Cisco JabberおよびSIP OAuthモード

内容

はじめに

このドキュメントでは、Cisco Jabberを使用してSIP OAuthモードを実装するための設定および基本的なトラブルシューティング手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Jabber softphone登録
- Unified Communications Manager（UCM）
- Mobile and Remote Access(MRA)ソリューション

使用するコンポーネント

SIP OAuthモードをサポートするための最小ソフトウェアバージョン：

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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

制約事項

SIP OAuthモードが有効な場合、ダイジェスト認証の有効化オプションとTFTP暗号化設定オプションはサポートされません。

背景説明

主な利点

Cisco Jabber softphoneのSIPシグナリングとメディアの保護には、現在複数の設定手順が必要です。最も困難な作業は、クライアント証明書(LSC)のインストールと更新です。特に、Cisco Jabberデバイスがオンプレミスとオフプレミスを切り替えている場合は、CTLファイル内の証明書を最新の状態に保ちます。

SIP OAuthモードでは、Cisco Jabber Softphoneは、セキュアSIPインターフェイスでの認証に、クライアントLSC証明書の代わりにOAuth自己記述トークンを使用できます。UCM SIPインターフェイスでOAuthをサポートすることで、混合モードやCAPF操作を必要とせずに、Jabberのオンプレミスおよびの導入でセキュアなシグナリングとメディアを実現できます。

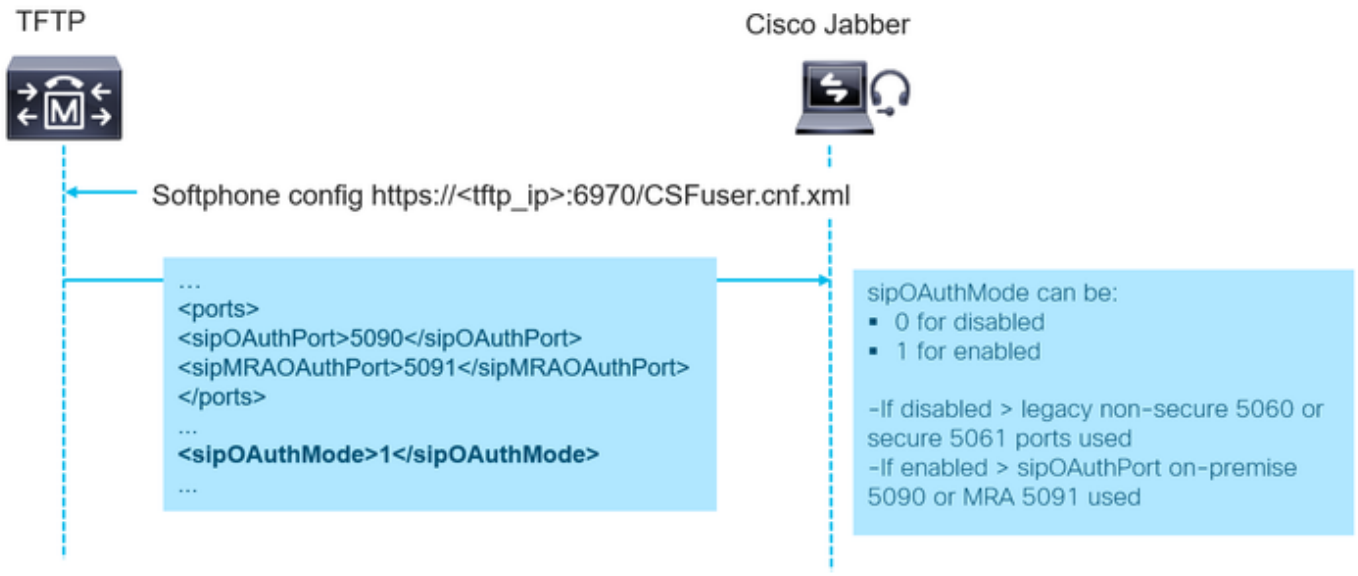
SIP OAuthモードのCisco Jabberサポートの主な利点は次のとおりです。

- 管理者の負担を増やすことなく、暗号化を常時有効にします。
- 混合モードを必要としないCisco Jabberのシグナリングとメディアの保護（CTLの更新、証明書のメンテナンスなど）
- JabberクライアントにLSCをインストールして維持する必要はありません。
    - 複数のデバイス（ラップトップ/モバイルデバイスなど）でのLSCに関する課題

- 新しいデバイスにJabberをインストールするたびにCAPF操作が必要になりました。
- CAPF操作はMRA経由ではサポートされません。

全体的なアーキテクチャ

Cisco Jabberデバイスは、CSFコンフィギュレーションファイル(http://<cucmIP>:6970/<CSF-device-name>.cnf.xml)の例（簡略化のために一部の行を省略）を解析することにより、SIPインターフェイスでOAuth認証が有効になっていることを認識します。



Cisco JabberはsipOAuthModeパラメータを読み取って、SIP OAuthモードが有効かどうかを判断します。このパラメータには、次のいずれかの値を指定できます。

- 0 - SIP OAuthが無効
- 1 - SIP OAuthが有効

SIP OAuthモードが有効になっている場合、Jabberは次のパラメータのいずれかを使用してSIP TLS接続のポート(オンプレミスの場合はsipOAuthPort、MRAベースの導入の場合はsipMRAOAuthPort)を決定します。この例では、デフォルト値のsipOAuthPort 5090とsipMRAOAuthPort 5091を示しています。これらの値は設定可能で、CUCMノードごとに異なる場合があります。

SIP OAuthモードが無効の場合、JabberはSIP登録に従来の非セキュアポート(5060)またはセキュアポート(5061)を使用します。

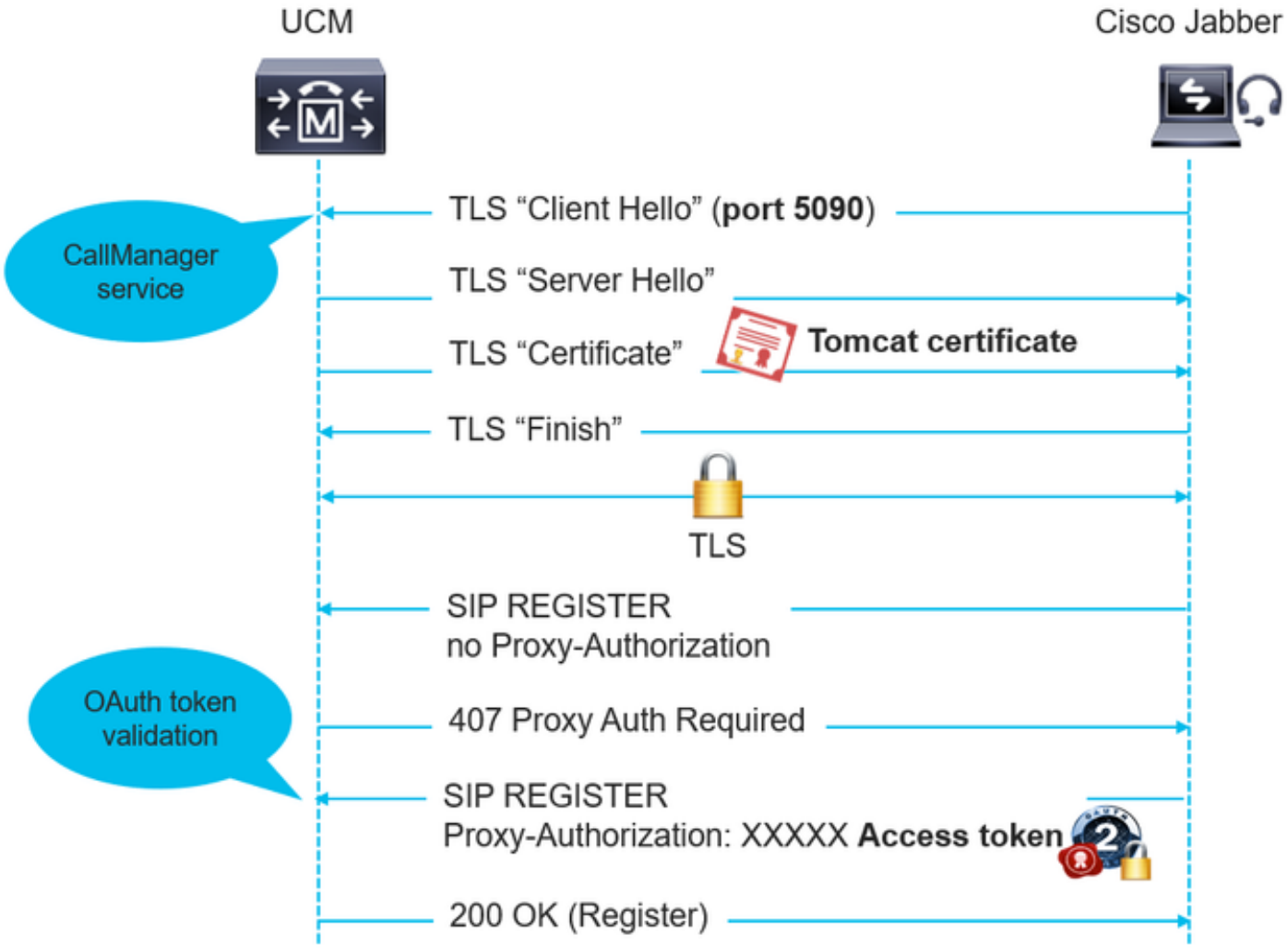
注:Cisco UCMは、SIP電話OAuthポート(5090)を使用して、TLS経由でJabber OnPremiseデバイスからのSIP回線登録をリッスンします。ただし、UCMはSIP Mobile Remote Access Port（デフォルトは5091）を使用して、mLTS経由でJabber over ExpresswayからのSIP回線登録をリッスンします。これらのポートはどちらも設定可能です。設定のセクションを参照してください。

CallManagerサービスは、sipOAuthPortとsipMRAOAuthPortの両方でリッスンします。ただし、どちらのポートも着信TLS/mTLS接続にTomcat証明書とTomcat-trust証明書を使用しま

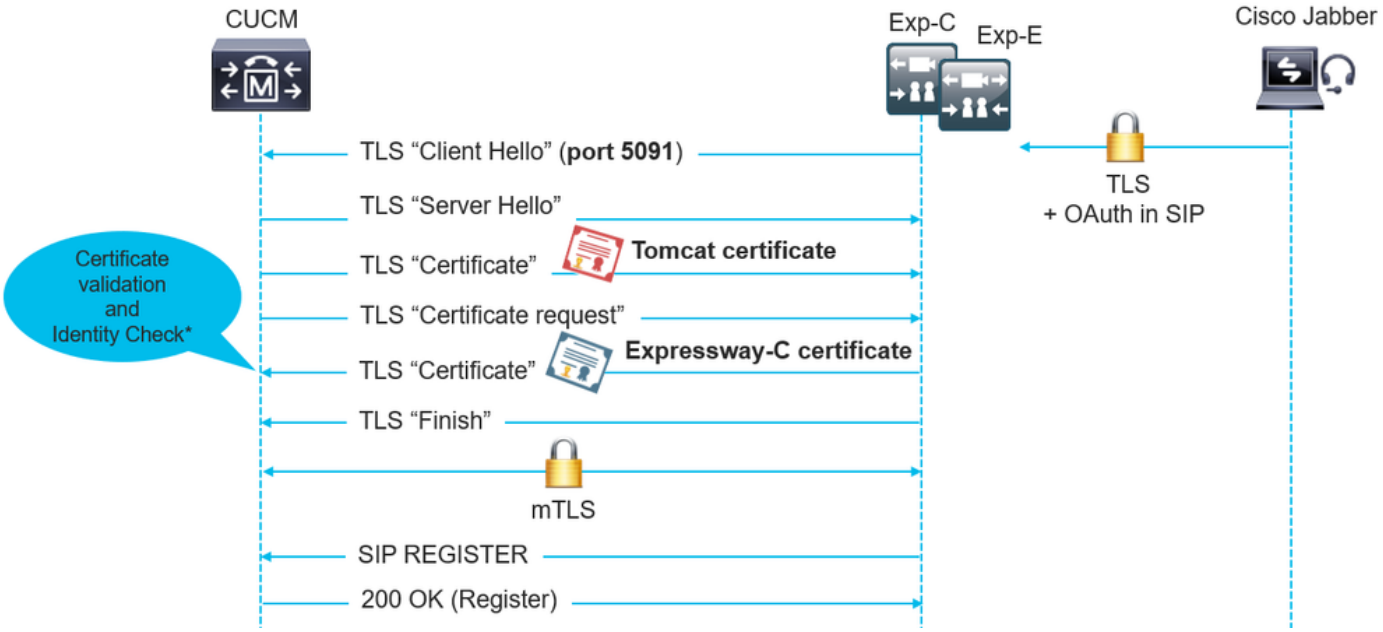
す。MRAが正しく機能するように、Tomcat-trustストアが SIP OAuthモードのExpressway-C証明書を検証できることを確認します。

状況によっては、Tomcat証明書が再生成された後で、影響を受けるノードでCallManagerプロセスを再起動する必要があります。これは、CCMプロセスがsipOAuthポートに新しい証明書をロードして使用するために必要です。

次の図に、オンプレミスでのCisco Jabberの登録を示します。



次の図に、MRAでのCisco Jabber の登録を示します。



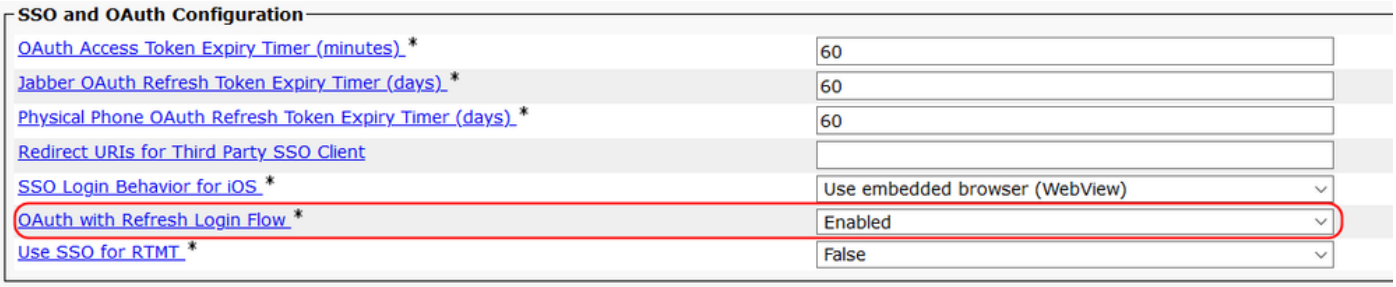
*Expressway-CノードはAXL APIを使用して、証明書のCN/SANをUCMに通知します。相互TLS接続が確立されると、UCMはこの情報を使用してExp-C証明書を検証します。

設定 – Jabber On Premises

注：
SIP OAuthモードを設定する前に、次の点を確認してください。
- MRAが設定され、Unified Communication Manager(UCM)とExpressway間の接続が確立されます（MRAが使用されている場合にのみ適用）。
- UCMがスマートアカウントまたは仮想アカウントに登録されており、エクスポート制御機能を使用できます。

1. 更新ログインを構成します。

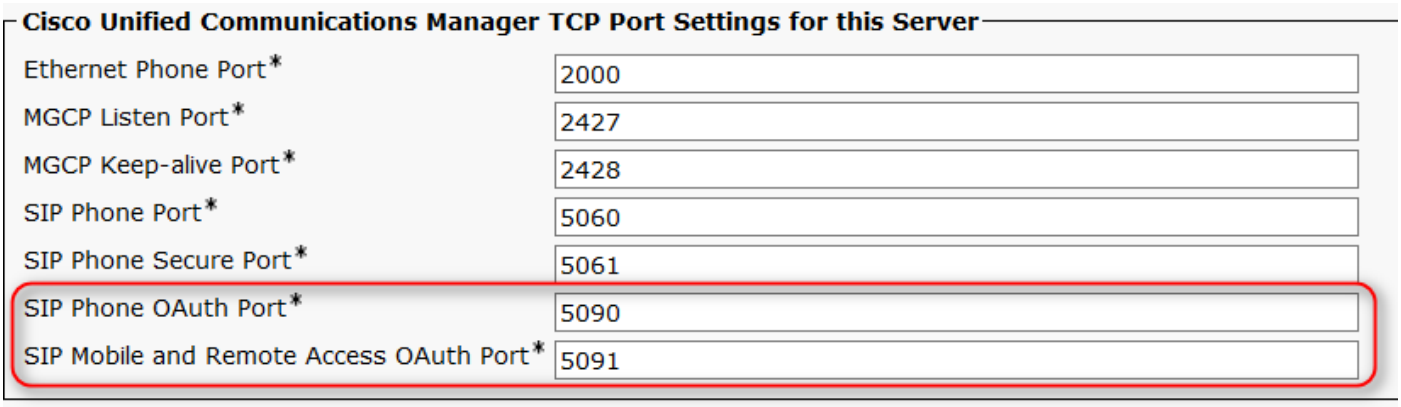
OAuthアクセストークンを使用した更新ログインの設定と、Cisco Jabberクライアントの更新トークンの設定 Cisco Unified CM Administrationで、System > Enterprise Parametersの順に選択します。



2. OAuthポートを構成します。

System > Cisco Unified CMの順に選択します。このステップは任意で実行します。この図はデフ

ォルト値を示しています。設定可能な範囲は1024 ~ 49151です。各サーバに対して同じ手順を繰り返します。



3. SIP OAuthモードを有効にします。

パブリッシャのコマンドラインインターフェイスを使用して、SIP OAuthモードをグローバルに有効にします。 utils sipOAuth-mode enableコマンドを実行します。

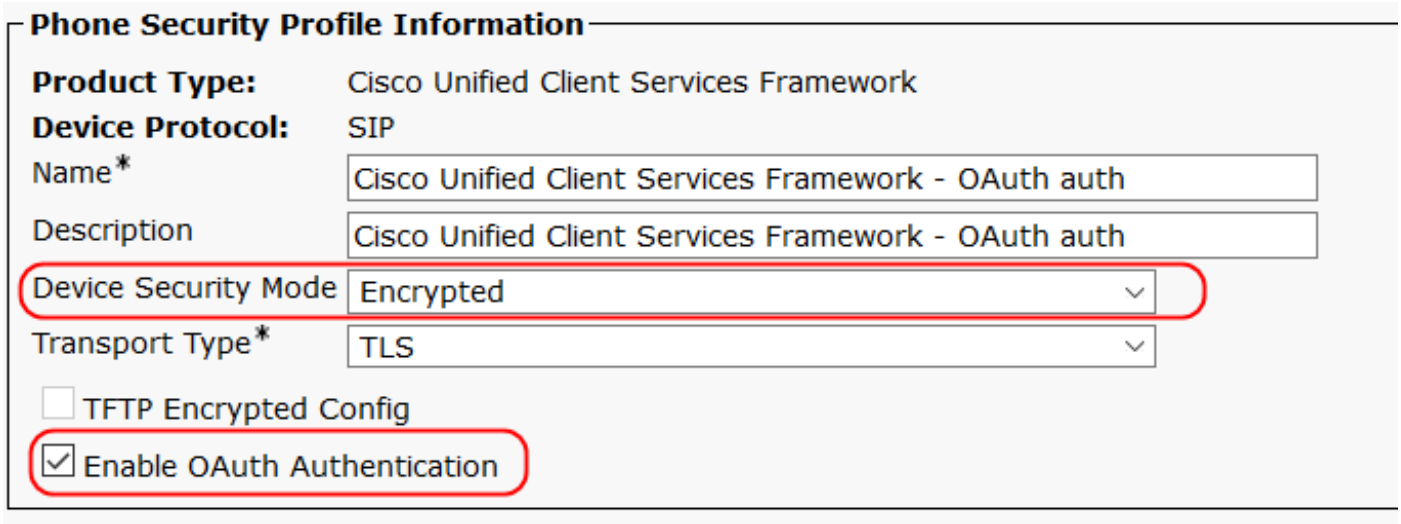
```
admin:utils sipOAuth-mode enable
SIP OAuth mode enabled.
Please restart the Cisco CallManager service on all nodes in the cluster where it is running.
admin:
```

4. Cisco CallManagerサービスを再起動します。

Cisco Unified Serviceabilityから、Tools > Control Center - Feature Servicesの順に選択します。サービスがアクティブになっているすべてのノードで、Cisco CallManagerサービスを選択して再起動します。

5. セキュリティプロファイルでOAuthサポートを構成します。

Cisco Unified CM Administrationで、System > Phone Security Profileの順に選択します。エンドポイントでSIP OAuthサポートを有効にするには、Enable OAuth Authenticationを選択します。



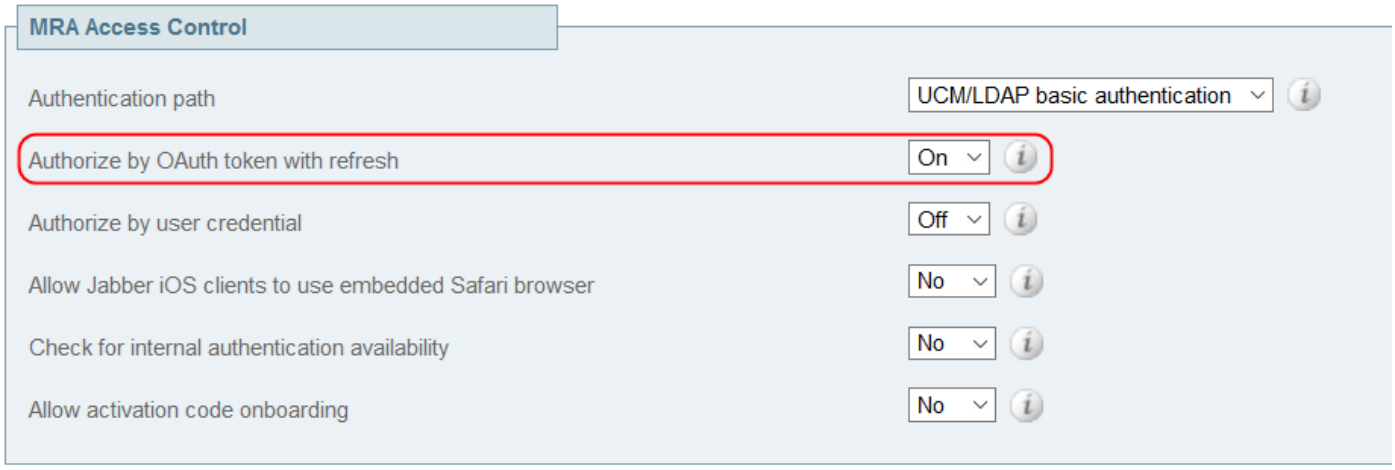
設定：Jabber over MRA

前提条件

Jabber over MRA用のSIP OAuthモードを設定する前に、この記事の「設定 – Jabber On Premises」の章でステップ1 ～ 4を実行してください。

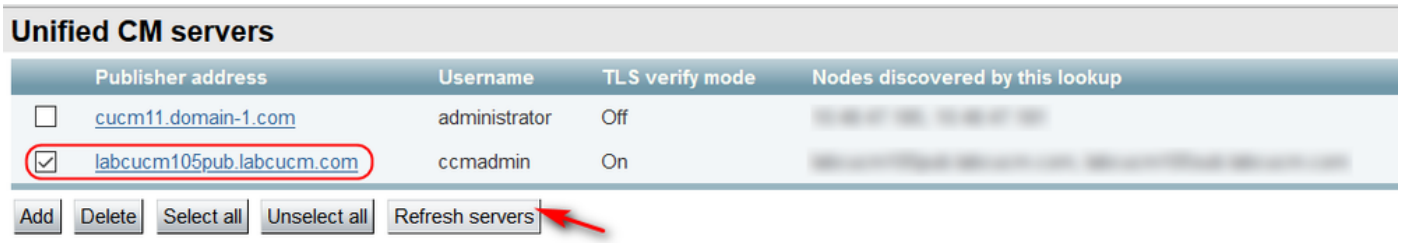
ステップ 1：MRA経由の更新ログインを有効にします。

Cisco Jabber over MRAでSIP OAuth認証を設定する前に、Expresswayで更新ログイン（自己記述トークンとも呼ばれます）を有効にする必要があります。 Expressway-Cで、Configuration > Unified Communications > Configurationの順に移動し、Authorize by OAuth Token with refreshパラメータがOnに設定されていることを確認します。



ステップ 2：Expressway-CでUnified CMノードを更新します。

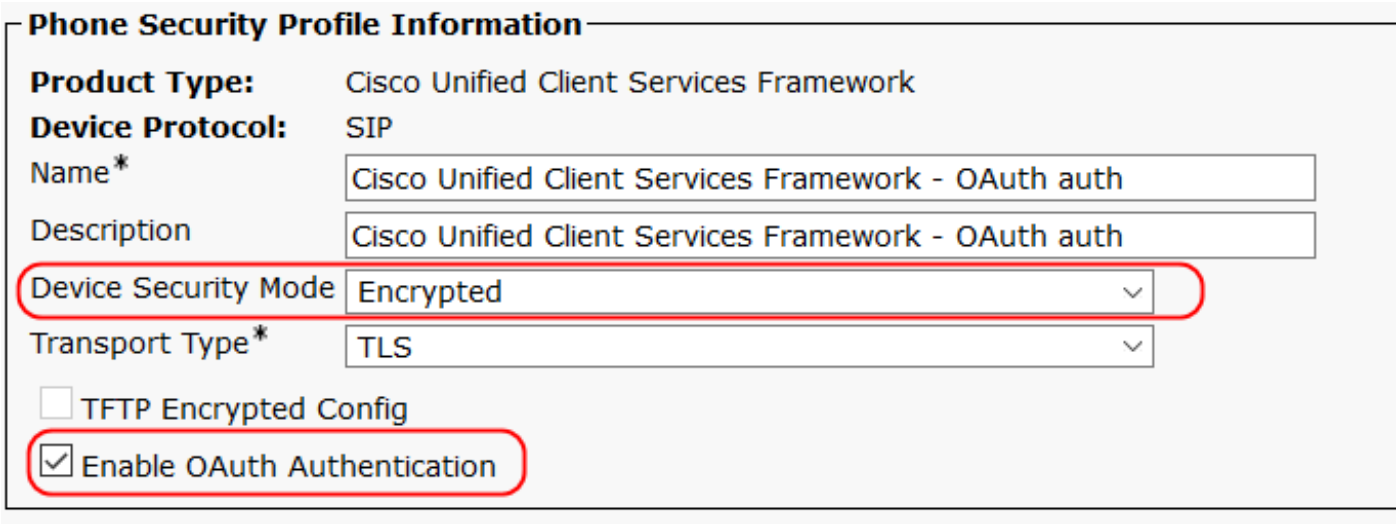
Configuration > Unified Communications > Unified CM serversの順に移動します。Expressway-CでUnified CMノードを検出または更新します。



注：新しいCEOAuth(TLS)ゾーンがExpressway-Cで自動的に作成されます。たとえば、CEOAuth <Unified CM名>などです。検索ルールは、Jabber over MRAから発信されたSIP要求をUnified CMノードにプロキシするために作成されます。このゾーンでは、Unified CMが混合モードで設定されているかどうかに関係なく、TLS接続が使用されます。 信頼を確立するため、Expressway-Cはホスト名とサブジェクト代替名(SAN)の詳細もUnified CMクラスタに送信します。適切な設定が行われていることを確認するには、この記事の検証の部分を参照してください。

ステップ 3：セキュリティプロファイルでOAuthサポートを設定します。

Cisco Unified CM Administrationで、System > Phone Security Profileの順に選択します。Cisco Jabberに割り当てられているプロファイルでOAuthサポートを有効にします。



確認

1. SIP OAuthモードがグローバルに有効になっているかどうかを確認します。

Cisco Unified CM AdministrationからOAuthモードを確認し、System > Enterprise Parametersの順に選択します。

または、管理CLIを使用して、コマンドを実行します。run sql select paramvalue FROM processconfig WHERE paramname = 'ClusterSIPOAuthMode'

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

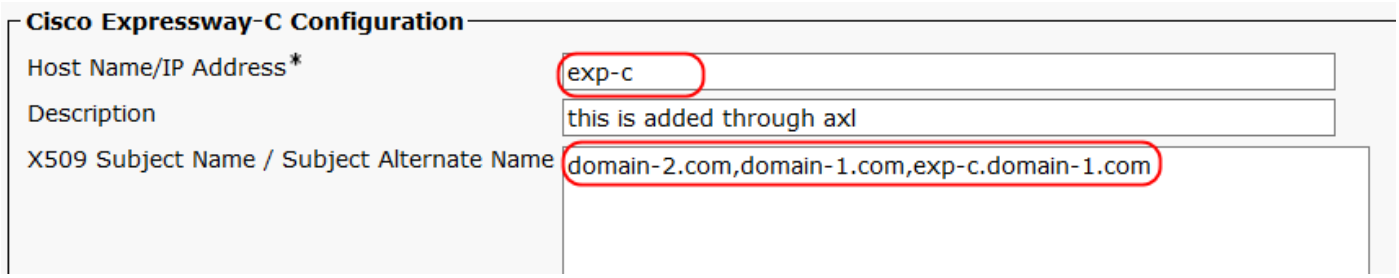
取り得る値は、0 - Disabled（デフォルト）、1 - Enabledです。

2. Expressway-C SANエントリがCUCMに正常にプッシュされたことを確認します。

Expressway-CはAXLを介して証明書のCN/SANの詳細をUCMに送信します。これらの詳細は、expresswayconfigurationテーブルに保存されます。このプロセスは、Expressway-CでUnified CMノードを検出または更新するたびに起動されます。これらのエントリは、UCMとExpressway-

C間の信頼を確立するために使用されます。Expressway-C証明書のCN/SANフィールドは、SIP MRA OAuthポート（デフォルトでは5091）へのMTLS接続中にこれらのエントリに対してチェックされます。 検証に失敗すると、MTLS接続は失敗します。

Cisco Unified CM Administrationからエントリを確認し、Device > Expressway-Cの順に選択します（UCM 12.5.1Su1以降から使用可能）

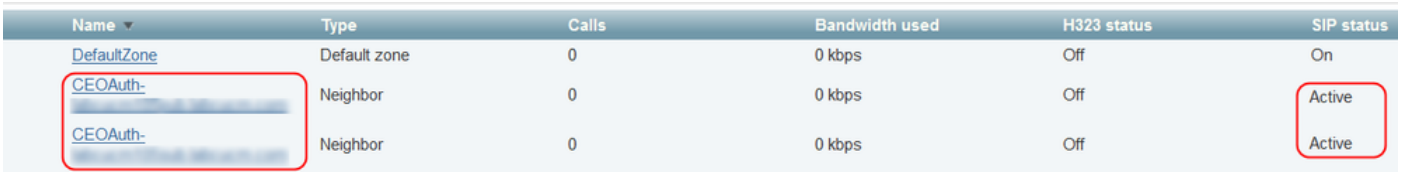


または、管理CLIを使用して、コマンドを実行します。run sql select * from expresswaycconfiguration

```
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. Expressway-CでCEOAuth Zone(s)を確認します。

Expressway-C > Configuration > Zones > Zonesの順に移動します。新しく作成されたすべてのCEOAuthゾーンがアクティブ状態であることを確認します。



4. CallManagerプロセスがSIP OAuthポートでリッスンすることを確認します。

管理CLIから、show open ports regexp 5090（デフォルトのSIP OAuthポート）コマンドを実行します。

```
admin:show open ports regexp 5090

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

管理CLIから、show open ports regexp 5091（デフォルトのSIP MRA OAuthポート）コマンドを実行します。

```
admin:show open ports regexp 5091

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

トラブルシュート

Jabberログの例（オンプレミス）

Jabberログの観点から、ポート5090でのオンプレミスSIP OAuth登録のログ例。

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

シナリオ1:SIP OAuth登録ポートの不一致

SIP OAuthモードのオンプレミスのJabberデバイスがUCMに登録できません。UCMがRegisterメッセージに403を送信：

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

考えられる解決方法：次の条件が満たされていることを確認します。

- OAuthモードはグローバルに有効です
- デバイスに関連付けられたデバイスセキュリティプロファイルでOAuthサポートが有効になっています
- mTLSではなくTLSを介して5090ポートでメッセージを受信

シナリオ2:Expresswayからの不明なCA

Expressway-CがsipMRAOAuthport（デフォルトは5091）でUCMとのmTLSハンドシェイクを確立できません。 Expressway-CはUCMによって共有される証明書を信頼せず、mTLSセットアップ中に不明なCAメッセージで応答します。

解決策：CallManagerサービスはmTLSハンドシェイク中にTomcat証明書を送信します。Expressway-CがUCMのTomcat証明書の署名者を信頼していることを確認します。

シナリオ3:UCMからの不明なCA

Expressway-CがsipMRAOAuthport（デフォルトは5091）でUCMとのmTLSハンドシェイクを確立できません。 UCMはExpresswayで共有される証明書を信頼せず、mTLSセットアップ中に不明なCAメッセージで応答します。

この通信からのパケットキャプチャ(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=

考えられる解決方法：UCMは、SIP OAuthポートでのmTLSハンドシェイク中に、Tomcat-trustストアを使用して着信証明書を確認します。Expressway-Cの署名者の証明書がUCMに正しくアップロードされていることを確認します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。