# 安全外部電話服務配置示例

## 目錄



## 簡介

本文說明如何配置安全外部電話服務。此配置可與任何第三方服務配合使用，但是為了進行演示，本文檔使用遠端Cisco Unified Communications Manager(CUCM)伺服器。

作者：Cisco TAC工程師Jose Villalobos。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- CUCM
- CUCM證書
- 電話服務

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- CUCM 10.5.X/CUCM 11.X
- 瘦客戶端控制協議(SCCP)和會話初始協定(SIP)電話註冊到CUCM
- 本實驗使用主題備用名稱(SAN)證書。
- 外部目錄將位於SAN證書上。
- 對於本示例上的所有系統，證書頒發機構(CA)將相同，所有使用的證書都是CA符號。
- 域名伺服器(DNS)和網路時間協定(NTP)需要設定屬性，並且工作正常。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路處於活動狀態，請確保您瞭解任何更改的潛在影響。

### 相關產品

本文件也適用於以下硬體和軟體版本：

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

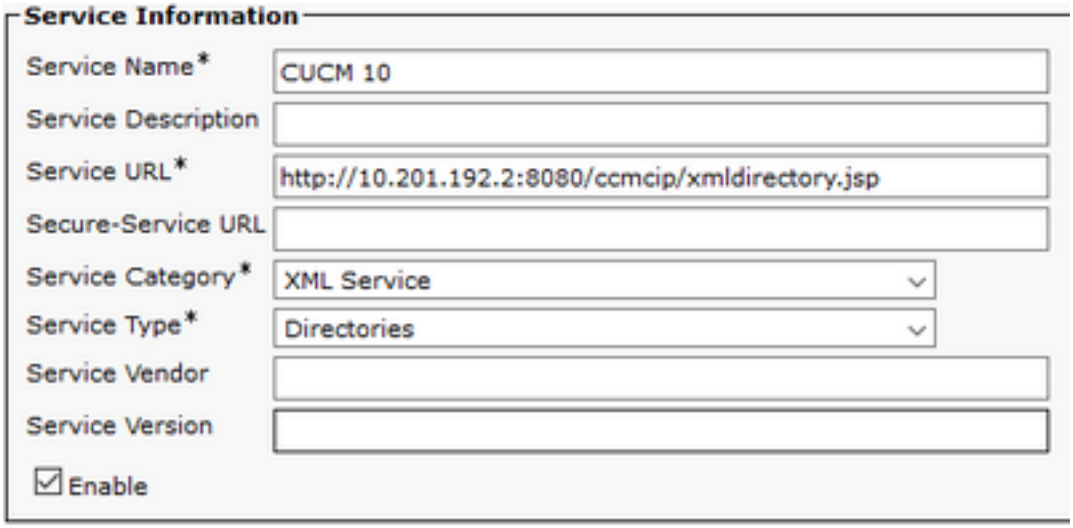
# 配置步驟

**步驟1.**在系統上設定服務URL。

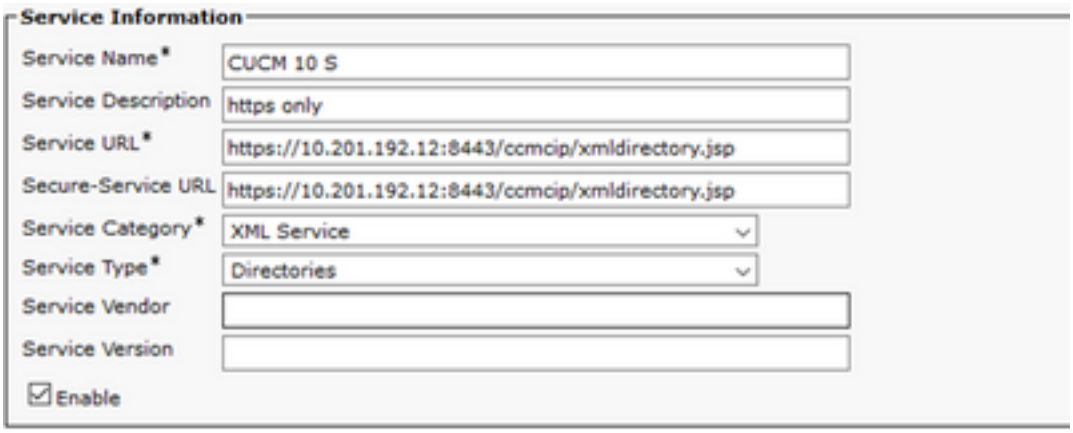
設定超文本傳輸協定(HTTP)和超文本傳輸協定安全(HTTPS)作為概念驗證。最終的想法是僅使用安全HTTP流量。

導航到**Device > Device Settings> Phone service > Add new**

僅限HTTP



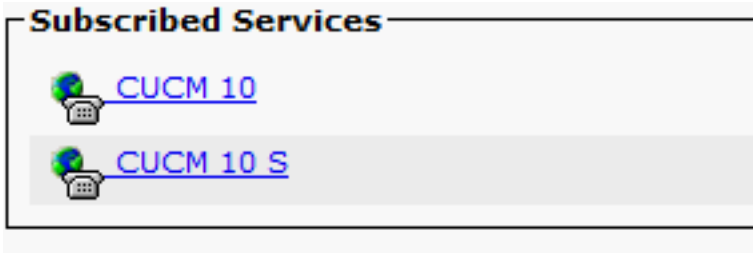

僅限HTTPS




> **警告**：如果為**Enterprise Subscription新增檢查，**則可以跳過第二步。但是，此更改將重置所有電話，以確保您瞭解潛在的影響。

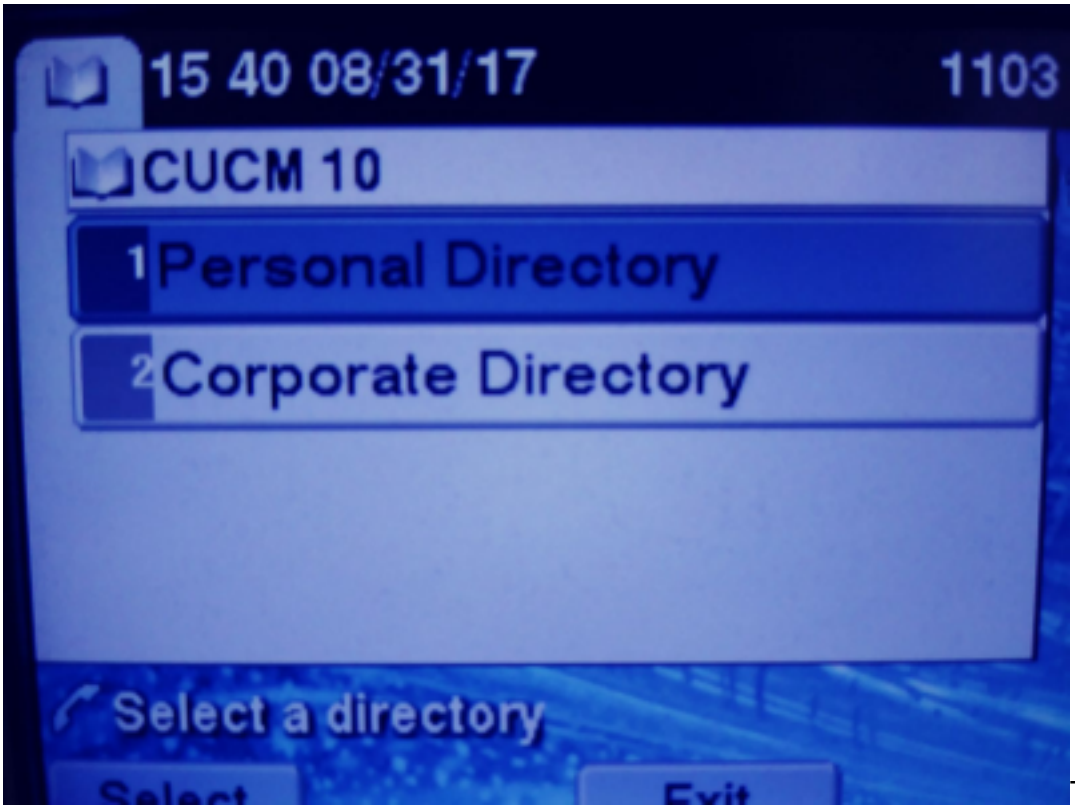
**步驟2.**為電話訂購服務。

Natigate to **Device>Phone>>Subscriber/Unsubscribe服務。**



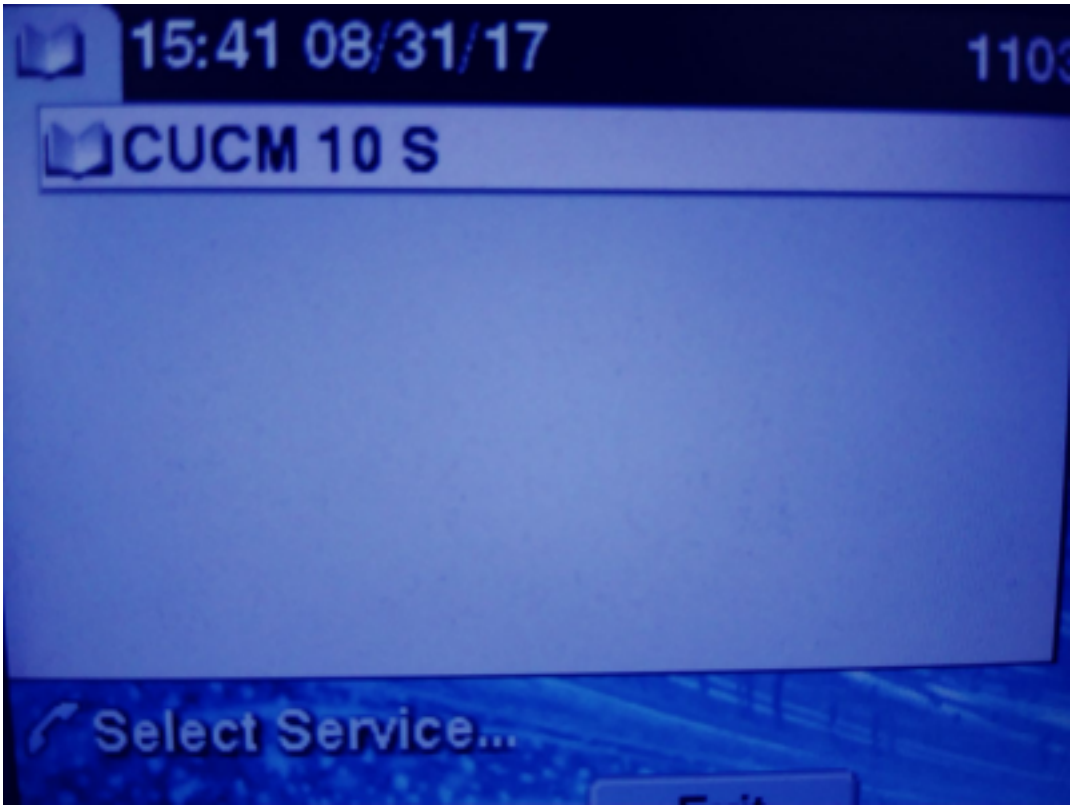

此時，如果應用程式提供HTTP，您必須能夠訪問該服務，但https仍未啟用。

HTTP




TTP

HTTPS




HTTPS將顯示「Host not found」錯誤，因為TVS服務無法對電話進行身份驗證。

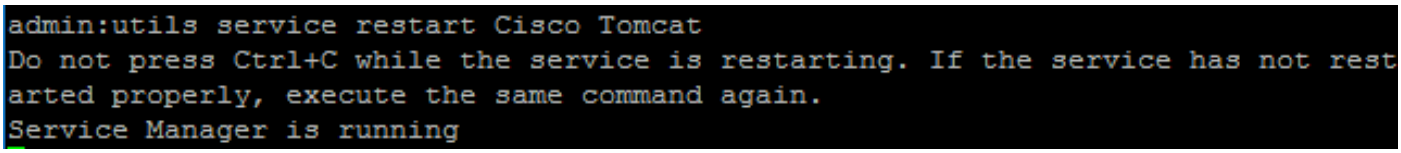
**步驟3.**將外部服務證書上傳到CUCM。

僅將外部服務上**傳為Tomcat信任**。確保服務在所有節點上重置。

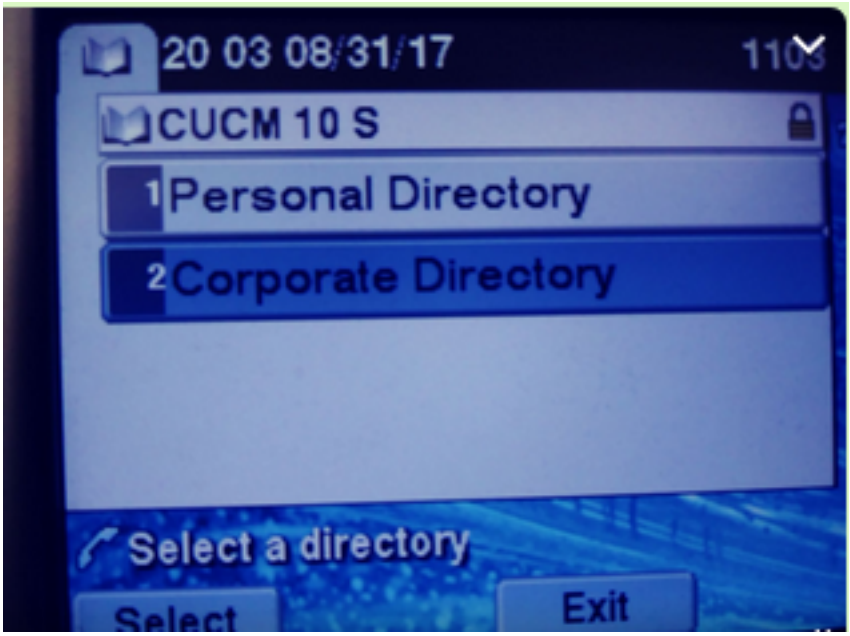
這種型別的證書不儲存在電話上，電話必須與TVS服務進行檢查以檢視它是否建立HTTPS連線。

導航到**OS admin> Certificate> Certificate upload。**


從SSH重置所有節點上的CUCM Tomcat服務。




完成這些步驟後，電話必須能夠順利存取HTTPS服務




# 常見問題(FAQ)

交換憑證後，HTTPS仍會失敗，並顯示「未找到主機」。

— 檢查電話註冊所在的節點，並確保您看到該節點上的第三方證書。

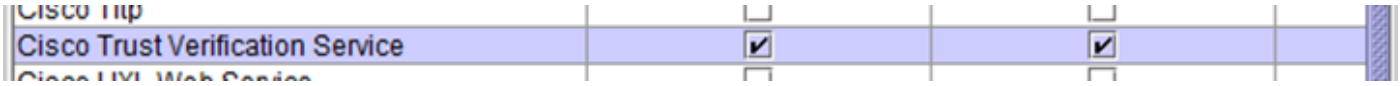
— 重置特定節點上的tomcat。

— 檢查DNS，確保可以解析證書的公用名(CN)。

# 疑難排解

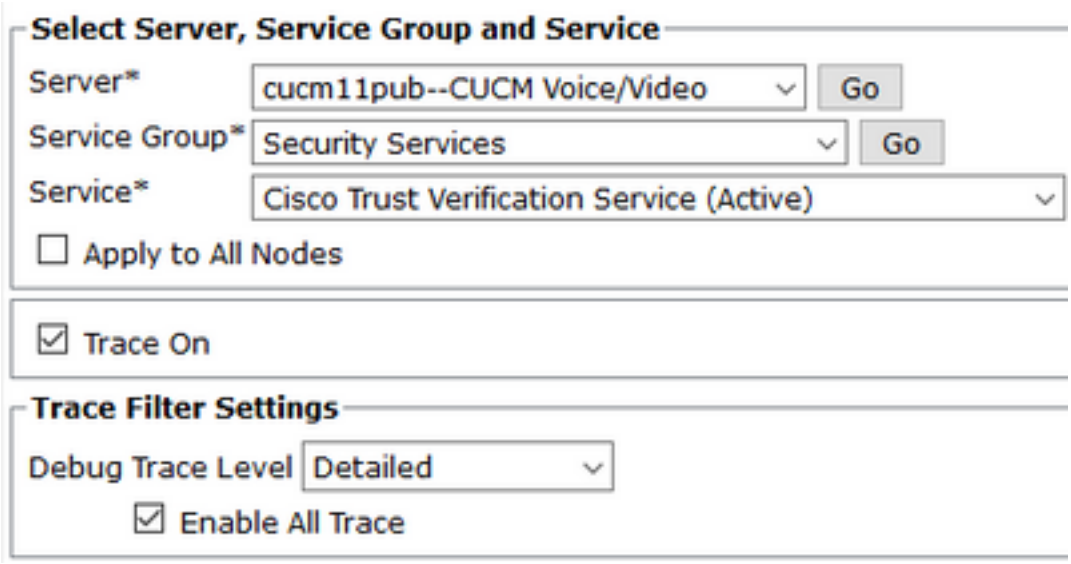
收集CUCM TVS日誌必須提供良好的資訊

導航到**RTMT>System>Trace & log Central >收集日誌檔案**




**附註**：從所有節點收集日誌並確保TVS日誌設定為詳細。

TVS日誌設定為detailed




跟蹤示例

```
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</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
```