

# 外部電話サービス 設定例を保護して下さい

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定手順](#)

[頻繁して下さい質問 \(FAQ\) を](#)

[トラブルシューティング](#)

## 概要

この資料にセキュア外部電話サービスを設定する方法を記述されています。この設定はあらゆるサードパーティサービスと機能できますがデモのために、この資料は遠隔 Cisco Unified Communications Manager ( CUCM ) サーバを使用します。

ホセ Villalobos によって貢献される、Cisco TAC エンジニア。

## 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 認証
- 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くものです。

- CUCM 10.5.X/CUCM 11.X
- CUCM の Skinny Client Control Protocol ( SCCP ) および Session Initiation Protocol ( SIP ) 電話レジスタ
- ラボ使用認証対象代替名 ( SAN ) 認証。
- 外部ディレクトリは SAN 証明書にあります。
- この例のすべてのシステムに関しては認証局 ( CA ) は同じ、すべての証明書使用です CA サインです。
- Domain Name server ( DNS ) および Network Time Protocol ( NTP ) はプロパティ セットアップおよびはたらくことである必要があります。

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たものです。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。ネットワークがライブである場合、あらゆる変更の潜在的影響を理解するようにして下

さい。

## 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 を設定して下さい。

Hyper Text Transfer Protocol ( HTTP ) を設定し、プルーフ オブ コンセプトとして Hypertext Transfer Protocol ( HTTP ) ( HTTPS ) 保護して下さい。最終的な概念はトラフィックだけセキュア HTTP ( S-HTTP ) 使用することです。

Device> デバイス Settings> 電話 service> へのナビゲートは新しい追加します

HTTP だけ

Service Information	
Service Name*	CUCM 10
Service Description	
Service URL*	http://10.201.192.2:8080/ccmcip/xmldirectory.jsp
Secure-Service URL	
Service Category*	XML Service
Service Type*	Directories
Service Vendor	
Service Version	
<input checked="" type="checkbox"/> Enable	

HTTPS だけ

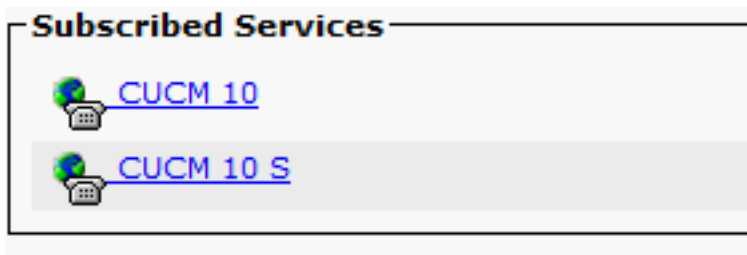
Service Information	
Service Name*	CUCM 10 S
Service Description	https only
Service URL*	https://10.201.192.12:8443/ccmcip/xmldirectory.jsp
Secure-Service URL	https://10.201.192.12:8443/ccmcip/xmldirectory.jsp
Service Category*	XML Service
Service Type*	Directories
Service Vendor	
Service Version	
<input checked="" type="checkbox"/> Enable	

**警告：** 企業サブスクリプションのためのチェックを追加する場合、ステップ 2 はスキップすることができます。ただし、この変更はすべての電話をリセットします、従って潜在的

影響を理解するようにして下さい。

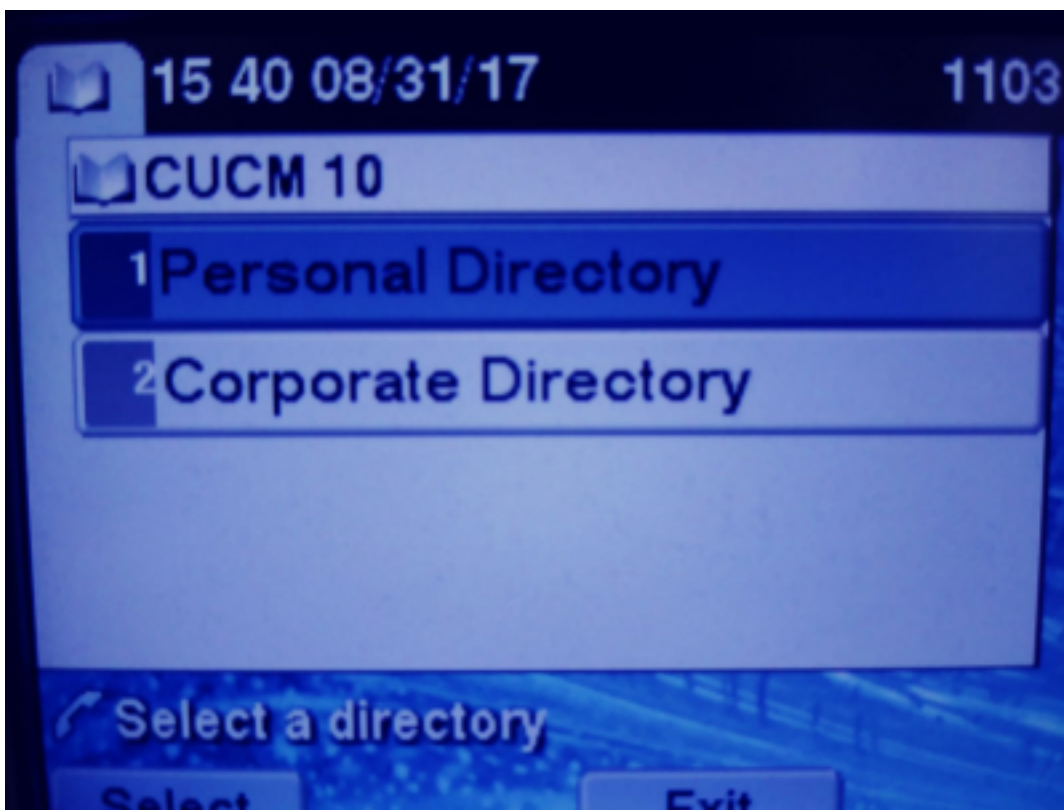
ステップ 2.サービスを電話を定期講読して下さい。

Device>Phone>>Subscriber/Unsubscribe サービスへの Natigate。

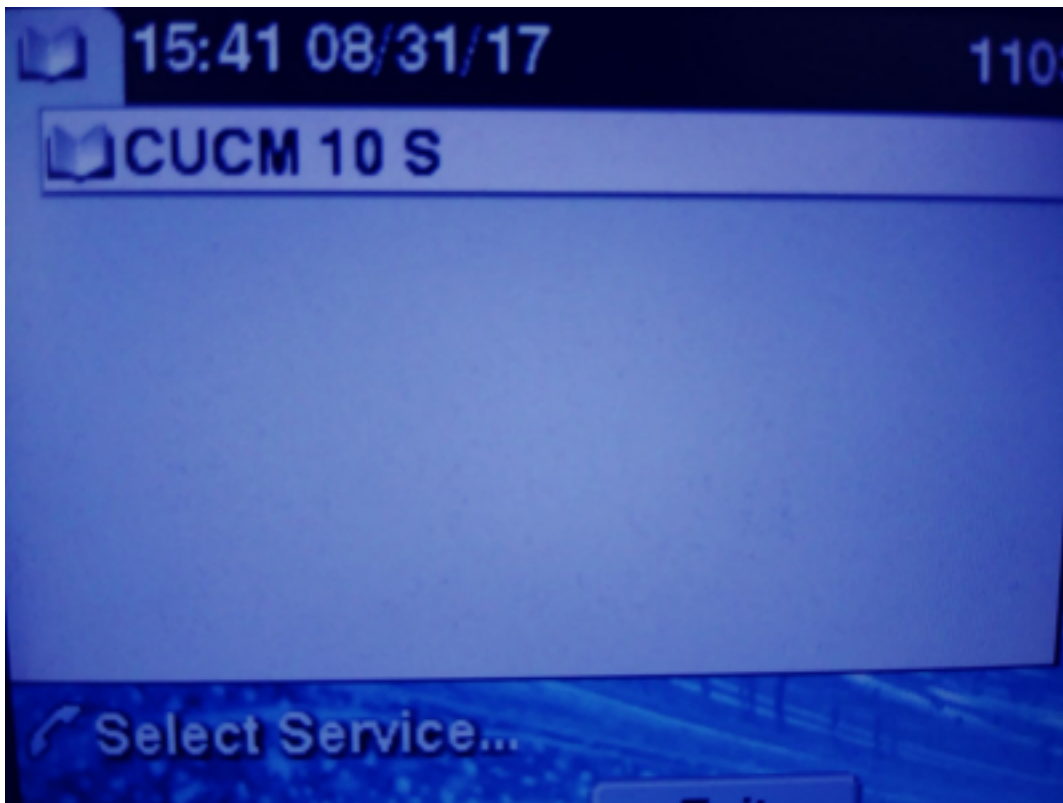


この時点でアプリケーションが HTTP を提供すれば、サービスに達できる必要がありますが https はまだありません。

HTTP



HTTPS



HTTPS はファクトによる「ホスト検出されなかった」エラーをサービスが電話のためにこれを認証できない TV 示します。

ステップ 3. CUCM に外部サービス認証をアップロードして下さい。

Tomcat 信頼だけとして外部サービスをアップロードして下さい。サービスをリセットされますすべてのノードで確認して下さい。

証明書のこの型は TV サービスと電話で、むしろ電話必要がありますチェックする HTTPS 接続を確立するかどうか見るために保存されません。

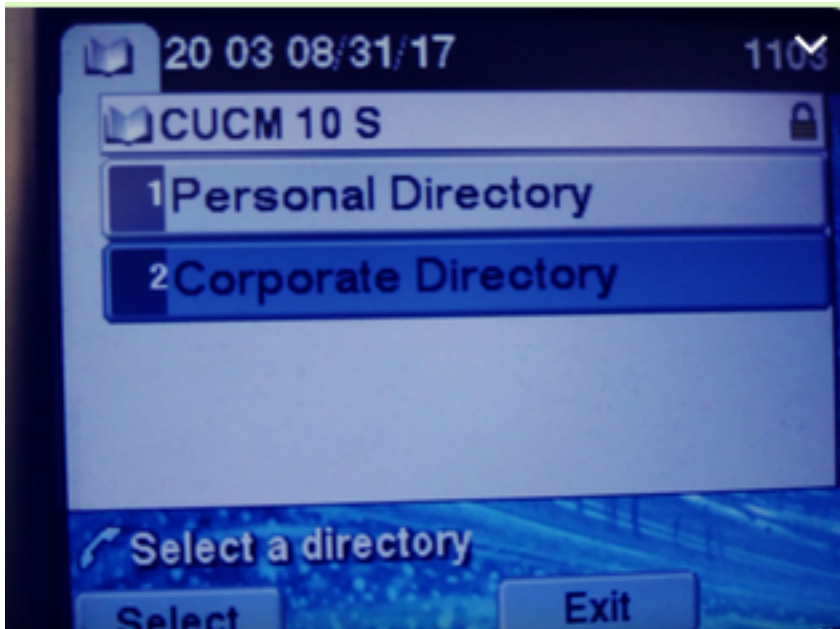
OS admin> Certificate> 認証アップロードへのナビゲート。

tomcat-trust josevil-105 CA-signed RSA josevil-105 pablogon-CA 08/30/2019 CUCM 10 tomcat cert

すべてのノードの CUCM Tomcat サービス リセットされる SSH から。

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

これらのステップの後で、電話は問題なしで HTTPS サービスにアクセスできる必要があります



## 頻繁して下さい質問 (FAQ) を

認証が交換された後、HTTPS はまだ「見つけれない」ホストと失敗します。

-ノードを電話レジスタ チェックし、見るノードのサードパーティ 認証を確認下さい。

-特定のノードの Tomcat をリセットして下さい。

- DNS を、確認します認証のよくある Name (CN) を解決されますチェックして下さい。

## トラブルシューティング

ログがよい情報を提供する必要がある CUCM TV を集めて下さい

RTMT>System>Trace 及びログ本部へのナビゲートは > ログファイルを集めます

Cisco Tftp	<input type="checkbox"/>	<input type="checkbox"/>
Cisco Trust Verification Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cisco LVM Web Service	<input type="checkbox"/>	<input type="checkbox"/>

注: ログをすべてのノードから集め、ログが詳しいに設定される TV を確認して下さい。

詳しいに設定される TV ログ

**Select Server, Service Group and Service**

Server\*

Service Group\*

Service\*

Apply to All Nodes

---

Trace On

---

**Trace Filter Settings**

Debug Trace Level

Enable All Trace

## トレース例

```

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</cdrtime
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><issuename>CN=pablogon-
CA,DC=rcdncollab,DC=com</issuename><serialnumber>3d0000008230ded92f687ec03000000000008</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

```