# RTP sécurisé entre CUCM et VCS ou exemple de configuration d'Expressway

## Contenu



## Introduction

Ce document décrit comment installer un Protocole RTP (Real-Time Transport Protocol) sécurisé entre le serveur de communication vidéo de Cisco (VCS) et le gestionnaire de Cisco Unified Communications (CUCM).

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CUCM
- VCS ou Cisco Expressway de Cisco

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- CUCM
- VCS ou Cisco Expressway de Cisco

  **Note**: Cet article utilise les Produits de Cisco Expressway aux fins de l'explication (sauf là où indiqué), mais les informations s'appliquent également si votre déploiement utilise le VCS de Cisco.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

# Informations générales

### Conditions

- Appels de Protocole SIP (Session Initiation Protocol) conduits entre CUCM et Expressway
- Le cryptage de medias est meilleur effort/facultatif entre Expressway-C et CUCM

### Description

Il y a eu des difficultés signalées pour la configuration du cryptage de medias de meilleur effort pour les appels de SIP qui sont conduits entre CUCM et VCS/Expressway. Une mauvaise configuration commune affecte la signalisation des medias chiffrés, par l'intermédiaire du protocole de transport en temps réel sécurisé (SRTP), qui entraîne la panne des appels chiffrés par meilleur effort quand le transport entre CUCM et Expressway n'est pas sécurisé.

Si le transport n'est pas sécurisé, alors la signalisation de cryptage de medias pourrait être lue par une oreille indiscrète. Dans ce cas, les informations de signalisation de cryptage de medias sont éliminées de la Session Description Protocol (SDP). Cependant, il est possible de configurer CUCM pour envoyer (et compter recevoir) le cryptage de medias signalant au-dessus d'une connexion sans garantie. Vous pouvez travailler autour de cette mauvaise configuration dans une de deux manières, dépendant au moment si les appels sont joncteur réseau-side conduit ou ligne-side à CUCM.

### Joncteur réseau-side et exemples de Ligne-side

Joncteur réseau-side : Un joncteur réseau de SIP est configuré sur CUCM vers Expressway. Une

zone voisine correspondante est configurée sur Expressway vers CUCM. Vous auriez besoin d'un joncteur réseau si vous vouliez que (Expressway n'est pas un registrar, mais le VCS est) les points finaux VCS-enregistrés appelassent des points finaux CUCM-enregistrés. Un autre exemple serait d'activer H.323 le dialogue dans votre déploiement.

Ligne-side : les appels de Ligne-side vont directement à CUCM, pas par l'intermédiaire d'un joncteur réseau. Si tous les enregistrement et Contrôle d'appel est fourni par CUCM, votre déploiement ne pourrait pas exiger un joncteur réseau à Expressway. Par exemple, si Expressway est déployé purement pour le mobile et l'Accès à distance (MRA), il proxys que le ligne-side appelle des points finaux externes à CUCM.

### Stratégie de réduction

S'il y a un joncteur réseau de SIP entre CUCM et Expressway, un script de normalisation sur le CUCM réécrit le SDP convenablement de sorte que l'appel de cryptage de meilleur effort ne soit pas rejeté. Ce script est automatiquement installé avec des versions ultérieures de CUCM, mais si vous faites rejeter des appels chiffrés par meilleur effort, Cisco recommande que vous téléchargiez et installiez le dernier script de VCS-interop pour votre version de CUCM.

Si l'appel va le ligne-side à CUCM, alors CUCM compte voir l'en-tête de x-Cisco-srtp-`retour` si le cryptage de medias est facultatif. Si CUCM ne voit pas cette en-tête, elle considère comme étant l'appel cryptage-obligatoire. Le soutien de cette en-tête a été ajouté à Expressway dans la version X8.2, ainsi Cisco recommande X8.2 ou plus tard pour MRA (périphérie de Collaboration).

## Configurez

### configuration de Ligne-side

[CUCM] <--meilleur effort--> [Expressway-C] <--obligatoire--> [Expressway-e] <--obligatoire--> [point final]

Afin d'activer le cryptage de meilleur effort des appels de ligne-side d'Expressway-C à CUCM :

- Utilisez un déploiement/solution pris en charge (par exemple, MRA)
- Sécurité de mode mixte d'utilisation sur CUCM
- Assurez cette confiance d'Expressway et CUCM (l'Autorité de certification (CA) qui signe la nécessité des Certificats de chaque interlocuteur sont de confiance par l'autre interlocuteur)
- Version X8.2 d'utilisation ou plus tard d'Expressway
- Profils téléphoniques sécurisés d'utilisation sur CUCM, avec le positionnement de mode de sécurité des périphériques authentifié ou chiffré - pour ces modes le type de transport est Transport Layer Security (le TLS)

### configuration de Joncteur réseau-side

- Utilisez un déploiement/solution pris en charge
- Sécurité de mode mixte d'utilisation sur CUCM
- Assurez cette confiance d'Expressway et CUCM (le CA qui signe la nécessité des Certificats

de chaque interlocuteur sont de confiance par l'autre interlocuteur)
- Choisissez le meilleur effort comme le mode de chiffrement et le TLS comme transport sur la zone voisine d'Expressway à CUCM (ces valeurs prepopulated automatiquement dans le cas de ligne-side)
- TLS choisi comme transport d'arrivée et sortant sur le profil de Sécurité de joncteur réseau de SIP
- Vérifiez SRTP permis (voyez la déclaration d'attention) sur le joncteur réseau de SIP de CUCM à Expressway
- Vérifiez, et appliquez s'il y a lieu, le script correct de normalisation pour vos versions de CUCM et Expressway

**Attention** : Si vous cochez la case permise par SRTP, Cisco recommande vivement que vous utilisiez un profil chiffré de TLS de sorte que les clés et d'autres informations liées à la sécurité n'obtienne pas exposé pendant les négociations d'appel. Si vous utilisez un profil non-sécurisé, SRTP fonctionnera toujours. Cependant, les clés seront exposées dans la signalisation et les suivis. Dans ce cas, vous devez assurer la Sécurité du réseau entre CUCM et le côté de destination du joncteur réseau.

## Options de chiffrement de medias

### Aucun

On ne permet pas le cryptage. Appelle qui exigent le cryptage devrait échouer parce qu'ils ne peuvent pas être sécurisés. CUCM et Expressway sont cohérents dans la signalisation pour ce cas.

CUCM et Expressway chacun des deux emploient `m=RTP/AVP` afin de décrire les medias dans le SDP. Il n'y a aucun crypto attribut (aucune lignes d'`a=crypto…` dans les sections de medias du SDP).

### Obligatoire

Le cryptage de medias est exigé. Les appels décryptés devraient toujours échouer ; on ne permet aucun retour. CUCM et Expressway sont cohérents dans la signalisation pour ce cas.

CUCM et Expressway chacun des deux emploient `m=RTP/SAVP` afin de décrire les medias dans le SDP. Le SDP a de cryptos attributs (des lignes d'`a=crypto…` dans les sections de medias du SDP).

### Meilleur effort

Appelle qui peut être chiffré sont chiffrés. Si le cryptage ne peut pas être établi, les appels pourraient et devraient retomber aux medias décryptés. CUCM et Expressway sont contradictoires dans ce cas.

Expressway refuse toujours le cryptage si le transport est Protocole TCP (Transmission Control Protocol) ou Protocole UDP (User Datagram Protocol). Vous devez sécuriser le transport entre

CUCM et Expressway si vous voulez le cryptage de medias.

SDP (comme CUCM l'écrit) : Le support chiffré est décrit pendant que des lignes `m=RTP/SAVP` et d'`a=crypto` sont écrites dans le SDP. C'est la signalisation correcte pour le cryptage de medias, mais les cryptos lignes sont accessibles en lecture si le transport n'est pas sécurisé.

Si CUCM voit l'en-tête de x-Cisco-srtp-`retour`, elle permet à l'appel de retomber à décrypté. Si cette en-tête est absente, CUCM suppose que l'appel exige le cryptage (ne permet pas le retour).

En date de X8.2, Expressway fait le meilleur effort la même manière que CUCM fait dans le cas de ligne-side.

SDP (comme Expressway écrit le joncteur réseau-side) : Le support chiffré est décrit pendant que des lignes `m=RTP/AVP` et d'`a=crypto` sont écrites dans le SDP.

Cependant, il y a de deux raison pour laquelle les lignes d'a=crypto pourraient être absentes :

1. Quand un saut de transport à ou du proxy SIP sur Expressway n'est pas sécurisé, le proxy élimine les cryptos lignes afin de les empêcher de l'exposition sur le saut unsecure.
2. L'interlocuteur de réponse élimine les cryptos lignes afin de signaler qu'il ne peut pas ou ne fera pas le cryptage.

L'utilisation du script correct de normalisation de SIP sur CUCM atténue cette question.

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

## Informations connexes

### Lecture relative

- Guide de Sécurité de Cisco Unified Communications Manager, version 10.0(1)
- Conférences optimalisées guide de solution pour de Cisco Unified Communications Manager et de Cisco VCS (version 2.0)
- Cisco Unified Communications Manager avec le guide de déploiement de Cisco Expressway (joncteur réseau de SIP) (pour Cisco Expressway X8.2 et Unified CM 8.6x et 9.x)
- Cisco Unified Communications Manager avec le guide de déploiement de VCS de Cisco (joncteur réseau de SIP) (pour VCS X8.2 de Cisco et Unified CM 8.6.x et 9.x)
- Mobile unifié et Accès à distance de transmissions par l'intermédiaire de guide de déploiement de VCS de Cisco (pour VCS X8.2 de Cisco et Cisco Unified CM 9.1(2)SU1 ou

plus tard)
- Mobile unifié et Accès à distance de transmissions par l'intermédiaire de guide de déploiement de Cisco Expressway (pour Cisco Expressway X8.2 et Cisco Unified CM 9.1(2)SU1 ou plus tard)
- Support et documentation techniques - Cisco Systems

## RFC relatifs

- RFC 3261 SIP : Protocole SIP
- RFC 4566 SDP : Session Description Protocol
- RFC 4568 SDP : Descriptions de Sécurité