Modo OAuth do Cisco Jabber e SIP

Contents

Introdução

Este documento descreve a configuração e as etapas básicas de solução de problemas para implementar o modo SIP OAuth com o Cisco Jabber.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Registro de softphone Jabber
- Unified Communications Manager (UCM)
- Solução de acesso remoto e móvel (MRA)

Componentes Utilizados

Versão mínima do software para suportar o modo SIP OAuth:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Restrição

Quando o modo OAuth do SIP está ativado, as opções Ativar Autenticação Digest e Configuração Criptografada do TFTP não são suportadas.

Informações de Apoio

Principais benefícios

Proteger a sinalização e a mídia SIP para o softphone Cisco Jabber atualmente envolve várias etapas de configuração. O mais difícil é instalar e renovar certificados de cliente (LSCs), especialmente se um dispositivo Cisco Jabber estiver alternando entre o local e o externo, e manter os certificados dentro do arquivo CTL atualizados.

O modo OAuth do SIP permite que o Cisco Jabber Softphone use tokens autodescritivos OAuth em vez do certificado LSC do cliente para autenticação em uma interface SIP segura. O suporte a OAuth na interface SIP do UCM permite sinalização e mídia seguras para implantações Jabber locais e MRA sem a necessidade do modo misto ou operação CAPF.

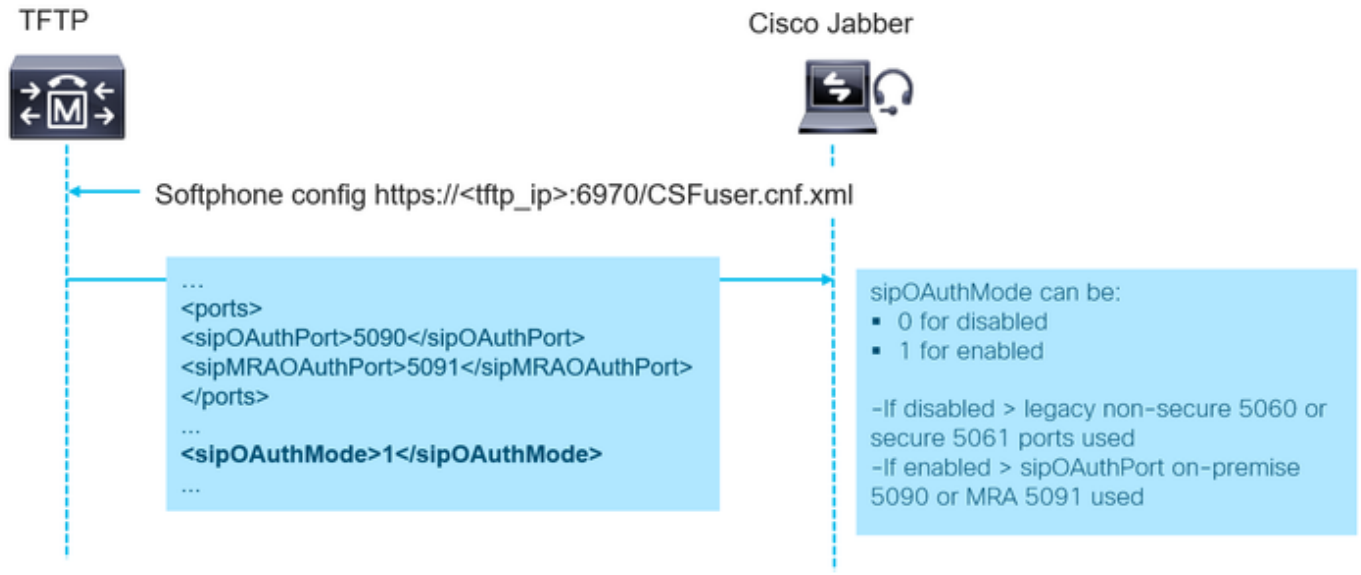
Principais benefícios do suporte ao modo SIP OAuth para o Cisco Jabber:

- Habilita a criptografia sempre ativa sem carga administrativa adicional.
- Sinalização e mídia seguras para o Cisco Jabber sem a necessidade do modo Misto (sem atualizações de CTL, manutenção de certificados e assim por diante)
- Não há necessidade de instalar e manter o LSC em clientes Jabber.
    - Desafios com LSC em vários dispositivos (laptops/dispositivos móveis..)

- A operação CAPF é necessária sempre que o Jabber é instalado em um novo dispositivo.
- Não há suporte para a operação CAPF em MRA.

Arquitetura geral

O dispositivo Cisco Jabber reconhece que a autenticação OAuth é habilitada na interface SIP analisando o arquivo de configuração CSF (http://<cucmIP>:6970/<CSF-device-name>.cnf.xml), exemplo de arquivo de configuração (algumas linhas são deixadas de fora para serem resumidas):



O Cisco Jabber lê o parâmetro sipOAuthMode para determinar se o modo SIP OAuth está ativado ou não. Esse parâmetro pode assumir um dos seguintes valores:

- 0 - SIP OAuth está desabilitado
- 1 - SIP OAuth está habilitado

Se o modo SIP OAuth estiver habilitado, o Jabber usará um desses parâmetros para determinar a porta para conexão SIP TLS - sipOAuthPort para implantações no local ou sipMRAOAuthPort para implantações baseadas em MRA. O exemplo apresenta os valores padrão - sipOAuthPort 5090 e sipMRAOAuthPort 5091. Esses valores são configuráveis e podem ser diferentes em cada nó do CUCM.

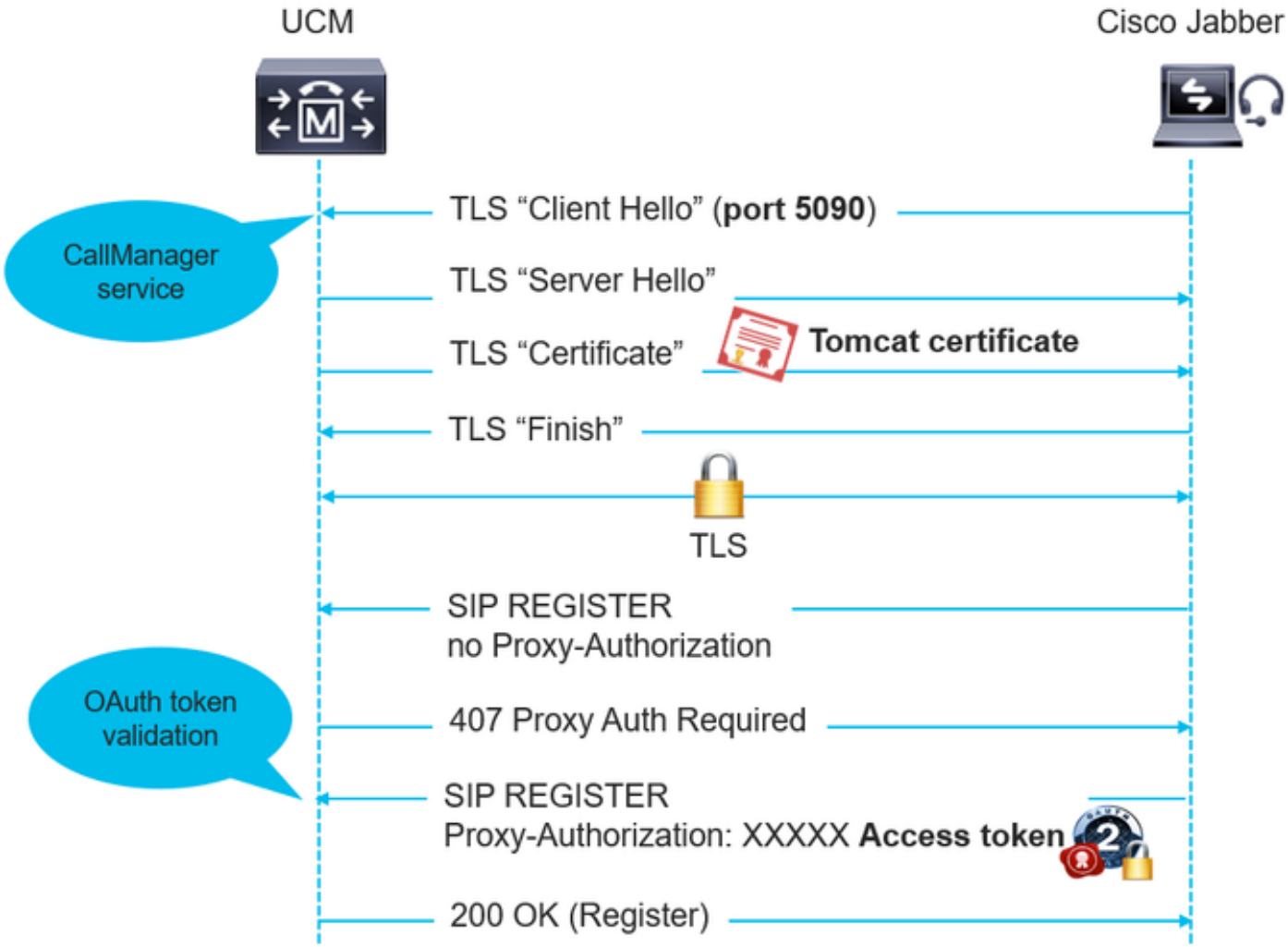
Se o modo OAuth do SIP estiver desabilitado, o Jabber usará portas não seguras (5060) ou seguras (5061) para o registro do SIP.

Note: O Cisco UCM usa a porta OAuth do telefone SIP (5090) para ouvir o registro de linha SIP de dispositivos Jabber OnPremise sobre TLS. No entanto, o UCM usa a porta de acesso remoto móvel SIP (padrão 5091) para ouvir registros de linha SIP do Jabber sobre Expressway através de mLTS. Ambas as portas são configuráveis. Consulte a seção de configuração.

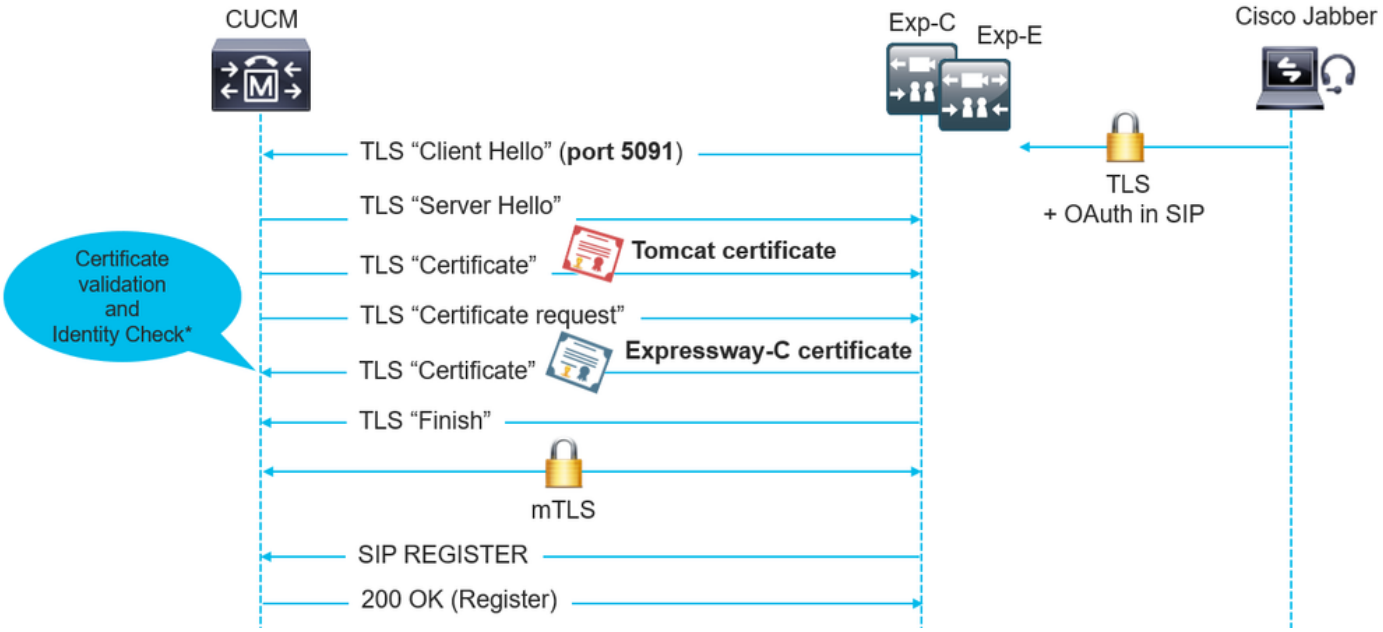
O serviço CallManager escuta no sipOAuthPort e no sipMRAOAuthPort. No entanto, ambas as portas usam o certificado Tomcat e Tomcat-trust para conexões TLS/mTLS de entrada. Certifique-se de que o armazenamento Tomcat-trust possa verificar o certificado Expressway-C para o modo OAuth do SIP para que o MRA funcione com precisão.

Em situações em que o certificado Tomcat é gerado novamente, o processo CallManager também deve ser reiniciado nos nós afetados posteriormente. Isso é necessário para que o processo CCM carregue e use novos certificados em portas sipOAuth.

Esta imagem representa o registro do Cisco Jabber enquanto no local:



Esta imagem representa o registro do Cisco Jabber sobre MRA:



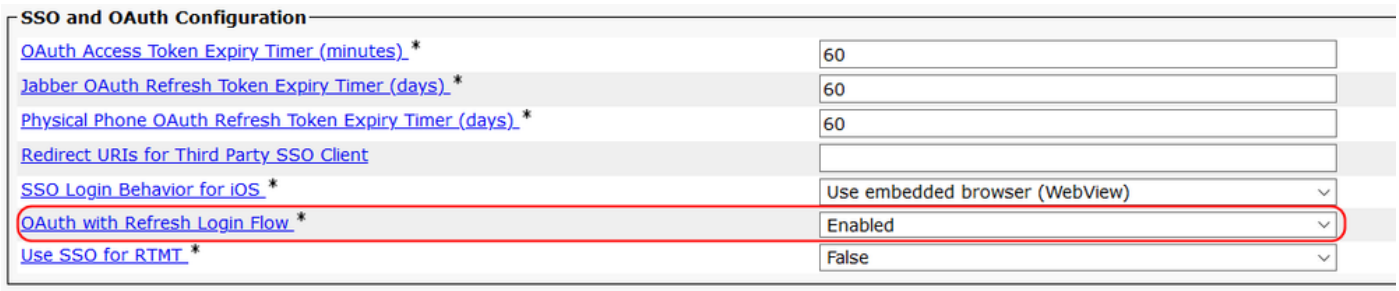
*Os nós do Expressway-C usam API AXL para informar ao UCM o CN/SAN em seu certificado. O UCM usa essas informações para validar o certificado Exp-C quando uma conexão TLS mútua é estabelecida.

Configuração - Jabber no local

Note:
Verifique se você concluiu os pontos abaixo antes da configuração do modo OAuth do SIP:
- O MRA é configurado e a conexão é estabelecida entre o Unified Communication Manager (UCM) e o Expressway (aplicável somente se o MRA estiver em uso).
- O UCM está registrado em uma Smart ou Virtual Account com a funcionalidade de permitir exportação controlada.

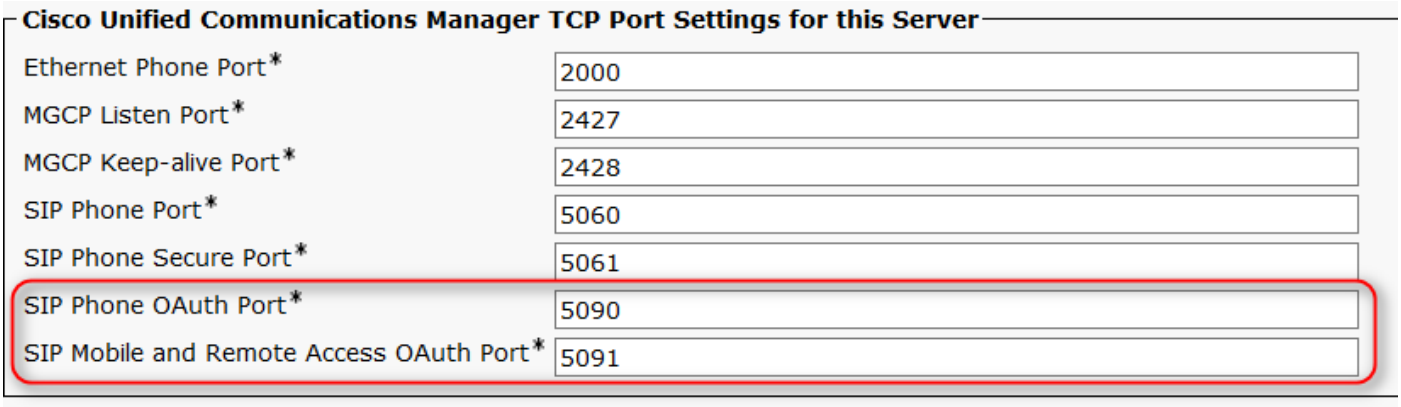
1. Configure os Logons de Atualização.

Configure Logons de Atualização com tokens de acesso OAuth e tokens de atualização para clientes Cisco Jabber. No Cisco Unified CM Administration, escolha Sistema > Parâmetros Corporativos.



2. Configure as Portas OAuth.

Escolha Sistema > Cisco Unified CM. Esta é uma etapa opcional. A figura apresenta os valores padrão. O intervalo configurável aceitável é de 1024 a 49151. Repita o mesmo procedimento para cada servidor.



3. Ative o Modo OAuth do SIP.

Use a Interface de Linha de Comando do Publicador para habilitar o modo SIP OAuth globalmente. Execute o comando: utils sipOAuth-mode enable.

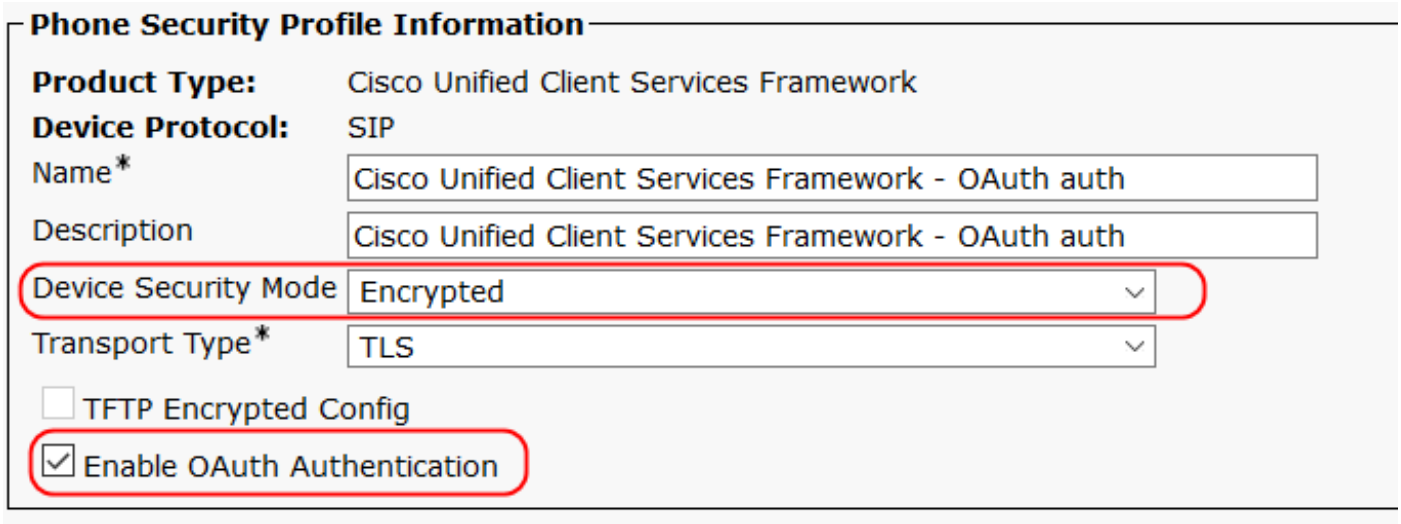
```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

4. Reinicie o Cisco CallManager Service.

Em Cisco Unified Serviceability, escolha Ferramentas > Centro de controle - Serviços de recurso. Selecione e reinicie o serviço Cisco CallManager em todos os nós onde o serviço está ativo.

5. Configure o Suporte OAuth no Perfil de Segurança.

No Cisco Unified CM Administration, escolha System > Phone Security Profile. Selecione Enable OAuth Authentication para habilitar o suporte SIP OAuth para o ponto final.



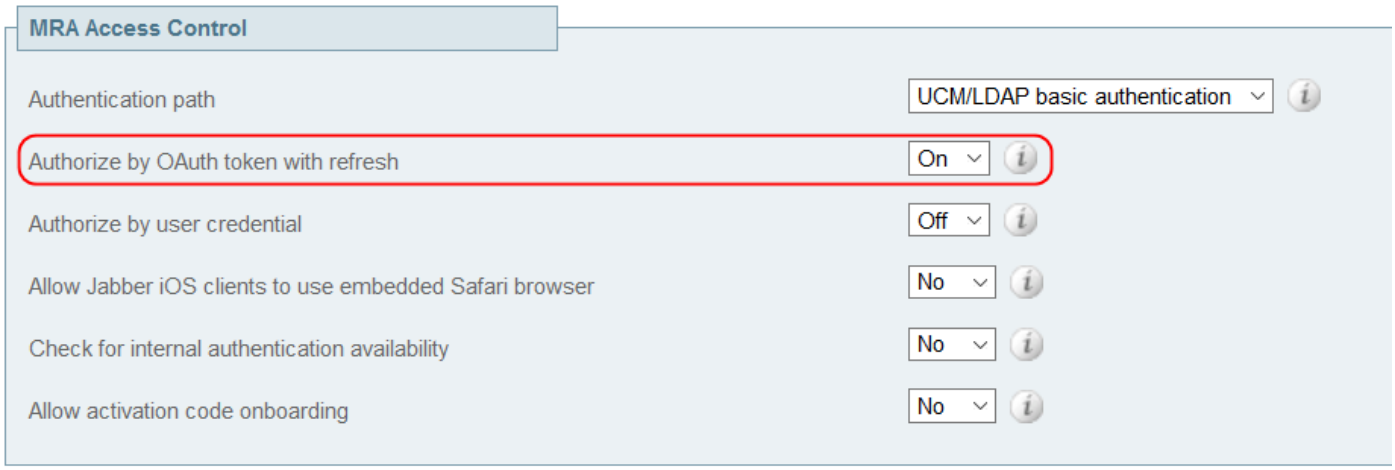
Configuração - Jabber sobre MRA

Pré-requisitos

Antes da configuração do modo SIP OAuth para Jabber sobre MRA, conclua as etapas 1 a 4 do capítulo Configuração - Jabber no local deste artigo.

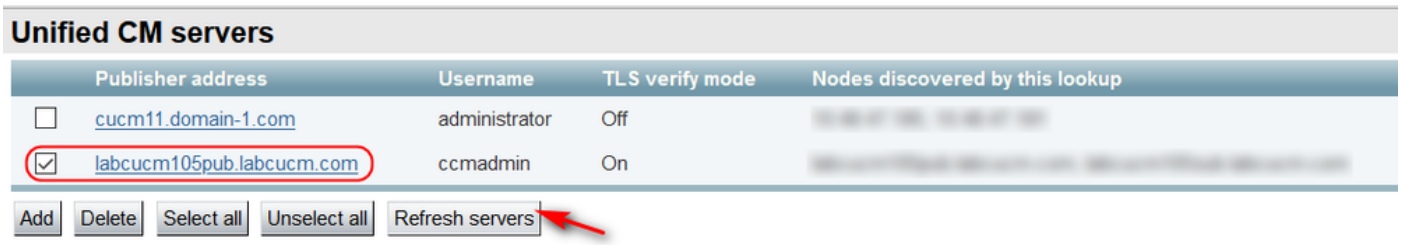
Etapa 1. Habilitar Renovar Logon por MRA.

Os logons de atualização devem ser habilitados no Expressway (também chamado de tokens autodescritivos) antes da configuração da autenticação OAuth do SIP com o Cisco Jabber sobre MRA. No Expressway-C, navegue para Configuração > Comunicações Unificadas > Configuração e verifique se o parâmetro Autorizar pelo Token OAuth com atualização está definido como Ativado.



Etapa 2. Atualizar os nós do Unified CM no Expressway-C.

Navegue até Configuration > Unified Communications > Unified CM servers. Descubra ou atualize os nós do Unified CM no Expressway-C.

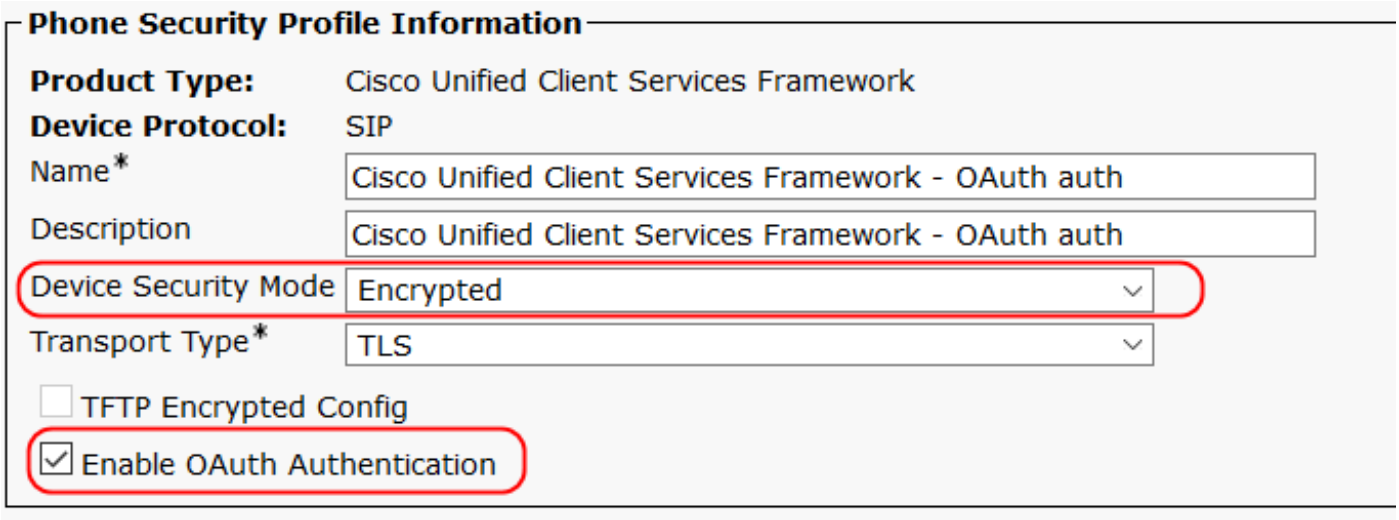


Note: Uma nova zona CEOAuth (TLS) é criada automaticamente no Expressway-C. Por exemplo, CEOAuth <nome do Unified CM>. Uma regra de pesquisa é criada para proxy das solicitações SIP originadas do Jabber sobre MRA para o nó Unified CM. Esta zona usa conexões TLS independentemente de o Unified CM estar configurado com modo misto. Para estabelecer confiança, o Expressway-C também envia os detalhes do nome do host e do Nome Alternativo da Entidade (SAN) ao cluster do Unified CM. Consulte a parte de

verificação deste artigo para garantir que a configuração apropriada esteja em vigor.

Etapa 3. Configurar o Suporte OAuth no Perfil de Segurança.

No Cisco Unified CM Administration, escolha System > Phone Security Profile. Ative o suporte OAuth no perfil atribuído ao Cisco Jabber.



Verificar

1. Verifique se o Modo OAuth do SIP está Habilitado Globalmente.

Verifique o modo OAuth em Cisco Unified CM Administration, escolha System > Enterprise Parameters.

Como alternativa, use o Admin CLI - Execute o comando: run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'

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

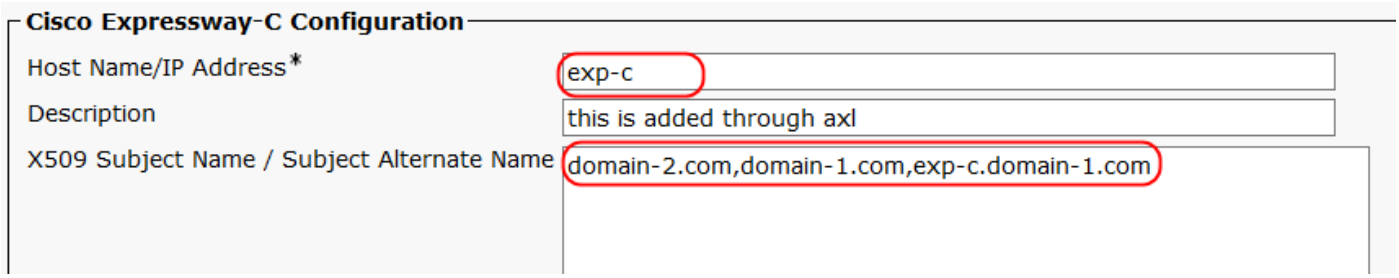
Valores possíveis: 0 - para Desativado (Padrão), 1 - para Ativado.

2. Verifique se as entradas de SAN do Expressway-C foram enviadas com êxito para o CUCM.

O Expressway-C envia os detalhes CN/SAN de seu certificado para o UCM por meio do AXL.

Esses detalhes são salvos na tabela expresswaycconfiguration. Esse processo é chamado toda vez que você descobre ou atualiza os nós do Unified CM no Expressway-C. Essas entradas são usadas para estabelecer confiança entre o UCM e o Expressway-C. O campo CN/SAN do certificado Expressway-C é comparado a essas entradas durante a conexão MTLS com a porta SIP MRA OAuth (5091 por padrão). Se a verificação não for bem-sucedida, a conexão MTLS falhará.

Verifique as entradas do Cisco Unified CM Administration, escolha Device > Expressway-C (disponível no UCM 12.5.1Su1 em diante)

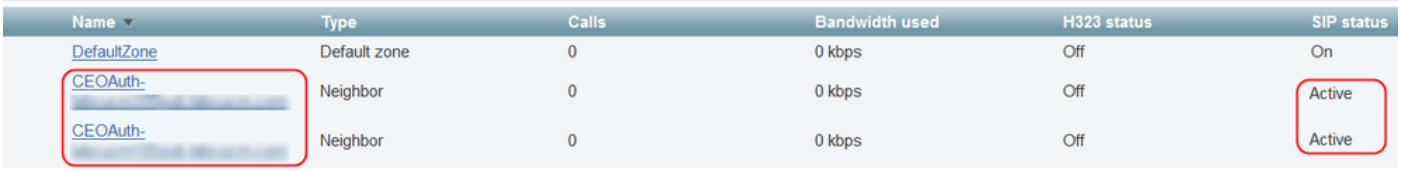


Como alternativa, use o Admin CLI - Execute o comando: run sql select * from expresswaycconfiguration

```
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. Verifique as zonas CEOAuth no Expressway-C.

Navegue até Expressway-C > Configuração > Zonas > Zonas. Verifique se todas as zonas CEOAuth recém-criadas estão no estado ativo.



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. Verifique se o processo do CallManager escuta nas portas OAuth do SIP.

Execute o comando a partir da CLI do administrador: show open ports regexp 5090 (default SIP OAuth Port)

```
admin:show open ports regexp 5090

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

Execute o comando a partir da CLI do administrador: show open ports regexp 5091 (default SIP MRA OAuth Port)

```
admin:show open ports regexp 5091

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

Troubleshooting

Exemplo de log do Jabber (no local)

Exemplo de registro para registro SIP OAuth local na porta 5090 da perspectiva de registro 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=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: 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

Cenário 1 - Incompatibilidade da porta de Registro OAuth do SIP

O dispositivo Jabber instalado localmente no modo OAuth do SIP não consegue se registrar no UCM. O UCM envia 403 para a mensagem 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

Possível solução: Certifique-se de que as seguintes condições sejam atendidas:

- O modo OAuth está globalmente habilitado
- O perfil de segurança do dispositivo associado ao dispositivo tem suporte OAuth habilitado
- Mensagem recebida na porta 5090 sobre TLS em vez de mTLS

Cenário 2 - CA desconhecida do Expressway

O Expressway-C não consegue estabelecer o handshake mTLS com o UCM no sipMRAOAuthport (padrão 5091). O Expressway-C não confia no certificado compartilhado pelo UCM e responde com a mensagem CA desconhecida durante a instalação do mTLS.

Possível solução: O serviço CallManager envia seu certificado Tomcat durante o handshake mTLS. Verifique se o Expressway-C confia no assinante do certificado Tomcat do UCM.

Cenário 3 - CA desconhecida do UCM

O Expressway-C não consegue estabelecer o handshake mTLS com o UCM no sipMRAOAuthport (padrão 5091). O UCM não confia no certificado compartilhado pelo Expressway e responde com a mensagem CA desconhecida durante a instalação do mTLS.

Captura de pacote desta comunicação (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=

Possível solução: O UCM usa o armazenamento Tomcat-trust para verificar certificados recebidos durante o handshake mTLS nas portas OAuth do SIP. Verifique se o certificado do assinante do

Expressway-C foi carregado corretamente no UCM.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.