セキュアな外部電話サービスの設定例

内容

概要

このドキュメントでは、セキュアな外部電話サービスを設定する方法について説明します。この設定は任意のサードパーティサービスで使用できますが、デモンストレーション用に、このドキュメントではリモートのCisco Unified Communications Manager(CUCM)サーバを使用します。

著者：Cisco TACエンジニア、Jose Villalobos

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。

- CUCM
- CUCM証明書
- 電話サービス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM 10.5.X/CUCM 11.X
- Skinny Client Control Protocol(SCCP)およびSession Initiation Protocol(SIP)電話機はCUCMに登録されます
- ラボでは、サブジェクト代替名(SAN)証明書を使用します。
- 外部ディレクトリはSAN証明書に含まれます。
- この例のすべてのシステムで、認証局(CA)が同じになり、使用される証明書はすべてCA署名になります。
- ドメインネームサーバ(DNS)とネットワークタイムプロトコル(NTP)は、プロパティの設定と動作が必要です。

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、初期（デフォルト）設定の状態から起動しています。ネットワークが稼働中の場合は、変更が及ぼす潜在的な影響について確実に理解しておく必要

があります。

関連製品

このドキュメントは、次のバージョンのハードウェアとソフトウェアにも使用できます。

- CUCM 9.X/10.X/11.X

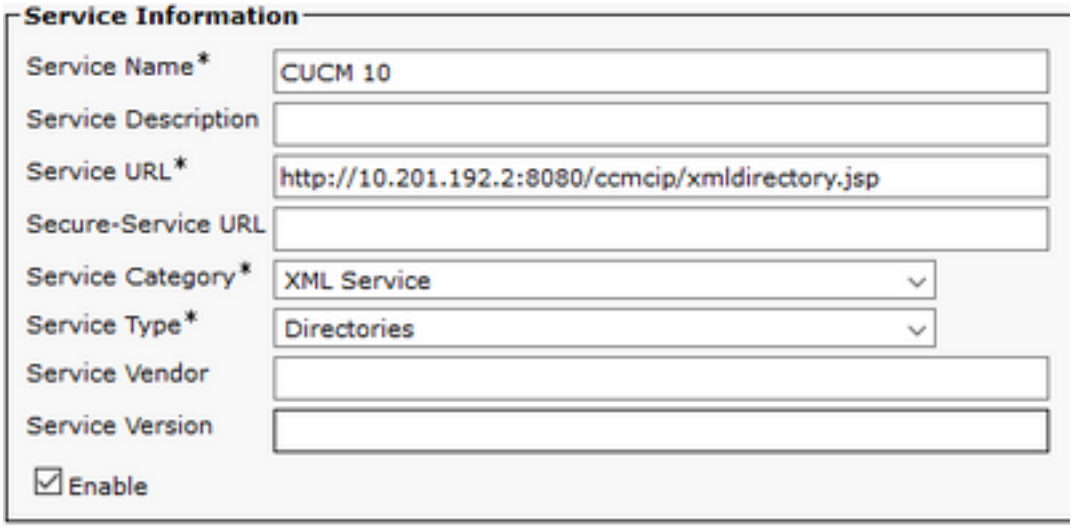
設定手順

ステップ1：システムのサービスURLを設定します。

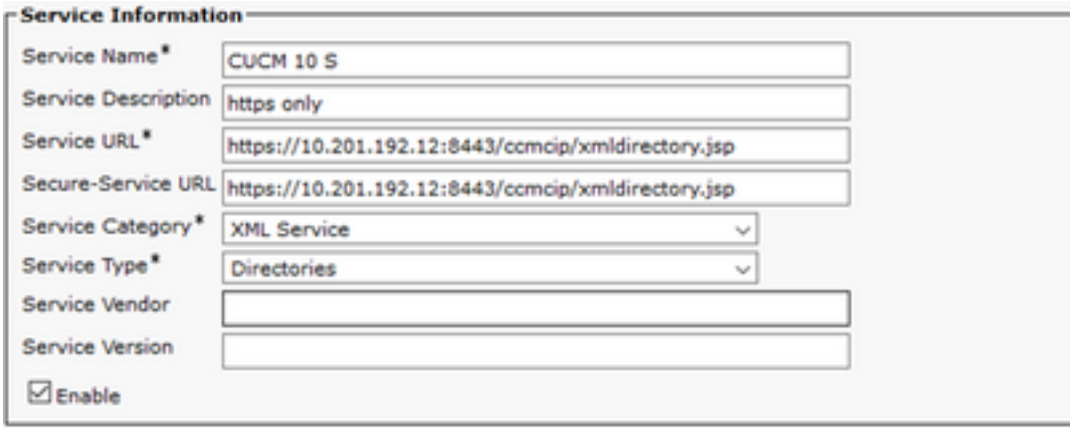
コンセプトの実証として、ハイパーテキスト転送プロトコル(HTTP)とハイパーテキスト転送プロトコルセキュア(HTTPS)を設定します。最後に、セキュアHTTPトラフィックだけを使用します。

[Device] > [Device Settings] > [Phone service] > [Add new]**に移動します。**

HTTPのみ



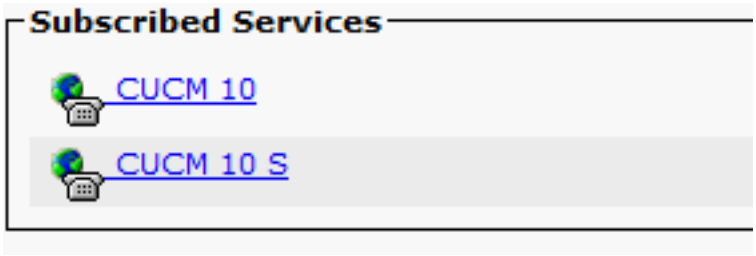
HTTPSのみ



> **警告**：エンタープライズサブスクリプションのチェ**ックを追加する**と、ステップ2をスキップできます。ただし、この変更により、すべての電話機がリセットされるので、潜在的な影響を確実に理解してください。

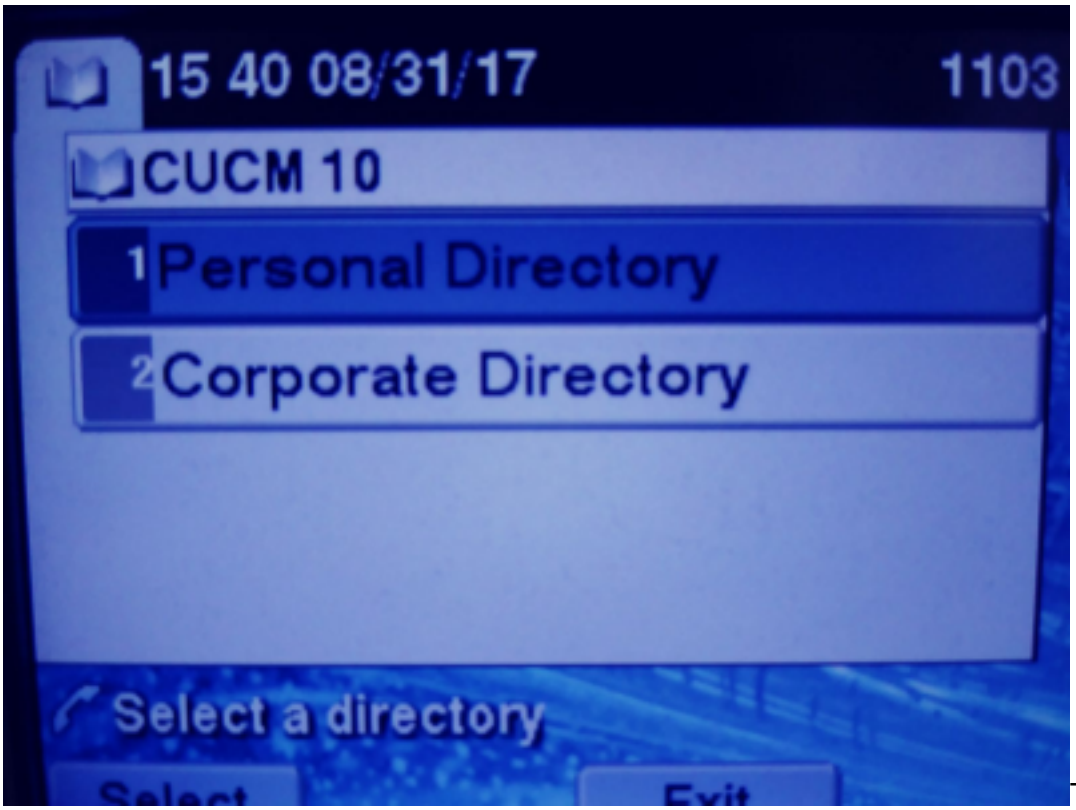
ステップ2：電話機をサービスに登録します。

[Device] **> [Phone] > [Subscriber/Unsubscribe service]に移動します。**



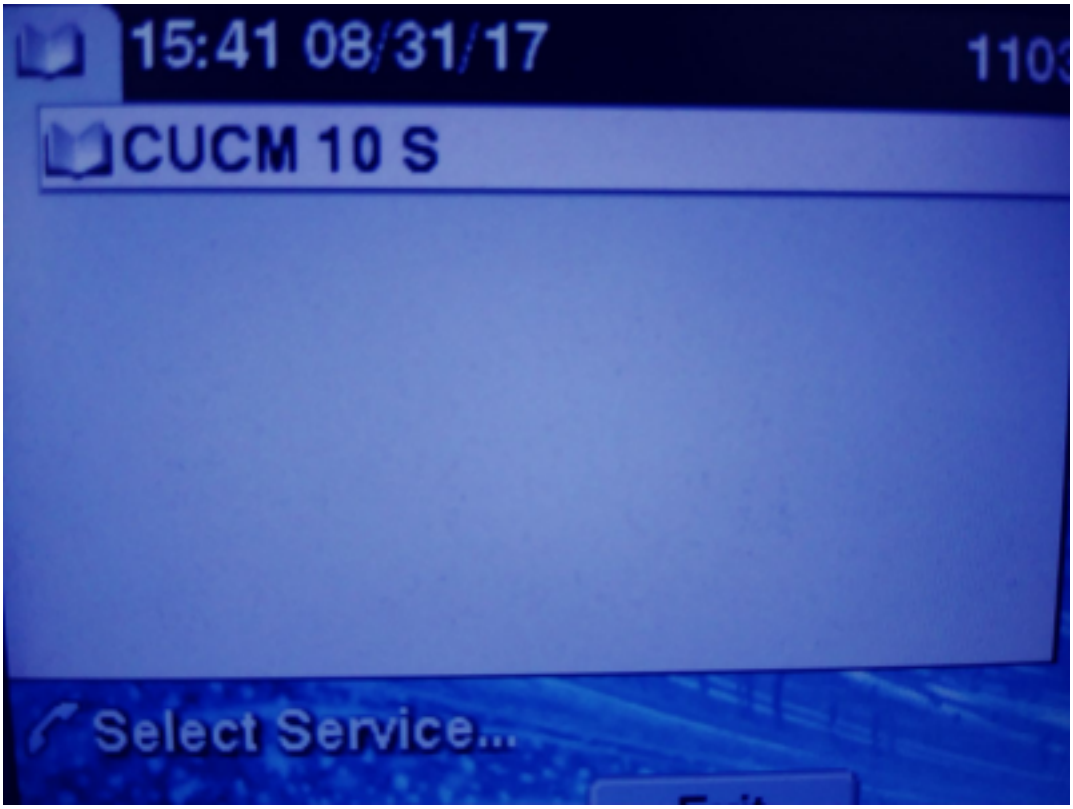
この時点で、アプリケーションがHTTPを提供している場合は、サービスに到達できる必要がありますが、httpsはまだ起動していません。

HTTP



TTP

HTTPS



HTTPSで「Host not found」**エラーが表示され**ます。これは、TVSサービスが電話に対してこれを認証できないためです。

ステップ3：外部サービス証明書をCUCMにアップロードします。

外部サービスをTomcat信頼のみとし**てアップロードします**。すべてのノードでサービスがリセットされていることを確認します。

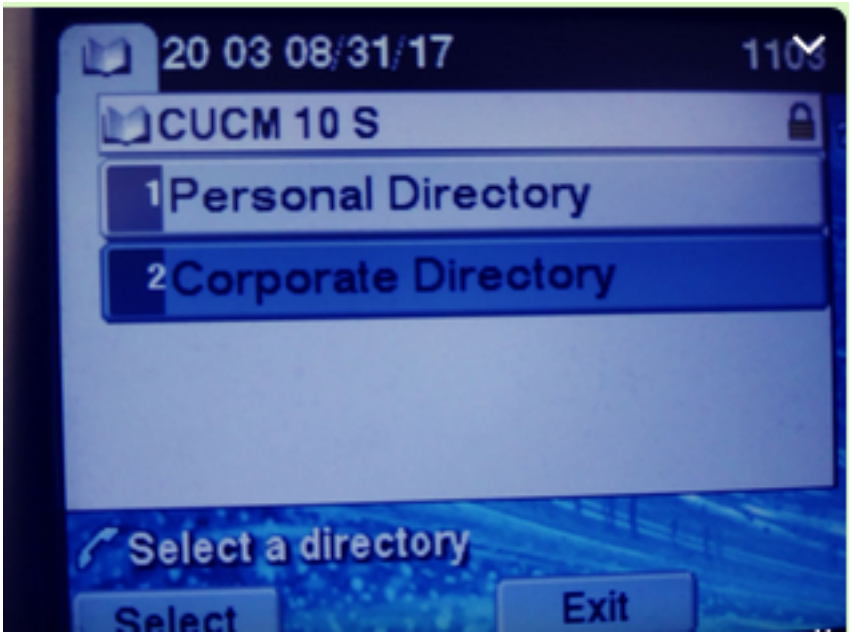
このタイプの証明書は電話機に保存されず、電話機はTVSサービスを使用してHTTPS接続を確立するかどうかを確認する必要があります。

[OS admin] > [**Certificate] > [Certificate upload]に移動します。**

SSHから、すべてのノードのCUCM Tomcatサービスをリセットします。

```
admin:utils service restart Cisco Tomcat
Do not press Ctrl+C while the service is restarting. If the service has not rest
arted properly, execute the same command again.
Service Manager is running
```

これらの手順が完了したら、電話機は問題なくHTTPSサービスにアクセスできる必要があります



よく寄せられる質問(FAQ)

証明書が交換された後も、HTTPSは「ホストが見つかりません」と失敗します。

– 電話機が登録されているノードを確認し、ノードにサードパーティ証明書が表示されていることを確認します。

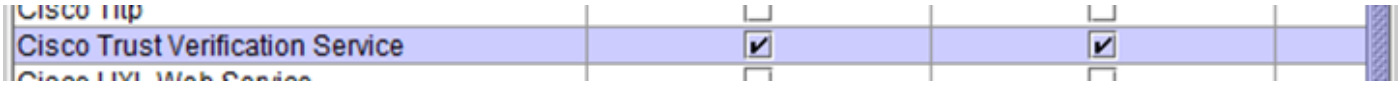
– 特定のノードのtomcatをリセットします。

- DNSをチェックし、証明書の共通名(CN)が解決できることを確認します。

トラブルシューティング

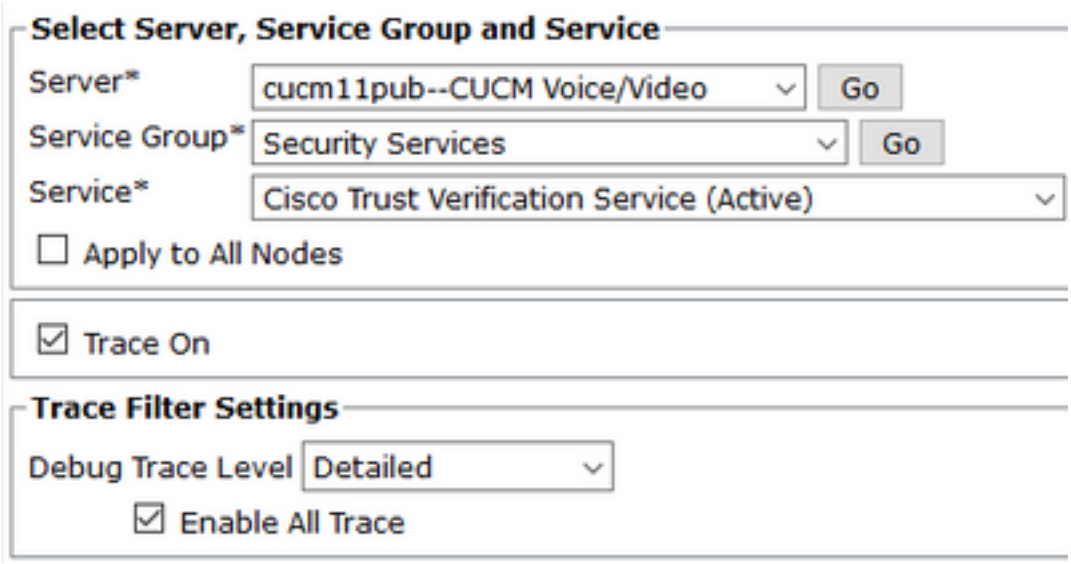
CUCM TVSログを収集すると、適切な情報が得られます

[RTMT] > [System] > [Trace & log Central] > [Collect log files] に移動します



> **注**：すべてのノードからログを収集し、TVSログが詳細に設定されていることを確認します。

TVSログをdetailedに設定



トレースの例

```
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificate</table><tableid>46</tableid><action>I</action>
<user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>1504203457</cdrtim
e><pkid>e6148ee3-3eb5-e955-fa56-
2baa538a88fb</pkid><servername>cucm11pub</servername><subjectname>CN=10.201.192.12,OU=RCH,O=Cisc
o,L=RCH,ST=Tx,C=US</subjectname><issuername>CN=pablogon-
CA,DC=rcdncollab,DC=com</issuername><serialnumber>3d00000008230ded92f687ec03000000000008</serial
number><certificate></certificate><ipv4address>10.201.192.13</ipv4address><ipv6address></ipv6add
ress><timetolive>NULL</timetolive><tkcertificatedistribution>1</tkcertificatedistribution><ifx_r
eplcheck>6460504654345273346</ifx_replcheck></new></msg>
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificate" has been changed
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Looking up the
roles for
11:17:38.291 |   debug Pkid : fead9987-66b5-498f-4e41-c695c54fac98
11:17:38.291 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - DBChange Notification
received
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () -
CDBString=<msg><type>DBL</type><table>certificatetrustrolemap</table><tableid>50</tableid><actio
n>I</action><user>repl</user><time>1504203458</time><new><cdrserver>2</cdrserver><cdrtime>150420
3457</cdrtime><pkid>5ae6e1d2-63a2-4590-bf40-1954bfa79a2d</pkid><fkcertificate>e6148ee3-3eb5-
e955-fa56-
2baa538a88fb</fkcertificate><tktrustrole>7</tktrustrole><ifx_replcheck>6460504654345273346</ifx_
replcheck></new></msg>
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessChangeNotification () - Database table
"certificatetrustrolemap" has been changed
11:17:38.300 |   debug CTVSChangeNotifyServer::ProcessThreadProc () - Waiting for DBChange
Notification
11:17:46.811 |   debug updateLocalDBCache : Refreshing the local DB certificate cache
11:34:00.131 |   debug Return value after polling is 1
11:34:00.131 |   debug FD_ISSET i=0, SockServ=14

11:34:00.131 |   debug Accepted TCP connection from socket 0x00000014
```