Ejemplo de Configuración de Servicios de Teléfono Externos Seguros

Contenido

Introducción

Este documento describe cómo configurar Secure External Phone Service. Esta configuración puede funcionar con cualquier servicio de terceros, pero para demostrarlo, este documento utiliza un servidor remoto de Cisco Unified Communications Manager (CUCM).

Colaborado por Jose Villalobos, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM
- certificados CUCM
- Servicios telefónicos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- CUCM 10.5.X/CUCM 11.X
- Los teléfonos Skinny Client Control Protocol (SCCP) y Session Initiation Protocol (SIP) se registran con CUCM
- El laboratorio utiliza certificados de nombre alternativo del sujeto (SAN).
- El directorio externo estará en los certificados SAN.
- Para todos los sistemas de este ejemplo, la autoridad de certificación (CA) será la misma, todos los certificados utilizados son signos de CA.
- El servidor de nombres de dominio (DNS) y el protocolo de tiempo de red (NTP) deben configurarse y funcionar correctamente.

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. Si su red está activa, asegúrese de comprender el impacto potencial de cualquier cambio.

Productos Relacionados

Este documento también puede utilizarse con estas versiones de software y hardware:

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

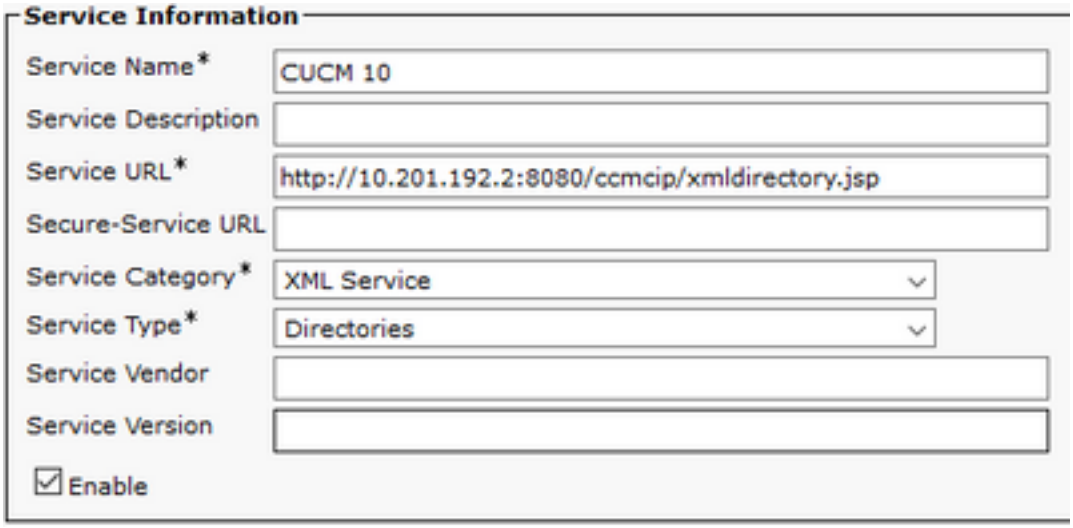
Configuration Steps

Paso 1. Configure la URL del servicio en el sistema.

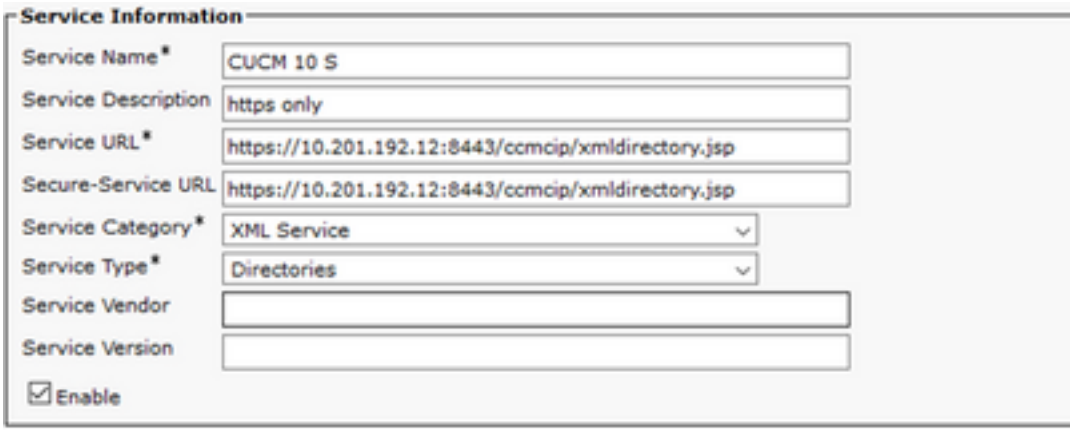
Configure Hyper Text Transfer Protocol (HTTP) y Hypertext Transfer Protocol Secure (HTTPS) como prueba de conceptos. La idea final es utilizar sólo tráfico HTTP seguro.

Vaya a **Device> Device Settings> Phone service> Add new**

Sólo HTTP



Sólo HTTPS

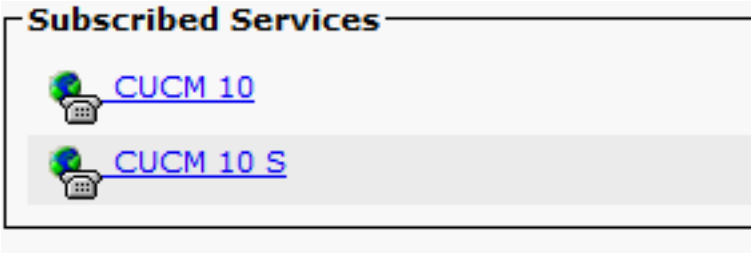


Advertencia: si agrega la comprobación de **suscripción empresarial,** se puede omitir el paso

dos. Sin embargo, este cambio restablece todos los teléfonos, por lo que asegúrese de comprender el impacto potencial.

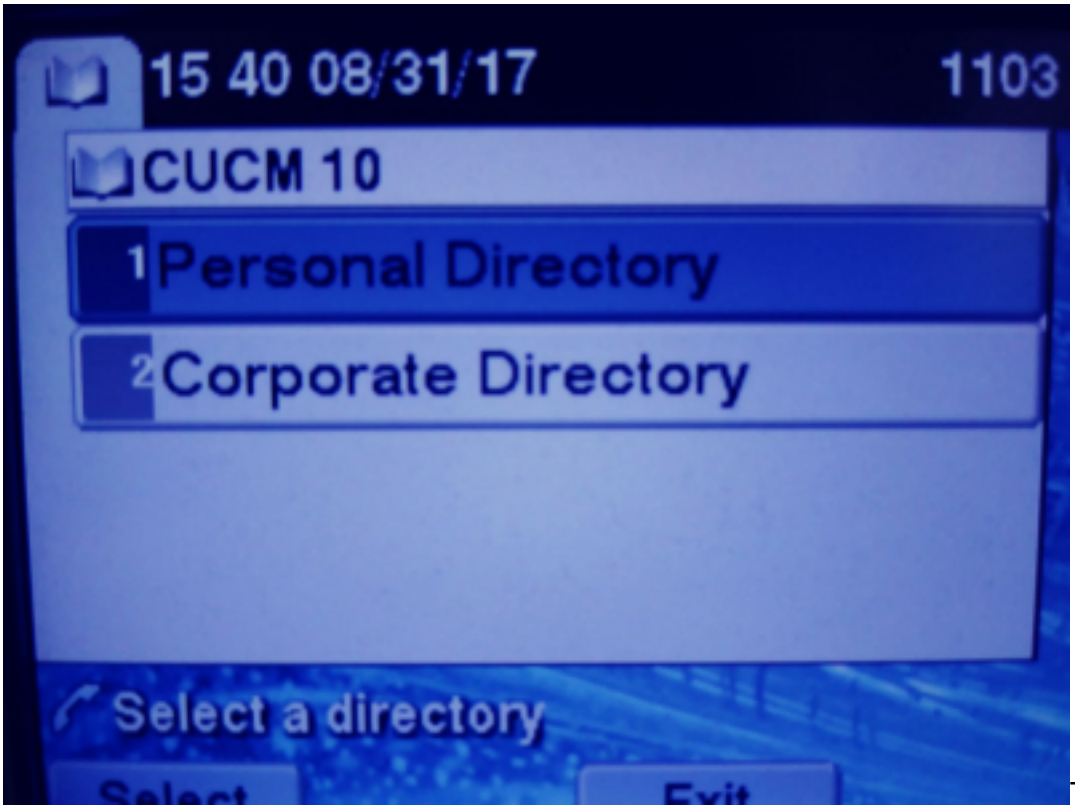
Paso 2. Suscríbase a los teléfonos a los servicios.

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



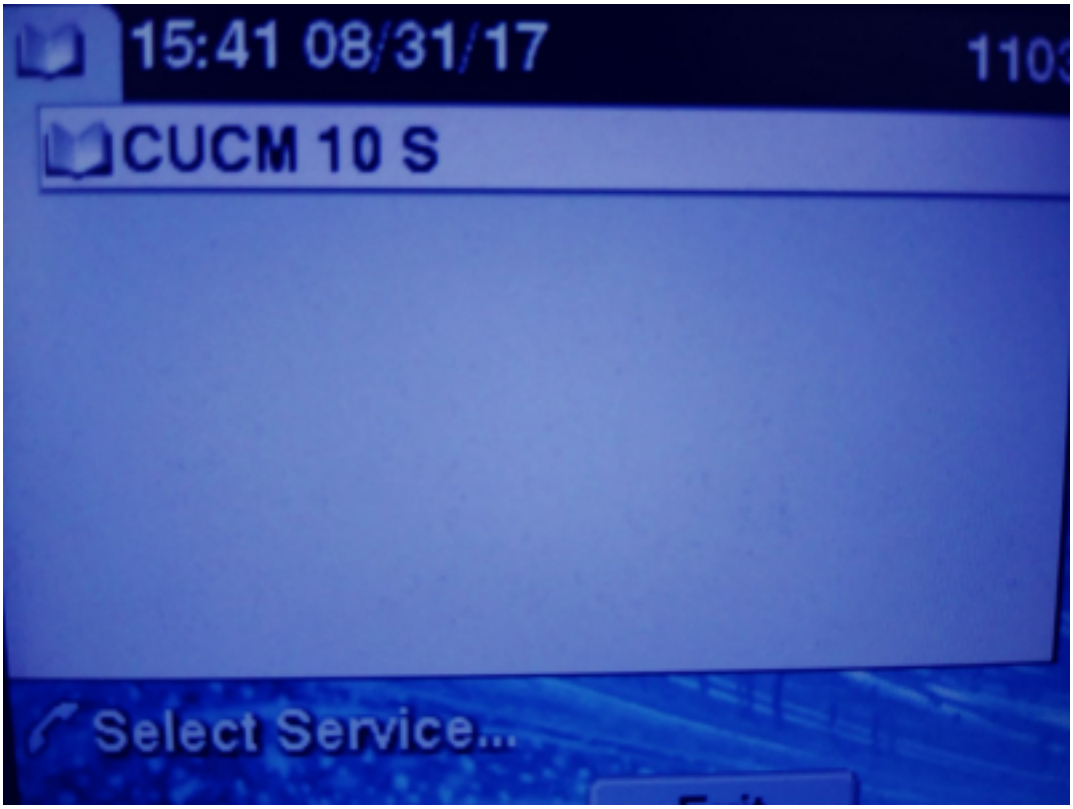
En este momento, si la aplicación ofrece HTTP, debe poder alcanzar el servicio, pero https todavía no está activo.

HTTP



TTP

HTTPS



HTTPS mostrará un error **"Host no encontrado"** debido a que el servicio TVS no puede autenticar esto para el teléfono.

Paso 3. Cargue los certificados de servicio externo en CUCM.

Cargue el Servicio Externo **sólo** como **confianza de Tomcat**. Asegúrese de que los servicios se restablezcan en todos los nodos.

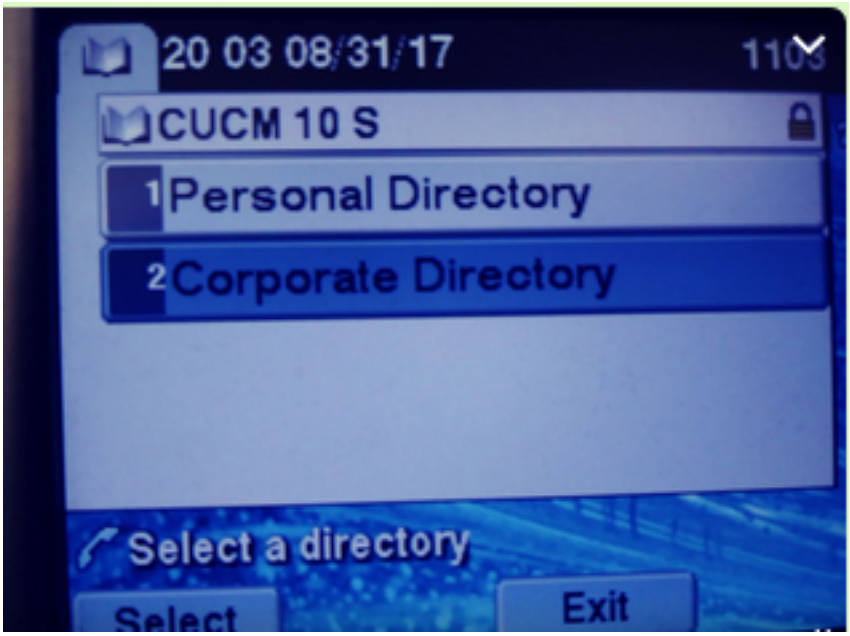
Este tipo de certificados no se almacena en el teléfono, sino que el teléfono debe comprobar con el servicio TVS para ver si establece la conexión HTTPS.

Vaya a **OS admin> Certificate> Certificate upload.**

Desde SSH, restablezca el servicio CUCM Tomcat en todos los nodos.

```
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
```

Después de estos pasos, los teléfonos deben poder acceder al servicio HTTPS sin problemas



Preguntas frecuentes (FAQ)

Después de intercambiar los certificados, HTTPS todavía falla con "host not found".

-Verifique el nodo en el que se registra el teléfono y asegúrese de ver el certificado de terceros en el nodo.

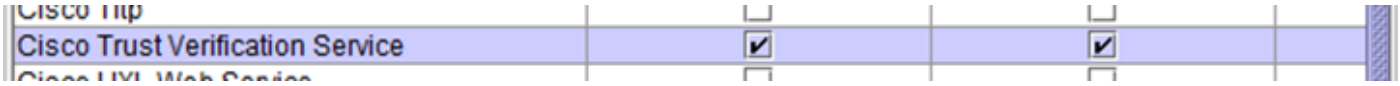
-Restablecer el tomcat en el nodo específico.

-Compruebe el DNS, asegúrese de que se puede resolver el Nombre común (CN) del certificado.

Resolución de problemas

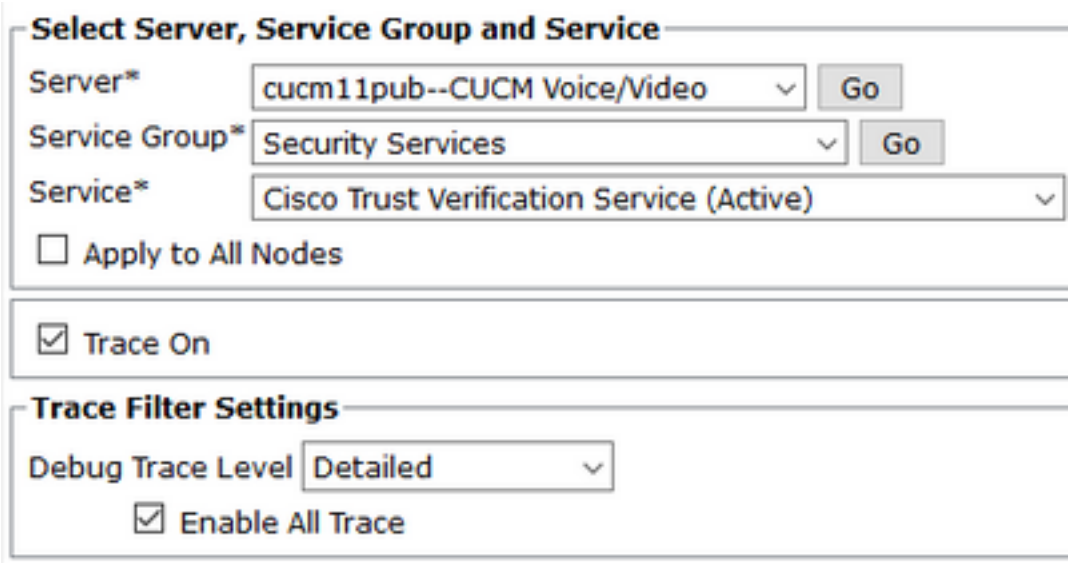
Recopilar registros de CUCM TVS debe proporcionarle buena información

Vaya a **RTMT>System>Trace & log Central > Recopilar archivos de registro**



> **Nota:** Recopile registros de todos los nodos y asegúrese de que los registros TVS estén configurados en detallados.

Registros de TVS configurados en detallados



Ejemplo de seguimiento

```
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
```