Cisco Jabber et SIP OAuth Mode

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Restriction
- Informations générales
  - Principaux avantages
  - Architecture globale
- Configuration - Jabber sur site
  - 1. Configurez les connexions d'actualisation.
  - 2. Configurez les ports OAuth.
  - 3. Activez le mode SIP OAuth.
  - 4. Redémarrez le service Cisco CallManager.
  - 5. Configurez le support OAuth dans le profil de sécurité.
- Configuration - Jabber sur MRA
  - Conditions préalables
  - Étape 1 : activation de l'option Refresh Login sur MRA
  - Étape 2 : actualisation des noeuds Unified CM dans Expressway-C
  - Étape 3 : configuration de la prise en charge OAuth dans le profil de sécurité
- Vérifier
  - 1. Vérifiez si le mode SIP OAuth est activé globalement.
  - 2. Vérifiez que les entrées SAN d'Expressway-C ont été correctement transmises à CUCM.
  - 3. Vérifiez la ou les zones CEOAuth sur Expressway-C.
  - 4. Vérifiez que le processus CallManager écoute les ports SIP OAuth.
- Dépannage
  - Exemple de journal Jabber (sur site)
  - Scénario 1 - Non-concordance du port d'enregistrement OAuth SIP
  - Scénario 2 - CA inconnue d'Expressway
  - Scénario 3 - Autorité de certification inconnue de UCM

Introduction

Ce document décrit la configuration et les étapes de dépannage de base pour mettre en oeuvre le mode SIP OAuth avec Cisco Jabber.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Inscription au téléphone logiciel Jabber
- Unified Communications Manager (UCM)
- Solution d'accès mobile et distant (MRA)

Composants utilisés

Version logicielle minimale pour la prise en charge du mode SIP OAuth :

- Cisco UCM 12.5
- Cisco Jabber 12.5
- Cisco Expressway X12.5

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Restriction

Lorsque le mode SIP OAuth est activé, les options Enable Digest Authentication et TFTP Encrypted Config ne sont pas prises en charge.

Informations générales

Principaux avantages

La sécurisation de la signalisation SIP et des supports pour le téléphone logiciel Cisco Jabber implique actuellement plusieurs étapes de configuration. Le plus difficile est d'installer et de renouveler les certificats clients (LSC), en particulier si un périphérique Cisco Jabber passe d'un site à un site hors site, et de maintenir à jour les certificats contenus dans le fichier CTL.

Le mode SIP OAuth permet au téléphone logiciel Cisco Jabber d'utiliser des jetons autodescriptifs OAuth au lieu du certificat LSC client pour l'authentification sur l'interface SIP sécurisée. La prise en charge d'OAuth sur l'interface SIP UCM permet une signalisation et des supports sécurisés pour les déploiements Jabber sur site et MRA sans nécessiter le mode mixte ou le fonctionnement CAPF.

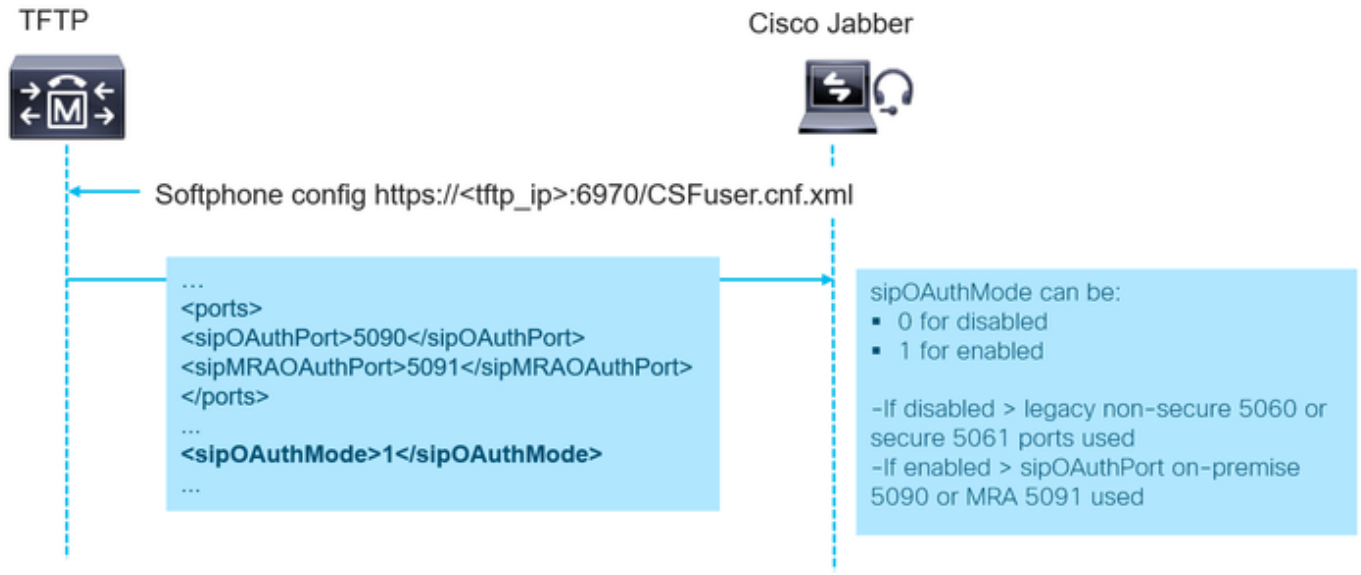
Principaux avantages du mode SIP OAuth pour Cisco Jabber :

- Active le cryptage permanent sans charge administrative supplémentaire.
- Signalisation et support sécurisés pour Cisco Jabber sans avoir recours au mode mixte (pas de mises à jour CTL, maintenance des certificats, etc.)
- Inutile d'installer et de gérer le contrôleur LSC sur les clients Jabber.
    - Défis posés par la technologie LSC sur plusieurs périphériques (ordinateurs

portables/périphériques mobiles..)
- Le fonctionnement CAPF nécessite l'installation de Jabber à tout moment sur un nouveau périphérique.
- Opération CAPF non prise en charge sur MRA.

Architecture globale

Le périphérique Cisco Jabber reconnaît que l'authentification OAuth est activée sur l'interface SIP en analysant le fichier de configuration CSF (http://<cucmIP>:6970/<CSF-device-name>.cnf.xml), exemple de fichier de configuration (certaines lignes sont omises pour des raisons de concision) :



Cisco Jabber lit le paramètre sipOAuthMode pour déterminer si le mode SIP OAuth est activé ou non. Ce paramètre peut prendre l'une des valeurs suivantes :

- 0 - SIP OAuth est désactivé
- 1 - SIP OAuth est activé

Si le mode SIP OAuth est activé, Jabber utilise l'un de ces paramètres pour déterminer le port pour la connexion SIP TLS : sipOAuthPort pour les déploiements sur site ou sipMRAOAuthPort pour les déploiements basés sur MRA. L'exemple présente les valeurs par défaut - sipOAuthPort 5090 et sipMAROAuthPort 5091. Ces valeurs sont configurables et peuvent être différentes sur chaque noeud CUCM.

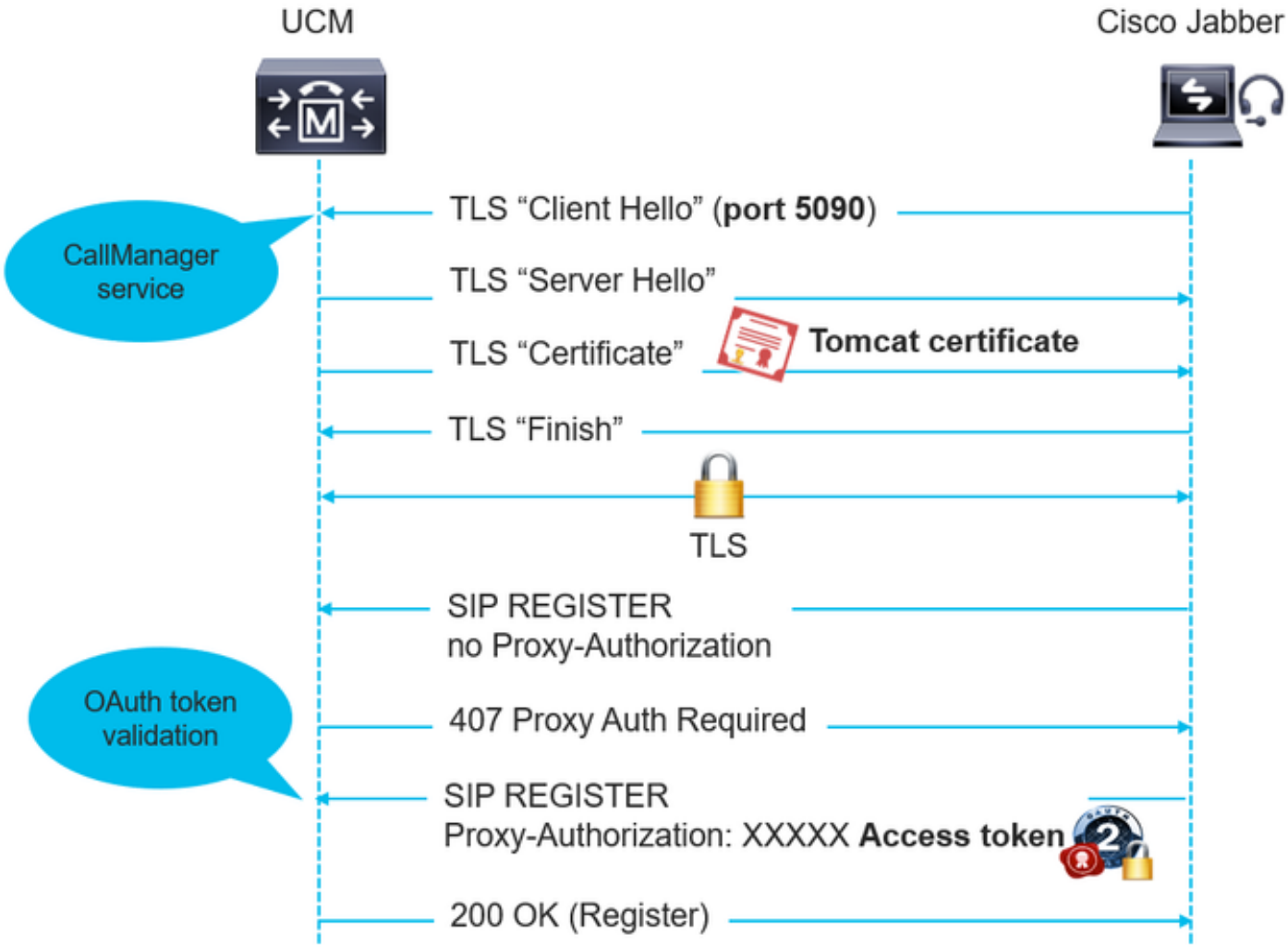
Si le mode SIP OAuth est désactivé, Jabber utilise des ports hérités non sécurisés (5060) ou sécurisés (5061) pour l'enregistrement SIP.

Remarque : Cisco UCM utilise le port OAuth (5090) du téléphone SIP pour écouter l'enregistrement de la ligne SIP à partir des périphériques Jabber OnPremise sur TLS. Cependant, UCM utilise le port d'accès à distance mobile SIP (5091 par défaut) pour écouter les enregistrements de ligne SIP de Jabber sur Expressway via mLTS. Ces deux ports sont configurables. Reportez-vous à la section Configuration.

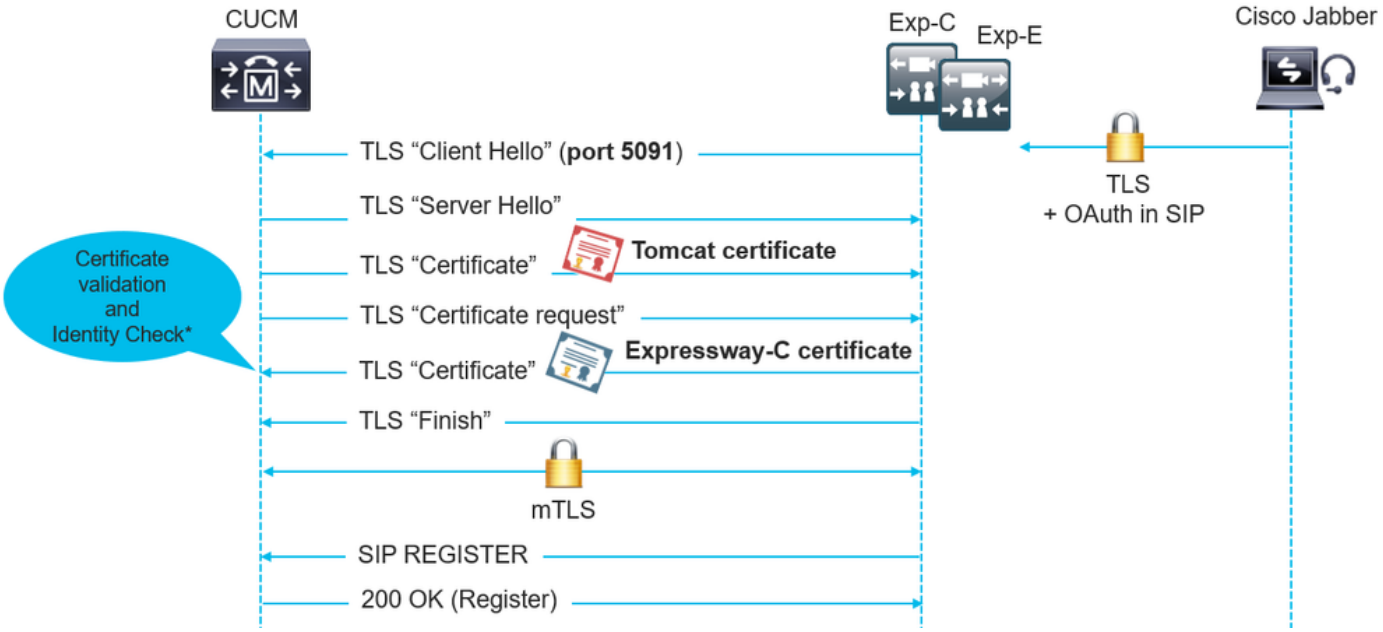
Le service CallManager écoute à la fois sipOAuthPort et sipMRAOAuthPort. Cependant, les deux ports utilisent le certificat Tomcat et Tomcat-trust pour les connexions TLS/mTLS entrantes. Assurez-vous que votre magasin Tomcat-trust est en mesure de vérifier le certificat Expressway-C pour le mode SIP OAuth pour que MRA fonctionne correctement.

Dans certains cas, lorsque le certificat Tomcat est régénéré, le processus CallManager doit également être redémarré sur les noeuds affectés. Cela est nécessaire pour que le processus CCM charge et utilise de nouveaux certificats sur les ports sipOAuth.

Cette image représente l'enregistrement de Cisco Jabber lors de ses déplacements :



Cette image représente l'enregistrement de Cisco Jabber sur MRA :



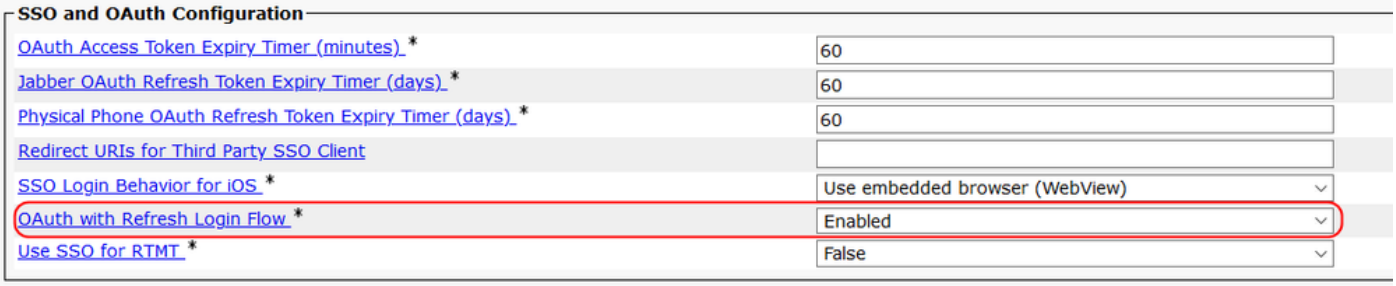
*Les noeuds Expressway-C utilisent l'API AXL pour informer UCM du CN/SAN dans leur certificat. UCM utilise ces informations pour valider le certificat Exp-C lorsqu'une connexion TLS mutuelle est établie.

Configuration - Jabber sur site

Remarque :
Assurez-vous que vous avez effectué les points ci-dessous avant de configurer le mode SIP OAuth :
- MRA est configuré et la connexion est établie entre Unified Communication Manager (UCM) et Expressway (applicable uniquement si MRA est utilisé).
- UCM est enregistré sur un compte Smart ou virtuel avec une fonctionnalité d'exportation contrôlée.

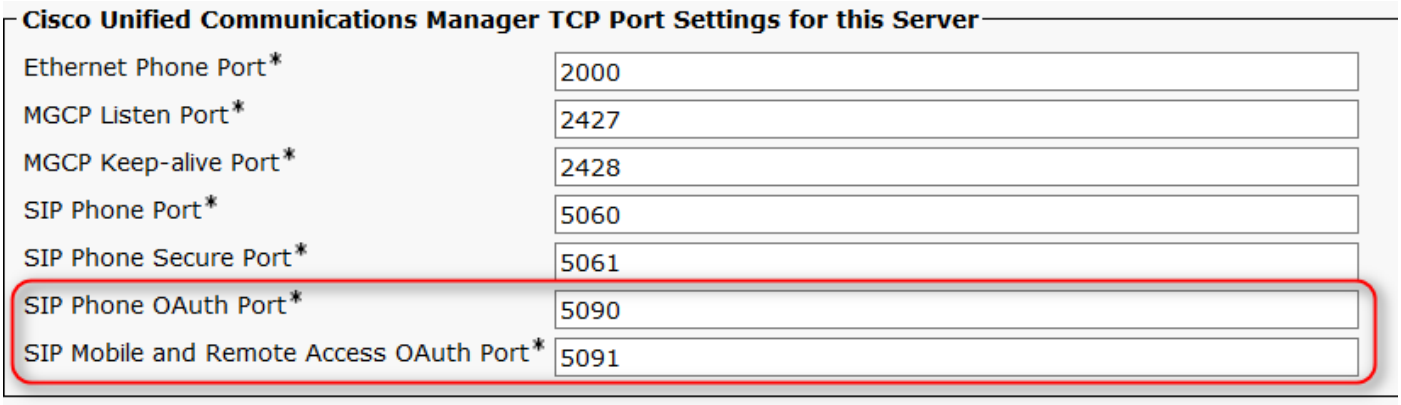
1. Configurez les connexions d'actualisation.

Configurez les connexions d'actualisation avec des jetons d'accès OAuth et actualisez les jetons pour les clients Cisco Jabber. Dans Cisco Unified CM Administration, sélectionnez Système > Paramètres d'entreprise.



2. Configurez les ports OAuth.

Choisissez System > Cisco Unified CM. Il s'agit d'une étape facultative. L'image présente les valeurs par défaut. La plage configurable acceptable est comprise entre 1024 et 49151. Répétez la même procédure pour chaque serveur.



3. Activez le mode SIP OAuth.

Utilisez l'interface de ligne de commande du serveur de publication pour activer le mode SIP OAuth globalement. Exécutez la commande : utils sipOAuth-mode enable.

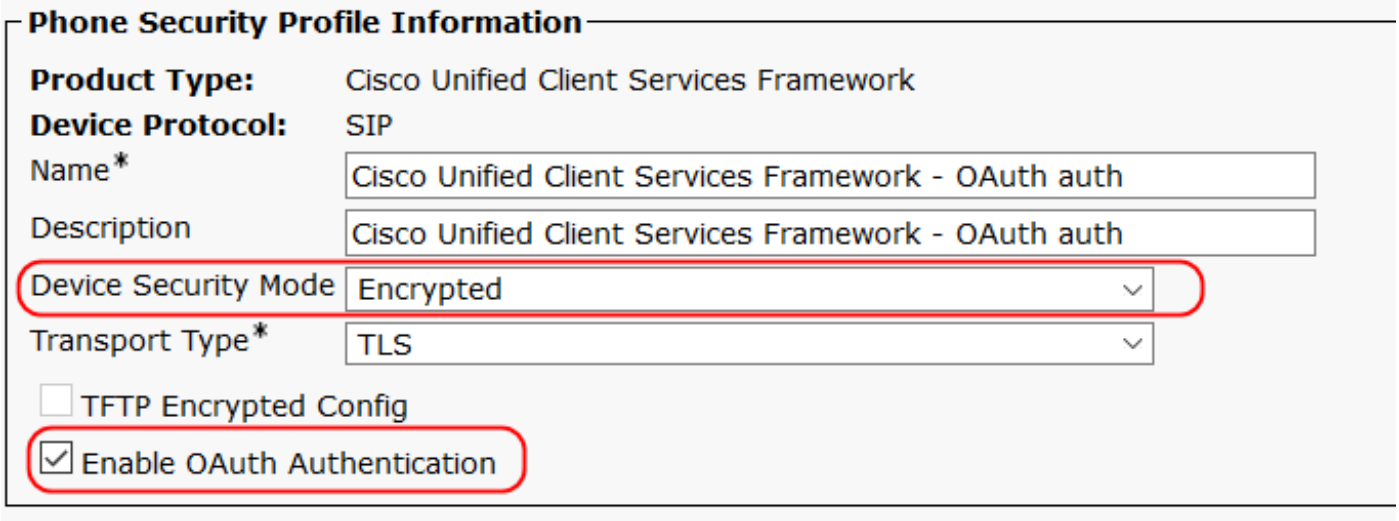
```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

4. Redémarrez le service Cisco CallManager.

Dans Cisco Unified Serviceability, choisissez Tools > Control Center - Feature Services. Sélectionnez et redémarrez le service Cisco CallManager sur tous les noeuds où le service est actif.

5. Configurez le support OAuth dans le profil de sécurité.

Dans Cisco Unified CM Administration, sélectionnez System > Phone Security Profile. Sélectionnez Enable OAuth Authentication pour activer la prise en charge SIP OAuth pour le terminal.



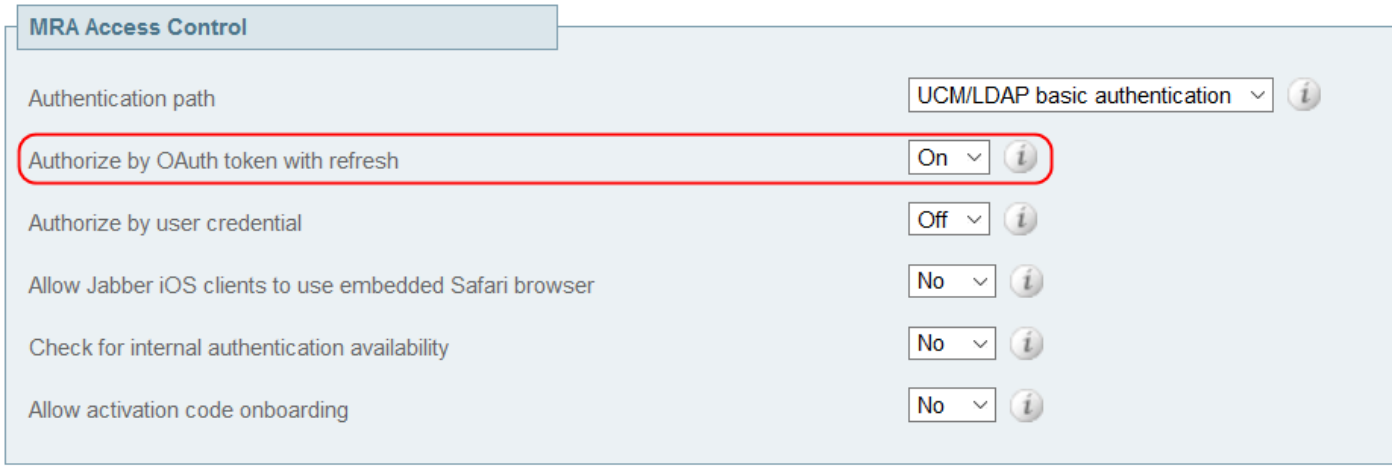
Configuration - Jabber sur MRA

Conditions préalables

Avant de configurer le mode SIP OAuth pour Jabber sur MRA, suivez les étapes 1 à 4 du chapitre Configuration - Jabber On Premises de cet article.

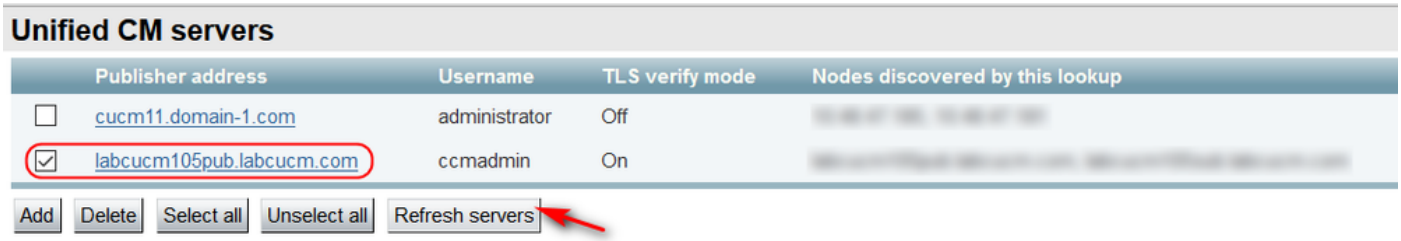
Étape 1 : activation de l'option Refresh Login sur MRA

Les connexions d'actualisation doivent être activées sur Expressway (également appelées jetons autodescriptifs) avant la configuration de l'authentification SIP OAuth avec Cisco Jabber sur MRA. Sur Expressway-C, accédez à Configuration > Unified Communications > Configuration et vérifiez que le paramètre Authorize by OAuth Token with refresh est activé.



Étape 2 : actualisation des noeuds Unified CM dans Expressway-C

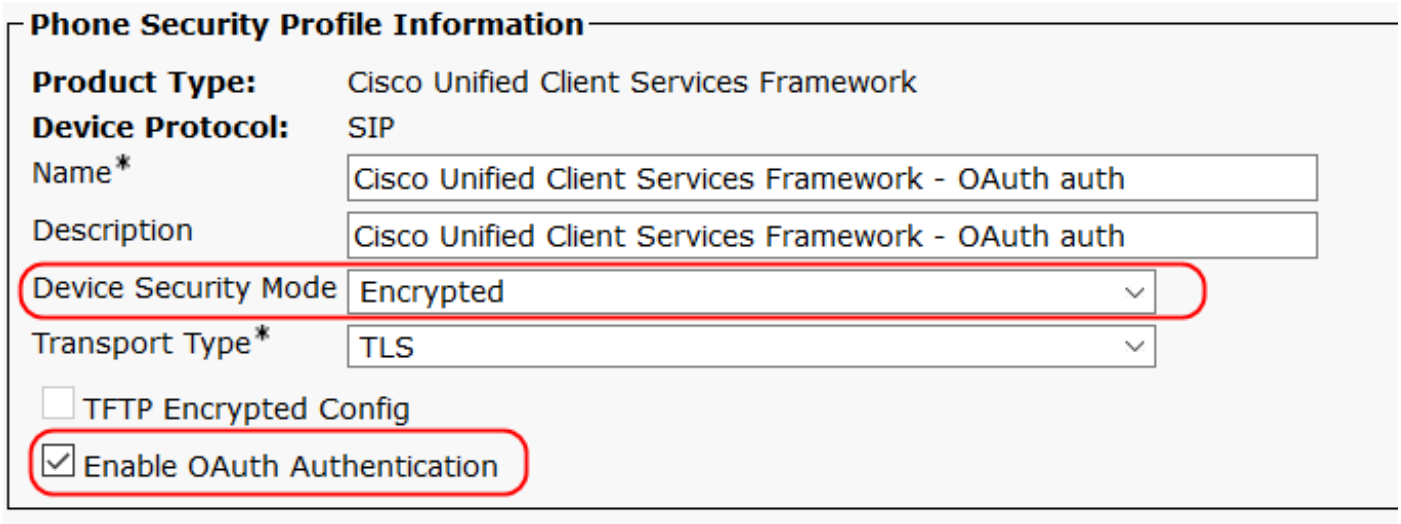
Accédez à Configuration > Unified Communications > Unified CM servers. Découvrir ou actualiser les noeuds Unified CM dans Expressway-C.



Remarque : Une nouvelle zone CEOAuth (TLS) est créée automatiquement dans Expressway-C. Par exemple, CEOAuth <nom Unified CM>. Une règle de recherche est créée pour envoyer par proxy les requêtes SIP provenant de Jabber sur MRA vers le noeud Unified CM. Cette zone utilise des connexions TLS, que Unified CM soit configuré ou non en mode mixte. Pour établir la confiance, Expressway-C envoie également les détails du nom d'hôte et du nom alternatif de l'objet (SAN) au cluster Unified CM. Reportez-vous à la partie vérification de cet article pour vous assurer que la configuration appropriée est en place.

Étape 3 : configuration de la prise en charge OAuth dans le profil de sécurité

Dans Cisco Unified CM Administration, sélectionnez System > Phone Security Profile. Activez la prise en charge OAuth sur le profil attribué à Cisco Jabber.



Vérifier

1. Vérifiez si le mode SIP OAuth est activé globalement.

Vérifiez le mode OAuth à partir de Cisco Unified CM Administration, choisissez System > Enterprise Parameters.



Vous pouvez également utiliser la commande Admin CLI - Run the command: run sql select

paramvalue FROM process config WHERE paramname = 'ClusterSIPOAuthMode'

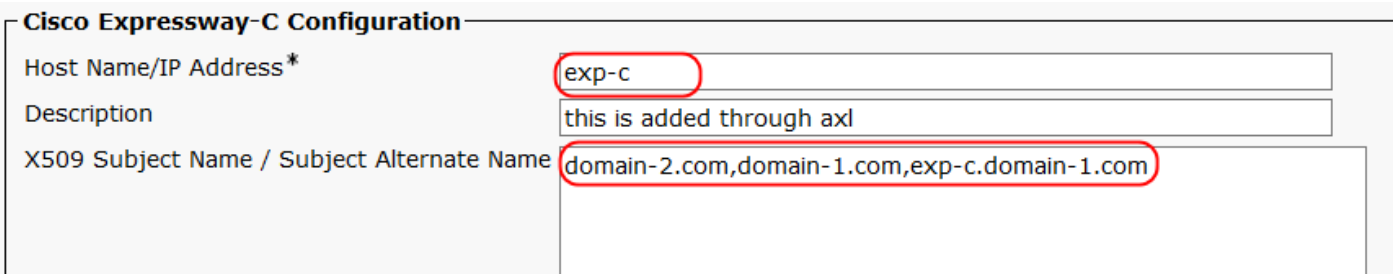
```
admin:run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'
paramvalue
==========
1
admin:
```

Valeurs possibles : 0 - pour Désactivé (par défaut), 1 - pour Activé.

2. Vérifiez que les entrées SAN d'Expressway-C ont été correctement transmises à CUCM.

Expressway-C envoie les détails CN/SAN de son certificat à UCM via AXL. Ces détails sont enregistrés dans la table expresswaycconfiguration. Ce processus est appelé chaque fois que vous détectez ou actualisez les noeuds Unified CM dans Expressway-C. Ces entrées sont utilisées pour établir la confiance entre UCM et Expressway-C. Le champ CN/SAN du certificat Expressway-C est comparé à ces entrées pendant la connexion MTLS au port SIP MRA OAuth (5091 par défaut). Si la vérification échoue, la connexion MTLS échoue.

Vérifiez les entrées de Cisco Unified CM Administration, choisissez Device > Expressway-C (disponible à partir de UCM 12.5.1Su1)



Vous pouvez également utiliser la commande Admin CLI - Run the command: run sql select * from expresswaycconfiguration

```
admin:run sql select * from expresswaycconfiguration
pkid                                 hostnameorip description              x509subjectnameoraltname
==================================== ============ ======================== ========================================================
d5fd15d5-b049-c5b5-0197-bd11a5641640 exp-c        this is added through axl domain-2.com,secure-phone-profile,domain-1.com,exp-c.domain-1.com
admin:
```

3. Vérifiez la ou les zones CEOAuth sur Expressway-C.

Accédez à Expressway-C > Configuration > Zones > Zones. Assurez-vous que toutes les zones CEOAuth nouvellement créées sont à l'état actif.



4. Vérifiez que le processus CallManager écoute les ports SIP OAuth.

Exécutez la commande à partir de l'interface de ligne de commande Admin : show open ports regexp 5090 (port SIP OAuth par défaut)

```
admin:show open ports regexp 5090

Executing.. please wait.
ccm       30622    ccmbase  364u  IPv4  207160      0t0  TCP 10.48.[redacted]:5090 (LISTEN)
```

Exécutez la commande à partir de l'interface de ligne de commande Admin : show open ports regexp 5091 (port SIP MRA OAuth par défaut)

```
admin:show open ports regexp 5091

Executing.. please wait.
ccm       30622    ccmbase  351u  IPv4  207155      0t0  TCP 10.48.[redacted]:5091 (LISTEN)
```

Dépannage

Exemple de journal Jabber (sur site)

Exemple de journal pour l'enregistrement SIP OAuth sur le port 5090 du point de vue du journal Jabber.

CSF configuration retrieved 2020-03-30 13:03:18,278 DEBUG [0x000012d8] [src\callcontrol\ServicesManager.cpp(993)] [csf.ecc] [csf::ecc::ServicesManager::fetchDeviceConfig] - fetchDeviceConfig() retrieved config for CSFrado 2020-03-30 13:03:18,278 DEBUG [0x000012d8] [rc\callcontrol\ServicesManager.cpp(1003)] [csf.ecc] [csf::ecc::ServicesManager::fetchDeviceConfig] - Device Config:

10.10.10.1

ccm12pub

2000

5060

5061

5090

5091

…

1
Setting SIP oauth mode to 1 2020-03-30 13:03:18,747 DEBUG [0x00002968] [ig\CertificateVerificationHelper.cpp(35)] [csf.ecc] [csf::ecc::CertificateVerificationHelper::setSipOauthMode] - sip OAuth Mode=1 ## Setting OAuth ports (5090 and 5091) for each UCM server 13:03:19,013 INFO [0x00002484] [\core\ccapp\config\config_parser.c(1491)] [csf.sip-call-control] [config_process_ccm_properties] - ccm0=10.10.10.1 ccm1=10.10.10.2 ccm2= sip_oauth_port_0=5090 sip_oauth_port_1=5090 sip_oauth_port_2=5090 length=0 13:03:19,013 INFO [0x00002484] [\core\ccapp\config\config_parser.c(1494)] [csf.sip-call-control] [config_process_ccm_properties] - sip_mar_oauth_port_0=5091 sip_mar_oauth_port_1=5091 sip_mar_oauth_port_2=5091 ## Open TLS connection to 5090 2020-03-30 13:03:18,528 DEBUG [0x00000e2c] [sipstack\sip_transport_connection.c(431)] [csf.sip-call-control] [sip_create_transport_connection] - [SIP][CONN][0] create TLS connection 10.10.10.10:5061-----10.10.10.1:5090. ## Sending register message 2020-03-30 13:03:19,200 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-sent---> REGISTER sip:10.10.10.1 SIP/2.0 Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00001188 From:

;tag=8823234512340890000003bdd-00005eff To:

Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Max-Forwards: 70 Date: Mon, 30 Mar 2020 11:03:19 GMT CSeq: 2270 REGISTER User-Agent: Cisco-CSF Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-config,X-cisco-sis-7.0.0,X-cisco-xsi-8.5.1,X-cisco-graceful-reg,X-cisco-duplicate-reg ## 407 Proxy Authentication Required 2020-03-30 13:03:19,310 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-recv<--- SIP/2.0 407 Proxy Authentication Required Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00001188 From:

;tag=8823234512340890000003bdd-00005eff To:

;tag=441122775 Date: Mon, 30 Mar 2020 11:03:31 GMT Call-ID: 88232345-12340017-

00001c0b-00000cfa@10.10.10.10 Server: Cisco-CUCM12.5 CSeq: 2270 REGISTER Proxy-Authenticate: Bearer realm="ccmsipline" Content-Length: 0 ## Register with OAuth token included in the Proxy-Authorization header 2020-03-30 13:03:19,310 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-sent---> REGISTER sip:10.10.10.1 SIP/2.0 Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00004a82 From:

;tag=882323451234089000003bdd-00005eff To:

Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Max-Forwards: 70 Date: Mon, 30 Mar 2020 11:03:19 GMT CSeq: 2271 REGISTER User-Agent: Cisco-CSF Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video Proxy-Authorization: Bearer token="

" Supported: replaces,join,sdp-anat,norefersub,resource-priority,extended-refer,X-cisco-callinfo,X-cisco-serviceuri,X-cisco-escapecodes,X-cisco-service-control,X-cisco-srtp-fallback,X-cisco-monrec,X-cisco-config,X-cisco-sis-7.0.0,X-cisco-xsi-8.5.1,X-cisco-graceful-reg,X-cisco-duplicate-reg Reason: SIP;cause=200;text="cisco-alarm:111 Name=CSFrado ActiveLoad=Jabber_for_Windows-12.8.0.51973 InactiveLoad=Jabber_for_Windows-12.8.0.51973 Last=Application-Requested-Destroy" Expires: 3600 Content-Type: multipart/mixed; boundary=uniqueBoundary Mime-Version: 1.0 Content-Length: 1271 # 200 OK for Register 2020-03-30 13:03:19,325 DEBUG [0x00000e2c] [\sipcc\core\sipstack\ccsip_debug.c(1041)] [csf.sip-call-control] [platform_print_sip_msg] - sipio-recv<--- SIP/2.0 200 OK Via: SIP/2.0/TLS 10.10.10.10:62162;branch=z9hG4bK00004a82 From:

;tag=882323451234089000003bdd-00005eff To:

;tag=1915868308 Date: Mon, 30 Mar 2020 11:03:31 GMT Call-ID: 88232345-12340017-00001c0b-00000cfa@10.10.10.10 Server: Cisco-CUCM12.5 CSeq: 2271 REGISTER Expires: 120 Contact:

;+sip.instance="

";+u.sip!devicename.ccm.cisco.com="CSFrado";+u.sip!model.ccm.cisco.com="503";video;x-cisco-newreg Supported: X-cisco-srtp-fallback,X-cisco-sis-9.1.0 Content-Type: application/x-c

Scénario 1 - Non-concordance du port d'enregistrement OAuth SIP

Le périphérique Jabber sur site en mode SIP OAuth ne parvient pas à s'enregistrer auprès d'UCM. UCM envoie 403 pour le message Register :

SIP/2.0 403 Forbidden Via: SIP/2.0/TLS 10.5.10.121:50347;branch=z9hG4bK00005163 From:

;tag=005056867e66010a00006698-00002a32 To:

;tag=1946377502 Date: Fri, 03 Aug 2018 05:00:18 GMT Call-ID: 00505686-7e660005-0000216b-0000366f@10.5.10.121 Server: Cisco-CUCM12.5 CSeq: 363 REGISTER Retry-After: 35 Warning: 399 UCM2-PUB "SIP OAuth Registration port Mismatch" Content-Length: 0

Solution possible : Assurez-vous que les conditions suivantes sont remplies :

- Le mode OAuth est globalement activé
- La prise en charge OAuth est activée sur le profil de sécurité du périphérique associé
- Message reçu sur le port 5090 via TLS au lieu de mTLS

Scénario 2 - CA inconnue d’Expressway

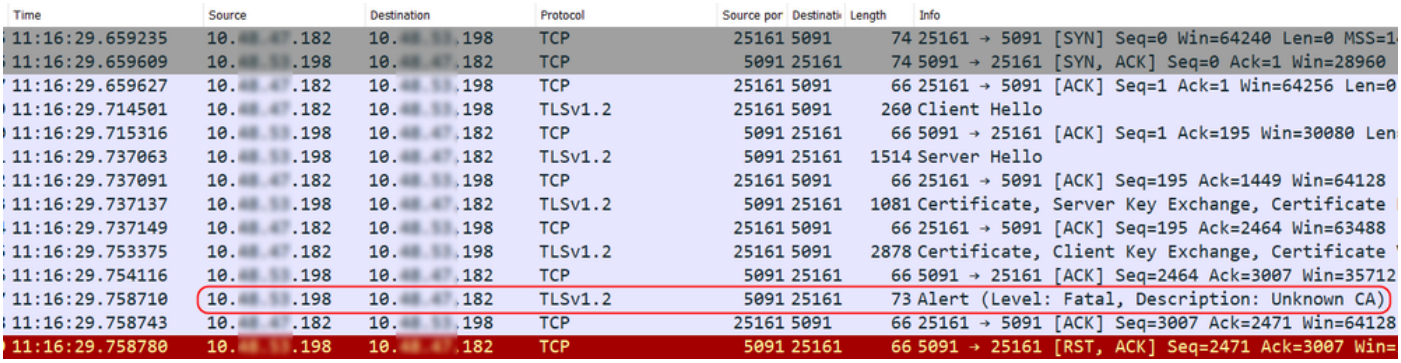
Expressway-C ne parvient pas à établir la connexion mTLS avec UCM sur sipMAROAuthport (valeur par défaut 5091). Expressway-C ne fait pas confiance au certificat partagé par UCM et répond avec le message Unknown CA pendant la configuration de mTLS.

Solution possible : Le service CallManager envoie son certificat Tomcat lors de la connexion mTLS. Assurez-vous que votre Expressway-C fait confiance au signataire du certificat Tomcat d’UCM.

Scénario 3 - Autorité de certification inconnue de UCM

Expressway-C ne parvient pas à établir la connexion mTLS avec UCM sur sipMAROAuthport (valeur par défaut 5091). UCM ne fait pas confiance au certificat partagé par Expressway et répond avec le message Unknown CA pendant la configuration de mTLS.

Capture de paquets de cette communication (UCM 10.x.x.198, Expressway-C 10.x.x.182) :



Time	Source	Destination	Protocol	Source por	Destinati	Length	Info
11:16:29.659235	10.[redacted].182	10.[redacted].198	TCP	25161	5091	74	25161 → 5091 [SYN] Seq=0 Win=64240 Len=0 MSS=1
11:16:29.659609	10.[redacted].198	10.[redacted].182	TCP	5091	25161	74	5091 → 25161 [SYN, ACK] Seq=0 Ack=1 Win=28960
11:16:29.659627	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=1 Ack=1 Win=64256 Len=0
11:16:29.714501	10.[redacted].182	10.[redacted].198	TLSv1.2	25161	5091	260	Client Hello
11:16:29.715316	10.[redacted].198	10.[redacted].182	TCP	5091	25161	66	5091 → 25161 [ACK] Seq=1 Ack=195 Win=30080 Len
11:16:29.737063	10.[redacted].198	10.[redacted].182	TLSv1.2	5091	25161	1514	Server Hello
11:16:29.737091	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=195 Ack=1449 Win=64128
11:16:29.737137	10.[redacted].198	10.[redacted].182	TLSv1.2	5091	25161	1081	Certificate, Server Key Exchange, Certificate
11:16:29.737149	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=195 Ack=2464 Win=63488
11:16:29.753375	10.[redacted].182	10.[redacted].198	TLSv1.2	25161	5091	2878	Certificate, Client Key Exchange, Certificate
11:16:29.754116	10.[redacted].198	10.[redacted].182	TCP	5091	25161	66	5091 → 25161 [ACK] Seq=2464 Ack=3007 Win=35712
11:16:29.758710	10.[redacted].198	10.[redacted].182	TLSv1.2	5091	25161	73	Alert (Level: Fatal, Description: Unknown CA)
11:16:29.758743	10.[redacted].182	10.[redacted].198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=3007 Ack=2471 Win=64128
11:16:29.758780	10.[redacted].198	10.[redacted].182	TCP	5091	25161	66	5091 → 25161 [RST, ACK] Seq=2471 Ack=3007 Win=

Solution possible : UCM utilise le magasin Tomcat-trust pour vérifier les certificats entrants lors de la connexion mTLS sur les ports SIP OAuth. Assurez-vous que le certificat du signataire pour Expressway-C est correctement téléchargé sur l'UCM.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.