Konfigurationsbeispiel für sichere externe Telefondienste

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie der sichere externe Telefondienst konfiguriert wird. Diese Konfiguration kann mit allen Services von Drittanbietern verwendet werden. Zur Demonstration wird in diesem Dokument jedoch ein Remote-Server von Cisco Unified Communications Manager (CUCM) verwendet.

Unterstützt von Jose Villalobos, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CUCM
- CUCM-Zertifikate
- Telefondienste

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- CUCM 10.5.X/CUCM 11.X
- Skinny Client Control Protocol (SCCP)- und Session Initiation Protocol (SIP)-Telefone werden bei CUCM registriert
- In der Übung werden Zertifikate für den Betreffalternativen Namen (SAN) verwendet.
- Das externe Verzeichnis befindet sich in SAN-Zertifikaten.
- Für alle Systeme in diesem Beispiel ist die Zertifizierungsstelle (Certificate Authority, CA) identisch. Alle Zertifikate werden als Zertifizierungsstelle verwendet.
- Domain Name Server (DNS) und Network Time Protocol (NTP) müssen eingerichtet und

funktionsfähig sein.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen jeder Änderung verstehen.

Zugehörige Produkte

Dieses Dokument kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

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

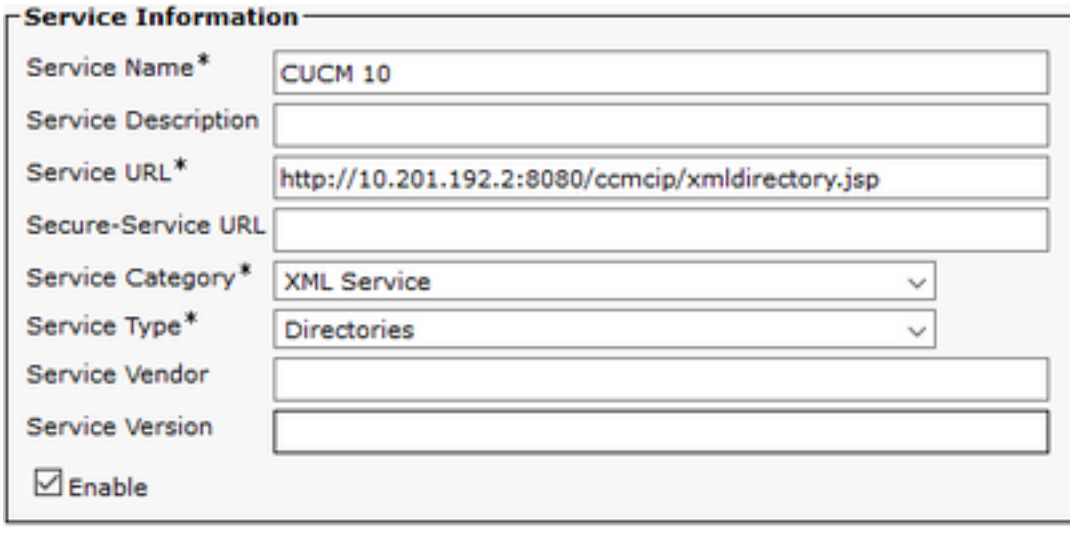
Konfigurationsschritte

Schritt 1: Stellen Sie die Service-URL auf dem System ein.

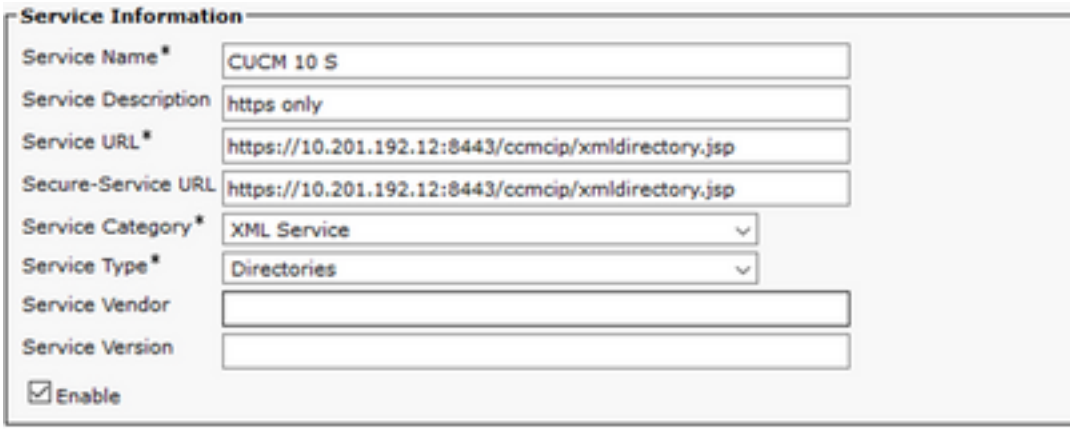
Einrichtung von Hyper Text Transfer Protocol (HTTP) und Hypertext Transfer Protocol Secure (HTTPS) als Nachweis für Konzepte. Die letzte Idee besteht darin, nur sicheren HTTP-Datenverkehr zu verwenden.

Navigieren Sie zu **Gerät > Geräteeinstellungen > Telefondienst> Neue Geräte hinzufügen.**

Nur HTTP



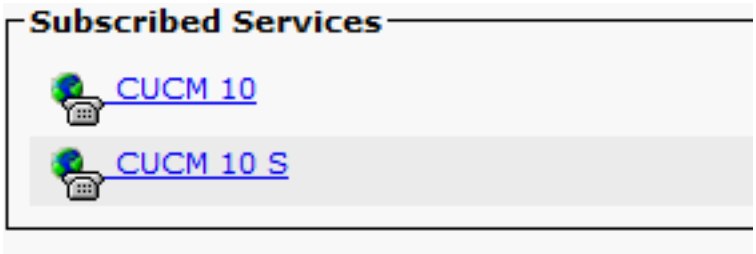
Nur HTTPS



> **Warnung**: Wenn Sie die Prüfung auf **Enterprise-Abonnement** hinzufügen**,** können Sie Schritt 2 überspringen. Diese Änderung setzt jedoch alle Telefone zurück. Stellen Sie daher sicher, dass Sie die potenziellen Auswirkungen verstehen.

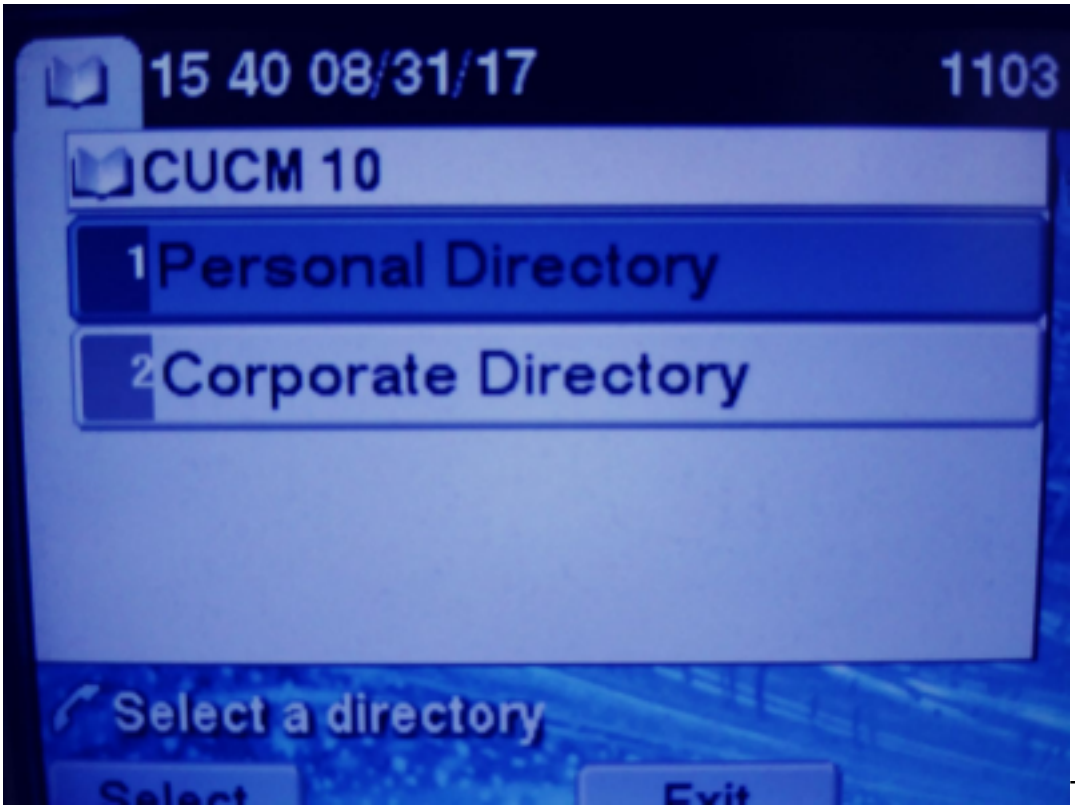
Schritt 2: Abonnieren Sie die Telefone für die Dienste.

Wechseln Sie zu **Gerät > Telefon >>Abonnent/Abbestellen.**



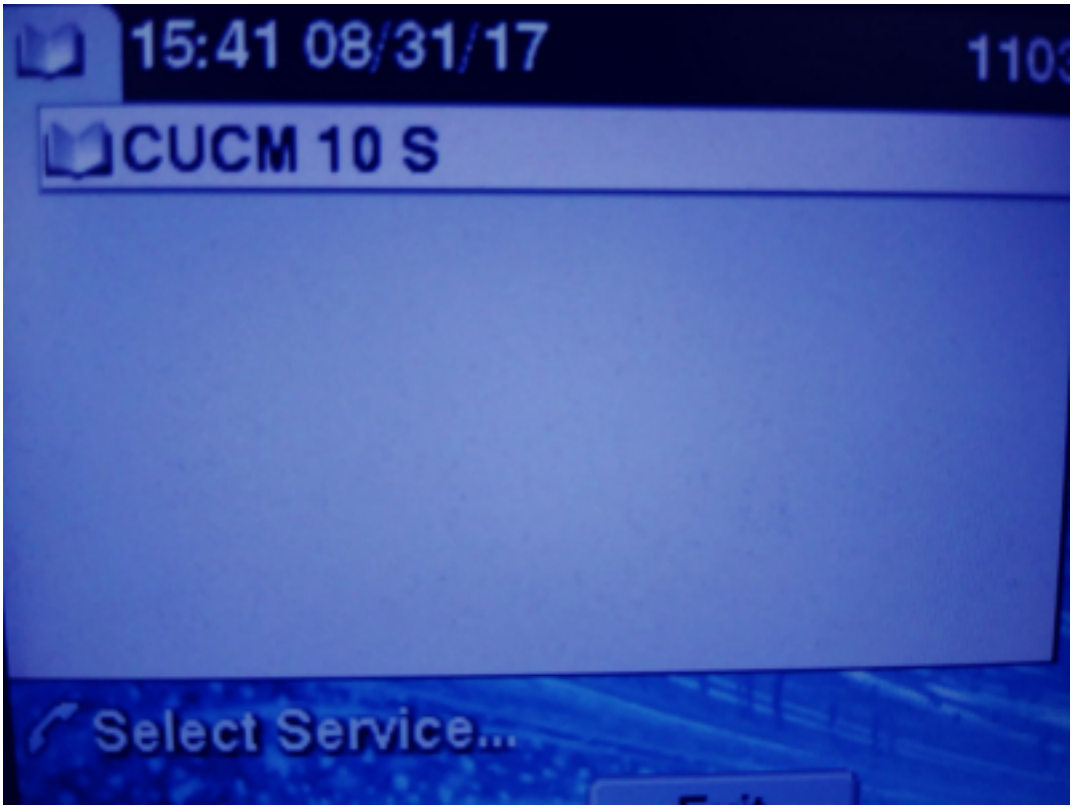
Wenn die Anwendung zu diesem Zeitpunkt HTTP anbietet, müssen Sie in der Lage sein, den Dienst zu erreichen, HTTPS ist jedoch noch nicht aktiv.

HTTP



TTP

HTTPS



HTTPS zeigt einen Fehler **"**Host not found**"** an, da der TVS-Dienst dies für das Telefon nicht authentifizieren kann.

Schritt 3: Laden Sie die Zertifikate für den externen Dienst in den CUCM hoch.

Laden Sie den externen Dienst **nur** als **Tomcat-Vertrauenswürdigkeit hoch**. Stellen Sie sicher, dass die Services auf allen Knoten zurückgesetzt werden.

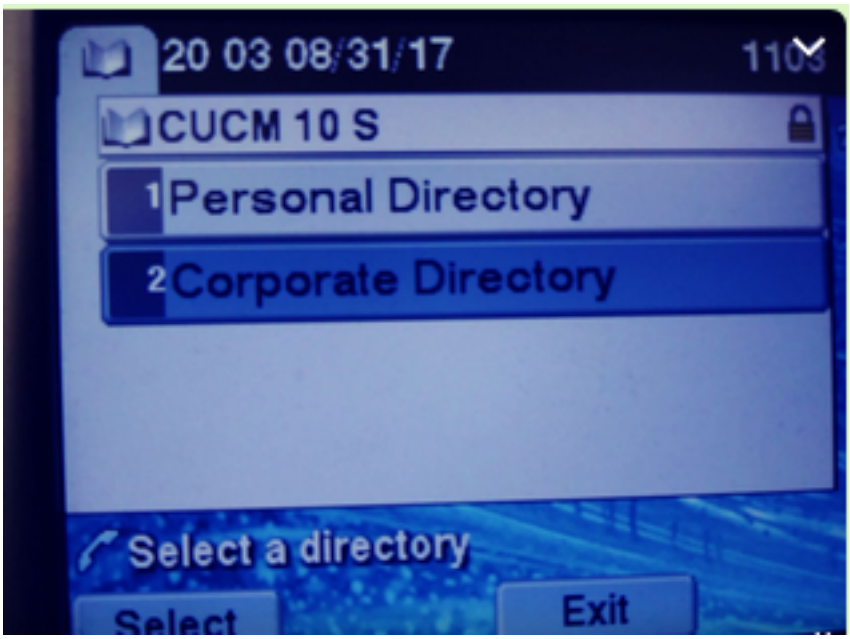
Diese Art von Zertifikaten wird nicht auf dem Telefon gespeichert, sondern das Telefon muss mit dem TVS-Dienst überprüfen, ob es die HTTPS-Verbindung herstellt.

Navigieren Sie zu **OS admin > Certificate > Certificate upload.**

Setzen Sie den CUCM Tomcat-Dienst auf allen Knoten vom SSH zurück.

```
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
```

Nach diesen Schritten müssen Telefone problemlos auf den HTTPS-Dienst zugreifen können.



Häufige Fragen (FAQ)

Nach dem Austausch von Zertifikaten schlägt HTTPS immer noch mit "Host nicht gefunden" fehl.

- Überprüfen Sie den Knoten, an dem das Telefon registriert ist, und stellen Sie sicher, dass das Drittanbieterzertifikat auf dem Knoten angezeigt wird.

-Setzen Sie die Tomcat auf dem spezifischen Knoten zurück.

- DNS überprüfen, sicherstellen, dass der Common Name(CN) des Zertifikats aufgelöst werden kann.

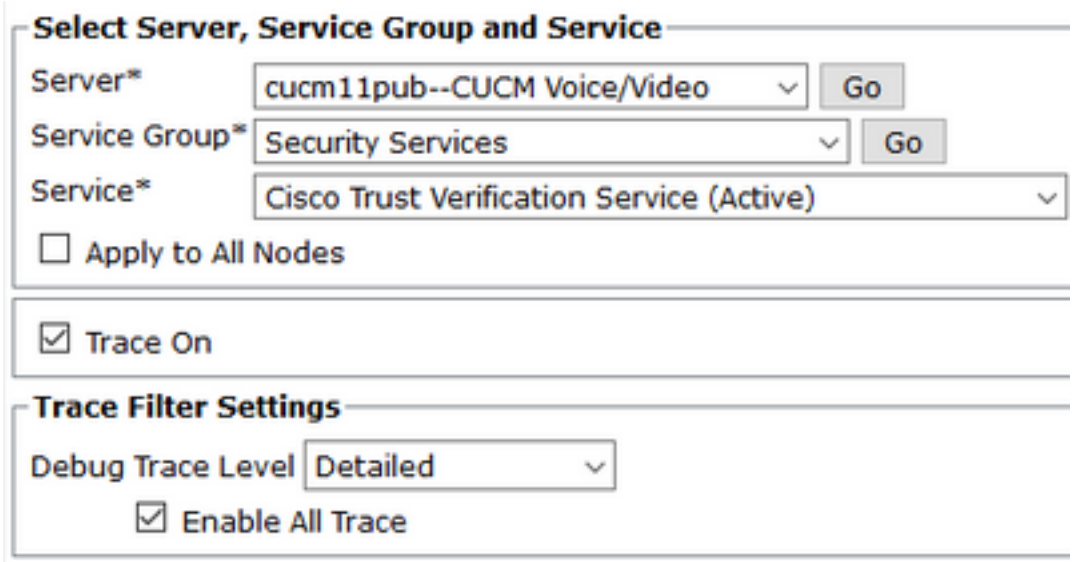
Fehlerbehebung

Erfassen Sie die CUCM-TVS-Protokolle, um Ihnen gute Informationen bereitstellen zu können.

Navigieren Sie zu **RTMT>System>Trace & Log Central > Protokolldateien sammeln.**

Hinweis: Sammeln Sie Protokolle von allen Knoten, und stellen Sie sicher, dass die TVS-Protokolle auf detailliert eingestellt sind.

TVS-Protokolle sind detailliert festgelegt



Ablaufverfolgungsbeispiel

```
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
```