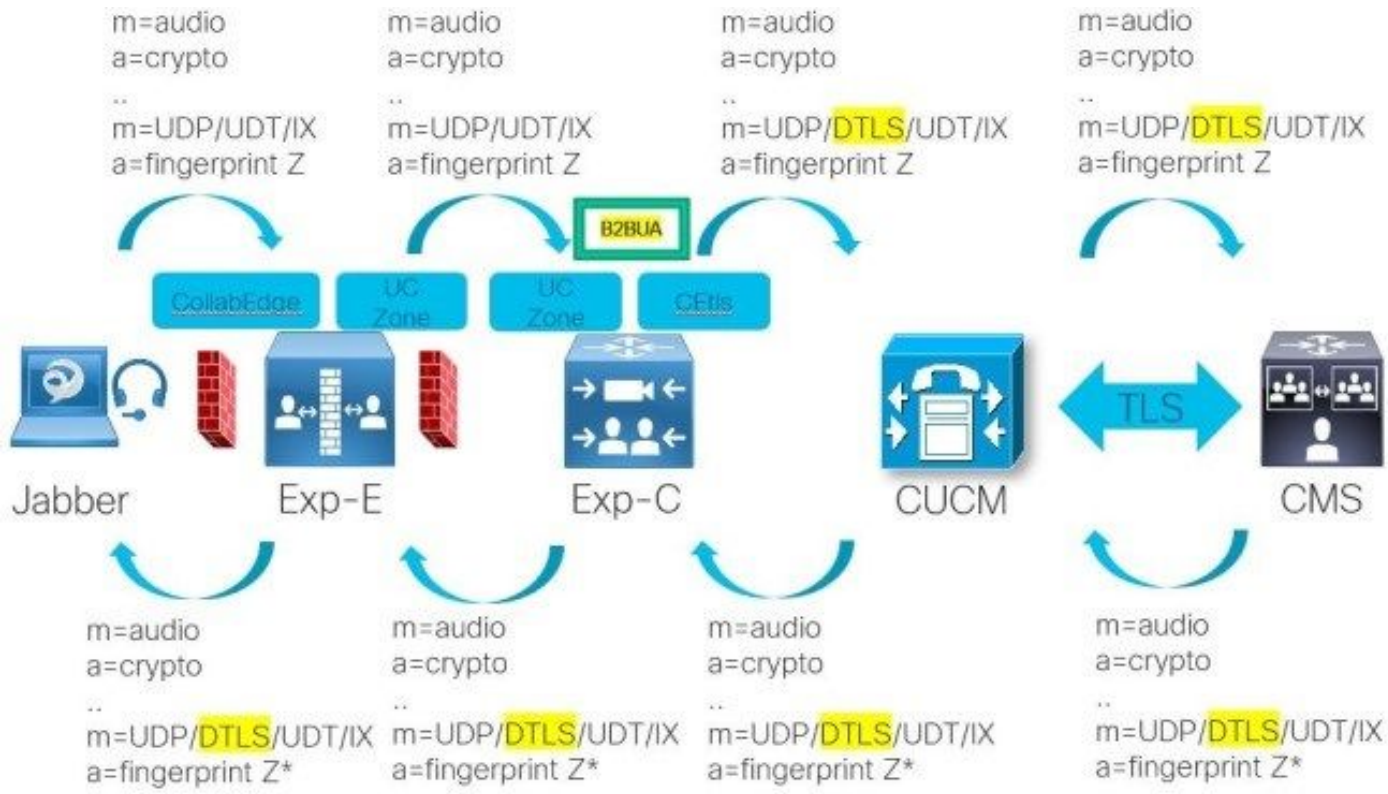
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

Solution

There are a couple of different options available with various requirements and various pro and cons. Each one of them is presented in a more detailed section. The different options are:

1. Secure phone security profiles for the endpoints (mixed mode CUCM)
2. SIP OAuth for Jabber
3. Encrypted iX channel for unsecure phone security profiles (CUCM 12.5(1)SU1 or higher)

Solution 1 : Secure phone security profiles for the endpoints (mixed mode CUCM)



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

Prerequisites:

- CUCM in mixed mode

Pro:

- Works on any CUCM version
- Works for all client devices

Con:

- Requires config of CUCM in mixed mode (and CAPF operations on on-prem endpoints)

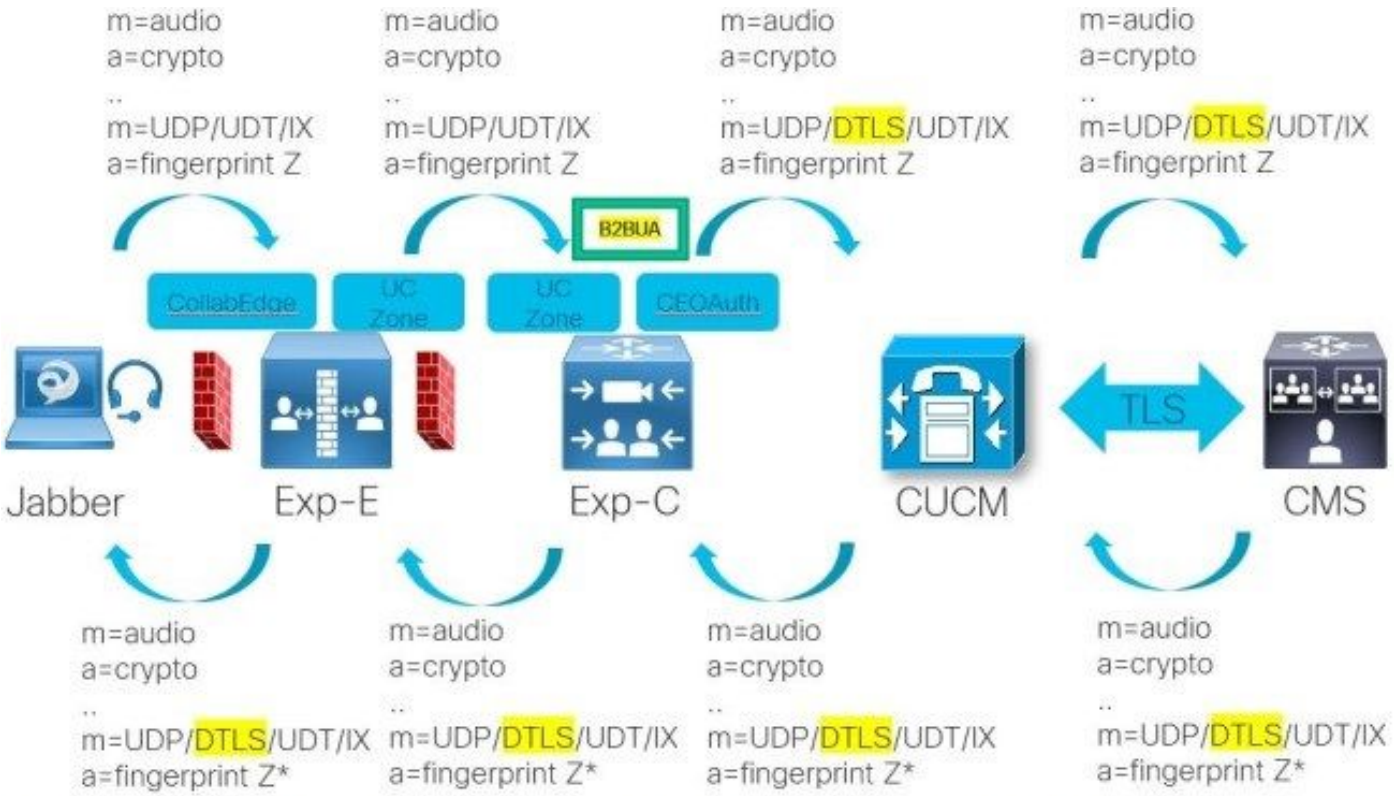
This is the method as covered up on the Problem section as well at the end where you ensure that you have an end-to-end encrypted call signaling and media path. It requires the CUCM to be set up in mixed mode as per following document.

For MRA clients, there is no CAPF operation required but ensure to follow on the extra configuration steps with the secure phone security profile with a name that matches one of the Subject Alternative Names of the Expressway-C server certificate as highlighted on the Collaboration Edge TC-based Endpoints Configuration Example (which also applies for CE-based endpoints and Jabber clients).

When connecting from an on-prem endpoint or Jabber client to a Webex Meeting, you need to perform on the CAPF operation to securely register the client to the CUCM. This is required to ensure the end-to-end secure call flow where the Expressway just can pass over the DTLS negotiation and not handle on it itself.

In order to make the call end-to-end secure, ensure as well that all relevant SIP trunks (to Expressway-C in case of call to Webex Meeting and to CMS in case of a call to CMS conference) are secure SIP trunks using TLS with a secure SIP Trunk Security Profile.

Solution 2 : SIP OAuth for Jabber



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

Prerequisites:

- Cisco Jabber 12.5 or higher (release notes)
- CUCM version 12.5 or higher (release notes) with *OAuth with Refresh Login Flow* enabled
- Expressway X12.5.1 or higher (release notes) with *Authorize by OAuth token with refresh* enabled

Pro:

- Allows for secure registrations and easy switching between on-prem and off-prem without renewal CAPF each time
- No need to set up CUCM in mixed mode

Con:

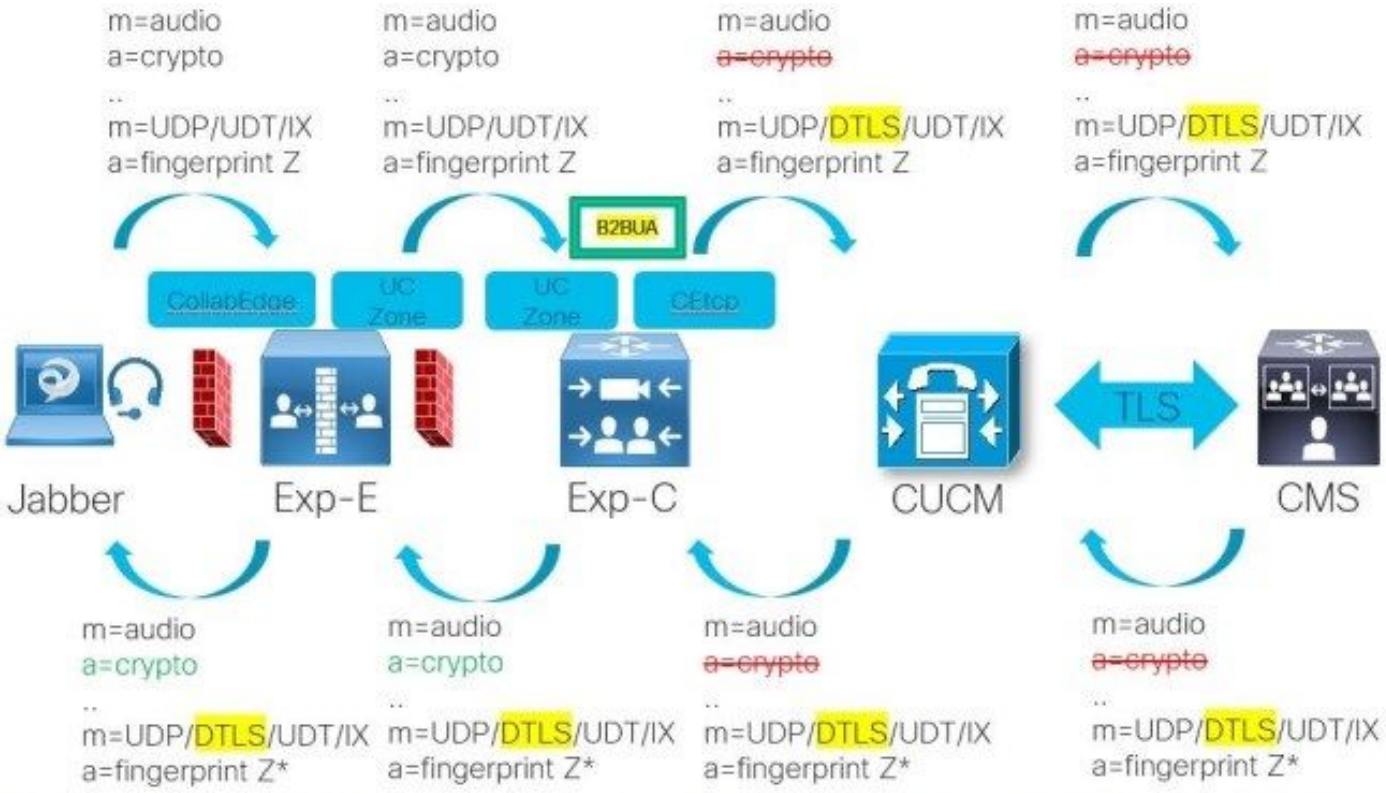
- Only applicable to Jabber, not applicable to TC/CE endpoints

SIP OAuth mode allows you to use OAuth refresh tokens for Cisco Jabber authentication in secure environments. It allows for secure signaling and media without the CAPF requirement from Solution 1. The token validation during the SIP registration is completed when OAuth based authorization is enabled on CUCM cluster and the Jabber endpoints.

The configuration on CUCM is documented on the feature configuration guide and requires that you have the OAuth with Refresh Login Flow under Enterprise Parameters already enabled. In order to enable this as well over MRA, ensure to refresh the CUCM nodes in the Expressway-C server under **Configuration > Unified Communication > Unified CM Servers** so that under **Configuration > Zones > Zones** you must now see the auto-created CEOAuth zones as well. Ensure as well that under **Configuration > Unified Communication > Configuration** that **Authorize by OAuth token with refresh** is enabled as well.

With this configuration, you can achieve a similar end-to-end secure call connection for both signaling and media and therefore the Expressway just passing over the DTLS negotiation as it does not terminate that traffic itself. This is seen on the image where the only difference as compared to the previous solution is that it uses the CEOAuth zone on the Expressway-C to the CUCM as opposed to the CEtls zone because it uses SIP OAuth rather than the secure device registration over TLS when CUCM operates in a mixed mode with a secure phone security profile but aside from that, all remains the same.

Solution 3 : Encrypted iX channel for unsecure phone security profiles (CUCM 12.5(1)SU1 or higher)



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

Prerequisites:

- CUCM version 12.5(1)SU1 or higher (release notes)
- Expressway X12.5.1 or higher (release notes)

Pro:

- No need to set up CUCM in mixed mode
- No need to set up secure end-to-end communications
- Applicable to both Jabber and TC/CE endpoints

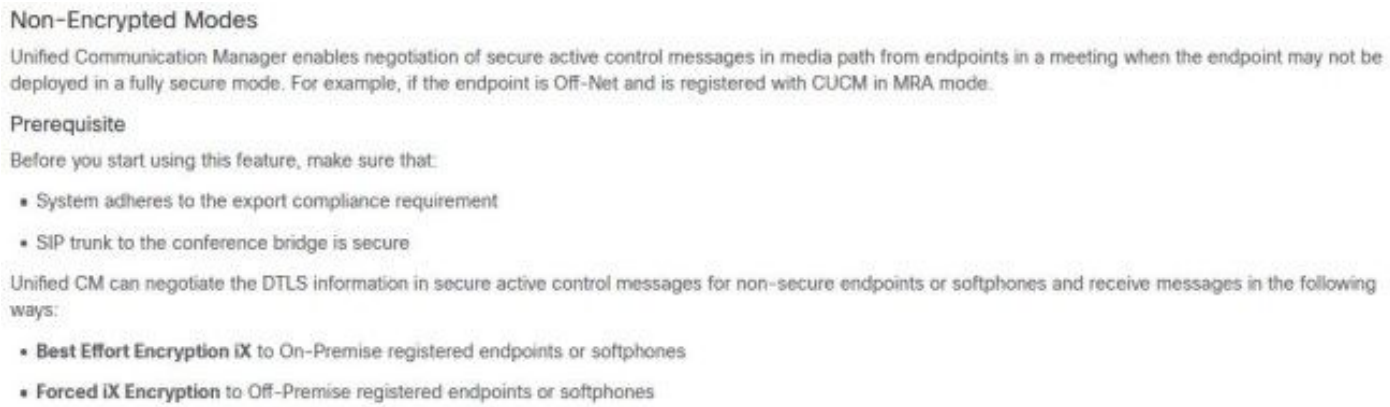
Con:

- Upgrade of CUCM required
- Only CUCM restricted versions are supported

From CUCM 12.5(1)SU1, it supports iX encryption negotiation for any SIP line device so it can negotiate the DTLS information in secure ActiveControl messages for non-secure endpoints or softphones. It sends over best effort iX encryption over TCP allowing phones to have an encrypted

iX channel end to end despite an unsecure TCP connection (not TLS) to the CUCM.

In the security guide of CUCM 12.5(1)SU1 under the section of 'Encrypted iX Channel', it shows that for non-encrypted modes with unsecure devices, best effort and forced iX encryption can be negotiated with the prerequisite that your system adheres to export compliance and the SIP trunk to your conference bridge is secure.



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

On CUCM:

- You have to use export restricted CUCM (not unrestricted)
- Under **System > Licensing > License Management**, you must have "Export-Controlled Functionality" set to allowed.
- Your SIP trunk must have the option "**SRTP Allowed**" enabled (regardless if the trunk itself is secure or unsecure)

On CMS:

- Your callbridge must have a license with encryption (so you do not have callBridgeNoEncryption license)
- On webadmin under **Configuration > Call Settings**, you must have set **SIP media encryption** to **allowed** (or **required**)

In the image, you can see that the connection is secure until the Expressway-C and then C sends over the SDP to CUCM without the crypto lines but it does include the iX media channel still. So the normal media for audio/video/.. is not secured with crypto lines but it does have a secure connection for iX media channel now so that the Expressway does not need to terminate the DTLS connection. Therefore ActiveControl can be negotiated between the client and the conference bridge directly, even with an unsecure phone security profile. In previous versions of CUCM, the flow would be different and ActiveControl is not negotiated because it does not pass over the iX channel to the CMS in the first place as that part would have been stripped off already.