Cisco Jabber和SIP OAuth模式

目錄

簡介

本文檔介紹使用Cisco Jabber實施SIP OAuth模式的配置和基本故障排除步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Jabber軟體電話註冊
- 整合通訊管理員(UCM)
- 行動與遠端存取(MRA)解決方案

採用元件

支援SIP OAuth模式的最低軟體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

限制

啟用SIP OAuth模式後，不支援Enable Digest Authentication和TFTP Encrypted Config選項。

背景資訊

主要優勢

保護Cisco Jabber軟體電話的SIP信令和媒體目前涉及多個配置步驟。最難的是安裝和續訂客戶端證書(LSC)，尤其是當思科Jabber裝置在內部和外部之間切換時，並且使CTL檔案中的證書保持最新。

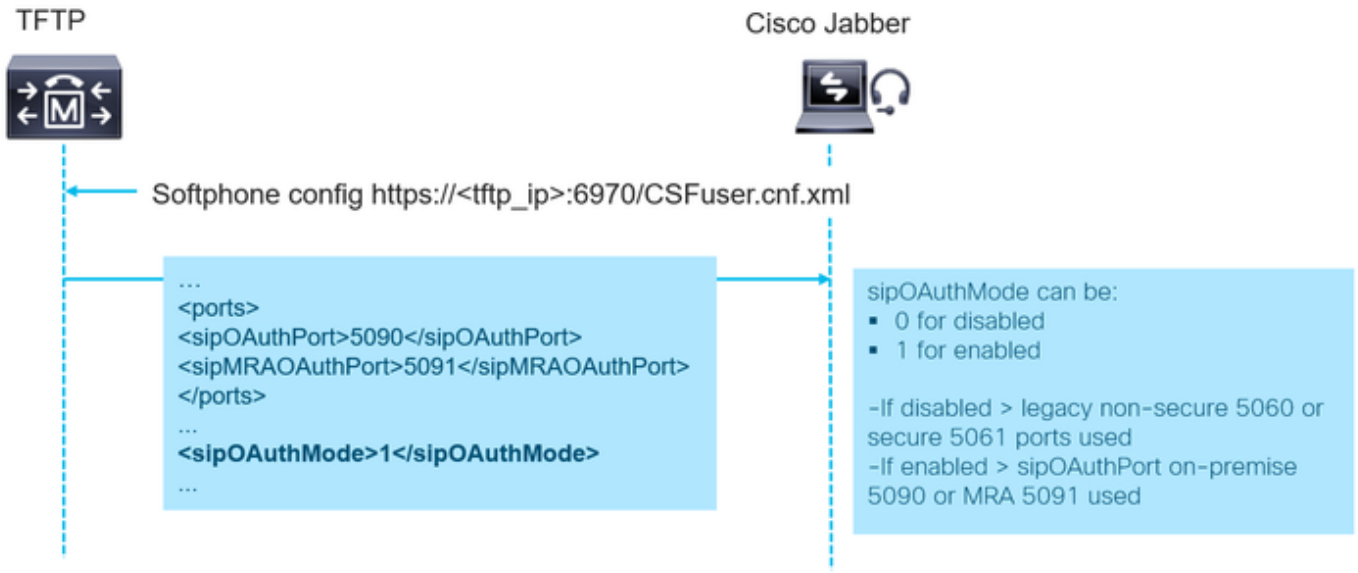
SIP OAuth模式允許Cisco Jabber軟體電話使用OAuth自描述令牌而不是客戶端LSC證書在安全SIP介面上進行身份驗證。在UCM SIP介面上支援OAuth允許為Jabber本地部署和MRA部署提供安全信令和媒體，而無需混合模式或CAPF操作。

適用於Cisco Jabber的SIP OAuth模式支援的主要優勢：

- 啟用永遠線上加密而不增加管理負擔。
- 適用於Cisco Jabber的安全訊號傳送和媒體，無需混合模式（無CTL更新、憑證維護等）
- 無需在Jabber客戶端上安裝並維護LSC。
    - LSC在多個裝置（筆記型電腦/流動裝置……）上面臨的挑戰
    - 每當在新裝置上安裝Jabber時，都需要執行CAPF操作。
    - MRA不支援CAPF操作。

整體架構

Cisco Jabber裝置通過解析CSF配置檔案(http://<cucmIP>:6970/<CSF-device-name>.cnf.xml)、配置檔案示例（為了簡潔而略去一些行）識別在SIP介面上啟用了OAuth身份驗證：



Cisco Jabber讀取sipOAuthMode引數以確定SIP OAuth模式是否已啟用。此引數可以採用以下值之一：

- 0 - SIP OAuth已禁用
- 1 — 啟用SIP OAuth

如果啟用SIP OAuth模式,Jabber將使用這些引數之一確定SIP TLS連線的埠 — sipOAuthPort（本地使用）或sipMAOAuthPort（基於MRA的部署）。示例顯示了預設值 — sipOAuthPort 5090和sipMAOAuthPort 5091。這些值是可配置的，並且在每個CUCM節點上可以不同。

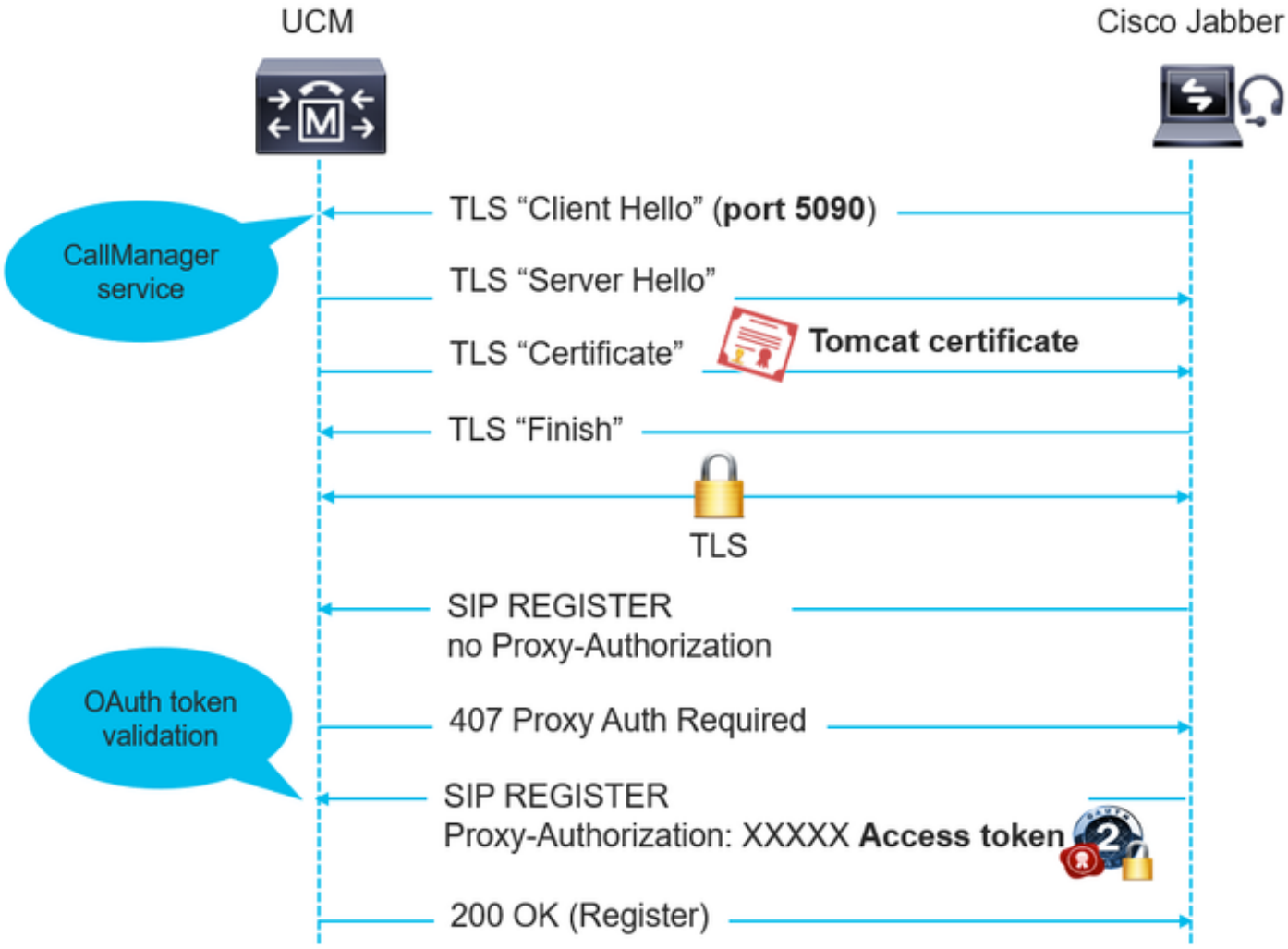
如果SIP OAuth模式已禁用，則Jabber使用舊版非安全(5060)或安全(5061)埠進行SIP註冊。

附註：Cisco UCM使用SIP電話OAuth埠(5090)通過TLS收聽Jabber OnPremise裝置的SIP線路註冊。但是，UCM使用SIP移動遠端訪問埠（預設5091）通過mLTS偵聽Jabber over Expressway的SIP線路註冊。這兩個連線埠均可設定。請參見配置部分。

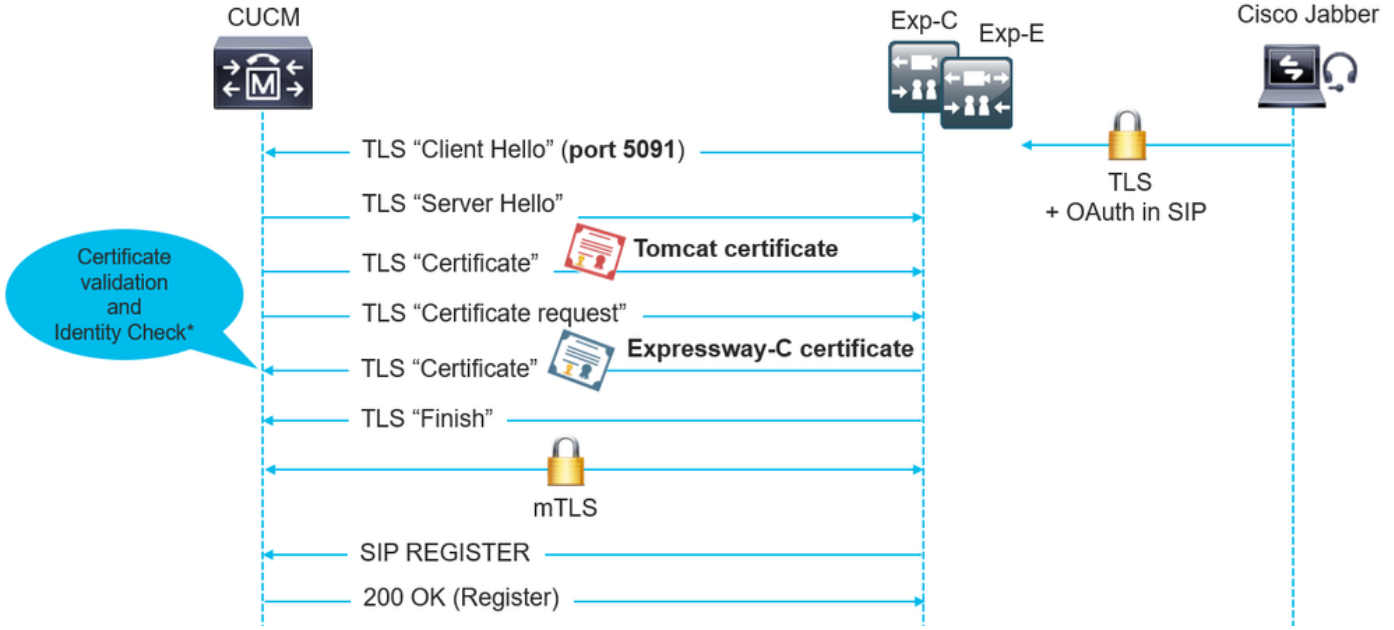
CallManager服務在sipOAuthPort和sipMAOAuthPort上偵聽。但是，兩個埠都使用Tomcat證書和Tomcat-trust進行傳入的TLS/mTLS連線。確保Tomcat信任儲存能夠驗證SIP OAuth模式的Expressway-C證書以使MRA正常運行。

如果重新生成Tomcat證書，則隨後必須在受影響的節點上重新啟動CallManager進程。CCM進程在sipOAuth埠上載入和使用新證書時需要此步驟。

此圖說明在內部部署時Cisco Jabber的註冊:



此圖說明Cisco Jabber over MRA的註冊：



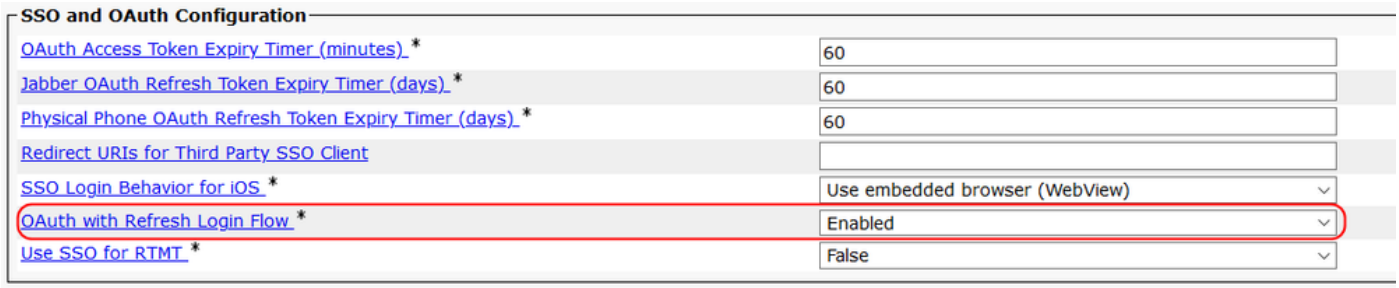
*Expressway-C節點使用AXL API通知UCM其證書中的CN/SAN。UCM使用此資訊驗證建立雙方TLS連線時的Exp-C證書。

配置 — 本地Jabber

附註：
在配置SIP OAuth模式之前，請確保完成以下幾點：
— 配置了MRA，並且在Unified Communication Manager(UCM)和Expressway之間建立連線（僅在使用MRA時適用）。
- UCM註冊到允許匯出控制功能的智慧或虛擬帳戶。

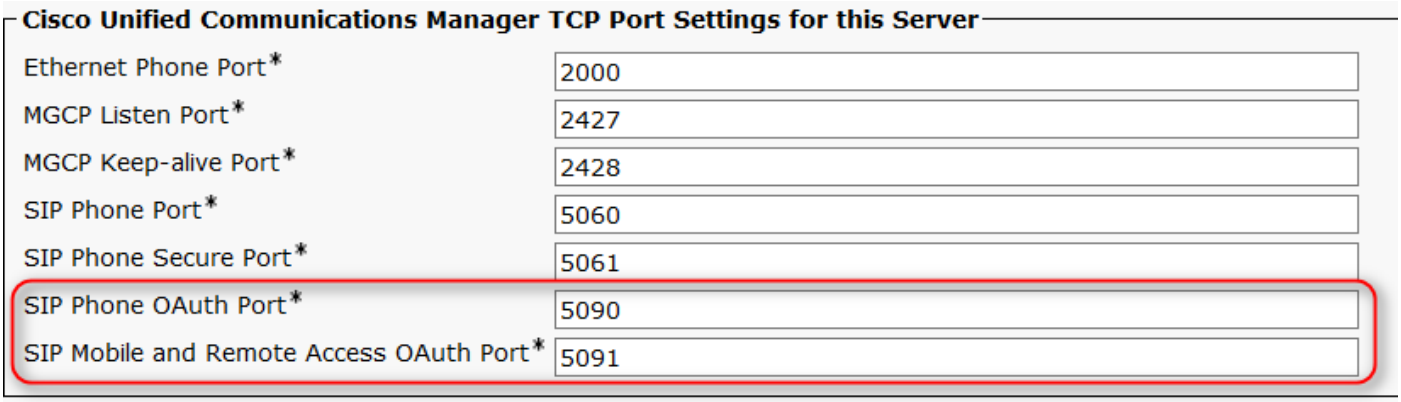
1.配置刷新登入。

使用OAuth訪問令牌配置「刷新登入」，並為Cisco Jabber客戶端配置刷新令牌。從Cisco Unified CM Administration中，選擇System > Enterprise Parameters。



2.配置OAuth埠

選擇System > Cisco Unified CM。這是選用步驟。圖片顯示預設值。可接受的可配置範圍為1024到49151。請對每個伺服器重複相同的過程。



3.啟用SIP OAuth模式。

使用發布器的命令列介面全域性啟用SIP OAuth模式。運行命令：utils sipOAuth-mode enable。

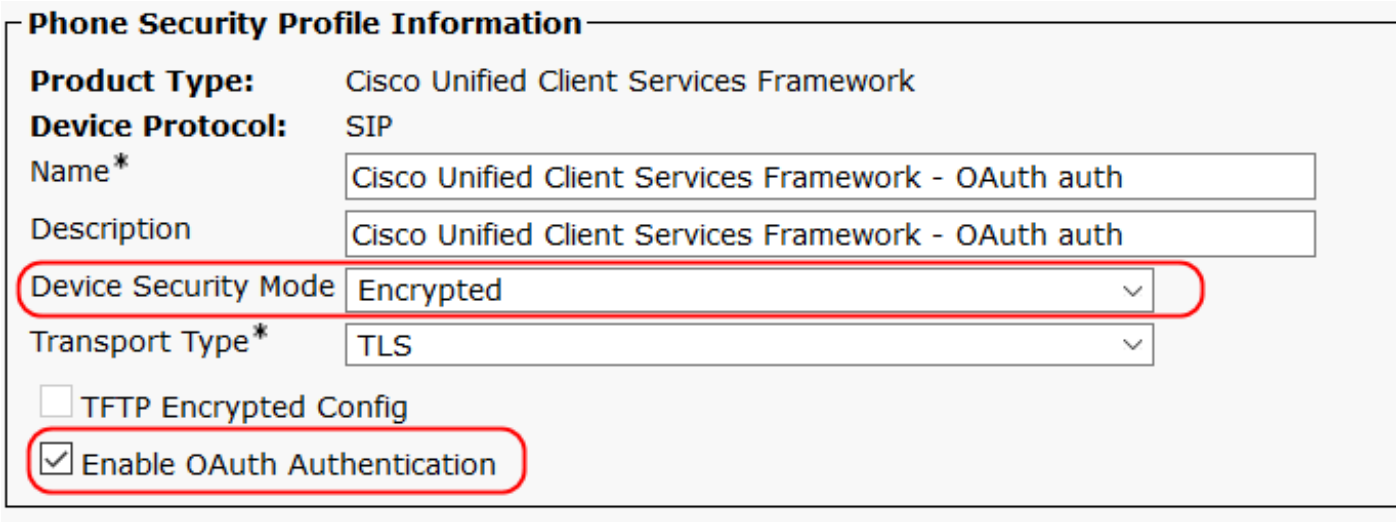
```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

4.重新啟動Cisco CallManager服務。

在Cisco Unified Serviceability中選擇Tools > Control Center - Feature Services。在服務處於活動狀態的所有節點上選擇並重新啟動Cisco CallManager服務。

5.在安全配置檔案中配置OAuth支援。

在Cisco Unified CM Administration中選擇System > Phone Security Profile。選擇Enable OAuth Authentication以啟用終端的SIP OAuth支援。



組態 — 使用MRA的Jabber

前提條件

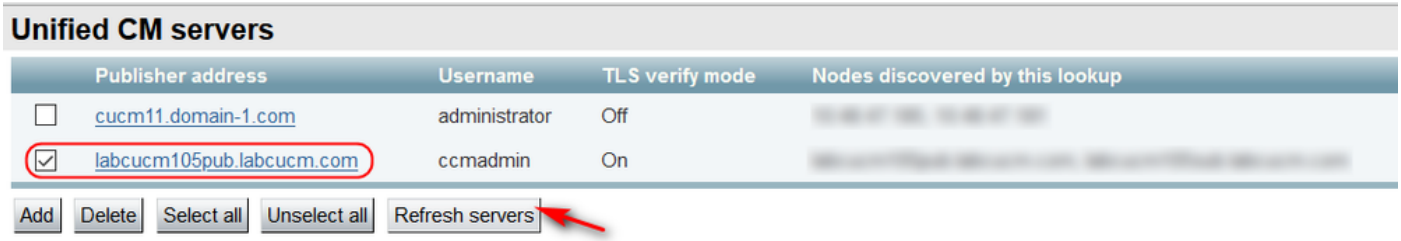
在配置SIP OAuth mode for Jabber over MRA之前，請完成本文的配置 — Jabber內部部署一章中的步驟1-4。

步驟1.啟用Refresh Login over MRA。

使用Cisco Jabber over MRA配置SIP OAuth身份驗證之前，必須在Expressway（也稱為自描述令牌）上啟用刷新登入。在Expressway-C上，導航到Configuration > Unified Communications > Configuration，確保Authorize by OAuth Token with refresh引數設定為On。

步驟2.刷新Expressway-C中的Unified CM節點。

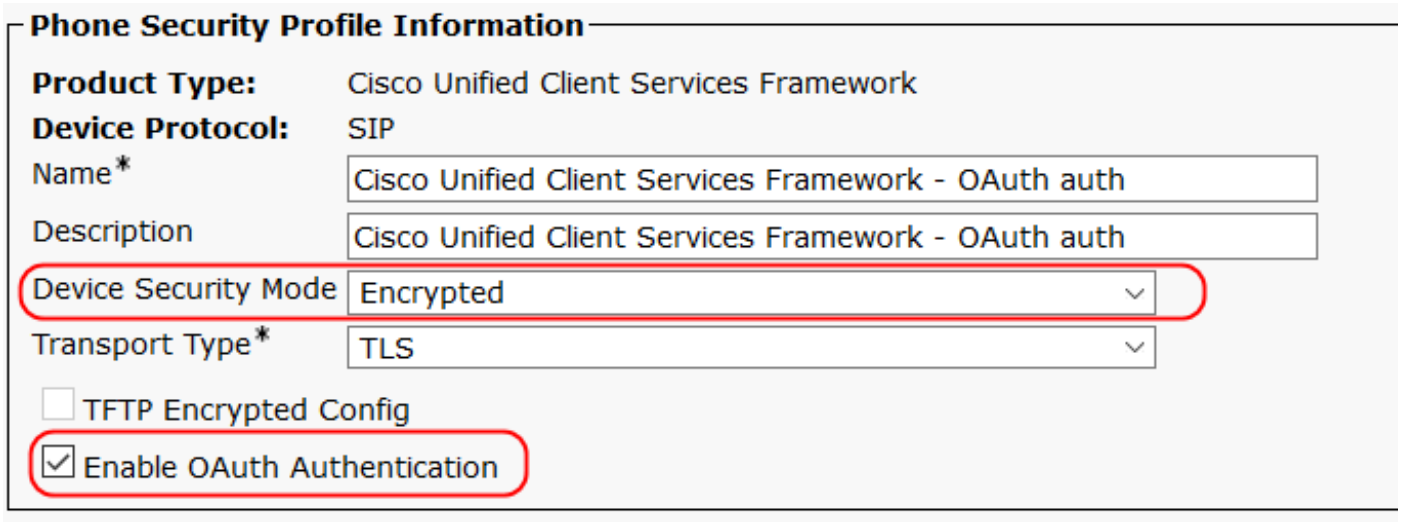
導航到Configuration > Unified Communications > Unified CM servers。發現或刷新Expressway-C中的Unified CM節點。



附註：在Expressway-C中自動建立新的CEOAuth(TLS)區域。例如CEOAuth <Unified CM name>。建立搜尋規則以將源自Jabber over MRA的SIP請求代理到Unified CM節點。此區域使用TLS連線，而不考慮Unified CM是否配置為混合模式。為了建立信任，Expressway-C還將主機名和主題備用名稱(SAN)詳細資訊傳送到Unified CM集群。請參閱本文的驗證部分，確保正確配置已就緒。

步驟3.在安全配置檔案中配置OAuth支援。

在Cisco Unified CM Administration中選擇System > Phone Security Profile。在分配給Cisco Jabber的配置檔案上啟用OAuth支援。



驗證

1.檢查SIP OAuth模式是否為「全域性啟用」。

從Cisco Unified CM Administration驗證OAuth模式，選擇System > Enterprise Parameters。

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

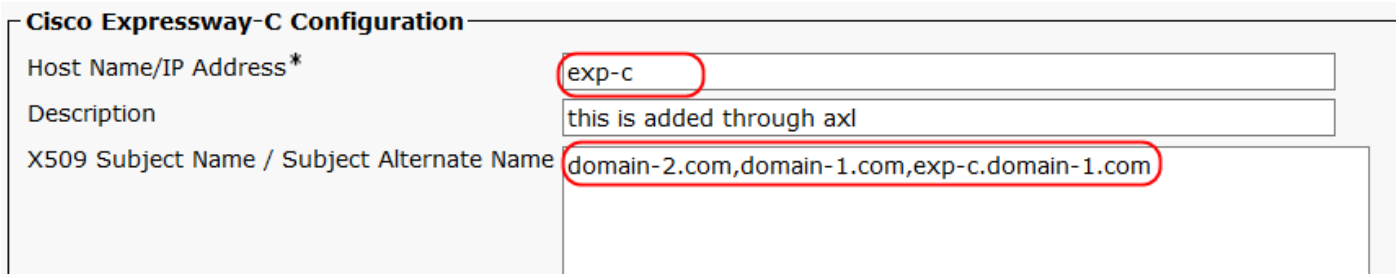
```
admin:run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'
paramvalue
==========
1
admin:
```

可能的值：0 — 表示已禁用（預設），1 — 表示已啟用。

2.驗證Expressway-C SAN條目是否已成功推送到CUCM。

Expressway-C通過AXL將其證書的CN/SAN詳細資訊傳送到UCM。這些詳細資訊儲存在expresswaycconfiguration表中。每次發現或刷新Expressway-C中的Unified CM節點時，都會呼叫此過程。這些條目用於建立UCM和Expressway-C之間的信任。在MTLS連線到SIP MRA OAuth埠（預設情況下為5091）期間，會針對這些條目檢查Expressway-C證書的CN/SAN欄位。 如果驗證失敗，MTLS連線將失敗。

驗證Cisco Unified CM Administration中的條目，選擇Device > Expressway-C（從UCM 12.5.1Su1開始）

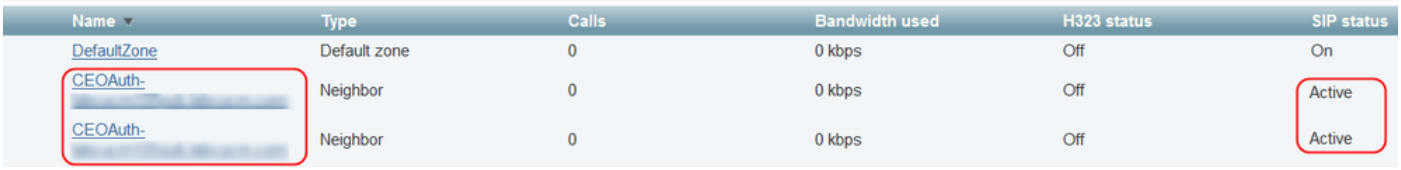


或者，也可以使用管理CLI — 運行命令：從expresswaycconfiguration運行sql select *

```
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.驗證Expressway-C上的CEOAuth區域。

導航到Expressway-C > Configuration > Zones > Zones。確保所有新建立的CEOAuth區域處於活動狀態。



4.驗證CallManager進程在SIP OAuth埠上偵聽。

從管理員CLI運行命令：show open ports regexp 5090(預設SIP OAuth埠)

```
admin:show open ports regexp 5090

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

從管理員CLI運行命令：show open ports regexp 5091(預設SIP MRA OAuth埠)

```
admin:show open ports regexp 5091

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

疑難排解

Jabber日誌示例（本地）

從Jabber日誌角度檢視埠5090上的本地SIP OAuth註冊的日誌示例。

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

場景1 - SIP OAuth註冊埠不匹配

在SIP OAuth模式下的內部部署Jabber裝置無法向UCM註冊。UCM為註冊消息傳送403:

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

可能的解決方案：確保滿足以下條件：

- OAuth模式已全域性啟用
- 與裝置關聯的裝置安全配置檔案已啟用OAuth支援
- 在5090埠上通過TLS而不是mTLS接收的消息

場景2 — 來自Expressway的未知CA

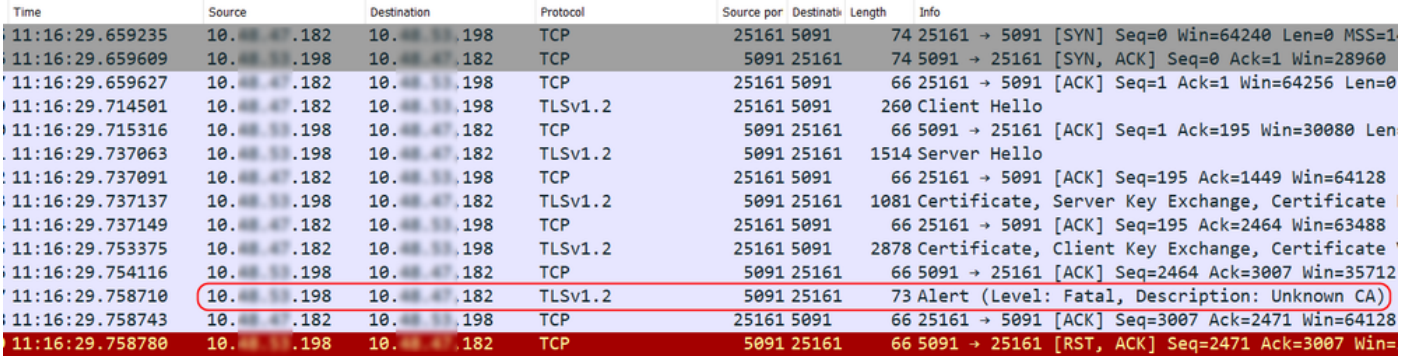
Expressway-C無法在sipMAOAuthport上與UCM建立mTLS握手（預設值為5091）。 Expressway-C不信任UCM共用的證書，並在mTLS設定期間使用未知CA消息進行響應。

可能的解決方案：CallManager服務在mTLS握手期間傳送其Tomcat證書。確保Expressway-C信任UCM Tomcat證書的簽名者。

案例3 - UCM中的未知CA

Expressway-C無法在sipMAOAuthport上與UCM建立mTLS握手（預設值為5091）。UCM不信任Expressway共用的證書，並在mTLS設定期間使用未知CA消息進行響應。

從此通訊捕獲的資料包(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=

可能的解決方案：UCM在SIP OAuth埠上的mTLS握手期間使用Tomcat-trust儲存驗證傳入證書。確保Expressway-C的簽名者證書正確上傳到UCM。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。