# Exemple de configuration de Secure RTP entre CUCM et VCS ou Expressway

## Contenu



## Introduction

Ce document décrit comment configurer un protocole de transport en temps réel (RTP) sécurisé entre Cisco Video Communication Server (VCS) et Cisco Unified Communication Manager (CUCM).

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CUCM
- Cisco VCS ou Cisco Expressway

### Components Used

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

- CUCM
- Cisco VCS ou Cisco Expressway

  **Note**: Cet article utilise les produits Cisco Expressway à des fins d'explication (sauf indication contraire), mais les informations s'appliquent également si votre déploiement utilise Cisco VCS.

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, make sure that you understand the potential impact of any command.

## Informations générales

### Conditions

- Appels SIP (Session Initiation Protocol) routés entre CUCM et Expressway
- Le cryptage des supports est optimisé/facultatif entre Expressway-C et CUCM

### Description

Des difficultés ont été signalées pour la configuration du chiffrement multimédia au mieux pour les appels SIP qui sont acheminés entre CUCM et VCS/Expressway. Une erreur de configuration fréquente affecte la signalisation des supports cryptés, via le protocole SRTP (Secure Real-time Transport Protocol), ce qui entraîne une défaillance des appels chiffrés au mieux lorsque le transport entre CUCM et Expressway n'est pas sécurisé.

Si le transport n'est pas sécurisé, la signalisation de chiffrement du support peut être lue par un écouteur. Dans ce cas, les informations de signalisation de chiffrement du support sont supprimées du protocole SDP (Session Description Protocol). Cependant, il est possible de configurer CUCM pour envoyer (et s'attendre à recevoir) la signalisation de cryptage de support sur une connexion non sécurisée. Vous pouvez contourner cette erreur de configuration de deux manières, selon que les appels sont acheminés côté ligne ou côté ligne vers CUCM.

### Exemples côté ligne et côté ligne

Côté liaison : Une liaison SIP est configurée sur CUCM vers Expressway. Une zone voisine correspondante est configurée sur l'Expressway vers CUCM. Vous avez besoin d'une agrégation si vous souhaitez que les terminaux enregistrés par VCS (Expressway n'est pas un bureau

d’enregistrement, mais VCS l’est) appellent des terminaux enregistrés par CUCM. Un autre exemple serait d'activer l'interconnexion H.323 dans votre déploiement.

Côté ligne : Les appels en ligne sont acheminés directement vers CUCM, et non via une liaison. Si l’enregistrement et le contrôle des appels sont fournis par CUCM, votre déploiement peut ne pas nécessiter de liaison vers Expressway. Par exemple, si Expressway est déployé uniquement pour l’accès mobile et distant (MRA), il proxie les appels en ligne des terminaux externes à CUCM.

### Stratégie d'atténuation

S’il existe une liaison SIP entre CUCM et Expressway, un script de normalisation sur CUCM réécrit le SDP de manière appropriée afin que l’appel de chiffrement au mieux ne soit pas rejeté. Ce script est automatiquement installé avec les versions ultérieures de CUCM, mais si les appels chiffrés au mieux sont rejetés, Cisco vous recommande de télécharger et d'installer le dernier script vcs-interop pour votre version de CUCM.

Si l'appel est acheminé côté ligne vers CUCM, CUCM s'attend à voir l'en-tête `x-cisco-srtp-fallback` si le chiffrement du support est facultatif. Si CUCM ne voit pas cet en-tête, il considère que l'appel est obligatoire pour le chiffrement. La prise en charge de cet en-tête a été ajoutée à Expressway dans la version X8.2. Cisco recommande donc X8.2 ou une version ultérieure pour MRA (collaboration edge).

## Configuration

### Configuration côté ligne

[CUCM]<—best effort—>[Expressway-C]<—obligatoire—>[Expressway-E]<—obligatoire—>[Endpoint]

Afin d’activer le chiffrement au mieux des appels en ligne d’Expressway-C à CUCM :

- Utiliser un déploiement/une solution pris en charge (par exemple, MRA)
- Utiliser la sécurité en mode mixte sur CUCM
- S’assurer que Expressway et CUCM se font mutuellement confiance (l’autorité de certification (AC) qui signe les certificats de chaque partie doit être approuvée par l’autre partie)
- Utiliser la version X8.2 ou ultérieure d’Expressway
- Utiliser des profils téléphoniques sécurisés sur CUCM, avec le mode de sécurité des périphériques défini sur Authentifié ou Crypté - pour ces modes, le type de transport est TLS (Transport Layer Security)

### Configuration côté liaison

- Utiliser un déploiement/une solution pris en charge
- Utiliser la sécurité en mode mixte sur CUCM
- Assurez-vous que Expressway et CUCM se font mutuellement confiance (l’autorité de certification qui signe les certificats de chaque partie doit être approuvée par l’autre partie)

- Choisissez le mode de cryptage au mieux et TLS comme transport sur la zone voisine d’Expressway à CUCM (ces valeurs sont automatiquement préremplies dans le cas de la ligne)
- Sélectionnez TLS comme transport entrant et sortant sur le profil de sécurité de la ligne principale SIP
- Cochez SRTP Allowed (voir l’instruction Caution) sur la liaison SIP de CUCM à Expressway
- Recherchez et appliquez le cas échéant le script de normalisation correct pour vos versions de CUCM et d’Expressway

  **Attention** : Si vous cochez la case SRTP Allowed (SRTP autorisé), Cisco vous recommande vivement d'utiliser un profil TLS chiffré afin que les clés et autres informations liées à la sécurité ne soient pas exposées lors des négociations d'appel. Si vous utilisez un profil non sécurisé, SRTP fonctionne toujours. Cependant, les clés seront exposées dans la signalisation et les traces. Dans ce cas, vous devez garantir la sécurité du réseau entre CUCM et le côté de destination de la liaison.

## Options de cryptage de support

### Aucune

Le chiffrement n'est pas autorisé. Les appels nécessitant un chiffrement doivent échouer car ils ne peuvent pas être sécurisés. CUCM et Expressway sont cohérents dans la signalisation de ce cas.

CUCM et Expressway utilisent tous deux `m=RTP/AVP` afin de décrire le support dans le SDP. Il n'y a aucun attribut de chiffrement (no `a=crypto...` dans les sections média du SDP).

### Obligatoire

Le chiffrement du support est requis. Les appels non chiffrés doivent toujours échouer ; aucun secours n'est autorisé. CUCM et Expressway sont cohérents dans la signalisation de ce cas.

CUCM et Expressway utilisent tous deux `m=RTP/SAVP` afin de décrire le support dans le SDP. Le SDP possède des attributs de chiffrement (`a=crypto...` dans les sections média du SDP).

### Meilleur effort

Les appels qui peuvent être chiffrés sont chiffrés. Si le chiffrement ne peut pas être établi, les appels peuvent et doivent revenir à des supports non chiffrés. CUCM et Expressway sont incohérents dans ce cas.

Expressway refuse toujours le chiffrement si le transport est TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol). Vous devez sécuriser le transport entre CUCM et Expressway si vous voulez un chiffrement multimédia.

SDP (comme l'écrit CUCM) : Les supports cryptés sont décrits comme `m=RTP/SAVP` et `a=crypto` lignes sont écrites dans le SDP. Il s'agit de la signalisation correcte pour le chiffrement des

supports, mais les lignes de chiffrement sont lisibles si le transport n'est pas sécurisé.

Si CUCM voit l'en-tête `x-cisco-srtp-fallback`, il permet à l'appel de revenir à un appel non chiffré. Si cet en-tête est absent, CUCM suppose que l'appel nécessite un chiffrement (ne permet pas le retour arrière).

Depuis X8.2, Expressway fait le meilleur effort de la même manière que CUCM dans le cas de ligne.

SDP (comme Expressway écrit trunk side) : Les supports cryptés sont décrits comme `m=RTP/AVP` et `a=crypto` lignes sont écrites dans le SDP.

Cependant, il y a deux raisons pour lesquelles les lignes a=crypto peuvent être absentes :

1. Lorsqu'un saut de transport vers ou depuis le proxy SIP sur l'Expressway n'est pas sécurisé, le proxy supprime les lignes de chiffrement afin de les empêcher d'être exposés au saut non sécurisé.
2. La personne qui répond supprime les lignes de chiffrement afin de signaler qu'elle ne peut pas ou ne veut pas procéder au chiffrement.

L'utilisation du script de normalisation SIP correct sur CUCM atténue ce problème.

# Vérification

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

# Dépannage

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

# Informations connexes

### Lecture associée

- Guide de sécurité de Cisco Unified Communications Manager, version 10.0(1)
- Guide des solutions de conférence optimisée pour Cisco Unified Communications Manager et Cisco VCS (version 2.0)
- Guide de déploiement de Cisco Unified Communications Manager avec Cisco Expressway (SIP Trunk) (pour Cisco Expressway X8.2 et Unified CM 8.6x et 9.x)
- Guide de déploiement de Cisco Unified Communications Manager avec Cisco VCS (SIP Trunk) (pour Cisco VCS X8.2 et Unified CM 8.6.x et 9.x)
- Unified Communications Mobile and Remote Access via Cisco VCS Deployment Guide (pour Cisco VCS X8.2 et Cisco Unified CM 9.1(2)SU1 ou version ultérieure)
- Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide (pour Cisco Expressway X8.2 et Cisco Unified CM 9.1(2)SU1 ou version ultérieure)

- Support et documentation techniques - Cisco Systems

## RFC associés

- SIP RFC 3261 : Protocole d'ouverture de session
- SDP RFC 4566 : Protocole de description de session
- SDP RFC 4568 : Description de la sécurité