Secure External Phone Services Configuration Example

Contents

Introduction

This document describes how to configure Secure External Phone Service. This configuration can work with any third party service, but for demonstration, This document uses a remote Cisco Unified Communications Manager (CUCM) server.

Contributed by Jose Villalobos, Cisco TAC Engineer.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CUCM
- CUCM certificates
- Phone Services

Components Used

The information in this document is based on these software and hardware versions:

- CUCM 10.5.X/CUCM 11.X
- Skinny Client Control Protocol (SCCP) and Session Initiation Protocol (SIP) phones register with CUCM
- The lab its using Subject Alternative Name (SAN) certificates.
- External directory will be on SAN certs.
- For all system on this example the Certificate Authority (CA) will be the same, all certs use are CA sign.
- Domain Name server(DNS) and Network Time Protocol (NTP) needs to be property setup and working.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any change.

Related Products

This document can also be used with these hardware and software versions:

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

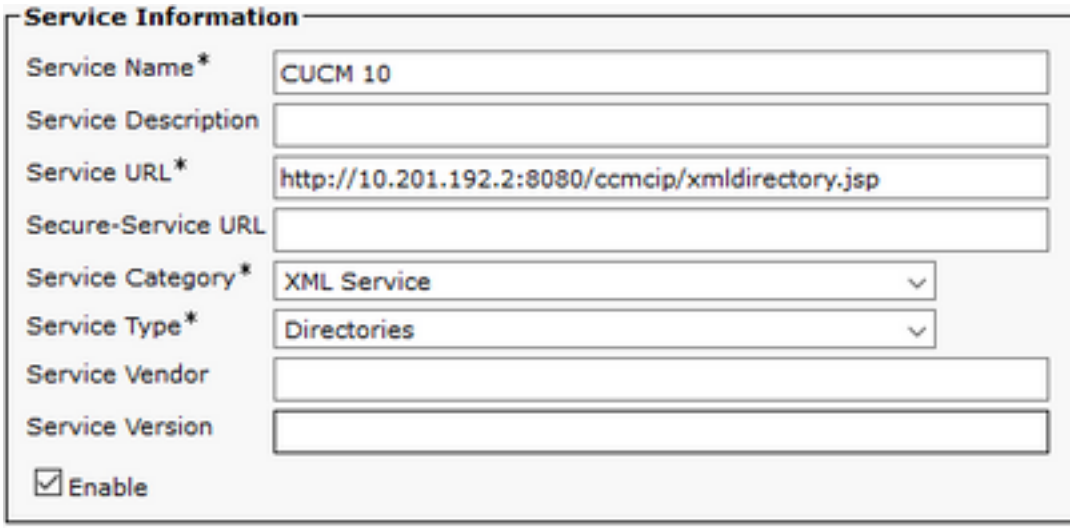
Configuration Steps

Step 1. Setup the service URL on the system.

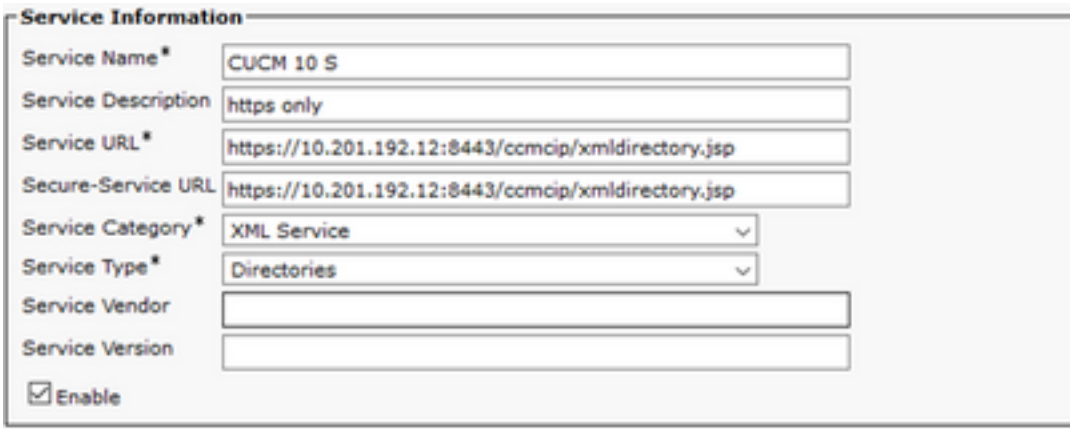
Setup Hyper Text Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) as proof of concepts. The final idea is to use only Secure HTTP traffic.

Navigate to **Device> Device Settings> Phone service> Add new**

HTTP only



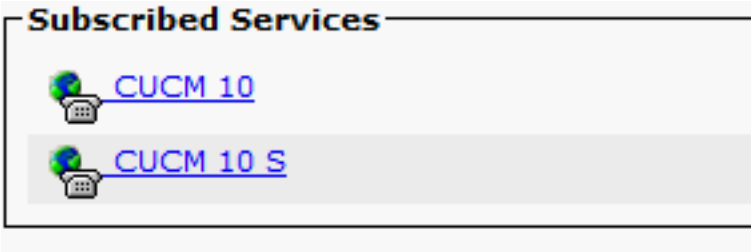
HTTPS only



> **Warning**: if you add the check for **Enterprise Subscription,** step two can be skipped. However, this change resets all phones, so ensure that you understand the potential impact.

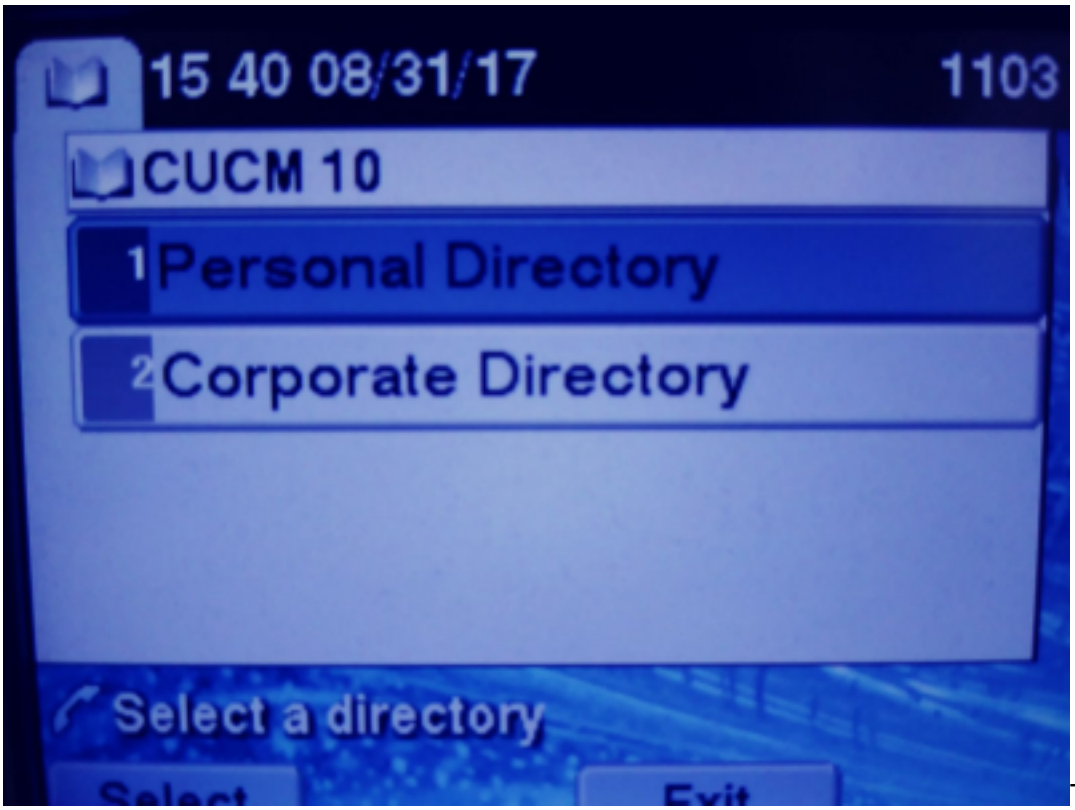
Step 2. Subscribe the phones to the services.

Natigate to **Device>Phone>>Subscriber/Unsubscribe service.**



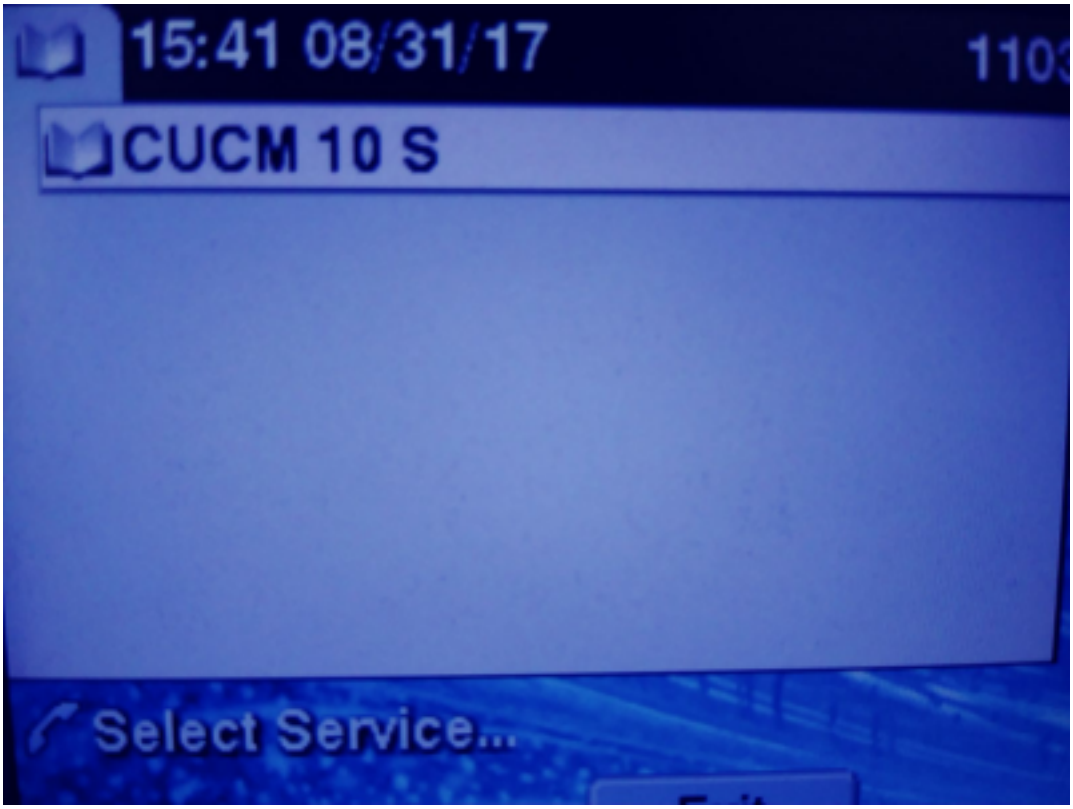
At this point, if the application offers HTTP, you must be able to reach the service, but https is still not up.

HTTP



TTP

HTTPS



HTTPS will show a **“**Host not found**”** error due to the fact, the TVS service can’t authenticate this for the phone.

Step 3. Upload the External Service certificates to the CUCM.

Upload the External Service as **Tomcat trust only**. Ensure services are reset on all nodes.

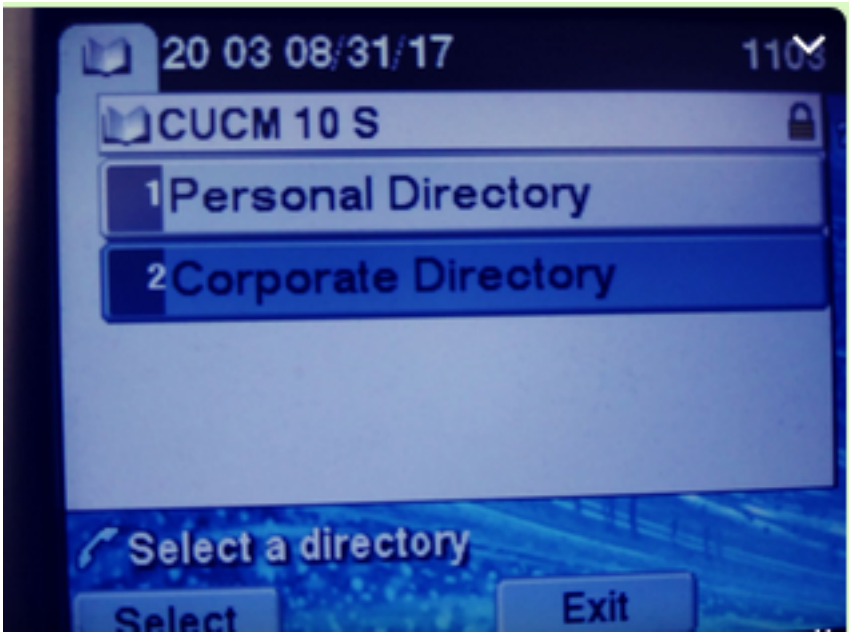
This type of certs is not stored on the phone, rather the phone must check with TVS service to see if it establishes the HTTPS connection.

Navigate to **OS admin> Certificate> Certificate upload.**

From SSH reset the CUCM Tomcat service on all nodes.

```
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
```

After these steps, phones must be able to access the HTTPS service without issues



Frequent Ask Questions (FAQ)

After certificates are exchanged, HTTPS still fails with "host not found".

-Check the node where the phone its register and ensure you see the third party certificate on the node.

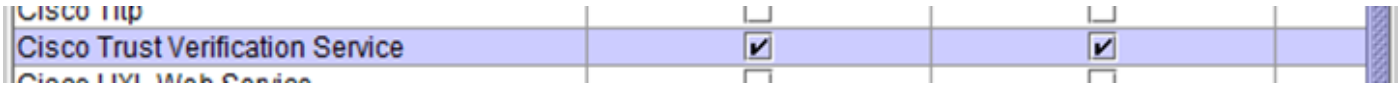
-Reset the tomcat on the specific node.

-Check DNS, ensure the Common Name(CN) of the certificate can be resolved.

Troubleshooting

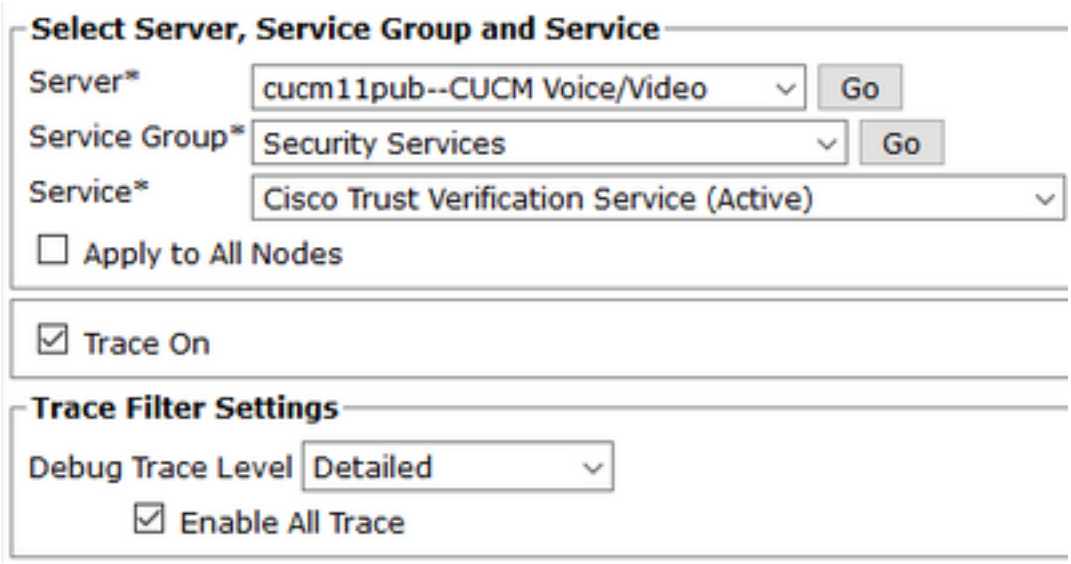
Collect CUCM TVS logs must provide you good information

Navigate to **RTMT>System>Trace & log Central > Collect log files**



> **Note**: Collect logs from all nodes and ensure TVS logs are set to detailed.

TVS logs set to detailed



Trace example

```
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
```