

Cisco Jabber en SIP OAuth-modus

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[beperking](#)

[Achtergrondinformatie](#)

[Belangrijkste voordelen](#)

[Algemene architectuur](#)

[Configuratie - Jabber on premises](#)

[1. Aanmeldingen voor vernieuwen configureren.](#)

[2. Configureer OAuth-poorten.](#)

[3. Schakel de SIP Outh-modus in.](#)

[4. Start Cisco CallManager Service opnieuw.](#)

[5. Configureer OAuth Support in het beveiligingsprofiel.](#)

[Configuratie - Jabber over MRA](#)

[voorwaarden](#)

[Stap 1. Inloggen bij Vernieuwen inschakelen via MRA.](#)

[Stap 2. Vernieuw de Unified CM Nodes in Expressway-C.](#)

[Stap 3. Configureer de OAuth-ondersteuning in het beveiligingsprofiel.](#)

[Verifiëren](#)

[1. Controleer of de SIP OAuth-modus wereldwijd is ingeschakeld.](#)

[2. Verifieer dat expressway-C SAN-items succesvol naar CUCM zijn gepusht.](#)

[3. Controleer CEOAuth Zone\(s\) op Expressway-C.](#)

[4. Controleren van de procesbeluisteringen van CallManager op SIP OAuth-poorten.](#)

[Problemen oplossen](#)

[Voorbeeld van Jabber-logboek \(on-premises\)](#)

[Scenario 1 - Mismatch SIP OAuth-registratiepoort](#)

[Scenario 2 - Onbekende CA van Expressway](#)

[Scenario 3 - Onbekende CA van UCM](#)

Inleiding

In dit document worden de stappen beschreven voor configuratie en probleemoplossing voor de implementatie van de SIP OAuth-modus met Cisco Jabber.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Jabber softphone registratie
- Unified Communications Manager (UCM)
- Mobile and Remote Access (MRA)-oplossing

Gebruikte componenten

Minimale softwareversie ter ondersteuning van de SIP OAuth-modus:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

beperking

Als de SIP OAuth-modus is ingeschakeld, worden de opties Digest-verificatie en Gecodeerde TFTP-configuratie niet ondersteund.

Achtergrondinformatie

Belangrijkste voordelen

Het beveiligen van SIP-signalering en media voor de Cisco Jabber-softphone omvat momenteel meerdere configuratiestappen. Het moeilijkst is om clientcertificaten (LSC's) te installeren en te vernieuwen, vooral als een Cisco Jabber-apparaat schakelt tussen on-premises en off-premises, en de certificaten in het CTL-bestand up-to-date te houden.

Met de SIP OAuth-modus kan Cisco Jabber Softphone OAuth-zelfbeschrijvende tokens gebruiken in plaats van client LSC-certificaat voor verificatie op een beveiligde SIP-interface. De ondersteuning van OAuth op de UCM SIP-interface maakt veilige signaling en media voor Jabber on-premises en MRA-implementaties mogelijk zonder de noodzaak van de gemengde modus of CAPF-werking.

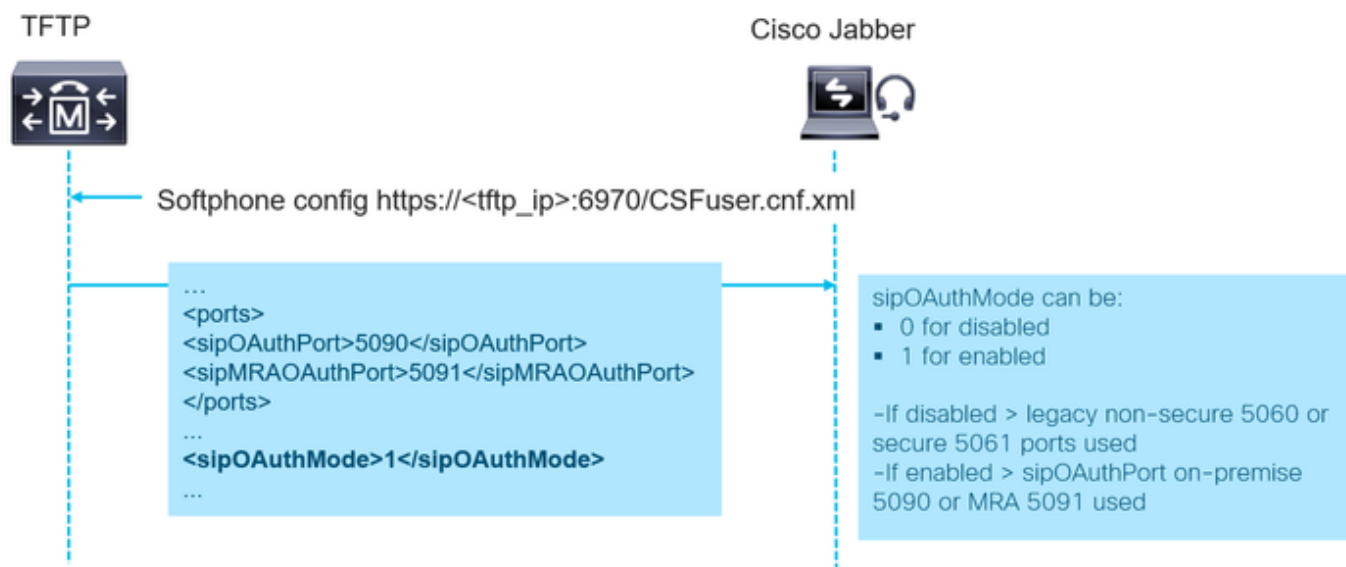
Belangrijkste voordelen van de ondersteuning voor de SIP OAuth-modus voor Cisco Jabber:

- Maakt always-on encryptie mogelijk zonder extra admin belasting.
- Beveiligde signaling en media voor Cisco Jabber zonder de noodzaak van de gemengde modus (geen CTL-updates, onderhoudscertificaten, enzovoort)
- Het is niet nodig om de LSC op Jabber-clients te installeren en te onderhouden.

- Uitdagingen met LSC op meerdere apparaten (laptops/mobiele apparaten..)
- CAPF-werking is vereist wanneer Jabber op een nieuw apparaat is geïnstalleerd.
- CAPF-bewerking wordt niet ondersteund via MRA.

Algemene architectuur

Cisco Jabber-apparaat herkent dat de OAuth-verificatie is ingeschakeld op de SIP-interface door het CSV-configuratiebestand te parseren (<http://<cucmIP>:6970/<CSF-device-name>.cnf.xml>), configuratiebestand (sommige regels zijn weggelaten voor beknoptheid):



Cisco Jabber leest de parameter sipOAuthMode om te bepalen of de SIP OAuth-modus is ingeschakeld of niet. Deze parameter kan uitgaan van een van de volgende waarden:

- 0 - SIP OAuth is uitgeschakeld
- 1 - SIP OAuth is ingeschakeld

Als de SIP OAuth-modus is ingeschakeld, gebruikt Jabber een van deze parameters om de poort voor de SIP TLS-verbinding te bepalen - sipOAuthPort voor on-premises of sipMRAAuthPort voor MRA-gebaseerde implementaties. In het voorbeeld worden de standaardwaarden sipOAuthPort 5090 en sipMRAOAuthPort 5091 weergegeven. Deze waarden zijn configureerbaar en kunnen op elke CUCM-node verschillend zijn.

Als de SIP OAuth-modus is uitgeschakeld, gebruikt Jabber niet-beveiligde (5060) of beveiligde (5061) poorten voor SIP-registratie.

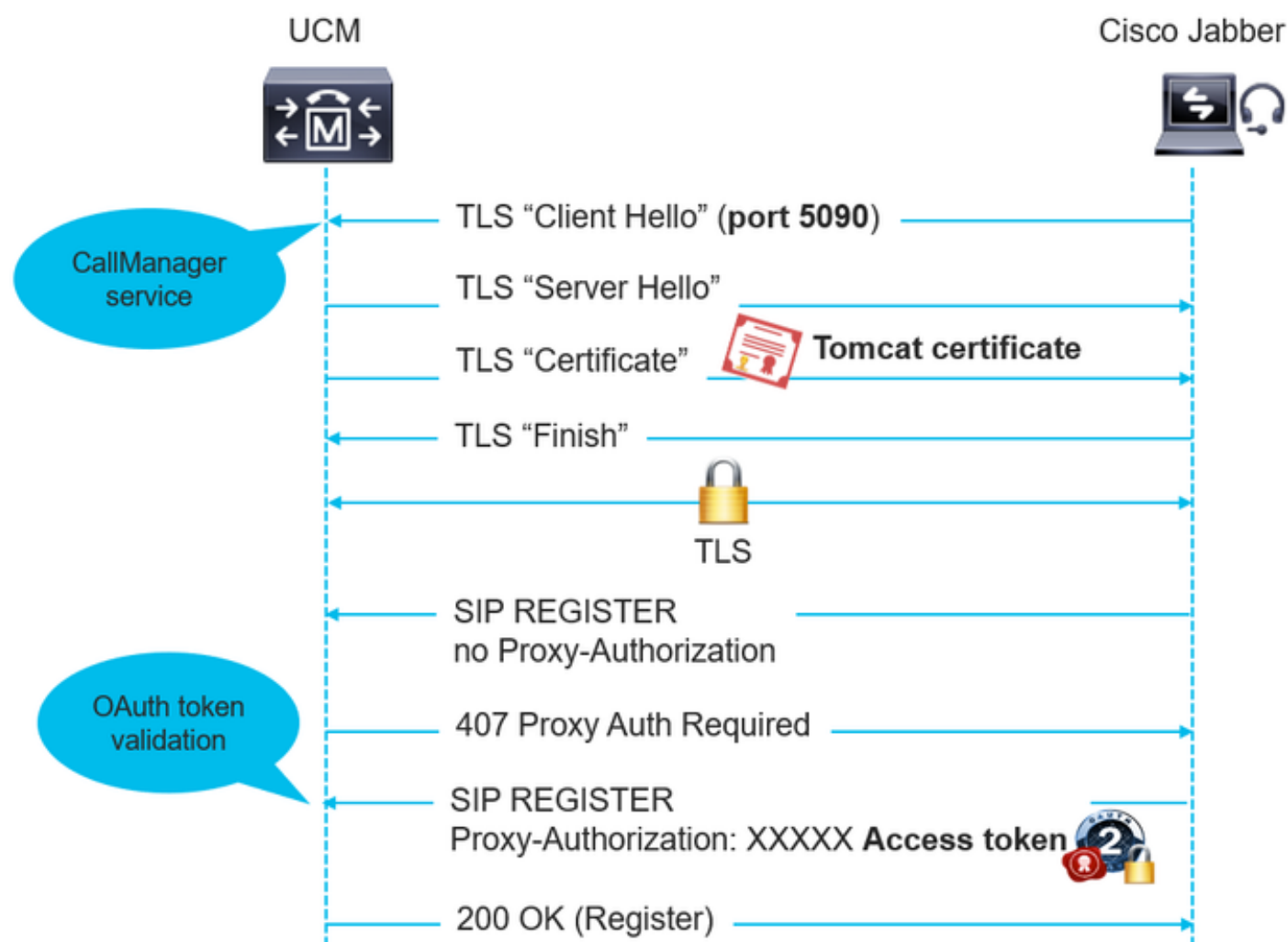
 **Opmerking:** Cisco UCM gebruikt SIP Phone OAuth Port (5090) om te luisteren naar SIP-lijnregistratie van Jabber OnPremise-apparaten via TLS. UCM gebruikt echter SIP Mobile Remote Access Port (standaard 5091) om te luisteren naar SIP-lijnregistraties van Jabber via Expressway via mLTS. Beide poorten zijn configureerbaar. Zie het gedeelte Configuratie.

De CallManager-service luistert naar zowel sipOAuthPort als sipMRAAuthPort. Beide poorten

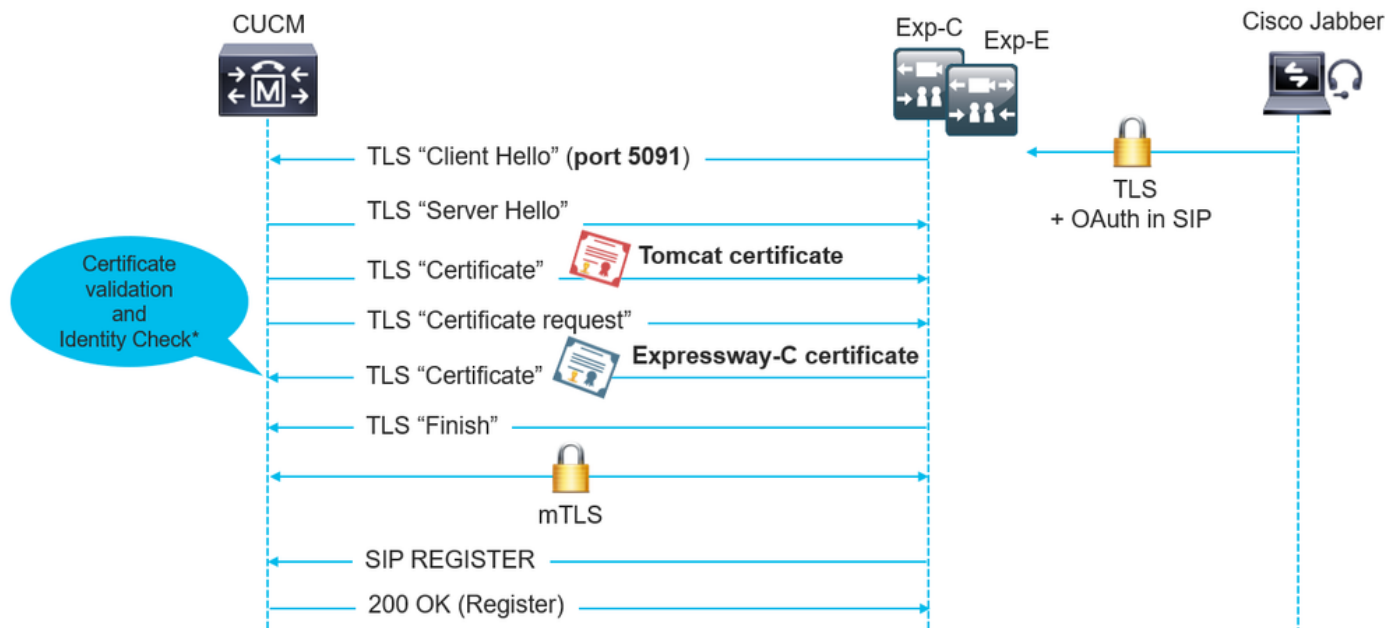
 gebruiken echter het Tomcat-certificaat en Tomcat-trust voor inkomende TLS/mTLS-verbindingen. Zorg ervoor dat uw Tomcat-trust-winkel in staat is om het Expressway-C-certificaat voor de SIP OAuth-modus te verifiëren zodat MRA nauwkeurig kan functioneren.

In situaties waarin het Tomcat-certificaat opnieuw wordt gegenereerd, moet het CallManager-proces ook daarna opnieuw worden gestart op de getroffen knooppunten. Dit is nodig voor het CCM-proces om nieuwe certificaten op sipOAuth-poorten te laden en te gebruiken.

Deze afbeelding toont de registratie van Cisco Jabber terwijl op locatie:



Deze afbeelding toont de registratie van Cisco Jabber over MRA:



*Expressway-C nodes gebruiken AXL API om UCM te informeren over de CN/SAN in hun certificaat. UCM gebruikt deze informatie om het Exp-C-certificaat te valideren wanneer een wederzijdse TLS-verbinding tot stand wordt gebracht.

Configuratie - Jabber on premises

- Opmerking:**
- Zorg ervoor dat u onderstaande punten hebt ingevuld voordat u de SIP OAuth-modus configureert:
- MRA is geconfigureerd en de verbinding is tot stand gebracht tussen Unified Communication Manager (UCM) en Expressway (alleen van toepassing als MRA in gebruik is).
 - UCM is geregistreerd op een Smart of Virtual account met exportgecontroleerde functionaliteit.

1. Aanmeldingen voor vernieuwen configureren.

Configureer aanmeldingen voor vernieuwen met OAuth-toegangstokens en vernieuw tokens voor Cisco Jabber-clients. Kies **Systeem > Bedrijfsparameters** in Cisco Unified CM Administration.

SSO and OAuth Configuration	
OAuth Access Token Expiry Timer (minutes) *	60
Jabber OAuth Refresh Token Expiry Timer (days) *	60
Physical Phone OAuth Refresh Token Expiry Timer (days) *	60
Redirect URIs for Third Party SSO Client	
SSO Login Behavior for IOS *	Use embedded browser (WebView)
OAuth with Refresh Login Flow *	Enabled
Use SSO for RTMT *	False

2. Configureer OAuth-poorten.

Kies Systeem > Cisco Unified CM. Dit is een optionele stap. De afbeelding bevat de standaardwaarden. Het acceptabele configureerbare bereik is 1024 tot 49151. Herhaal dezelfde procedure voor elke server.

Cisco Unified Communications Manager TCP Port Settings for this Server	
Ethernet Phone Port*	2000
MGCP Listen Port*	2427
MGCP Keep-alive Port*	2428
SIP Phone Port*	5060
SIP Phone Secure Port*	5061
SIP Phone OAuth Port*	5090
SIP Mobile and Remote Access OAuth Port*	5091

3. Schakel de SIP Outh-modus in.

Gebruik de opdrachtregelinterface van de uitgever om de SIP OAuth-modus wereldwijd in te schakelen. Voer de opdracht uit: sipOAuth-modus inschakelen.

```
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. Start Cisco CallManager Service opnieuw.

Kies in Cisco Unified Serviceability de optie Tools > Control Center – Feature Services. Selecteer en start de Cisco CallManager-service opnieuw op alle nodes waar de service actief is.

5. Configureer OAuth Support in het beveiligingsprofiel.

Kies Systeem > Beveiligingsprofiel telefoon in Cisco Unified CM Administration. Selecteer OAuth-verificatie inschakelen om SIP OAuth-ondersteuning voor het eindpunt in te schakelen.

Phone Security Profile Information	
Product Type:	Cisco Unified Client Services Framework
Device Protocol:	SIP
Name*	Cisco Unified Client Services Framework - OAuth auth
Description	Cisco Unified Client Services Framework - OAuth auth
Device Security Mode	Encrypted
Transport Type*	TLS
☐ TFTP Encrypted Config	
☒ Enable OAuth Authentication	

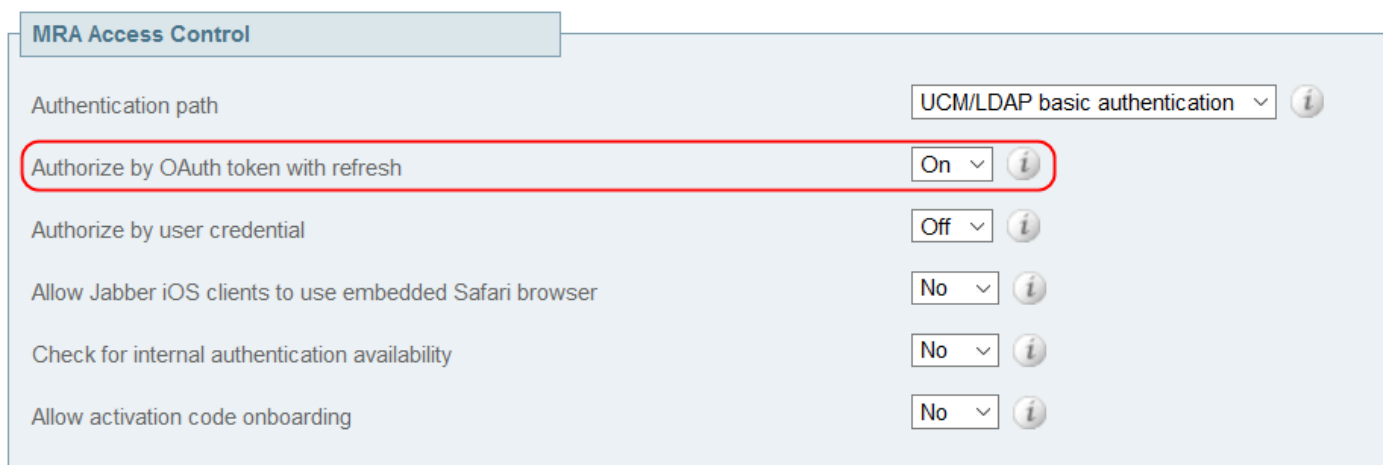
Configuratie - Jabber over MRA

voorwaarden

Voordat u de SIP OAuth-modus voor Jabber over MRA configureert, voert u de stappen 1-4 uit van het hoofdstuk Configuration - Jabber On Premises van dit artikel.

Stap 1. Inloggen bij Vernieuwen inschakelen via MRA.

Aanmeldingen vernieuwen moet zijn ingeschakeld op Expressway (ook wel zelfbeschrijvende tokens genoemd) voordat de SIP OAuth-verificatie met Cisco Jabber over MRA kan worden geconfigureerd. Navigeer op de Expressway-C naar Configuratie > Unified Communications > Configuration en zorg ervoor dat de parameter Autoriseren op OAuth-token met vernieuwen is ingesteld op Aan.



MRA Access Control

Authentication path: UCM/LDAP basic authentication ⓘ

Authorize by OAuth token with refresh: On ⓘ

Authorize by user credential: Off ⓘ

Allow Jabber iOS clients to use embedded Safari browser: No ⓘ

Check for internal authentication availability: No ⓘ

Allow activation code onboarding: No ⓘ

Stap 2. Vernieuw de Unified CM Nodes in Expressway-C.

Ga naar Configuratie > Unified Communications > Unified CM-servers. Ontdek of vernieuw de Unified CM-knooppunten in Expressway-C.

Unified CM servers

	Publisher address	Username	TLS verify mode	Nodes discovered by this lookup
☐	cucm11.domain-1.com	administrator	Off	10.46.0.100, 10.46.0.101
☒	labcucm105pub.labcucm.com	ccmadmin	On	10.46.0.102pub.labcucm.com, 10.46.0.103pub.labcucm.com

Add

Delete

Select all

Unselect all

Refresh servers

 **Opmerking:** in Expressway-C wordt automatisch een nieuwe CEOAuth-zone (TLS) gemaakt. Bijvoorbeeld CEOAuth <Unified CM name>. Er wordt een zoekregel gemaakt om de SIP-verzoeken van Jabber via MRA naar de Unified CM-node te proxyen. Deze zone maakt gebruik van TLS-verbindingen, ongeacht of Unified CM is geconfigureerd in de gemengde modus. Om vertrouwen te creëren, verzendt Expressway-C ook de hostnaam en de alternatieve naam van het onderwerp (SAN) naar het Unified CM-cluster. Zie het



verificatiegedeelte van dit artikel om ervoor te zorgen dat de juiste configuratie is geïnstalleerd.

Stap 3. Configureer de OAuth-ondersteuning in het beveiligingsprofiel.

Kies Systeem > Beveiligingsprofiel telefoon in Cisco Unified CM Administration. Schakel OAuth-ondersteuning in op het profiel dat is toegewezen aan Cisco Jabber.

Phone Security Profile Information

Product Type:	Cisco Unified Client Services Framework
Device Protocol:	SIP
Name*	Cisco Unified Client Services Framework - OAuth auth
Description	Cisco Unified Client Services Framework - OAuth auth
Device Security Mode	Encrypted
Transport Type*	TLS
☐ TFTP Encrypted Config	
☒ Enable OAuth Authentication	

Verifiëren

1. Controleer of de SIP OAuth-modus wereldwijd is ingeschakeld.

Controleer de OAuth-modus vanuit Cisco Unified CM Administration, kies Systeem > Bedrijfsparameters.

Security Parameters

Cluster Security Mode *	1
Cluster SIPOAuth Mode *	Enabled
LBM Security Mode *	Insecure

U kunt ook de Admin CLI gebruiken - Voer de opdracht uit: voer sql uit en selecteer paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'

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

Mogelijke waarden: 0 - voor Uitgeschakeld (standaard), 1 - voor Ingeschakeld.

2. Verifieer dat expressway-C SAN-items succesvol naar CUCM zijn gepusht.

Expressway-C verzendt de CN/SAN-details van zijn certificaat naar UCM via AXL. Deze gegevens

worden opgeslagen in de expressway-configuratie tabel. Dit proces wordt aangeroepen telkens wanneer u de Unified CM-knooppunten in Expressway-C ontdekt of vernieuwt. Deze vermeldingen worden gebruikt om het vertrouwen tussen UCM en Expressway-C te vestigen. CN/SAN veld van Expressway-C certificaat wordt gecontroleerd aan de hand van die vermeldingen tijdens MTLS verbinding met de SIP MRA OAuth poort (5091 standaard). Als de verificatie mislukt, mislukt de MTLS-verbinding.

Controleer de items van Cisco Unified CM Administration, kies Apparaat > Expressway-C (beschikbaar vanaf UCM 12.5.1Su1)

Cisco Expressway-C Configuration

Host Name/IP Address*	exp-c
Description	this is added through axl
X509 Subject Name / Subject Alternate Name	domain-2.com, domain-1.com, exp-c.domain-1.com

U kunt ook de Admin CLI gebruiken - Voer de opdracht uit: voer sql select * uit via expressconfiguratie

```
admin:run sql select * from expresswayconfiguration
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. Controleer CEOAuth Zone(s) op Expressway-C.

Navigeer naar Expressway-C > Configuratie > Zones > Zones. Zorg ervoor dat alle nieuw gecreëerde CEOAuth-zones zich in de actieve toestand bevinden.

Name ▼	Type	Calls	Bandwidth used	H323 status	SIP status
DefaultZone	Default zone	0	0 kbps	Off	On
CEOAuth-	Neighbor	0	0 kbps	Off	Active
CEOAuth-	Neighbor	0	0 kbps	Off	Active

4. Controleren van de procesbeluisteringen van CallManager op SIP OAuth-poorten.

Voer de opdracht uit vanuit de CLI voor beheerders: open poorten regexp 5090 (standaard SIP OAuth-poort) weergeven

```
admin:show open ports regexp 5090

Executing.. please wait.
ccm      30622      ccmbase  364u  IPv4  207160      0t0  TCP  10.48.10.10:5090 (LISTEN)
```

Voer de opdracht uit vanuit de CLI voor beheerders: open poorten regexp 5091 weergeven (standaard SIP MRA OAuth-poort)

```
admin:show open ports regexp 5091
```

```
Executing.. please wait.
```

```
ccm      30622      ccmbase  351u  IPv4  207155      0t0  TCP  10.48.  :5091 (LISTEN)
```

Problemen oplossen

Voorbeeld van Jabber-logboek (on-premises)

Log voorbeeld voor on-premises SIP OAuth registratie op poort 5090 vanuit Jabber log perspectief.

```
## 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=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: 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=882323451234089000003bdd-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

Jabber-apparaat op locatie in SIP OAuth-modus kan zich niet registreren bij UCM. UCM stuurt 403 voor het registerbericht:

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

Mogelijke oplossing: Zorg ervoor dat aan de volgende voorwaarden wordt voldaan:

- OAuth-modus is wereldwijd ingeschakeld
- Apparaatbeveiligingsprofiel dat aan het apparaat is gekoppeld, heeft OAuth-ondersteuning ingeschakeld
- Bericht ontvangen op 5090-poort via TLS in plaats van mTLS

Scenario 2 - Onbekende CA van Expressway

Expressway-C kan de mTLS-handshake met UCM niet instellen op sipMRAuthport (standaard 5091). Expressway-C vertrouwt het certificaat dat wordt gedeeld door UCM niet en reageert met het bericht Onbekende CA tijdens de installatie van mTLS.

Mogelijke oplossing: de CallManager-service verzendt het Tomcat-certificaat tijdens de mTLS-handshake. Zorg ervoor dat uw Expressway-C de ondertekenaar van het Tomcat-certificaat van UCM vertrouwt.

Scenario 3 - Onbekende CA van UCM

Expressway-C kan de mTLS-handshake met UCM niet instellen op sipMRAuthport (standaard 5091). UCM vertrouwt het certificaat dat wordt gedeeld door Expressway niet en reageert met het Onbekende CA-bericht tijdens de installatie van mTLS.

Pakketvastlegging uit deze mededeling (UCM 10.x.x.198, Expressway-C 10.x.x.182):

Time	Source	Destination	Protocol	Source port	Destination	Length	Info
11:16:29.659235	10.10.10.182	10.10.10.198	TCP	25161	5091	74	25161 → 5091 [SYN] Seq=0 Win=64240 Len=0 MSS=1
11:16:29.659609	10.10.10.198	10.10.10.182	TCP	5091	25161	74	5091 → 25161 [SYN, ACK] Seq=0 Ack=1 Win=28960
11:16:29.659627	10.10.10.182	10.10.10.198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=1 Ack=1 Win=64256 Len=0
11:16:29.714501	10.10.10.182	10.10.10.198	TLSv1.2	25161	5091	260	Client Hello
11:16:29.715316	10.10.10.198	10.10.10.182	TCP	5091	25161	66	5091 → 25161 [ACK] Seq=1 Ack=195 Win=30080 Len=0
11:16:29.737063	10.10.10.198	10.10.10.182	TLSv1.2	5091	25161	1514	Server Hello
11:16:29.737091	10.10.10.182	10.10.10.198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=195 Ack=1449 Win=64128
11:16:29.737137	10.10.10.198	10.10.10.182	TLSv1.2	5091	25161	1081	Certificate, Server Key Exchange, Certificate
11:16:29.737149	10.10.10.182	10.10.10.198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=195 Ack=2464 Win=63488
11:16:29.753375	10.10.10.182	10.10.10.198	TLSv1.2	25161	5091	2878	Certificate, Client Key Exchange, Certificate
11:16:29.754116	10.10.10.198	10.10.10.182	TCP	5091	25161	66	5091 → 25161 [ACK] Seq=2464 Ack=3007 Win=35712
11:16:29.758710	10.10.10.198	10.10.10.182	TLSv1.2	5091	25161	73	Alert (Level: Fatal, Description: Unknown CA)
11:16:29.758743	10.10.10.182	10.10.10.198	TCP	25161	5091	66	25161 → 5091 [ACK] Seq=3007 Ack=2471 Win=64128
11:16:29.758780	10.10.10.198	10.10.10.182	TCP	5091	25161	66	5091 → 25161 [RST, ACK] Seq=2471 Ack=3007 Win=0

Mogelijke oplossing: UCM gebruikt de Tomcat-trust store om inkomende certificaten te verifiëren tijdens de mTLS handshake op SIP OAuth-poorten. Zorg ervoor dat het certificaat van de ondertekenaar voor Expressway-C correct is geüpload naar de UCM.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.