ActiveControl über MRA/Expressway aktivieren

Inhalt

Einleitung

In diesem Dokument werden die verschiedenen Optionen zur Aktivierung des ActiveControl-Protokolls für Mobile and Remote Access (MRA)-Clients und für Anrufe von Endgeräten vor Ort bei WebEx Meetings über Expressway beschrieben. MRA ist eine Bereitstellungslösung für Jabber und Endgeräte ohne Virtual Private Network (VPN). Mit dieser Lösung können Endbenutzer von einem beliebigen Standort weltweit auf interne Unternehmensressourcen zugreifen. Das ActiveControl-Protokoll ist ein proprietäres Protokoll von Cisco, das eine verbesserte Konferenzerfahrung mit Laufzeitfunktionen wie Meeting-Listen, Änderungen des Video-Layouts, Stummschaltung und Aufzeichnungsoptionen ermöglicht.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Expressway (MRA- und B2B-Anrufe)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

In diesem Dokument liegt der Schwerpunkt auf der MRA-Client-Verbindung zu einem Cisco Meeting Server (CMS). Das Gleiche gilt jedoch für andere Plattformen oder Verbindungen, z. B. bei der Verbindung mit WebEx Meetings. Dieselbe Logik kann für die folgenden Arten von Anrufflüssen angewendet werden:

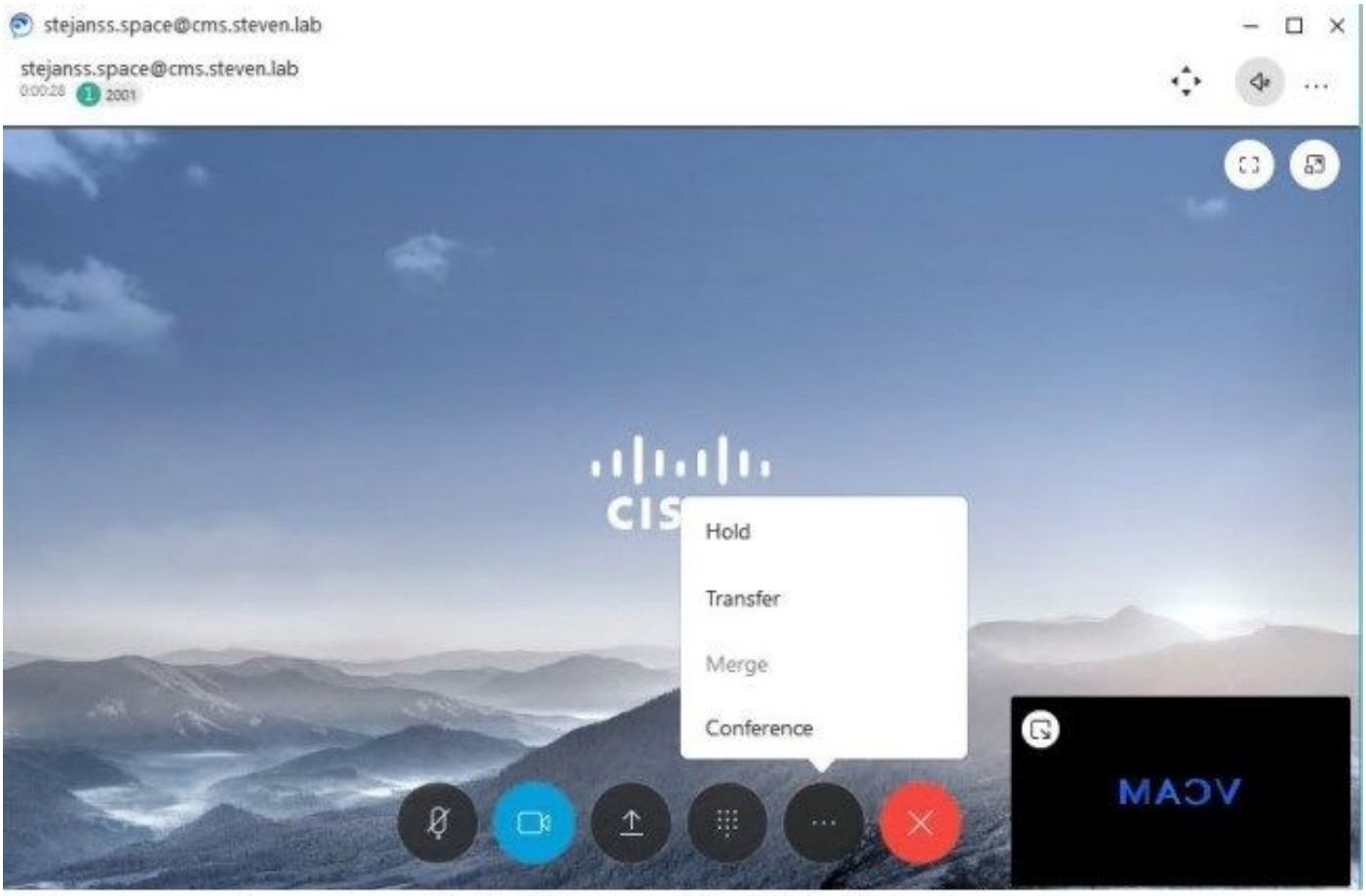
- Endgerät - CUCM - Expressway-C - Expressway-E - WebEx Meeting
- MRA-Endpunkt - (Expressway-E - Expressway-C) - CUCM - Expressway-C - Expressway-E - WebEx Meeting

  Hinweis: Die von WebEx Meetings unterstützten Funktionen von ActiveControl unterscheiden sich derzeit von denen von CMS und stellen nur eine begrenzte Teilmenge dar.

Die Cisco Meeting Server-Plattform bietet Meeting-Teilnehmern die Möglichkeit, ihre Meeting-Umgebung direkt vom Konferenzendpunkt aus über ActiveControl zu steuern, ohne dass externe Anwendungen oder Operatoren erforderlich sind. ActiveControl verwendet das iX-Medienprotokoll in Cisco Geräten und wird als Teil des SIP-Messaging eines Anrufs ausgehandelt. Ab CMS-Version 2.5 stehen die folgenden Hauptfunktionen zur Verfügung (diese können jedoch vom verwendeten Endgerätetyp und der verwendeten Softwareversion abhängen):

- Anzeigen einer Liste aller mit dem Meeting verbundenen Teilnehmer (Listen von Listen oder Teilnehmern)
- Stummschaltung für andere Teilnehmer aktivieren oder deaktivieren
- Hinzufügen oder Entfernen eines anderen Teilnehmers aus dem Meeting
- Starten oder Anhalten der Aufzeichnung eines Meetings
- Teilnehmer wichtig machen
- Anzeige für den Teilnehmer, der der aktive Sprecher im Meeting ist
- Indikator für den Teilnehmer, der derzeit Inhalte oder Präsentationen im Meeting teilt
- Sperren oder Entsperren der Konferenz

Auf dem ersten Bild sehen Sie eine Benutzeransicht von einem Jabber-Client, der einen Anruf in einen CMS-Raum ohne ActiveControl getätigt hat, während das zweite Bild die funktionsreichere Benutzeransicht zeigt, in der Jabber ActiveControl mit dem CMS-Server aushandeln konnte.



Jabber user experience when calling to CMS space without ActiveControl

Jabber user experience when calling to CMS space with ActiveControl

ActiveControl ist ein XML-basiertes Protokoll, das unter Verwendung des iX-Protokolls übertragen wird, das im Session Description Protocol (SDP) der SIP-Anrufe (Session Initiation Protocol) ausgehandelt wird. Es handelt sich um ein Protokoll von Cisco (eXtensible Conference Control Protocol (XCCP)), das nur in SIP ausgehandelt wird (sodass interworking calls nicht über ActiveControl verfügen) und UDP/UDT (UDP-based Data Transfer Protocol) für die Datenübertragung nutzt. Die sichere Aushandlung erfolgt über Datagram TLS (DTLS), das als

TLS-over-UDP-Verbindung betrachtet werden kann. Einige Beispiele für die Unterschiede in der Verhandlung sind hier aufgeführt.

Unverschlüsselt

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

Verschlüsselt (bestmögliche Leistung - Verschlüsselung versuchen, aber Fallback auf unverschlüsselte Verbindung zulassen)

m=Anwendung xxxx UDP/UDT/IX *****

a=ixmap:2 **xccp**

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

Verschlüsselung (Verschlüsselung erzwingen - Fallback auf unverschlüsselte Verbindung nicht zulassen)

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

a=ixmap:2 **xccp**

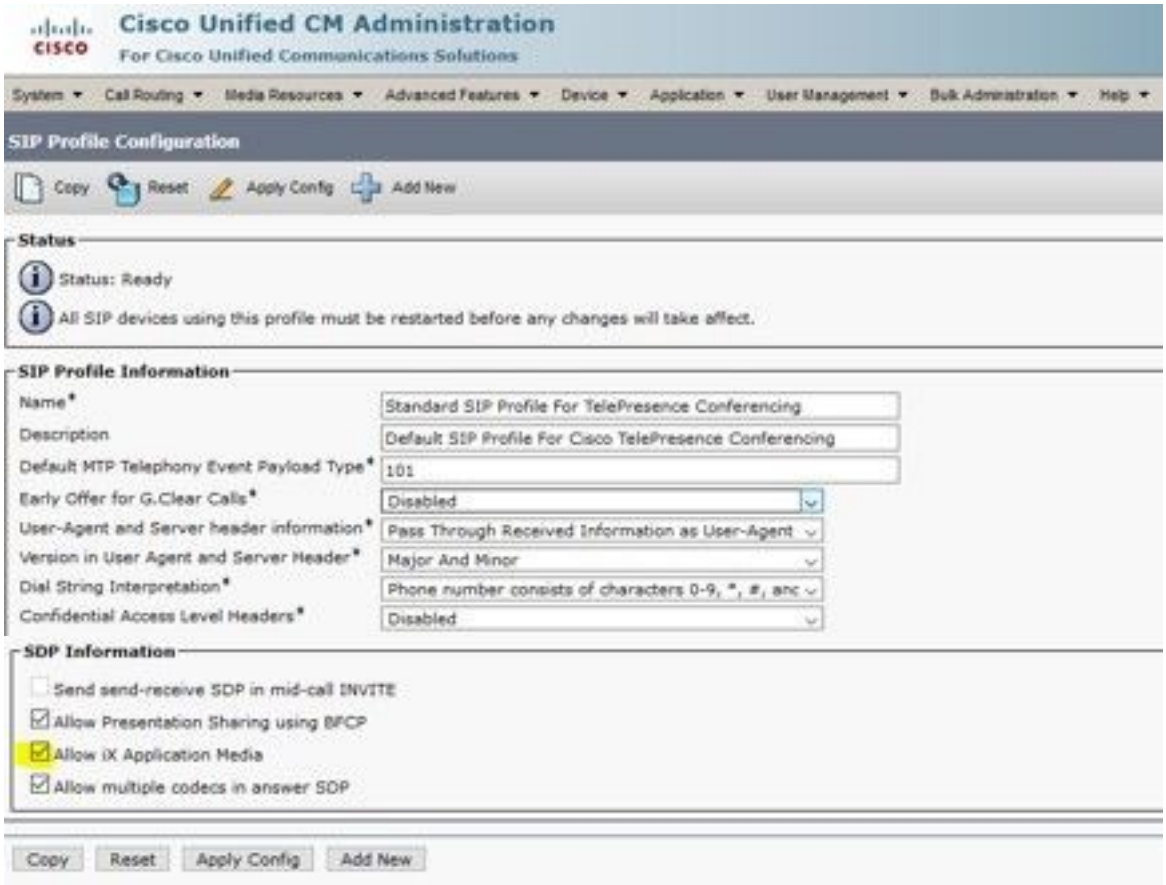
a=**Fingerabdruck**:sha-1 xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:

Es gibt einige Mindestsoftwareversionen, die für eine vollständige ActiveControl-Unterstützung erforderlich sind:

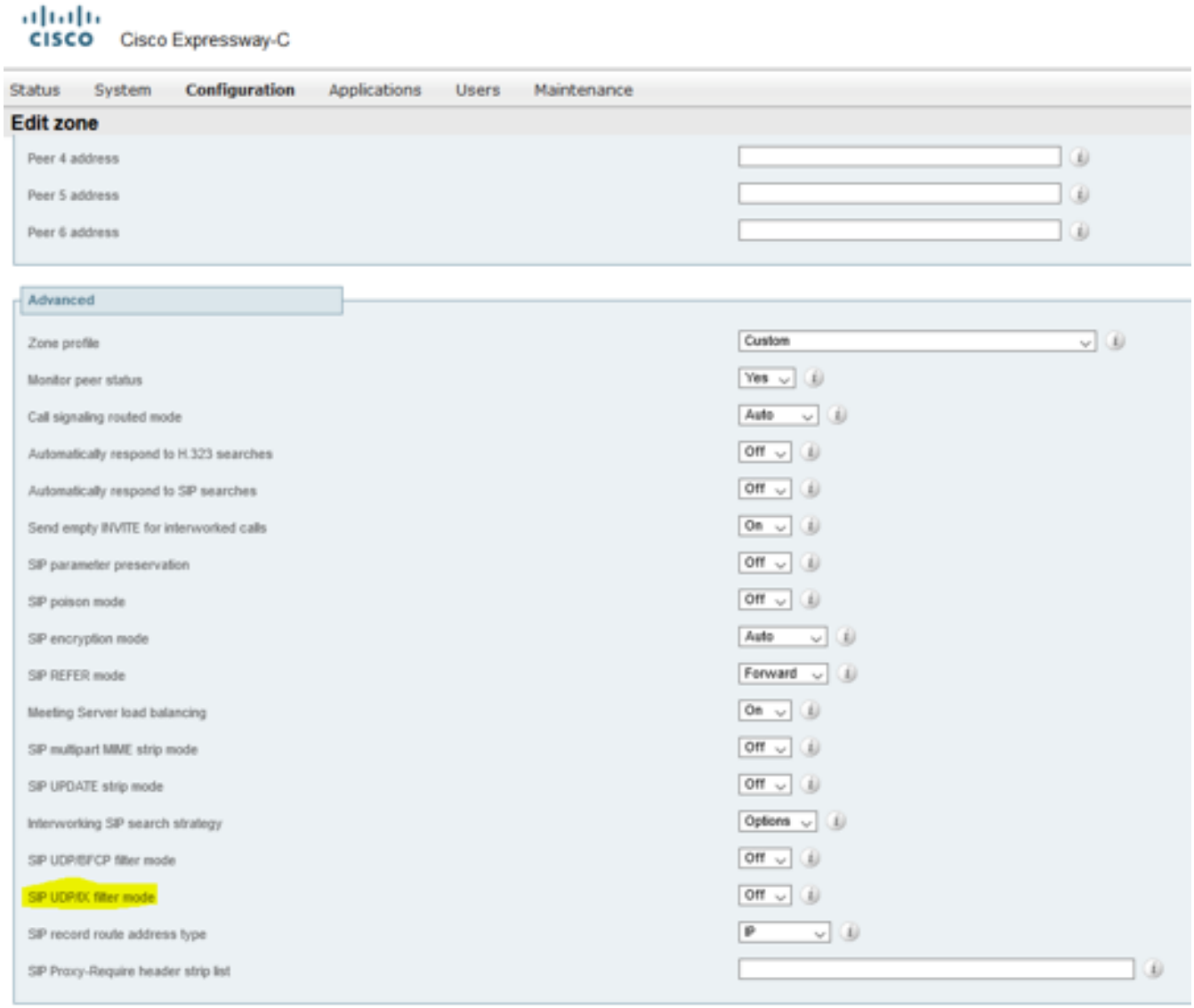
- Jabber Version 12.5 oder höher (Versionshinweise)
- CE-Endpunkte 8.3 oder höher, 9.6.2 oder höher, empfohlen gemäß CMS ActiveControl-Leitfaden (CE9.3.1 oder höher für WebEx gemäß dem WebEx Hilfe-Link)
- CUCM 10.5 oder höher (für Jabber 12.5 ActiveControl-Unterstützung) (11.5(1) oder höher für WebEx gemäß Link)
- CMS 2.1 oder höher, 2.5 oder höher, empfohlen gemäß CMS ActiveControl-Leitfaden
- Expressway X12.5 oder höher (Versionshinweise) zur Unterstützung von nicht verschlüsselten MRA-Clients

Es gibt einige Konfigurationsoptionen, die berücksichtigt werden müssen:

- Stellen Sie auf dem CUCM sicher, dass die relevanten SIP-Trunks (zu Expressway-C und CMS) mit einem SIP-Profil konfiguriert sind, auf dem die Option "iX-Anwendungsmedien zulassen" aktiviert ist.



- Auf CMS ist es standardmäßig ab 2.1 aktiviert, aber Sie können es über ein Kompatibilitätsprofil deaktivieren, auf dem Sie *sipUDT* auf false setzen können
- Stellen Sie auf Expressway in der Zonenkonfiguration unter den erweiterten Einstellungen (bei Verwendung eines benutzerdefinierten Zonenprofils) sicher, dass der *SIP-UDP/IX-Filtermodus* auf "Aus" gesetzt ist, wenn Sie iX das Passieren erlauben möchten.



Problem

Allgemeine Informationen

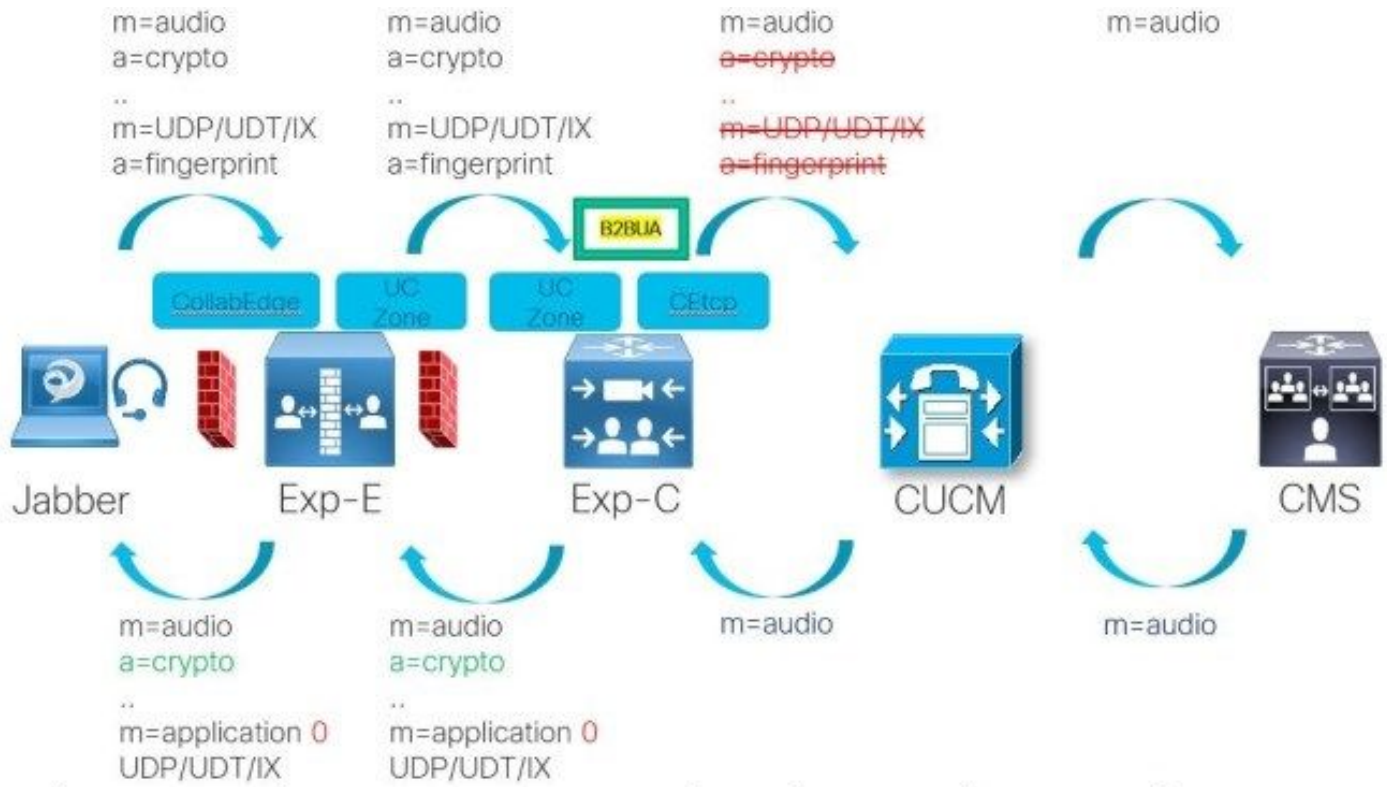
ActiveControl wird sicher anders als andere Medienkanäle ausgehandelt. Für andere Medienkanäle wie Audio und Video wird dem SDP eine Verschlüsselungsleitung angefügt, die dem Remote-Teilnehmer mitteilt, welcher Verschlüsselungsschlüssel für diesen Kanal verwendet werden soll. Der RTP-Kanal (Real-time Transport Protocol) kann daher als sicherer RTP-Kanal (Secure RTP) eingestuft werden. Für den iX-Kanal wird das DTLS-Protokoll verwendet, um den XCCP-Medien-Stream zu verschlüsseln, sodass ein anderer Mechanismus verwendet wird.

Die Expressway-Software terminiert das DTLS-Protokoll nicht. Dies wird im Abschnitt *Einschränkungen* unter *Nicht unterstützte Funktionen* der Expressway-Versionshinweise angegeben.

- 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-Versionen vor X12.5

Wenn eine Expressway-Version vor X12.5 ausgeführt wird und eine eingehende Verbindung mit einem verschlüsselten iX-Kanal besteht, der entlang einer unsicheren TCP-Zone weitergeleitet wird, entfernt der Expressway sowohl die Krypto-Leitungen der normalen Medienkanäle als auch den gesamten iX-Kanal. Dies wird visuell für einen MRA-Client dargestellt, der sich mit einem CMS-Bereich verbindet, in dem Sie sehen, dass die Verbindung vom MRA-Client zum Expressway-C sicher ist. Je nach dem auf dem CUCM für das Gerät eingerichteten Telefonsicherheitsprofil ist sie jedoch entweder unverschlüsselt (und über die CEtcp-Zone gesendet) oder verschlüsselt (und über die CEtls-Zone gesendet). Wenn es unverschlüsselt ist, wie auf dem Bild gezeigt, sehen Sie, dass der Expressway-C die Kryptozeilen für alle Medienkanäle abzieht und sogar den gesamten iX-Medienkanal abzieht, da er das DTLS-Protokoll nicht beenden kann. Dies geschieht über den Back-To-Back User Agent (B2BUA), da die Zonenkonfiguration für die CEtcp-Zone mit Medienverschlüsselung 'Force unencrypted' eingerichtet ist. In die entgegengesetzte Richtung (über die UC-Überbrückungszone mit "Force encrypted" Medienverschlüsselung), wenn die SDP-Antwort empfangen wird, werden die Krypto-Leitungen für die normalen Medienleitungen hinzugefügt, und der Port für den iX-Kanal wird auf Null gesetzt, was zu keiner ActiveControl-Aushandlung führt. Intern, wenn die Clients direkt beim CUCM registriert sind, ermöglicht dies sowohl verschlüsselte als auch unverschlüsselte iX-Medienkanäle, da sich der CUCM nicht selbst im Medienpfad befindet.



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

Die gleiche Logik gilt für die Anrufverbindungen über Expressway zu WebEx Meetings. Es erfordert, dass der vollständige Pfad durchgehend sicher ist, da die Expressway-Server (vor X12.5) nur die DTLS-Verbindungsinformationen weiterleiten, aber nicht selbst daran enden, um eine neue Sitzung zu starten oder den Medienkanal auf den verschiedenen Anrufabschnitten zu verschlüsseln/zu entschlüsseln.

Expressway-Versionen von X12.5 und höher

Wenn eine Expressway-Version von X12.5 oder höher ausgeführt wird, hat sich das Verhalten geändert, da es jetzt als erzwungene Verschlüsselung (UDP/DTLS/UDT/IX) über den iX-Kanal über die TCP-Zonenverbindung weitergeleitet wird, damit der iX-Kanal weiterhin ausgehandelt

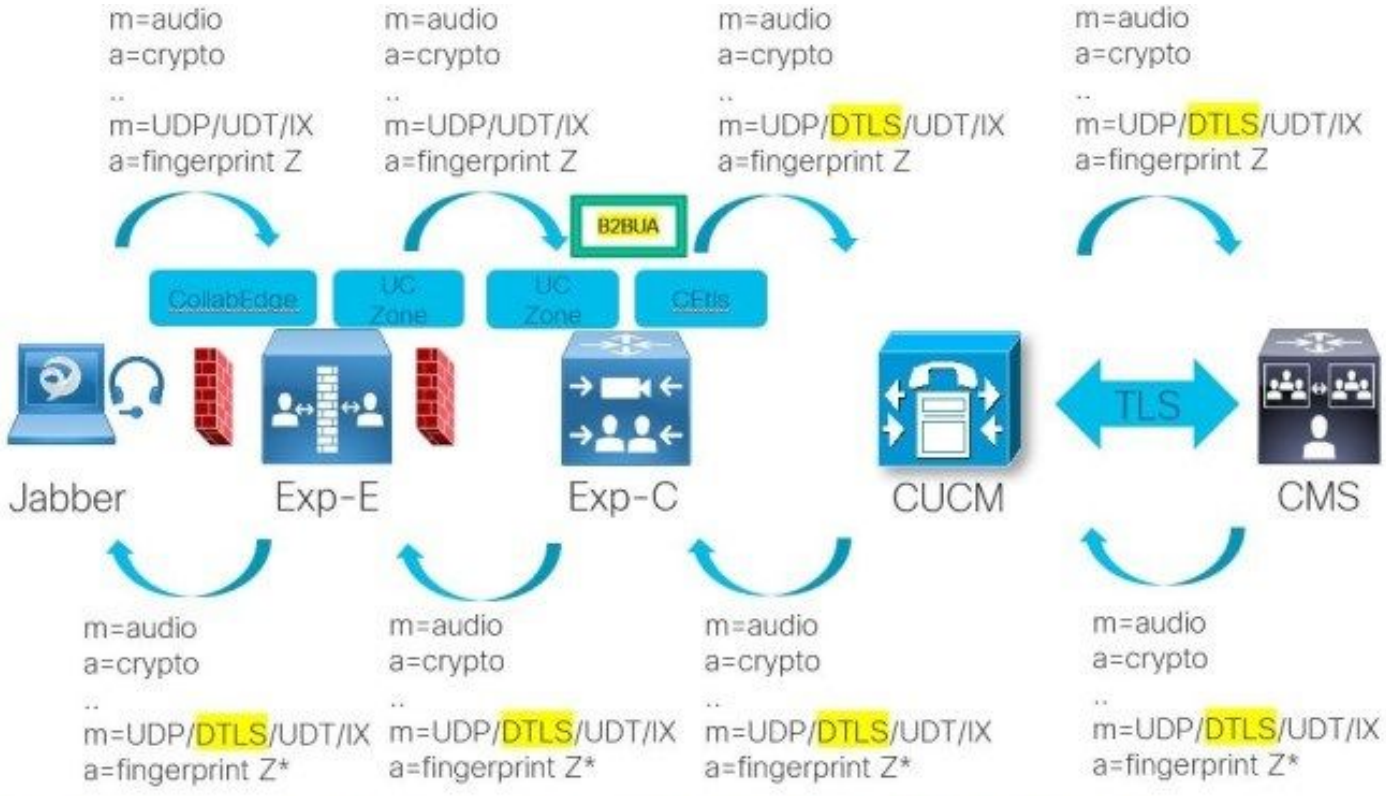
werden kann, allerdings nur, wenn das Remote-Ende ebenfalls Verschlüsselung verwendet. Sie erzwingt die Verschlüsselung, da der Expressway die DTLS-Sitzung nicht beendet und somit nur auf Pass-Through reagiert, sodass die DTLS-Sitzung dann vom Remote-Ende gestartet/beendet wird. Die Krypto-Leitungen werden jedoch aus Sicherheitsgründen über die TCP-Verbindung entfernt. Diese Verhaltensänderung wird in den Versionshinweisen im Abschnitt 'MRA: Unterstützung für verschlüsseltes iX (für ActiveControl)' behandelt. Was danach passiert, hängt von der CUCM-Version ab, da sich dieses Verhalten in 12.5(1)SU1 geändert hat. Dort kann es auch bei unsicheren eingehenden Verbindungen über den iX-Kanal übertragen. Selbst wenn ein sicherer TLS-SIP-Trunk zu CMS vorhanden wäre, würde der iX-Kanal bei Ausführung der CUCM-Version unter 12.5(1)SU1 entfernt, bevor er an das CMS weitergeleitet wird, was letztendlich zu einem ausgeschalteten Nullopport von CUCM an Expressway-C führen würde.

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.

Mit einem durchgängigen sicheren Signalisierungs- und Medienpfad für Anrufe kann der iX-Kanal direkt (über verschiedene Hops von Expressway-Servern) zwischen dem MRA-Client und der Konferenzlösung (CMS oder WebEx Meeting) ausgehandelt werden. Das Bild zeigt den gleichen Anrufverlauf für einen MRA-Client, der sich mit einem CMS-Bereich verbindet, jetzt jedoch mit einem auf CUCM konfigurierten sicheren Telefonsicherheitsprofil und einem sicheren TLS SIP-Trunk zu CMS. Sie können sehen, dass der Pfad durchgängig sicher ist und dass der DTLS-Fingerabdruckparameter einfach über den gesamten Pfad übertragen wird.

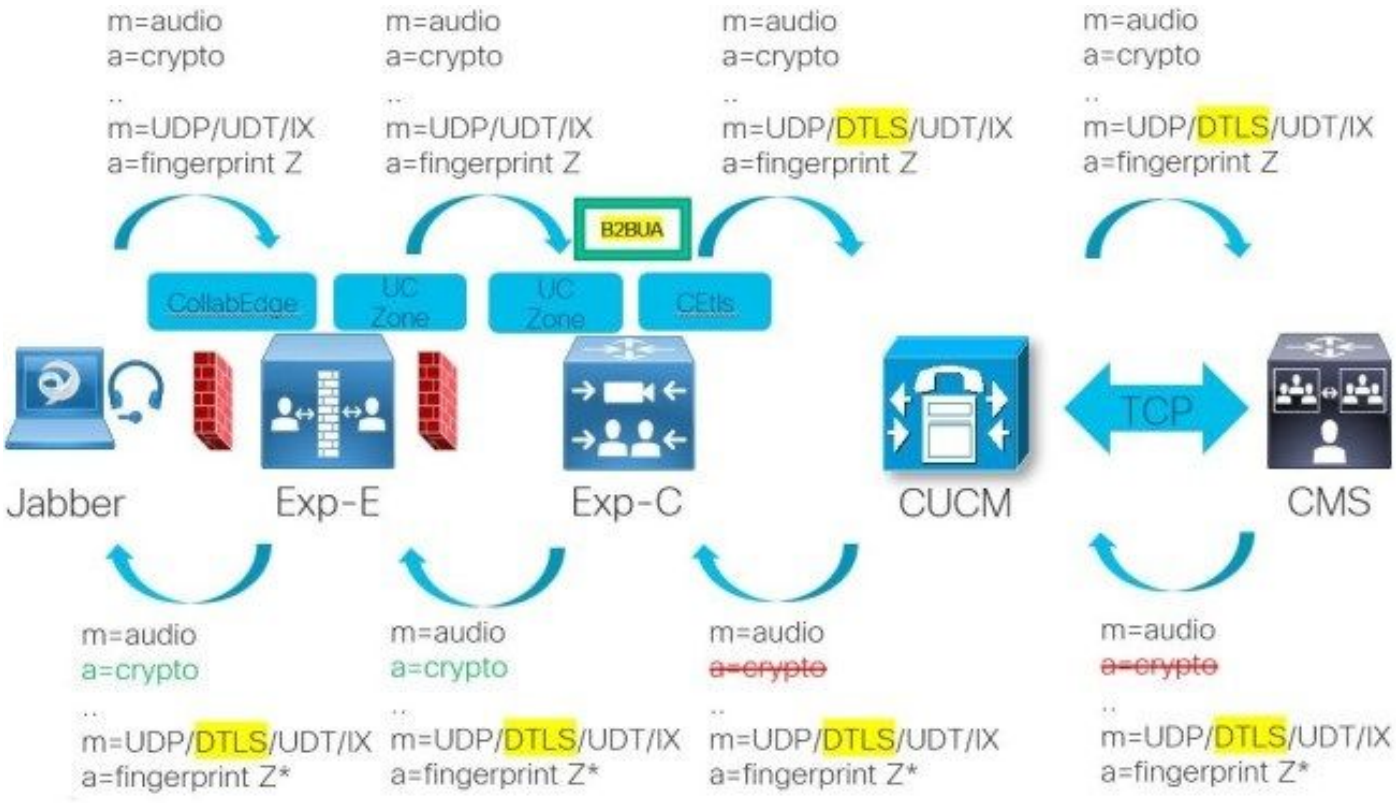


Media negotiation when using Expressway and CEtls SIP trunk with TLS SIP trunk to CMS

Um ein sicheres Gerätesicherheitsprofil einzurichten, müssen Sie sicherstellen, dass der CUCM in einem gemischten Modus eingerichtet ist. Dies kann ein mühsamer Prozess sein (auch wenn er betriebsbereit ist, da er CAPF (Certificate Authority Proxy Function) für eine sichere

standortbasierte Kommunikation erfordert). Aus diesem Grund können hier weitere praktische Lösungen angeboten werden, um die Verfügbarkeit von ActiveControl über MRA und Expressway im Allgemeinen zu unterstützen, wie in diesem Dokument beschrieben.

Sichere TLS-SIP-Trunks zu den CMS-Servern sind nicht erforderlich, da der CUCM (vorausgesetzt, für den SIP-Trunk ist die Option "SRTP erlaubt" aktiviert) immer noch von einer eingehenden sicheren SIP-Verbindung den iX-Kanal sowie die Verschlüsselungsleitungen weiterleitet, aber CMS antwortet nur mit Verschlüsselung auf den iX-Kanal (ermöglicht ActiveControl) (vorausgesetzt, **SIP-Medienverschlüsselung wird**vorausgesetzt) ist auf *CMS* unter **"Einstellungen" > "Anrufeinstellungen" (***erlaubt* oder *erzwungen*) eingestellt, hat aber keine Verschlüsselung auf den anderen Medienkanälen, da die Krypto-Leitungen von diesen gemäß Bild entfernt werden. Die Expressway-Server können die Krypto-Leitungen erneut hinzufügen, um den Teil der Verbindung noch zu sichern (und iX wird direkt zwischen den Endkunden noch über DTLS ausgehandelt). Dies ist jedoch aus Sicherheitssicht nicht ideal, und daher wird empfohlen, einen sicheren SIP-Trunk zur Konferenzbrücke einzurichten. Wenn **SRTP zulässig** auf dem SIP-Trunk nicht aktiviert ist, entfernt der CUCM die Krypto-Leitungen, und die sichere iX-Aushandlung schlägt ebenfalls fehl.



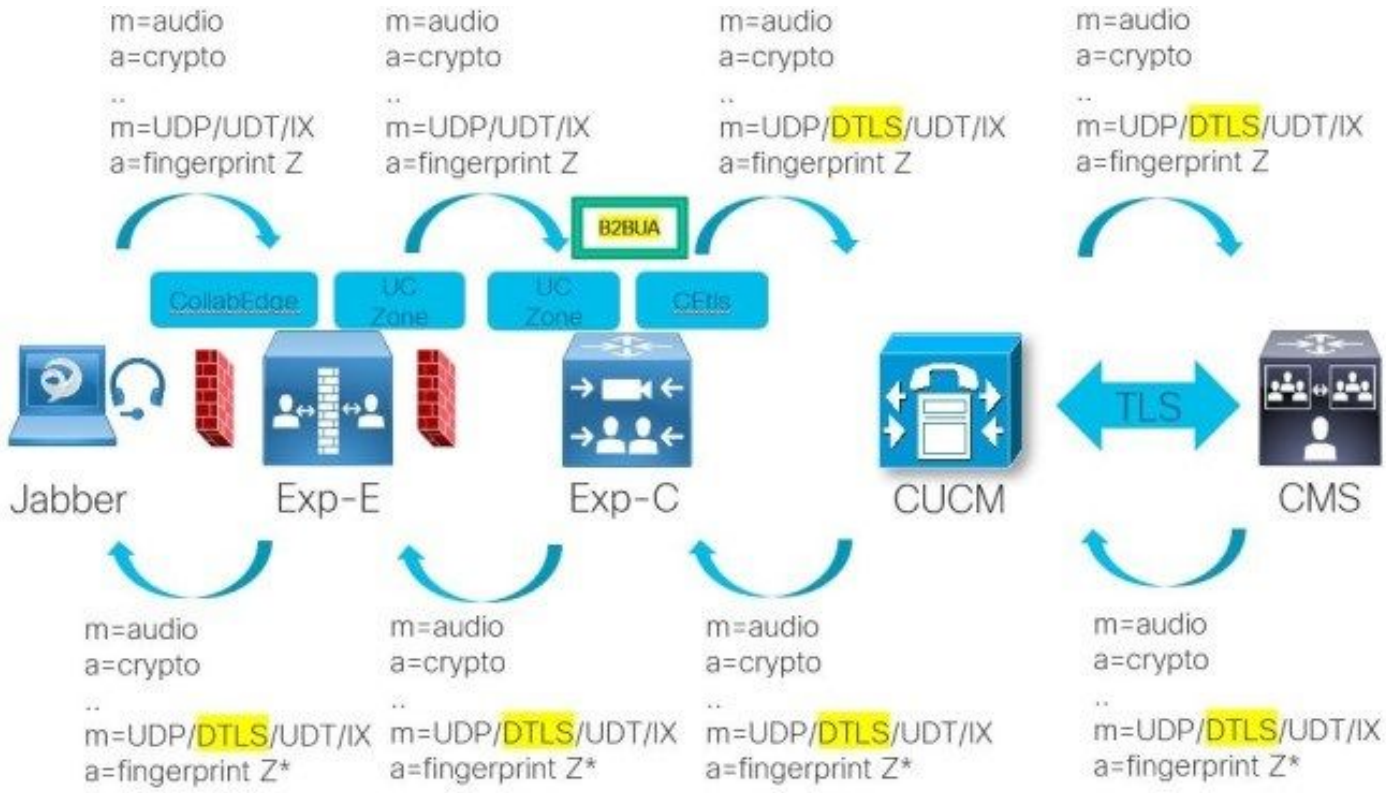
Media negotiation when using Expressway and CEtls SIP trunk with TCP SIP trunk to CMS

Lösung

Es gibt eine Reihe von verschiedenen Optionen mit verschiedenen Anforderungen und verschiedenen Vor-und Nachteile. Jede davon wird in einem detaillierteren Abschnitt vorgestellt. Folgende Optionen stehen zur Verfügung:

1. Sichere Telefonsicherheitsprofile für die Endpunkte (CUCM im gemischten Modus)
2. SIP OAuth für Jabber
3. Verschlüsselter iX-Kanal für unsichere Telefonsicherheitsprofile (CUCM 12.5(1)SU1 oder höher)

Lösung 1: Sichere Telefonsicherheitsprofile für die Endpunkte (CUCM im gemischten Modus)



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

Voraussetzungen:

- CUCM im gemischten Modus

Vorteile:

- Kompatibel mit allen CUCM-Versionen
- Funktioniert für alle Client-Geräte

Nachteile:

- Erfordert Konfiguration von CUCM im gemischten Modus (und CAPF-Vorgänge an lokalen Endpunkten)

Dies ist die Methode, die im Abschnitt "Problem" sowie am Ende beschrieben wird. Hier stellen Sie sicher, dass Sie über einen verschlüsselten End-to-End-Signalisierungs- und Medienpfad für Anrufe verfügen. Hierfür muss der CUCM gemäß dem folgenden Dokument im gemischten Modus eingerichtet werden.

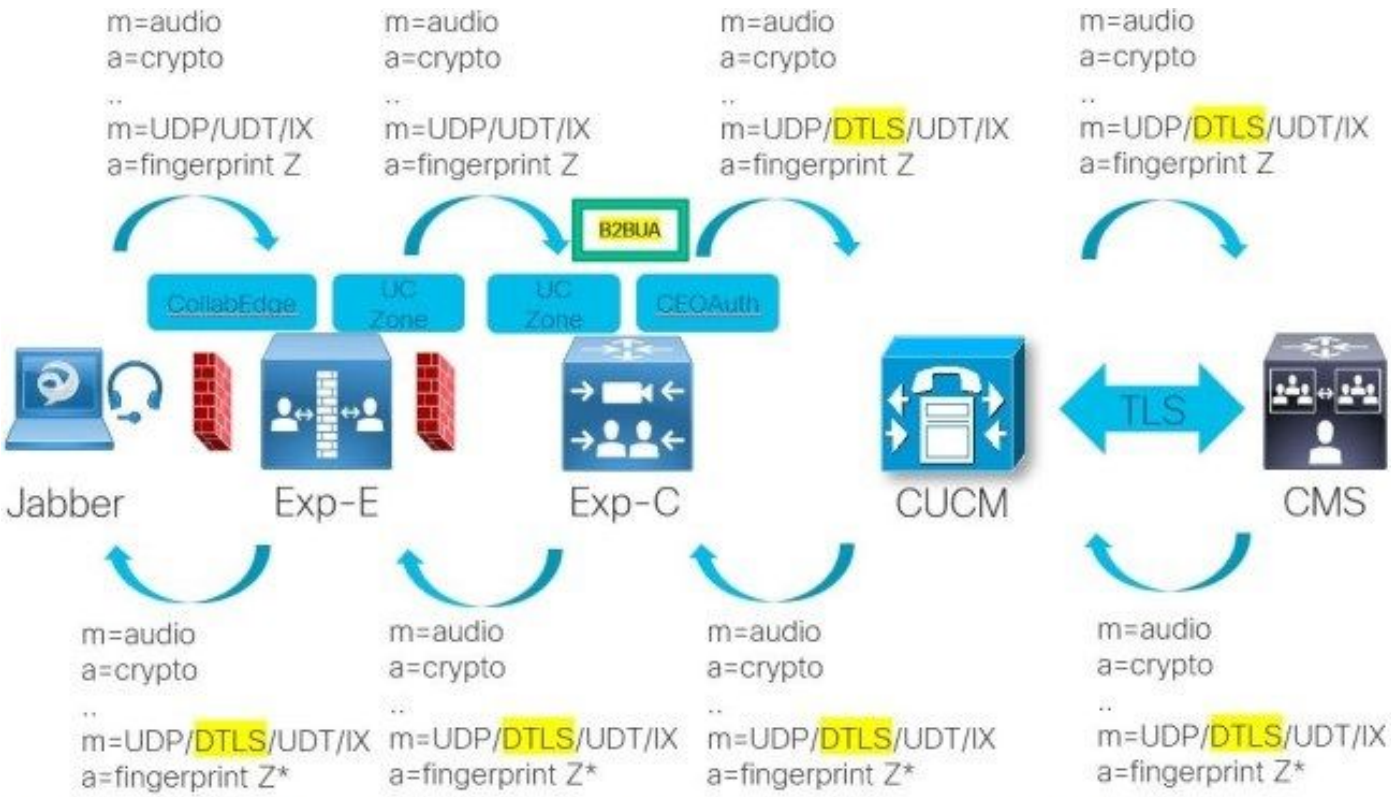
Für MRA-Clients ist kein CAPF-Vorgang erforderlich. Führen Sie jedoch die zusätzlichen Konfigurationsschritte mit dem sicheren Telefonsicherheitsprofil mit einem Namen aus, der mit einem der alternativen Antragstellernamen des Expressway-C-Serverzertifikats übereinstimmt, wie im Collaboration Edge TC-basierten Endgeräte-Konfigurationsbeispiel (das auch für CE-basierte Endgeräte und Jabber-Clients gilt) hervorgehoben wird.

Wenn Sie eine Verbindung von einem lokalen Endpunkt oder einem Jabber-Client zu einem

WebEx Meeting herstellen, müssen Sie den CAPF-Vorgang durchführen, um den Client sicher beim CUCM zu registrieren. Dies ist erforderlich, um einen sicheren End-to-End-Anruffluss sicherzustellen, bei dem der Expressway die DTLS-Aushandlung einfach weiterleiten kann und nicht selbst verarbeiten muss.

Um den Anruf durchgängig sicher zu machen, müssen alle relevanten SIP-Trunks (an Expressway-C bei Anrufen an Webex Meeting und an CMS bei Anrufen an CMS-Konferenz) ebenfalls sichere SIP-Trunks mit TLS mit sicherem SIP-Trunk-Sicherheitsprofil sind.

Lösung 2: SIP OAuth für Jabber



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

Voraussetzungen:

- Cisco Jabber 12.5 oder höher (Versionshinweise)
- CUCM-Version 12.5 oder höher (Versionshinweise) mit *OAuth mit* aktiviertem *Aktualisierungs-Anmeldungsablauf*
- Expressway X12.5.1 oder höher (Versionshinweise) mit *Autorisierung durch OAuth-Token bei* aktivierter *Aktualisierung*

Vorteile:

- Ermöglicht sichere Registrierungen und ein einfaches Umschalten zwischen standortbasierten und standortexternen Lösungen ohne jährliche CAPF-Verlängerung
- CUCM muss nicht im gemischten Modus eingerichtet werden.

Nachteile:

- Gilt nur für Jabber, nicht für TC/CE-Endgeräte

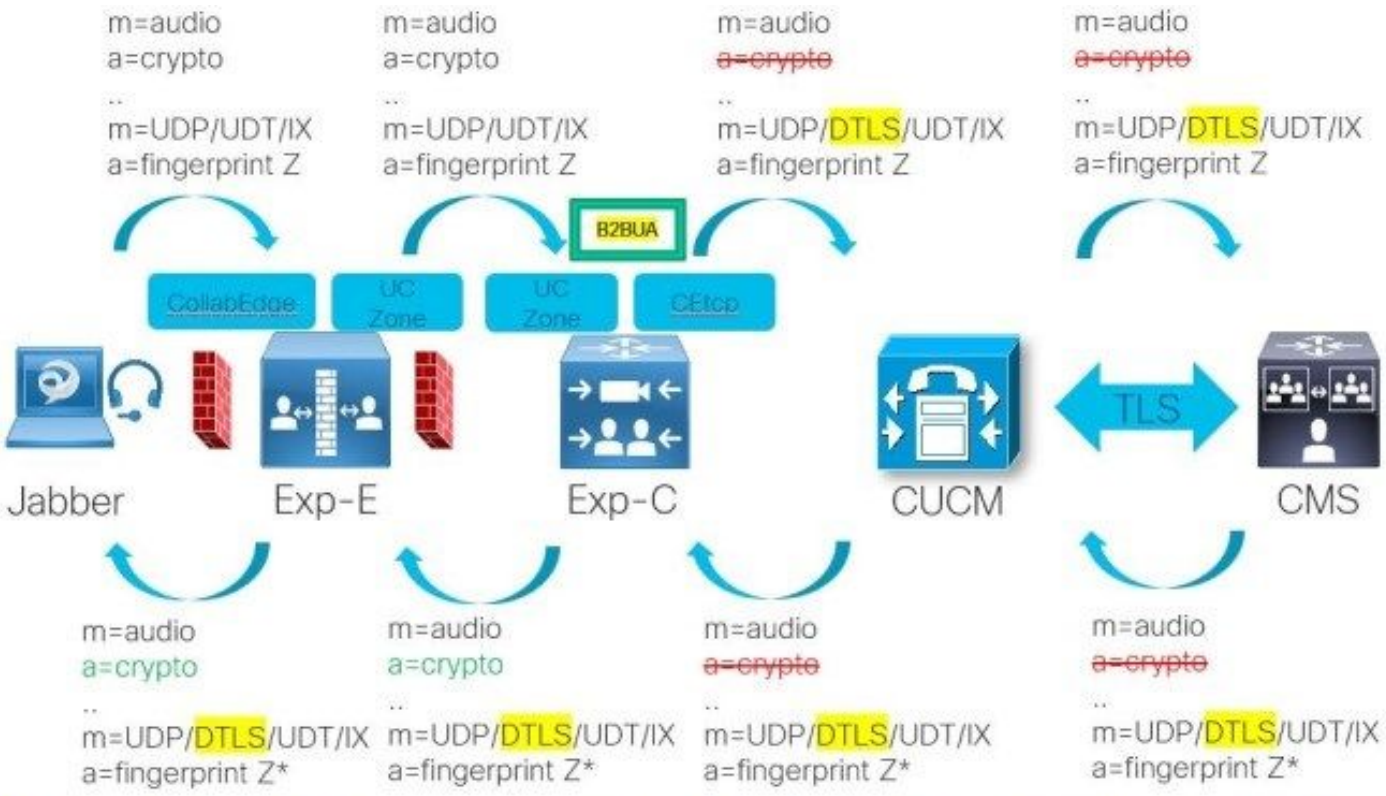
Im SIP-OAuth-Modus können Sie OAuth-Aktualisierungstoken für die Cisco Jabber-Authentifizierung in sicheren Umgebungen verwenden. Sie ermöglicht eine sichere Signalisierung

und sichere Medien ohne die CAPF-Anforderungen von Lösung 1. Die Tokenvalidierung während der SIP-Registrierung ist abgeschlossen, wenn die OAuth-basierte Autorisierung auf dem CUCM-Cluster und den Jabber-Endpunkten aktiviert ist.

Die Konfiguration in CUCM wird im Funktionskonfigurationsleitfaden dokumentiert und setzt voraus, dass OAuth mit Refresh Login Flow unter Enterprise Parameters bereits aktiviert ist. Um dies auch über MRA zu aktivieren, müssen Sie die CUCM-Knoten im Expressway-C-Server unter **Configuration > Unified Communication > Unified CM Servers** aktualisieren, sodass Sie unter **Configuration > Zones > Zones** nun auch die automatisch erstellten CEOAuth-Zonen sehen müssen. Stellen Sie außerdem sicher, dass unter **Configuration > Unified Communication > Configuration** das **Token Authorize by OAuth mit Aktualisierung** ebenfalls aktiviert ist.

Mit dieser Konfiguration können Sie eine ähnliche sichere End-to-End-Anrufverbindung sowohl für die Signalisierung als auch für die Medien herstellen. Daher wird der Expressway nur über die DTLS-Verhandlung geleitet, da er diesen Datenverkehr nicht selbst terminiert. Dies ist auf dem Bild zu sehen, wo der einzige Unterschied im Vergleich zur vorherigen Lösung ist, dass es die CEOAuth-Zone auf dem Expressway-C zum CUCM im Gegensatz zur CEtls-Zone verwendet, weil es SIP OAuth anstelle der sicheren Geräteregistrierung über TLS verwendet, wenn CUCM in einem gemischten Modus mit einem sicheren Telefon-Sicherheitsprofil arbeitet, aber abgesehen davon, bleibt alles gleich.

Lösung 3: Verschlüsselter iX-Kanal für unsichere Telefonsicherheitsprofile (CUCM 12.5(1)SU1 oder höher)



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

Voraussetzungen:

- CUCM-Version 12.5(1)SU1 oder höher (Versionshinweise)
- Expressway X12.5.1 oder höher (Versionshinweise)

Vorteile:

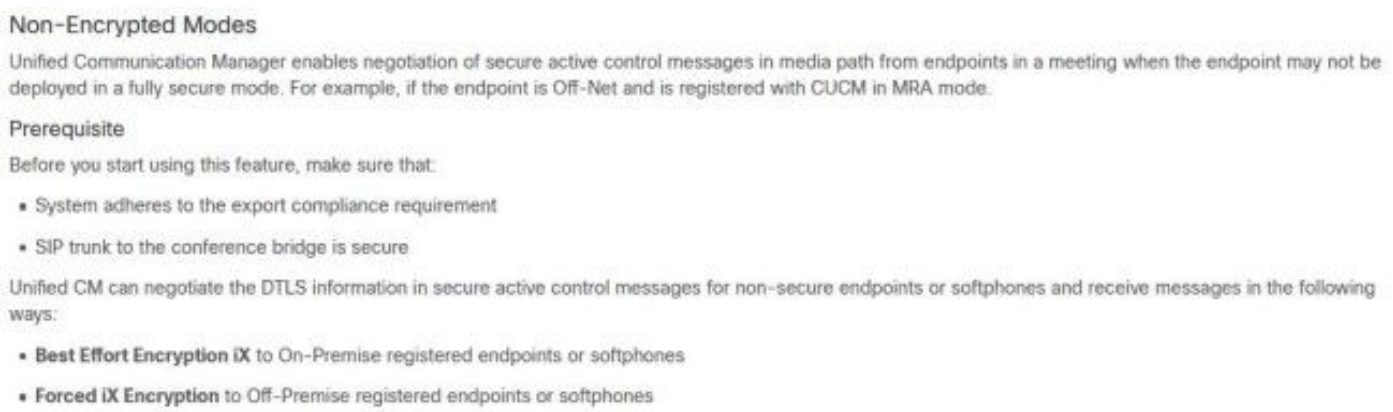
- CUCM muss nicht im gemischten Modus eingerichtet werden.
- End-to-End-Kommunikation muss nicht eingerichtet werden
- Gilt für Jabber- und TC/CE-Endgeräte

Nachteile:

- Aktualisierung von CUCM erforderlich
- Es werden nur eingeschränkte CUCM-Versionen unterstützt.

Ab CUCM 12.5(1)SU1 unterstützt es die iX-Verschlüsselungsaushandlung für jedes SIP-Leitungsgerät, sodass es die DTLS-Informationen in sicheren ActiveControl-Nachrichten für nicht sichere Endgeräte oder Softphones aushandeln kann. Es sendet über bestmögliche iX-Verschlüsselung über TCP, sodass Telefone trotz einer unsicheren TCP-Verbindung (nicht TLS) zum CUCM einen verschlüsselten iX-Kanal durchlaufen können.

Im Sicherheitsleitfaden von CUCM 12.5(1)SU1 im Abschnitt "Verschlüsselter iX-Kanal" wird gezeigt, dass für nicht verschlüsselte Modi mit unsicheren Geräten Best Effort und erzwungene iX-Verschlüsselung ausgehandelt werden können, vorausgesetzt, dass das System die Exportbestimmungen einhält und der SIP-Trunk zu Ihrer Konferenzbrücke sicher ist.



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

Auf CUCM:

- Sie müssen den export restricted CUCM (nicht unrestricted) verwenden.
- Unter **System > Licensing > License Management** muss "Export-Controlled Functionality" auf allowed eingestellt sein.
- Für Ihren SIP-Trunk muss die Option **"SRTP Allowed"** aktiviert sein (unabhängig davon, ob der Trunk selbst sicher oder unsicher ist).

Auf CMS:

- Ihre Callbridge muss über eine verschlüsselte Lizenz verfügen (Sie verfügen also nicht über eine callBridgeNoEncryption-Lizenz).
- Unter **Konfiguration > Anrufeinstellungen** müssen Sie für Webadmin die **SIP-Medienverschlüsselung** auf **Zulässig (**oder **Erforderlich)** eingestellt haben.

Im Bild können Sie sehen, dass die Verbindung sicher ist, bis der Expressway-C und dann C über das SDP an CUCM ohne die Krypto-Leitungen sendet, aber der iX-Medienkanal bleibt erhalten. Das normale Medium für Audio/Video/... ist also nicht mit Krypto-Leitungen gesichert, aber es hat jetzt eine sichere Verbindung für den iX-Medienkanal, sodass der Expressway die DTLS-Verbindung nicht beenden muss. Daher kann ActiveControl direkt zwischen dem Client und der Konferenz-Bridge ausgehandelt werden, selbst wenn das Sicherheitsprofil eines Telefons nicht

sicher ist. Bei früheren Versionen von CUCM wäre der Fluss anders, und ActiveControl wird nicht ausgehandelt, da es nicht von vornherein über den iX-Kanal an das CMS weitergeleitet wird, da dieser Teil bereits entfernt worden wäre.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.