Esempio di configurazione di Secure External Phone Services

Sommario

Introduzione

In questo documento viene descritto come configurare Secure External Phone Service. Questa configurazione può essere utilizzata con qualsiasi servizio di terze parti, ma per la dimostrazione il presente documento utilizza un server Cisco Unified Communications Manager (CUCM) remoto.

Contributo di Jose Villalobos, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CUCM
- certificati CUCM
- Servizi telefonici

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM 10.5.X/CUCM 11.X
- I telefoni Skinny Client Control Protocol (SCCP) e Session Initiation Protocol (SIP) si registrano con CUCM
- Il laboratorio usa i certificati SAN (Subject Alternative Name).
- La directory esterna sarà su certificati SAN.
- Per tutti i sistemi in questo esempio l'Autorità di certificazione (CA) sarà la stessa, tutti i certificati utilizzati sono il segno CA.
- Ènecessario che DNS (Domain Name server) e NTP (Network Time Protocol) siano impostati e funzionanti.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, accertarsi di comprendere il potenziale impatto di qualsiasi modifica.

Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

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

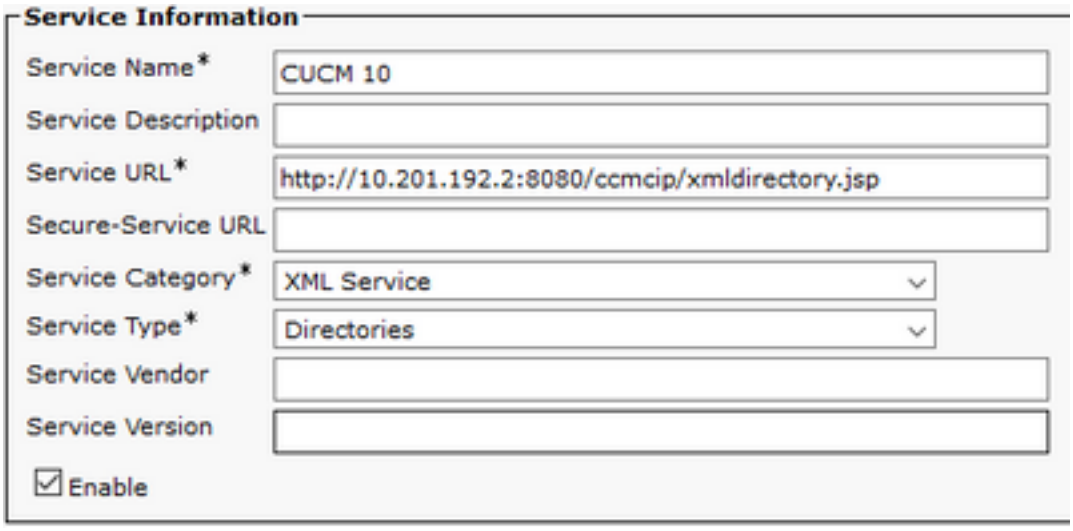
Procedura di configurazione

Passaggio 1. Configurare l'URL del servizio nel sistema.

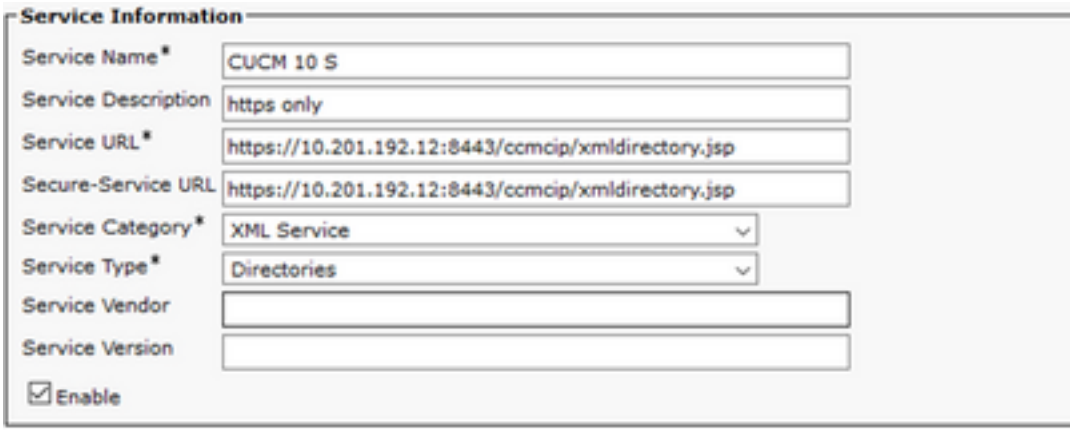
Configurare il protocollo HTTP (Hyper Text Transfer Protocol) e HTTPS (Hypertext Transfer Protocol Secure) come prova di concetti. L'idea finale è quella di utilizzare solo il traffico HTTP protetto.

Selezionare **Periferica> Impostazioni dispositivo> Servizio telefonico> Aggiungi nuovo**

Solo HTTP



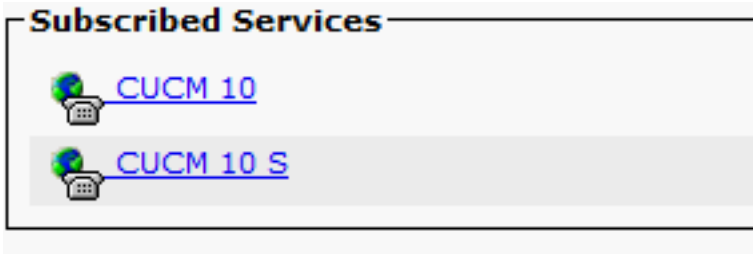
Solo HTTPS



Avviso: se si aggiunge il controllo per la **sottoscrizione Enterprise,** è possibile ignorare il secondo passaggio. Tuttavia, questa modifica reimposta tutti i telefoni, in modo da assicurarsi di capire il potenziale impatto.

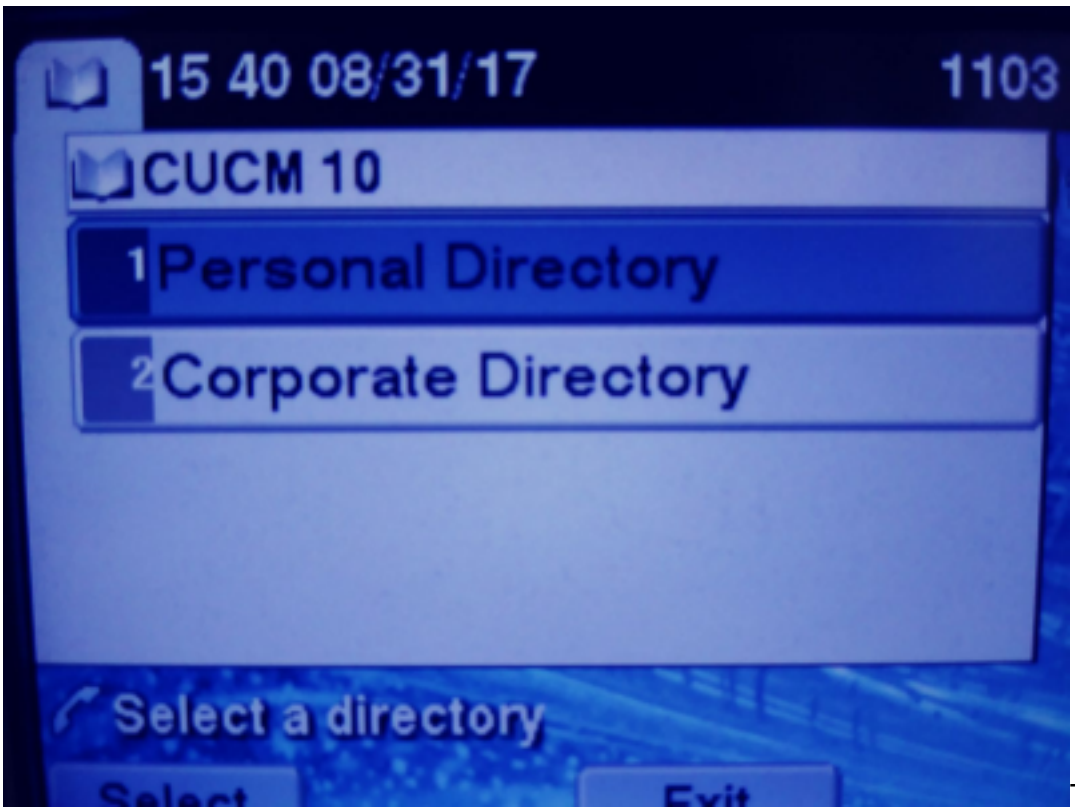
Passaggio 2. Sottoscrivere i telefoni ai servizi.

Passa a **Periferica>Telefono>>Sottoscrivi/Annulla sottoscrizione servizio.**



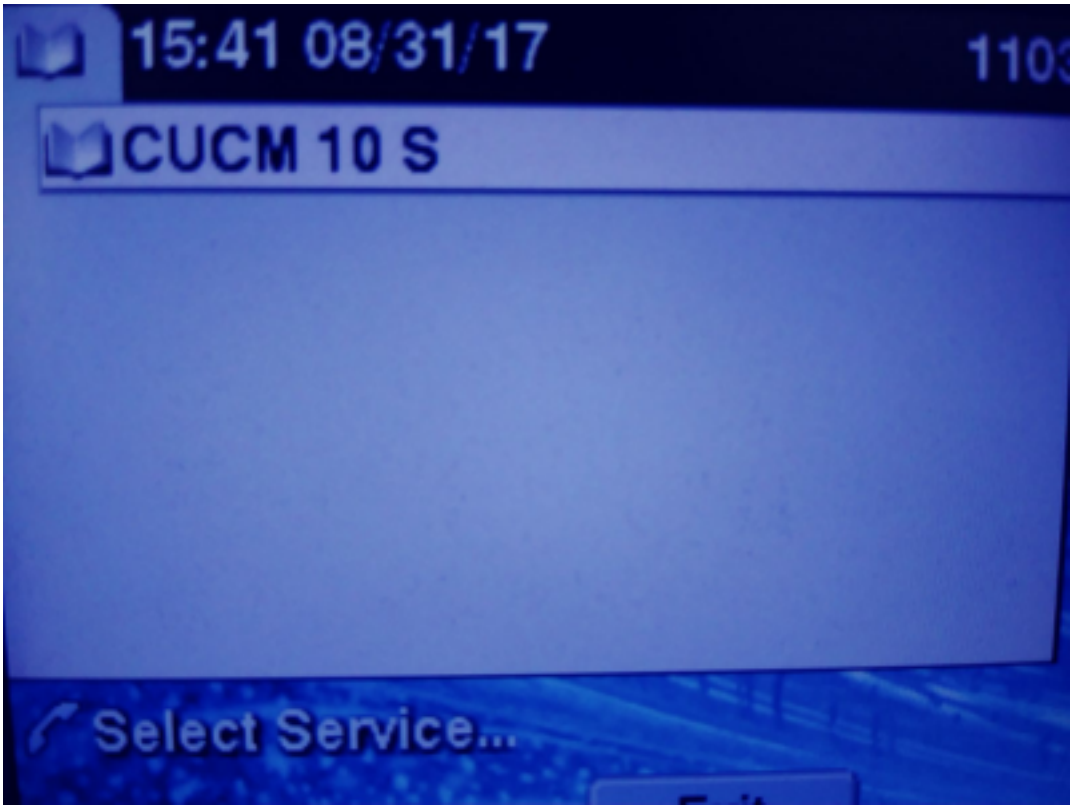
A questo punto, se l'applicazione offre HTTP, è necessario essere in grado di raggiungere il servizio, ma https non è ancora attivo.

HTTP



TTP

HTTPS



HTTPS visualizzerà un errore "Host non trovato" a causa del fatto che il servizio TVS non può autenticarlo per il telefono.

Passaggio 3. Caricare i certificati del servizio esterno in CUCM.

Caricare il servizio esterno **solo** come **trust Tomcat**. Assicurarsi che i servizi vengano reimpostati su tutti i nodi.

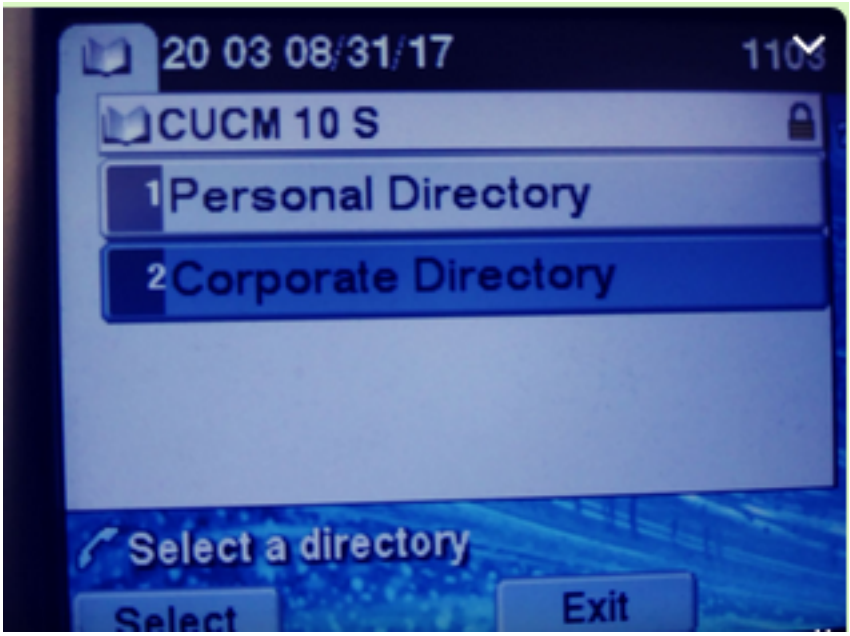
Questo tipo di certificati non è memorizzato sul telefono, ma il telefono deve controllare con il servizio TV per vedere se stabilisce la connessione HTTPS.

Passare a **Amministratore del sistema operativo> Certificato> Caricamento certificato.**

Dal protocollo SSH, ripristinare il servizio CUCM Tomcat su tutti i nodi.

```
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
```

Dopo questi passaggi, i telefoni devono essere in grado di accedere al servizio HTTPS senza problemi



Domande frequenti

Dopo lo scambio dei certificati, HTTPS continua a non funzionare con "host non trovato".

-Controllare il nodo in cui il telefono ha registrato e assicurarsi di vedere il certificato di terze parti sul nodo.

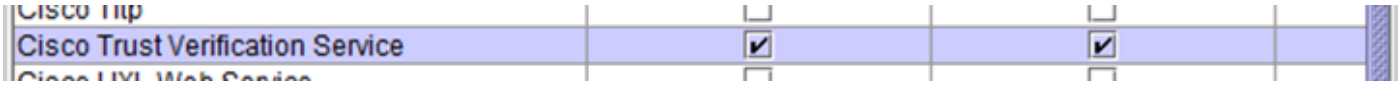
- Reimposta il gatto maschio sul nodo specifico.

-Controllare DNS, verificare che sia possibile risolvere il nome comune (CN) del certificato.

Risoluzione dei problemi

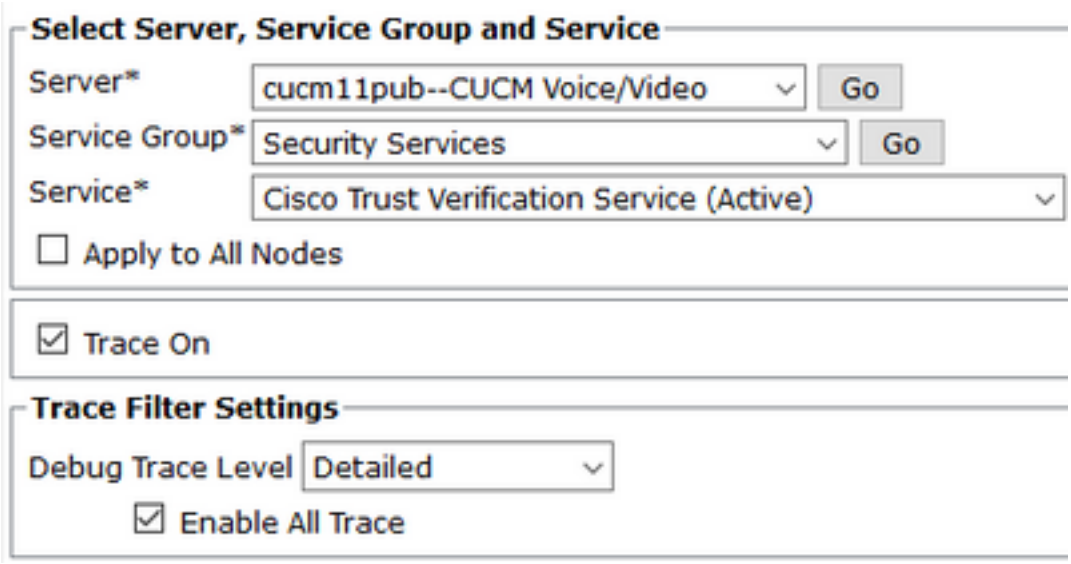
Raccogli i registri TVS CUCM devono fornire informazioni valide

Selezionare **RTMT>System>Trace & log Central > Raccogli file di log**



> **Nota:** Raccogliere i registri da tutti i nodi e verificare che i registri TVS siano impostati in modo dettagliato.

Registri TVS impostati su dettagliato



Esempio di traccia

```
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
```