Cisco Jabber和SIP OAuth模式

目录

简介

本文档介绍使用Cisco Jabber实施SIP OAuth模式的配置和基本故障排除步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Jabber软件电话注册
- 统一通信管理器(UCM)
- 移动和远程访问(MRA)解决方案

使用的组件

支持SIP OAuth模式的最低软件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

限制

启用SIP OAuth模式时，不支持启用摘要身份验证和TFTP加密配置选项。

背景信息

主要好处

保护Cisco Jabber软件电话的SIP信令和媒体当前涉及多个配置步骤。最难的是安装和续订客户端证书(LSC)，尤其是当Cisco Jabber设备在内部和外部之间切换时，并且使CTL文件中的证书保持最新。

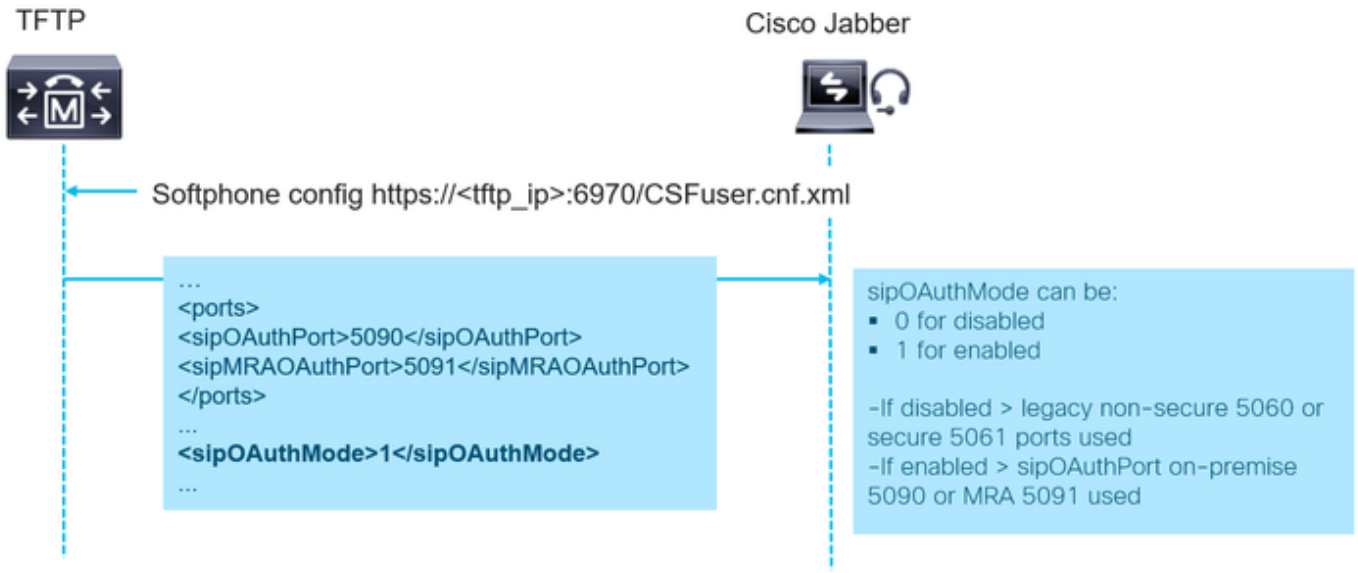
SIP OAuth模式允许Cisco Jabber软件电话使用OAuth自描述令牌而不是客户端LSC证书在安全SIP接口上进行身份验证。在UCM SIP接口上支持OAuth允许为Jabber本地部署和MRA部署提供安全信令和媒体，而无需混合模式或CAPF操作。

Cisco Jabber的SIP OAuth模式支持的主要优势：

- 启用无间断加密，无需额外管理负担。
- 用于Cisco Jabber的安全信令和媒体，无需混合模式（无CTL更新、证书维护等）
- 无需在Jabber客户端上安装和维护LSC。
    - LSC在多个设备（笔记本电脑/移动设备……）上面临的挑战
    - 每当在新设备上安装Jabber时，都需要执行CAPF操作。
    - MRA不支持CAPF操作。

整体架构

Cisco Jabber设备通过解析CSF配置文件(http://<cucmIP>:6970/<CSF-device-name>.cnf.xml)、配置文件示例（为简洁起见，省略了某些行）识别出SIP接口上启用了OAuth身份验证：



Cisco Jabber读取sipOAuthMode参数以确定是否启用了SIP OAuth模式。此参数可以采用以下值之一：

- 0 - SIP OAuth已禁用
- 1 — 启用SIP OAuth

如果SIP OAuth模式已启用，则Jabber使用这些参数之一确定SIP TLS连接的端口 — sipOAuthPort用于本地部署，或sipMAOAuthPort用于基于MRA的部署。示例显示默认值 — sipOAuthPort 5090和sipMAOAuthPort 5091。这些值可配置，并且可在每个CUCM节点上有所不同。

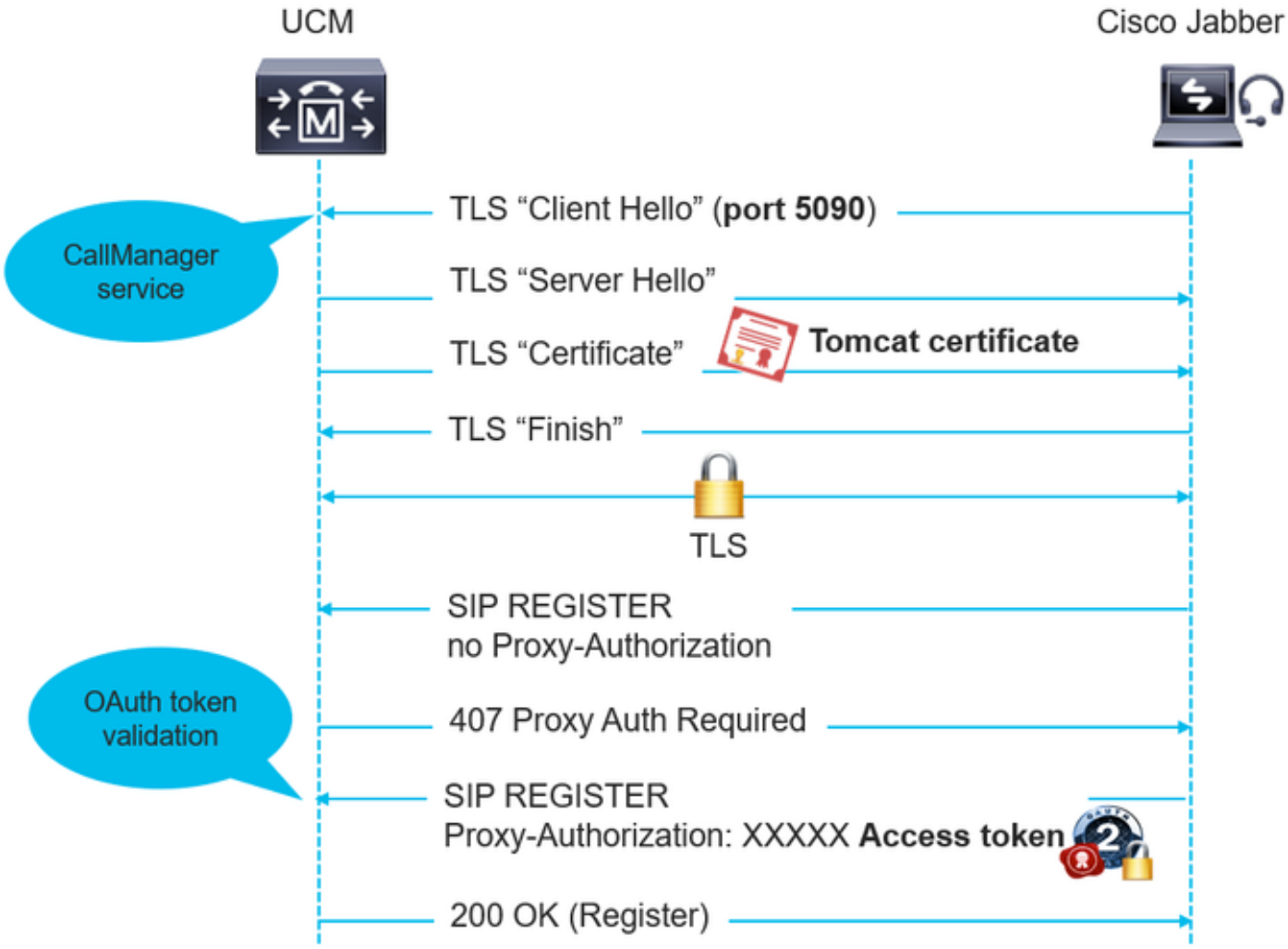
如果SIP OAuth模式已禁用，则Jabber使用传统非安全(5060)或安全(5061)端口进行SIP注册。

注意：Cisco UCM使用SIP电话OAuth端口(5090)侦听通过TLS从Jabber OnPremise设备进行的SIP线路注册。但是，UCM使用SIP移动远程访问端口（默认5091）通过mLTS侦听来自Jabber over Expressway的SIP线路注册。这两个端口都是可配置的。请参见配置部分。

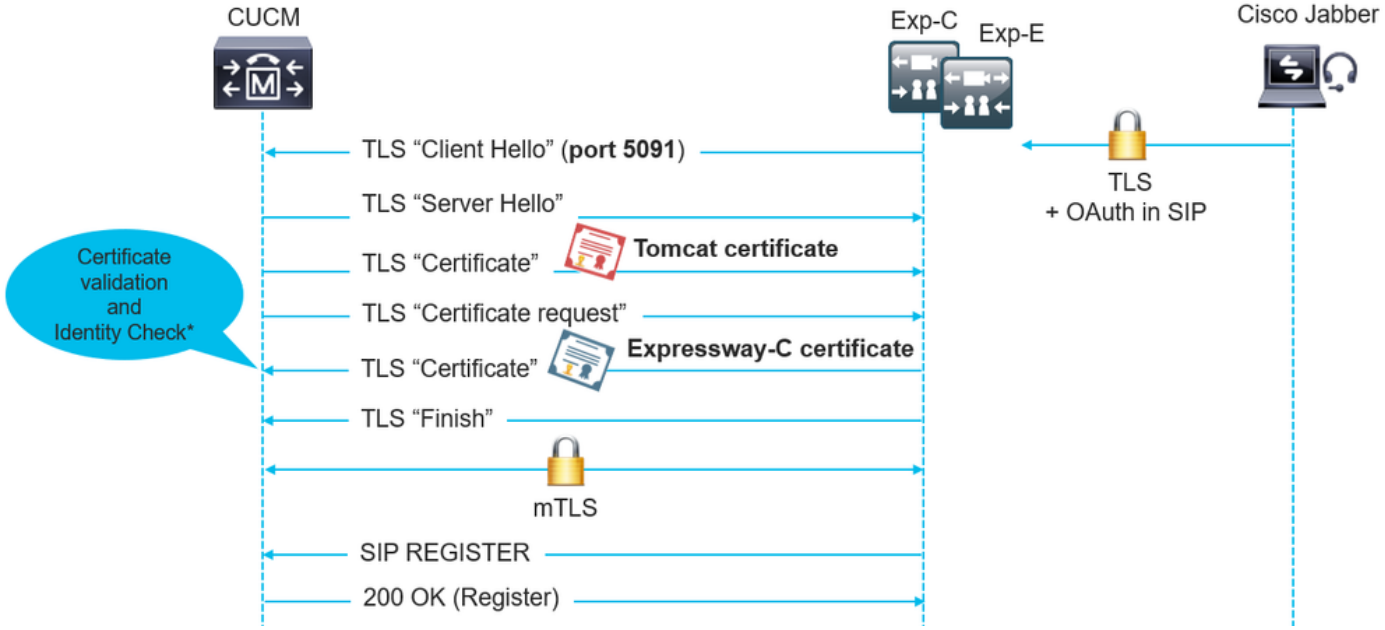
CallManager服务在sipOAuthPort和sipMAOAuthPort上侦听。但是，两个端口都使用Tomcat证书和Tomcat-trust进行传入TLS/mTLS连接。确保您的Tomcat-trust存储能够验证SIP OAuth模式的Expressway-C证书，以使MRA正常运行。

在重新生成Tomcat证书的情况下，随后必须在受影响的节点上重新启动CallManager进程。CCM进程在sipOAuth端口上加载和使用新证书时需要此步骤。

此图描述了本地时Cisco Jabber的注册:



此图描述通过MRA注册Cisco Jabber:



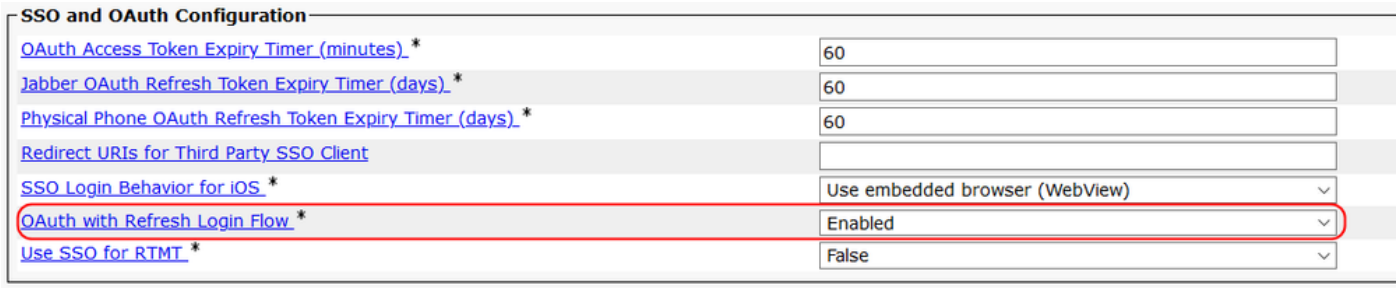
*Expressway-C节点使用AXL API通知UCM其证书中的CN/SAN。UCM使用此信息验证建立双向TLS连接时的Exp-C证书。

配置 — 本地Jabber

注意：
确保在配置SIP OAuth模式之前完成以下几点：
— 配置了MRA，并在Unified Communication Manager(UCM)和Expressway之间建立连接（仅在使用MRA时适用）。
- UCM注册到允许导出控制功能的智能或虚拟帐户。

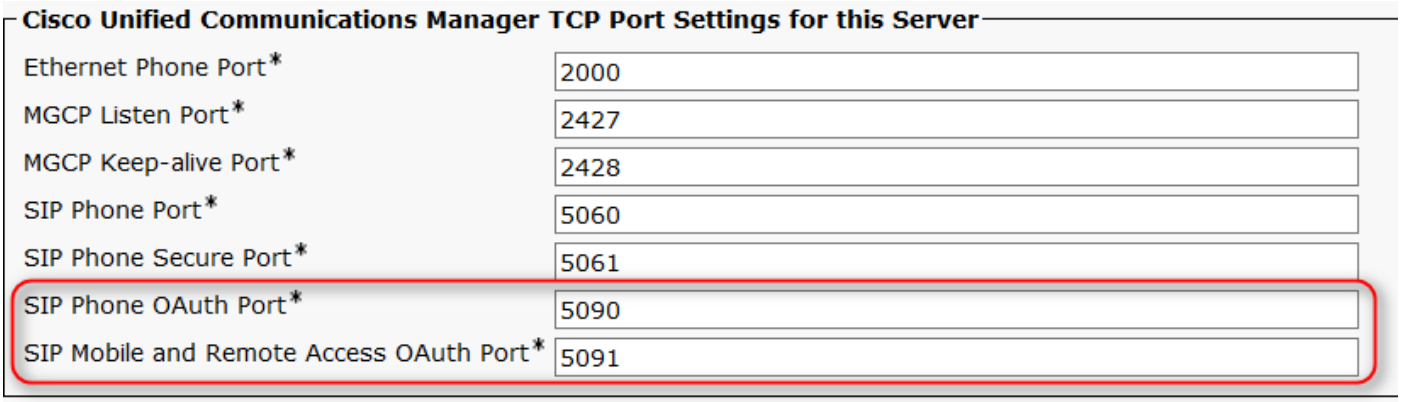
1.配置刷新登录。

使用OAuth访问令牌配置“刷新登录”，并为Cisco Jabber客户端配置刷新令牌。从Cisco Unified CM Administration中，选择System > Enterprise Parameters。



2.配置OAuth端口

选择System > Cisco Unified CM。这是可选步骤。图片显示默认值。可接受的可配置范围为1024至49151。请对每个服务器重复相同的过程。



3.启用SIP OAuth模式。

使用发布者的命令行界面全局启用SIP OAuth模式。运行以下命令：utils sipOAuth-mode enable。

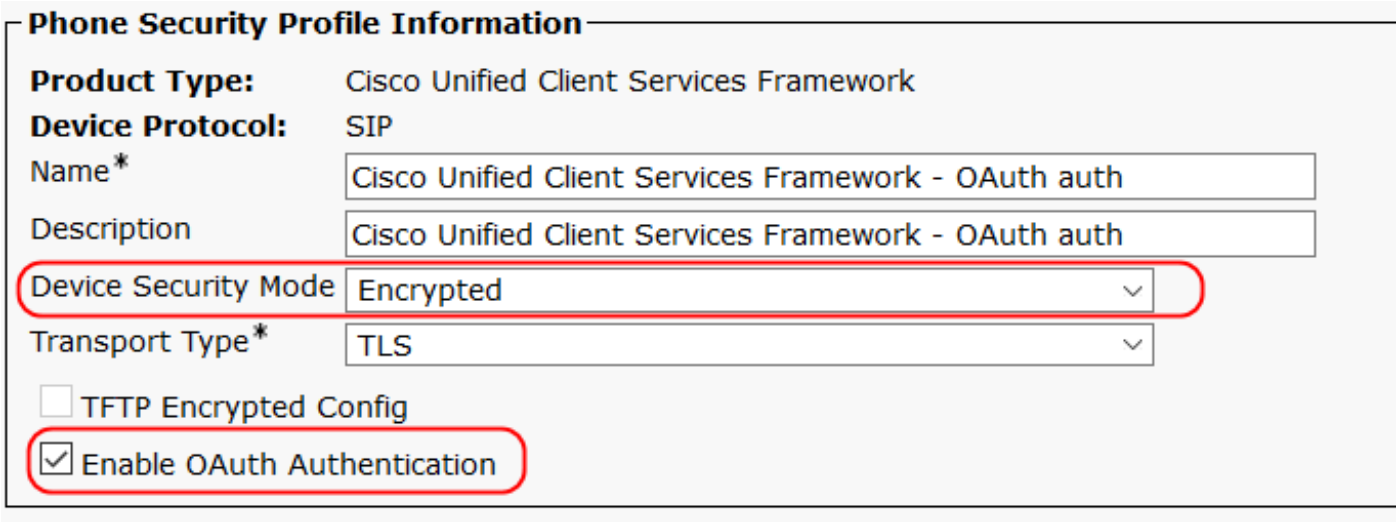
```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

4.重新启动Cisco CallManager服务。

从Cisco Unified Serviceability中选择Tools > Control Center - Feature Services。在服务处于活动状态的所有节点上选择并重新启动Cisco CallManager服务。

5.在安全配置文件中配置OAuth支持

从Cisco Unified CM Administration中，选择System > Phone Security Profile。选择Enable OAuth Authentication以启用终端的SIP OAuth支持。



配置 — 基于MRA的Jabber

前提条件

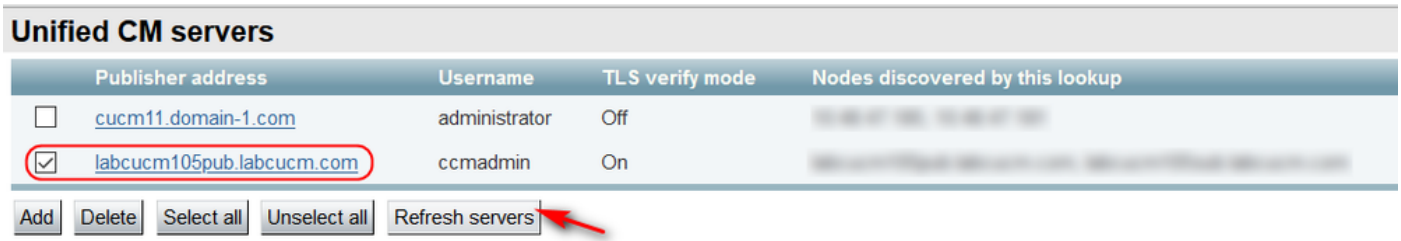
在配置用于MRA上的Jabber的SIP OAuth模式之前，请完成本文中配置 — Jabber本地一章中的步骤1-4。

步骤1.启用Refresh Login over MRA。

在使用Cisco Jabber over MRA配置SIP OAuth身份验证之前，必须在Expressway（也称为自描述令牌）上启用刷新登录。在Expressway-C上，导航到配置>统一通信>配置，并确保通过OAuth令牌进行授权并刷新参数设置为“打开”。

步骤2.刷新Expressway-C中的Unified CM节点。

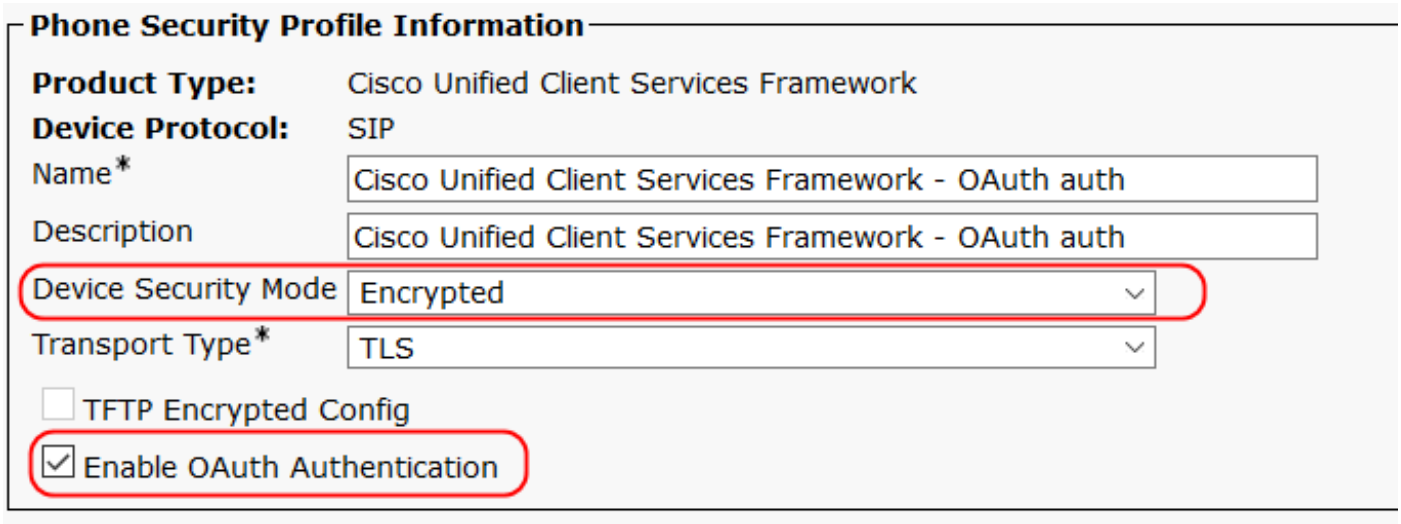
导航到配置>统一通信> Unified CM服务器。发现或刷新Expressway-C中的Unified CM节点。



注意：在Expressway-C中自动创建新的CEOAuth(TLS)区域。例如，CEOAuth <Unified CM name>。创建搜索规则，将来自Jabber over MRA的SIP请求代理到Unified CM节点。此区域使用TLS连接，而不管是否为Unified CM配置了混合模式。为了建立信任，Expressway-C还将主机名和主题备用名称(SAN)详细信息发送到Unified CM集群。请参阅本文的验证部分，确保正确配置到位。

步骤3.在安全配置文件中配置OAuth支持。

从Cisco Unified CM Administration中，选择System > Phone Security Profile。在分配给Cisco Jabber的配置文件上启用OAuth支持。



验证

1.检查SIP OAuth模式是否已全局启用。

从Cisco Unified CM Administration验证OAuth模式，选择System > Enterprise Parameters。

或者，使用Admin CLI — 运行命令：运行sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'

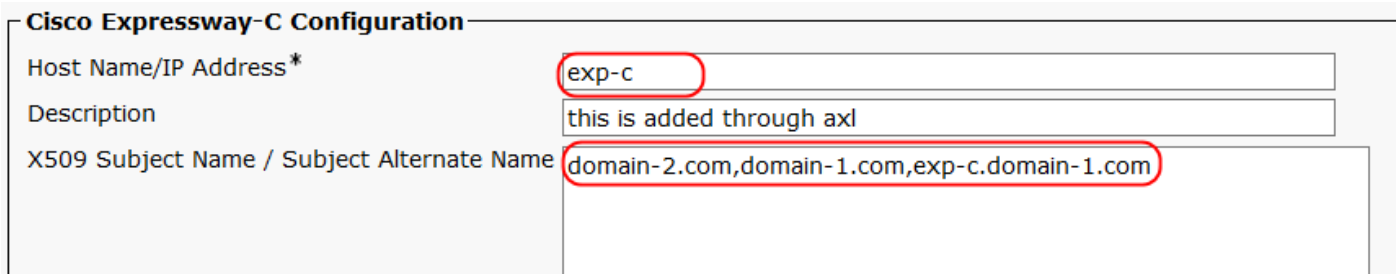
```
admin:run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'
paramvalue
==========
1
admin:
```

可能的值：0 — 表示已禁用（默认），1 — 表示已启用。

2.验证Expressway-C SAN条目是否已成功推送到CUCM。

Expressway-C通过AXL将其证书的CN/SAN详细信息发送到UCM。这些详细信息保存在expresswaycconfiguration表中。每次发现或刷新Expressway-C中的Unified CM节点时，都会调用此过程。这些条目用于在UCM和Expressway-C之间建立信任。在与SIP MRA OAuth端口（默认情况下为5091）的MTLS连接期间，Expressway-C证书的CN/SAN字段会对照这些条目进行检查。 如果验证失败，则MTLS连接失败。

验证来自Cisco Unified CM Administration的条目，选择Device > Expressway-C（从UCM 12.5.1Su1开始）

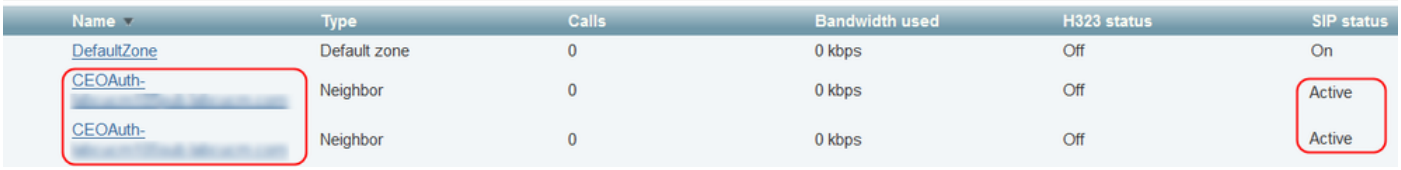


或者，使用Admin CLI — 运行命令：从expresswaycconfiguration运行sql select *

```
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.验证Expressway-C上的CEOAuth区域。

导航到Expressway-C > Configuration > Zones > Zones。确保所有新创建的CEOAuth区域处于活动状态。



4.验证CallManager进程侦听SIP OAuth端口。

从管理CLI运行命令：show open ports regexp 5090(默认SIP OAuth端口)

```
admin:show open ports regexp 5090

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

从管理CLI运行命令：show open ports regexp 5091(默认SIP MRA OAuth端口)

```
admin:show open ports regexp 5091

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

故障排除

Jabber日志示例（本地）

从Jabber日志角度查看端口5090上的本地SIP OAuth注册的日志示例。

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

场景1 - SIP OAuth注册端口不匹配

SIP OAuth模式下的本地部署Jabber设备无法向UCM注册。UCM发送403作为注册消息：

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

可能的解决方案:确保满足以下条件：

- OAuth模式已全局启用
- 与设备关联的设备安全配置文件已启用OAuth支持
- 通过TLS而不是mTLS在5090端口上接收的消息

场景2 — 来自Expressway的未知CA

Expressway-C无法与sipMAOAuthport上的UCM建立mTLS握手（默认值为5091）。 Expressway-C不信任UCM共享的证书，并在mTLS设置期间使用未知CA消息进行响应。

可能的解决方案:CallManager服务在mTLS握手期间发送其Tomcat证书。确保Expressway-C信任UCM Tomcat证书的签名者。

场景3 — 来自UCM的未知CA

Expressway-C无法与sipMAOAuthport上的UCM建立mTLS握手（默认值为5091）。UCM不信任Expressway共享的证书，并在mTLS设置期间以未知CA消息进行响应。

此通信的数据包捕获(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=

可能的解决方案:UCM使用Tomcat-trust存储区在SIP OAuth端口上的mTLS握手期间验证传入证书。确保Expressway-C的签名人证书正确上传到UCM。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。