在聯絡中心企業版中配置安全SIP信令

目錄

簡介

本文說明如何在Contact Center Enterprise(CCE)綜合呼叫流程中保護會話初始協定(SIP)信令。

必要條件

憑證產生和匯入不在本檔案的範圍之內，因此必須建立思科整合通訊管理員(CUCM)、客戶語音入口網站(CVP)通話伺服器、思科虛擬語音瀏覽器(CVVB)和思科整合邊界元件(CUBE)的憑證，並將其匯入到各自的元件。如果使用自簽名證書，則必須在不同元件之間執行證書交換。

需求

思科建議您瞭解以下主題：

- CCE
- CVP
- 立方體
- CUCM
- CVVB

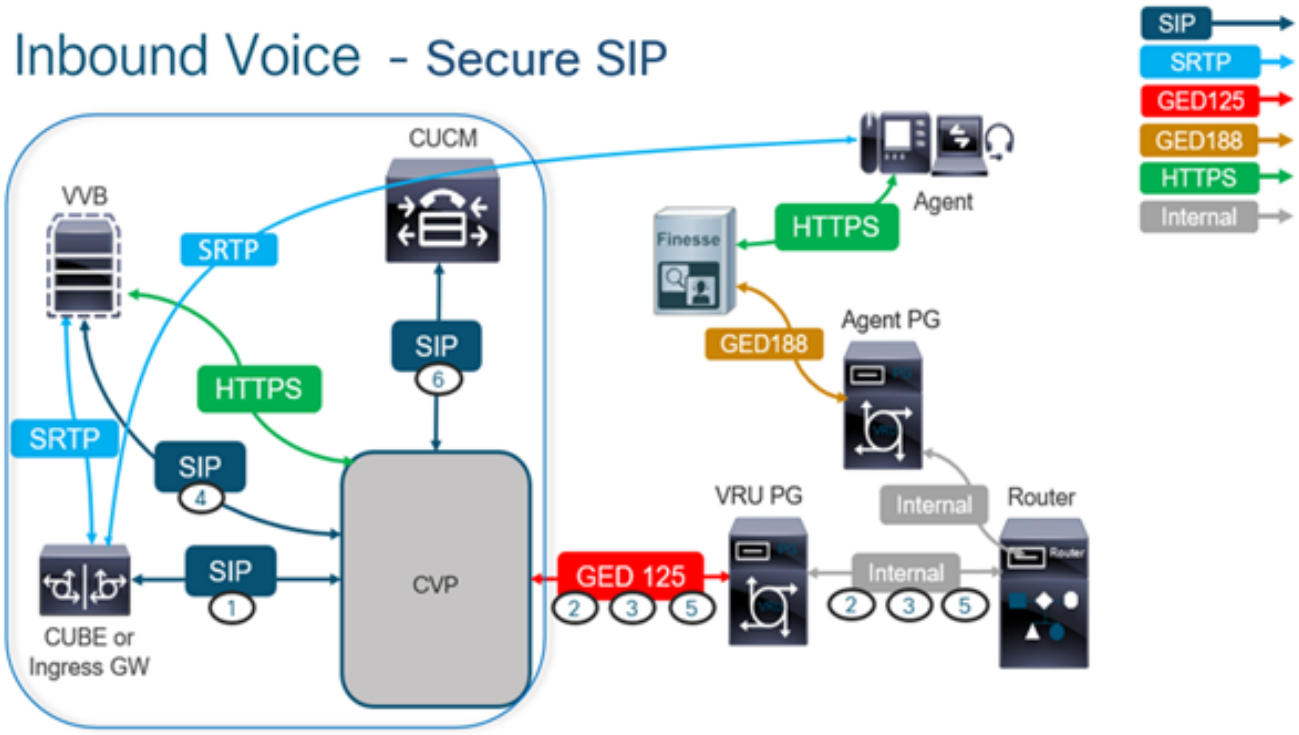
採用元件

本檔案中的資訊是根據套件客服中心企業版(PCCE)、CVP、CVVB和CUCM版本12.6，但也適用於之前的版本。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

下圖顯示了在聯絡中心綜合呼叫流程中參與SIP信令的元件。當語音呼叫進入系統時，首先通過入口網關或CUBE，因此在CUBE上開始安全SIP配置。接下來，配置CVP、CVVB和CUCM。



任務1.CUBE安全配置

在此任務中，配置CUBE以保護SIP協定消息。

必需的配置：

- 為SIP使用者代理(UA)配置預設信任點
- 修改撥號對等體以使用傳輸層安全(TLS)

步驟：

1. 開啟與CUBE的安全殼層(SSH)會話。
2. 運行這些命令以使SIP堆疊使用CUBE的證書頒發機構(CA)證書。CUBE建立與CUCM(198.18.133.3)和CVP(198.18.133.13)之間的SIP TLS連線。

conf t sip-ua transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit

```
CC-VCUBE(config)#sip-ua
CC-VCUBE(config-sip-ua)#transport tcp tls v1.2
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#exit
CC-VCUBE(config)#
```

3. 運行這些命令以在傳出撥號對等體上啟用CVP。在此示例中，撥號對等標籤6000用於將呼叫路由到CVP。

Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls exit

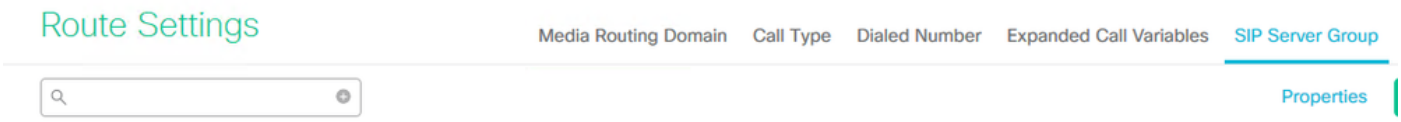
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#
CC-VCUBE(config-dial-peer)#exit
CC-VCUBE(config)#
```

任務2.CVP安全配置

在此任務中，配置CVP呼叫伺服器以保護SIP協定消息(SIP TLS)。

步驟：

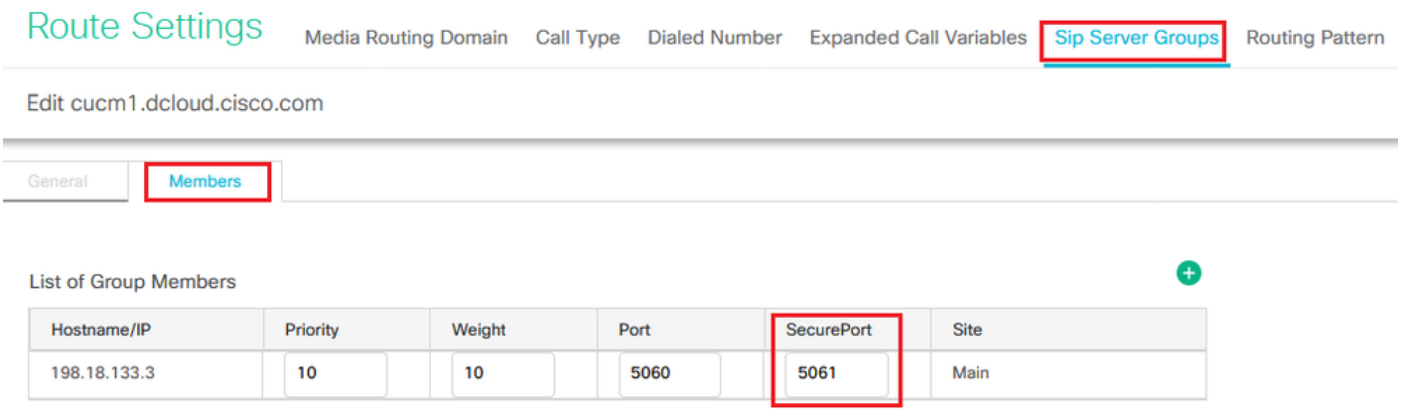
1. 登入到UCCE Web Administration.
2. 導航至 Call Settings > Route Settings > SIP Server Group.



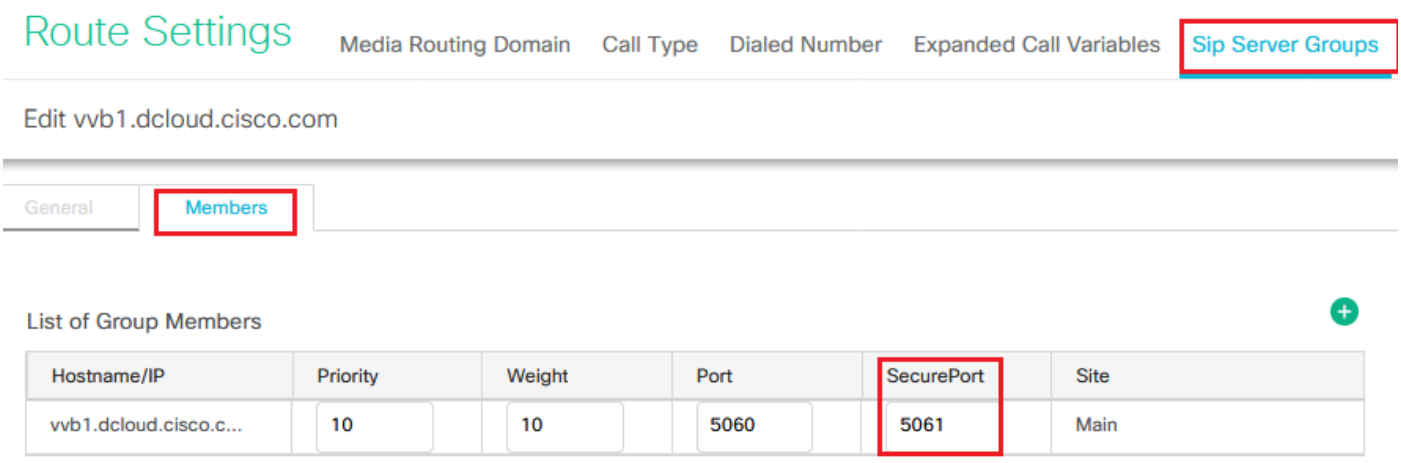
根據您的配置，您為CUCM、CVVB和CUBE配置了SIP伺服器組。您需要將所有安全SIP埠設定為5061。在此示例中，使用以下SIP伺服器組：

- cucm1.dcloud.cisco.com 對於CUCM
- vvb1.dcloud.cisco.com 適用於CVVB
- cube1.dcloud.cisco.com 對於CUBE

3. 按一下 cucm1.dcloud.cisco.com 然後在 **Members** 頁籤，其中顯示SIP伺服器組配置的詳細資訊。設定 SecurePort 成長至 5061 然後按一下 Save .



4. 按一下 vvb1.dcloud.cisco.com 然後在 **Members** 頁籤。將SecurePort設定為 5061 然後按一下 Save.

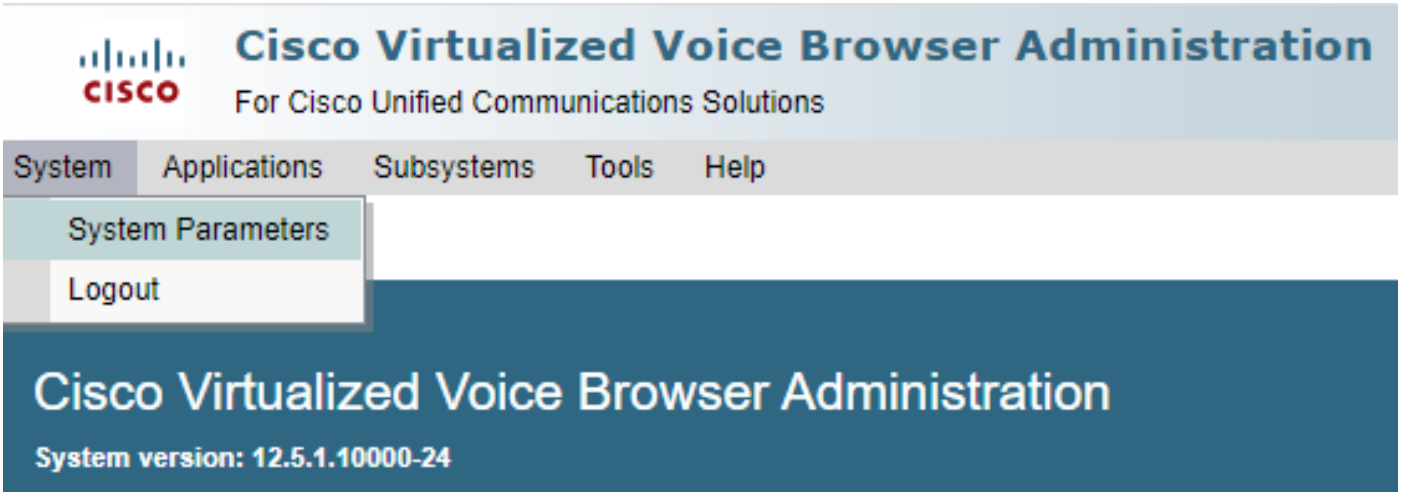


任務3.CVVB安全配置

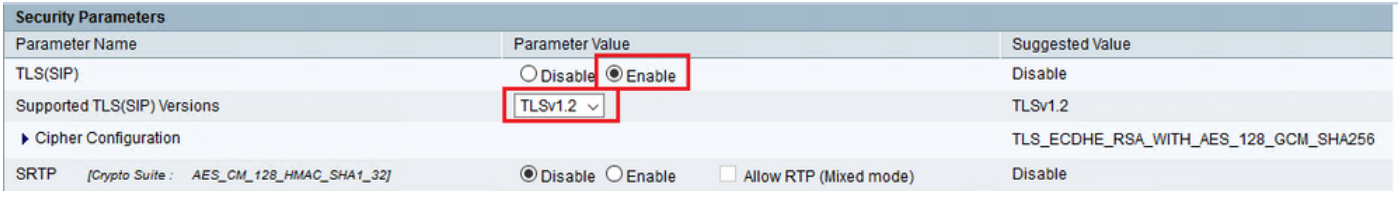
在此任務中，配置CVVB以保護SIP協定消息(SIP TLS)。

步驟：

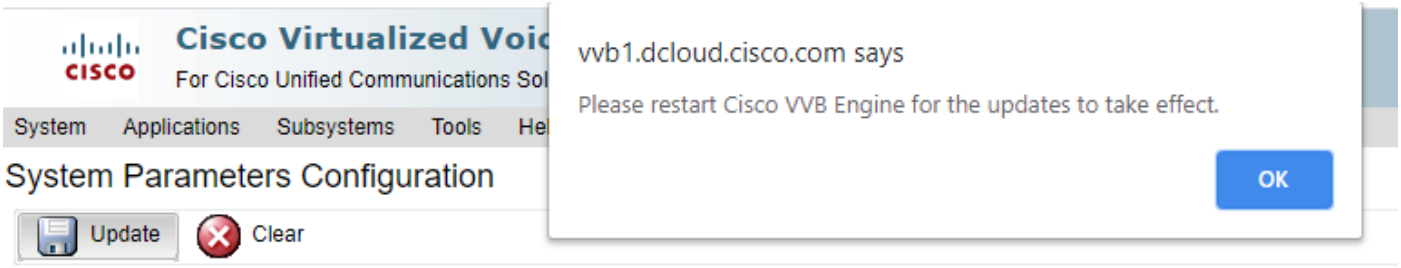
1. 登入到 **Cisco VVB Administration** 頁面。
2. 導航至 System > System Parameters.



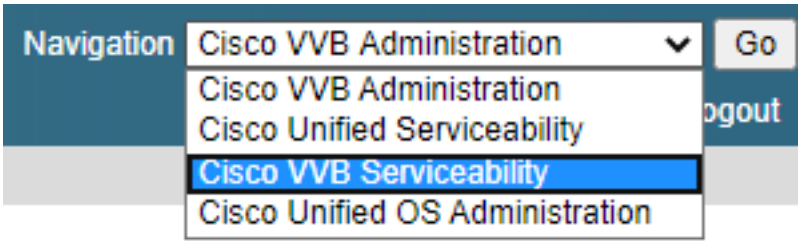
3. 在 Security Parameters 部分，選擇 Enable 對於 TLS(SIP)。保留 Supported TLS(SIP) version 作為 TLSv1.2.



4. 按一下「**Update**」。按一下 Ok 當提示重新啟動CVVB引擎時。

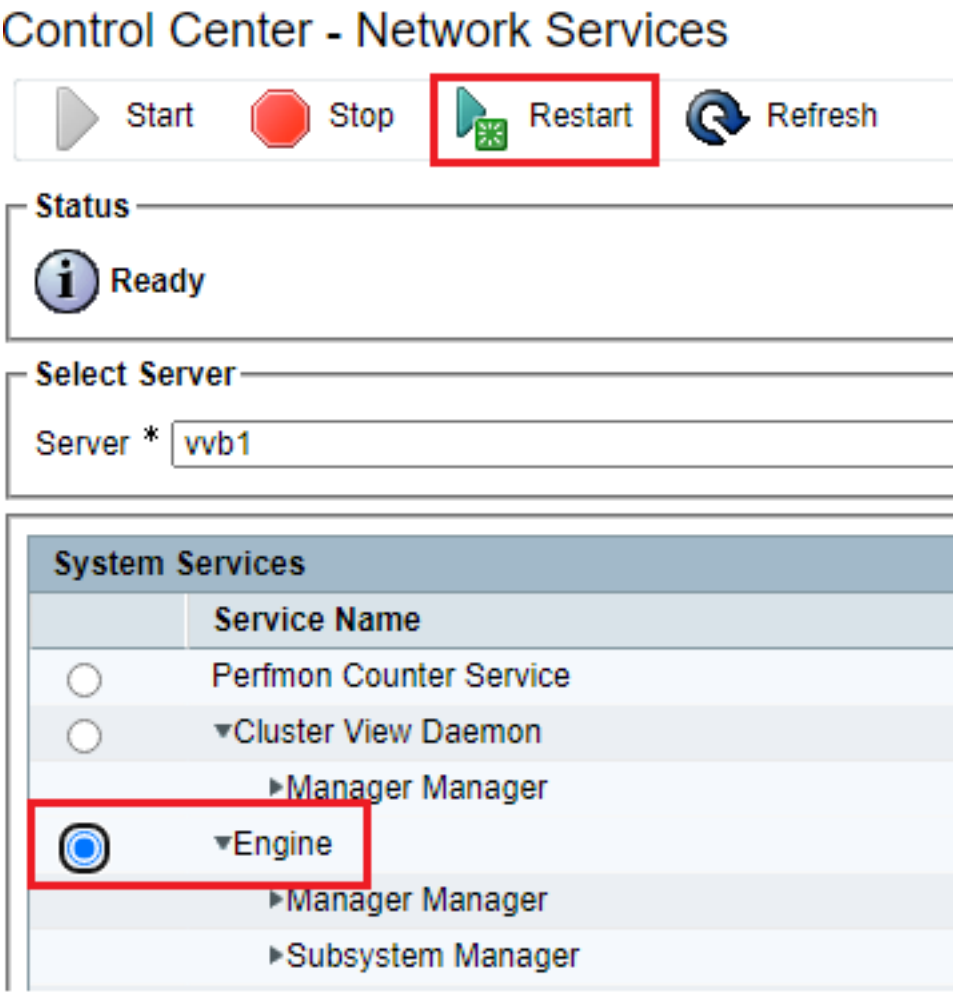


5. 這些更改需要重新啟動Cisco VVB引擎。要重新啟動VVB引擎，請導航至 Cisco VVB Serviceability 然後按一下 **Go**.



6. 導航至 Tools > Control Center – Network Services.

7. 選擇 Engine 然後按一下 Restart.



任務4.CUCM安全配置

要保護CUCM上的SIP消息，請執行以下配置：

- 將CUCM安全模式設定為混合模式
- 為CUBE和CVP配置SIP中繼安全配置檔案
- 將SIP中繼安全配置檔案關聯到各自的SIP中繼
- 安全代理與CUCM的裝置通訊

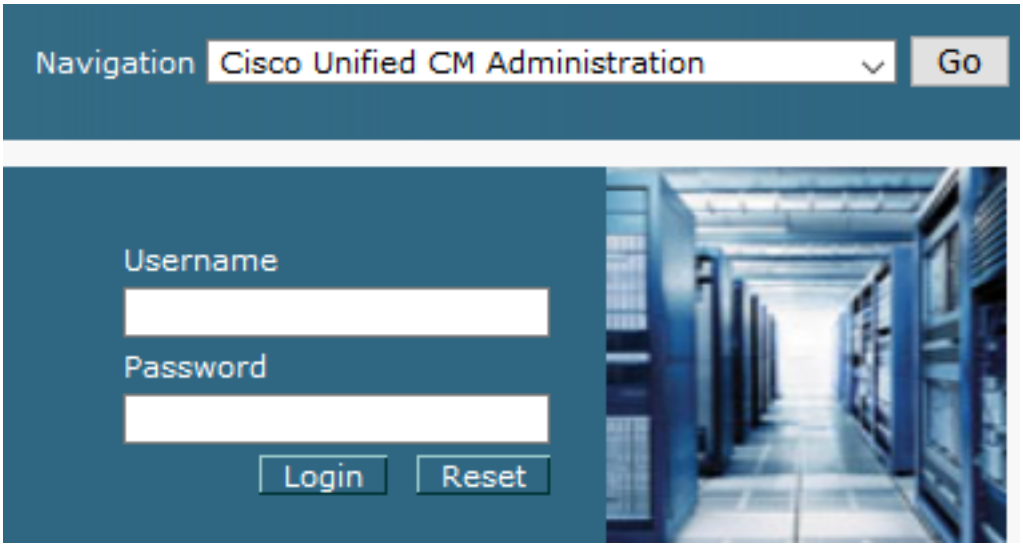
將CUCM安全模式設定為混合模式

CUCM支援兩種安全模式：

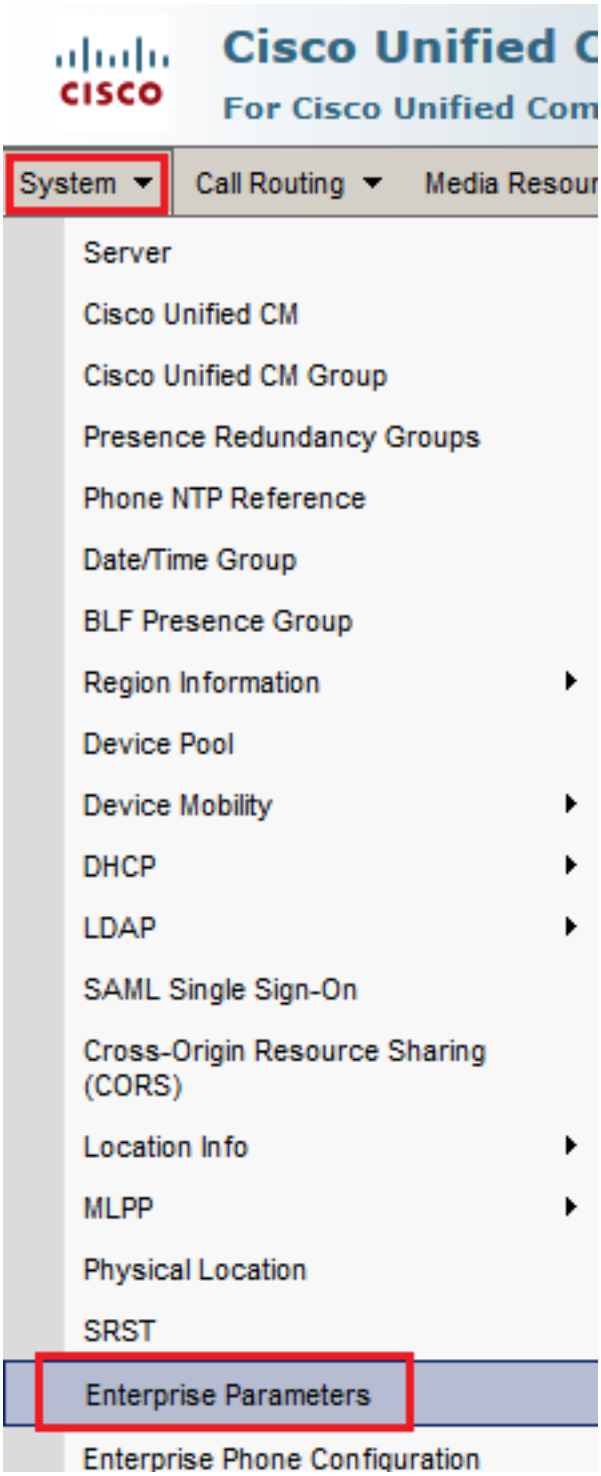
- 非安全模式（預設模式）
- 混合模式（安全模式）

步驟：

1. 若要將安全模式設定為混合模式，請登入到 Cisco Unified CM Administration 介面.



2. 成功登入到CUCM後，導航至 System > Enterprise Parameters.



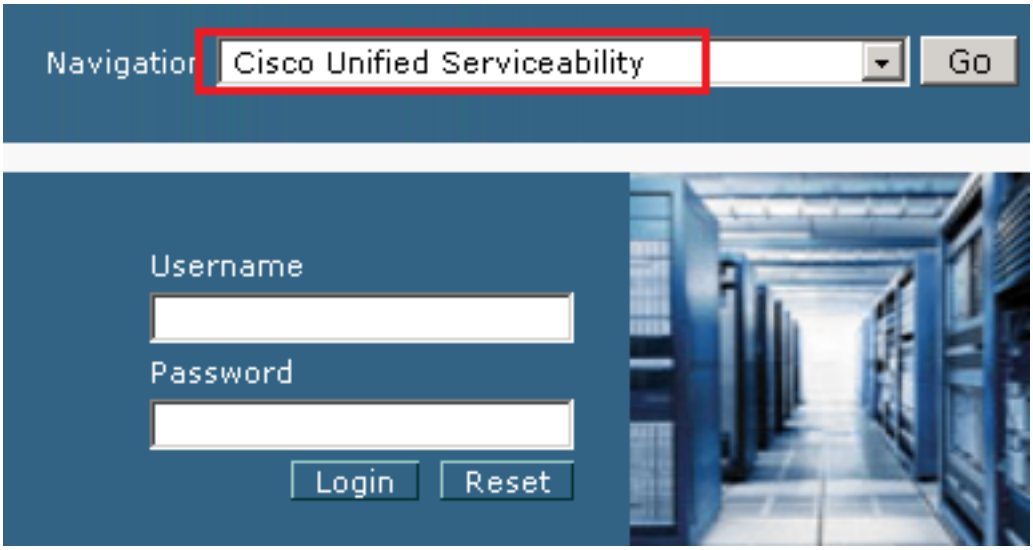
3. 在下面 Security Parameters 部分，檢查是否 Cluster Security Mode 設定為 0.

4. 如果群集安全模式設定為0，則表示群集安全模式設定為非安全。您需要從CLI啟用混合模式。
5. 開啟與CUCM的SSH會話。
6. 通過SSH成功登入到CUCM後，請運行以下命令： utils ctl set-cluster mixed-mode

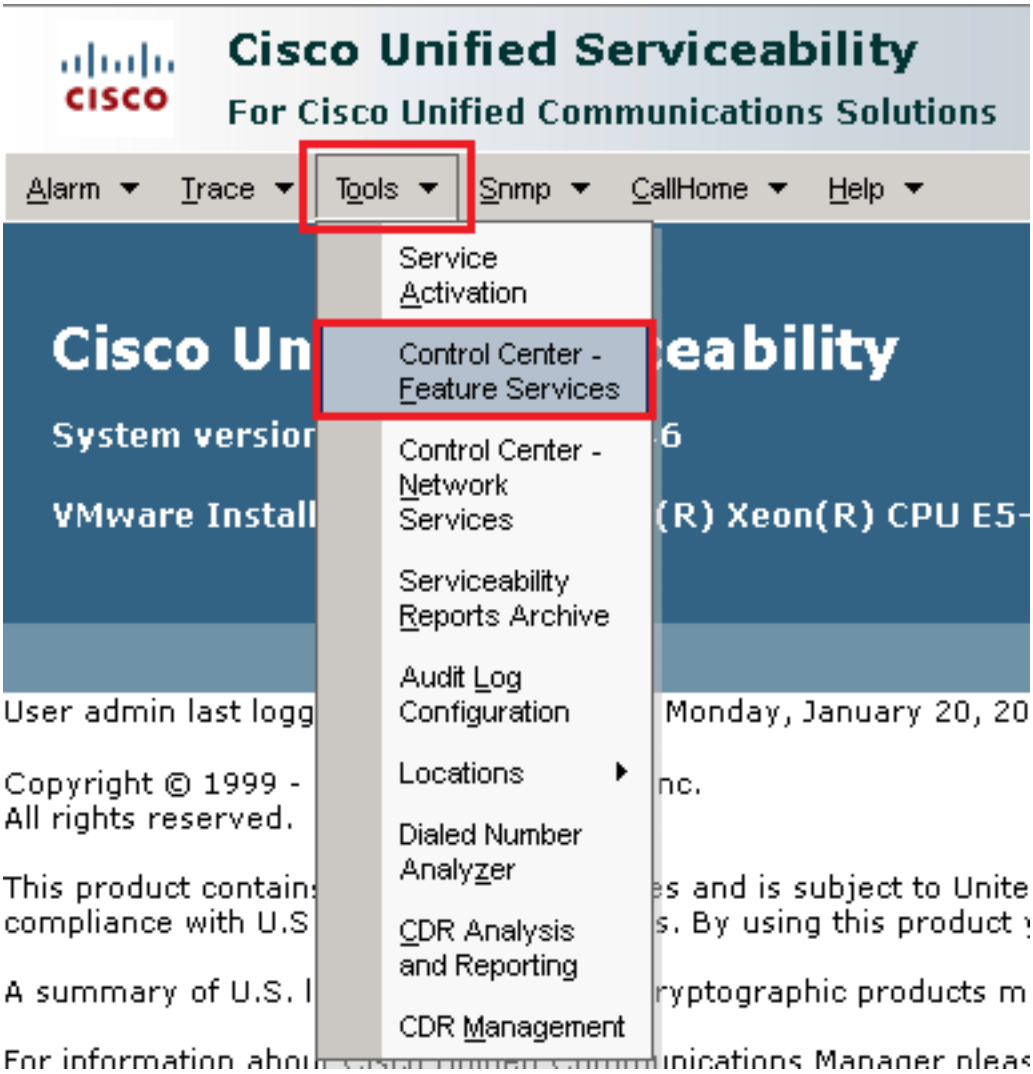
7. 類型 y 並在系統提示時按一下**Enter**。此命令將群集安全模式設定為混合模式。

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.

admin:
```

8. 要使更改生效，請重新啟動 Cisco CallManager 和 Cisco CTIManager 服務。
9. 要重新啟動服務，請導航並登入到 Cisco Unified Serviceability.

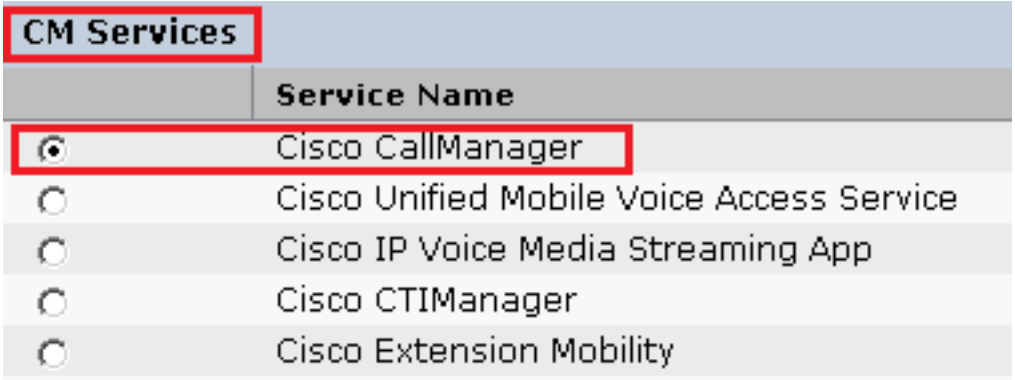


10. 成功登入後，導航至 Tools > Control Center – Feature Services.

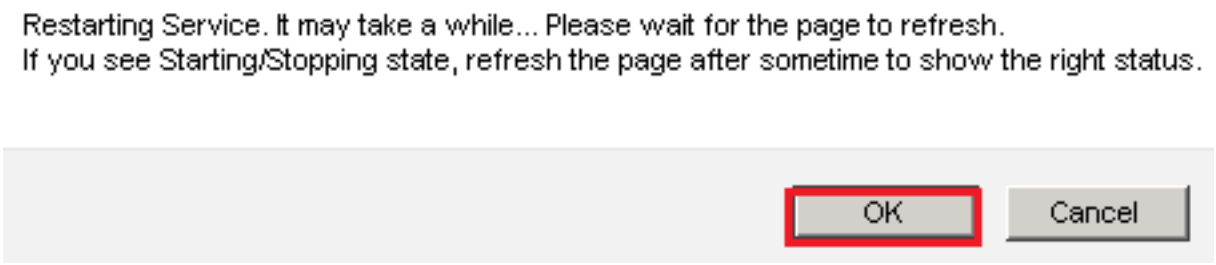


11. 選擇伺服器，然後按一下 Go.

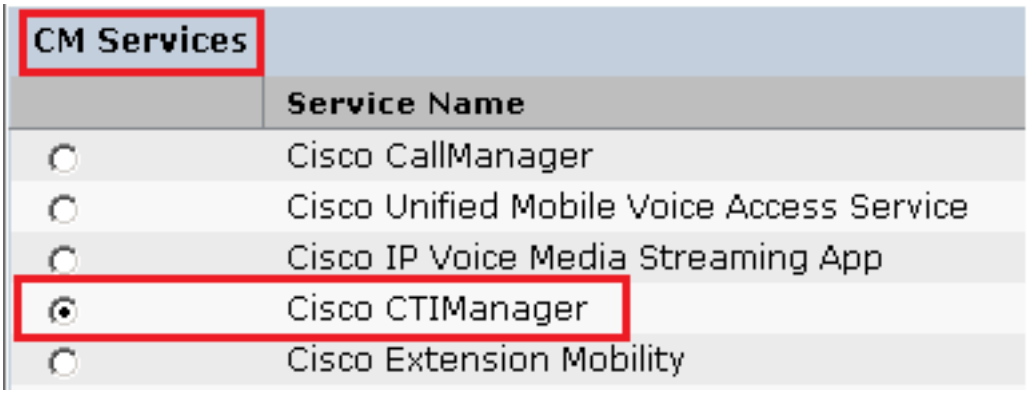
12. 在CM服務下，選擇 Cisco CallManager 然後按一下 Restart 按鈕。



13. 確認彈出消息，然後按一下 OK.等待服務成功重新啟動。



14. 成功重新啟動 Cisco CallManager，選擇Cisco CTIManager 然後按一下 Restart 按鈕以重新啟動 Cisco CTIManager 服務。



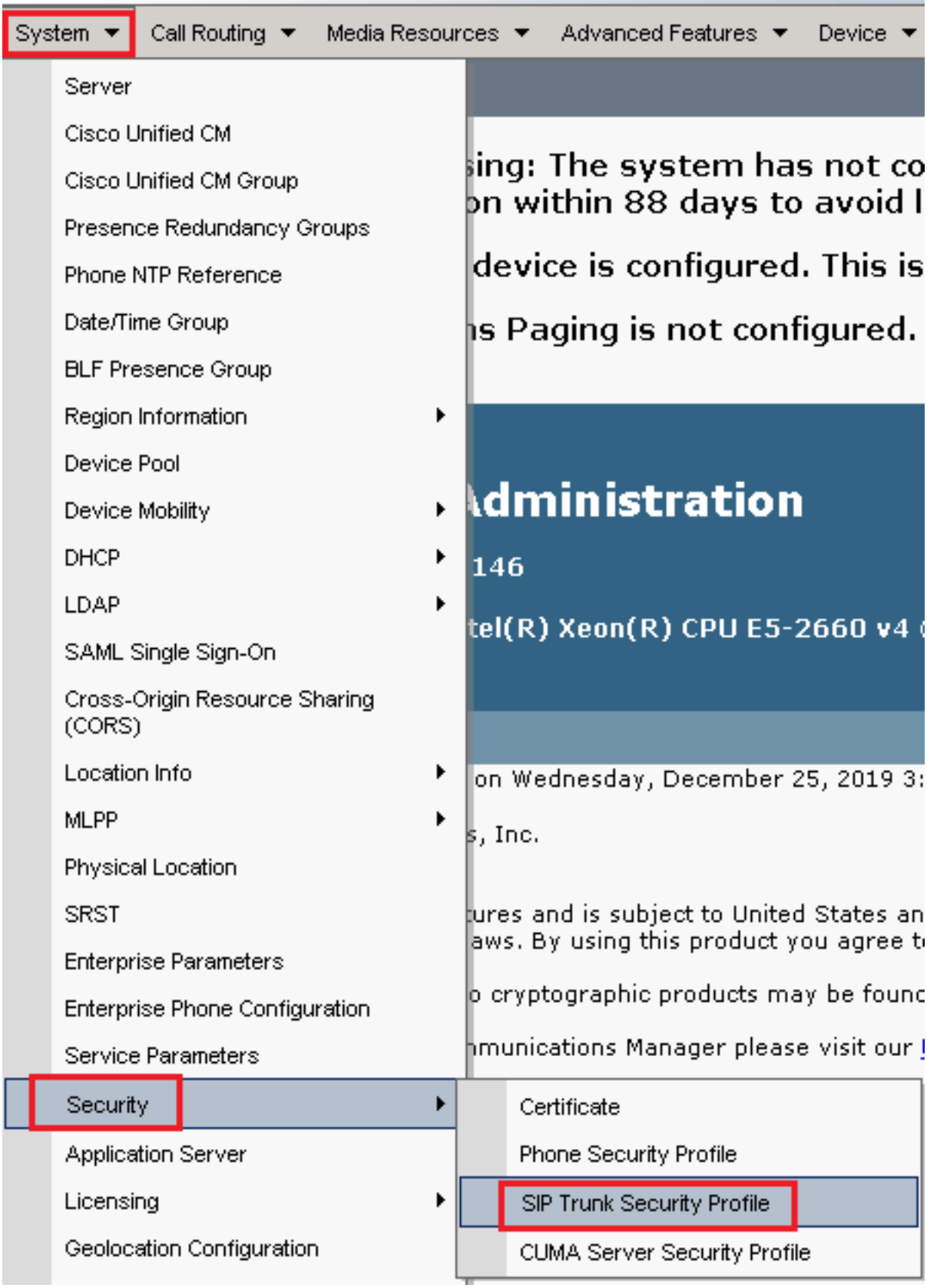
15. 確認彈出消息，然後按一下 OK.等待服務成功重新啟動。

16. 服務成功重新啟動後，驗證群集安全模式是否設定為混合模式，然後按照步驟5中的說明導航到CUCM管理。然後檢查 Cluster Security Mode.現在必須設定為 1.

為CUBE和CVP配置SIP中繼安全配置檔案

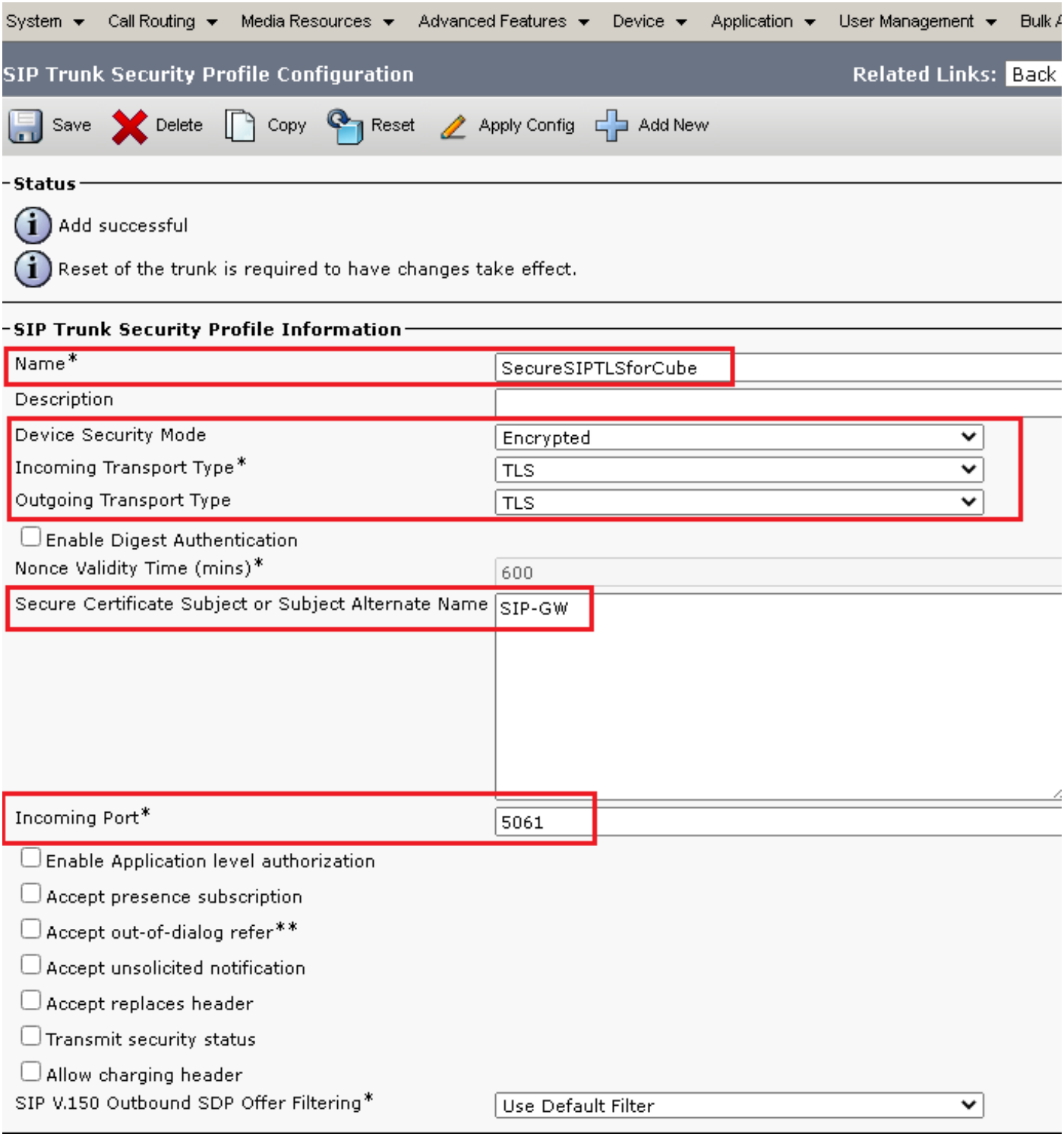
步驟：

1. 登入到 CUCM administration 介面.
2. 成功登入到CUCM後，導航至 System > Security > SIP Trunk Security Profile 以便為CUBE建立裝置安全配置檔案。



3. 在左上角，按一下 Add New 以便新增新配置檔案。

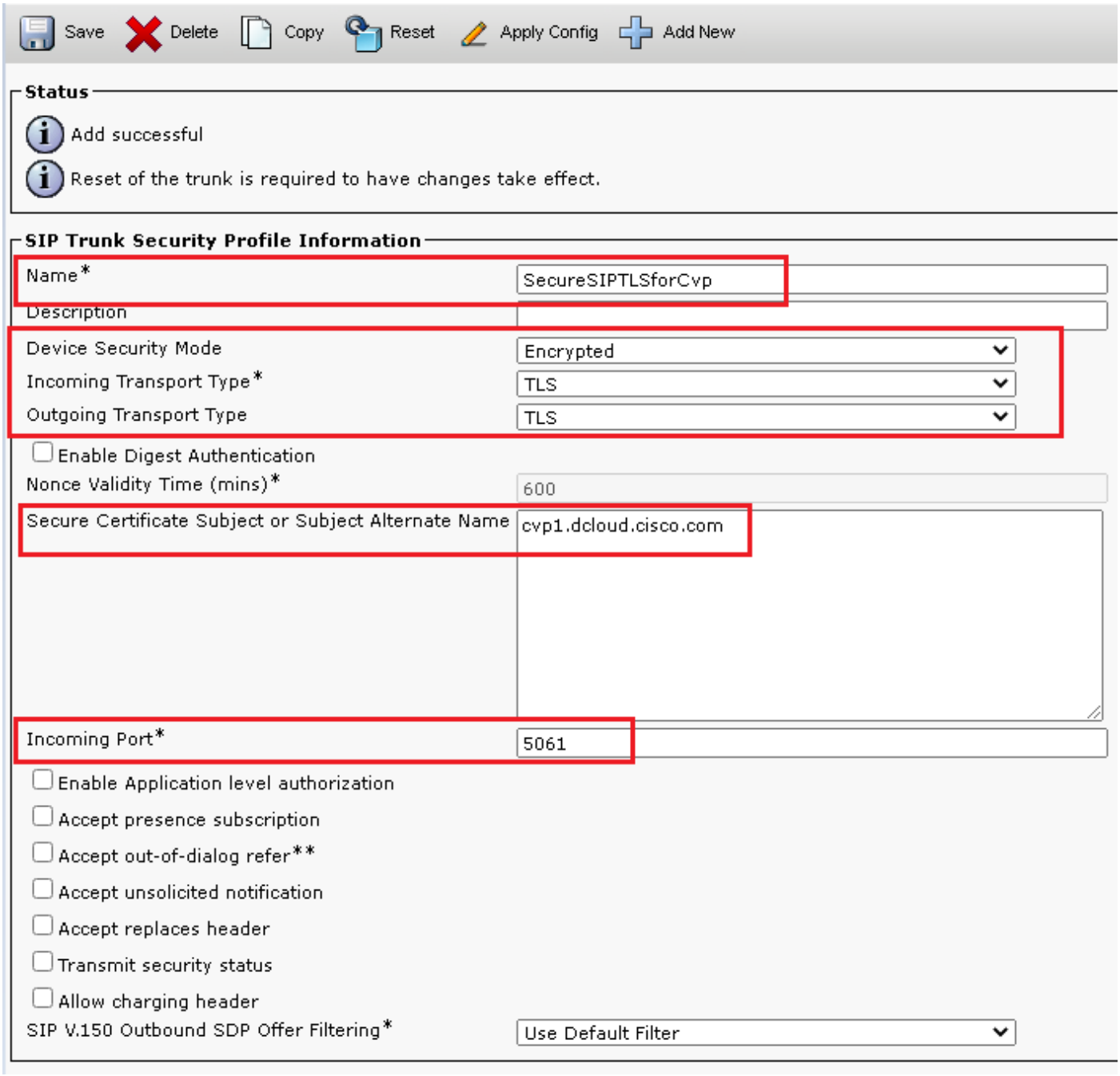
4. 設定 SIP Trunk Security Profile 如下圖所示，然後按一下 Save 位於頁面左下角 Save 它。



5.確保已設定好預設的 Secure Certificate Subject or Subject Alternate Name CUBE證書的公用名(CN)，因為它

必須匹配。

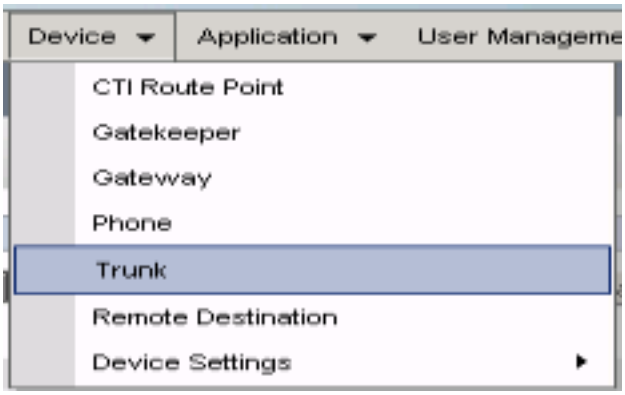
6.按一下 Copy 按鈕並更改 Name 成長至 SecureSipTLSforCVP 和 Secure Certificate Subject CVP呼叫伺服器證書的CN，因為它必須匹配。按一下 Save 按鈕。



將SIP中繼安全配置檔案關聯到各自的SIP中繼

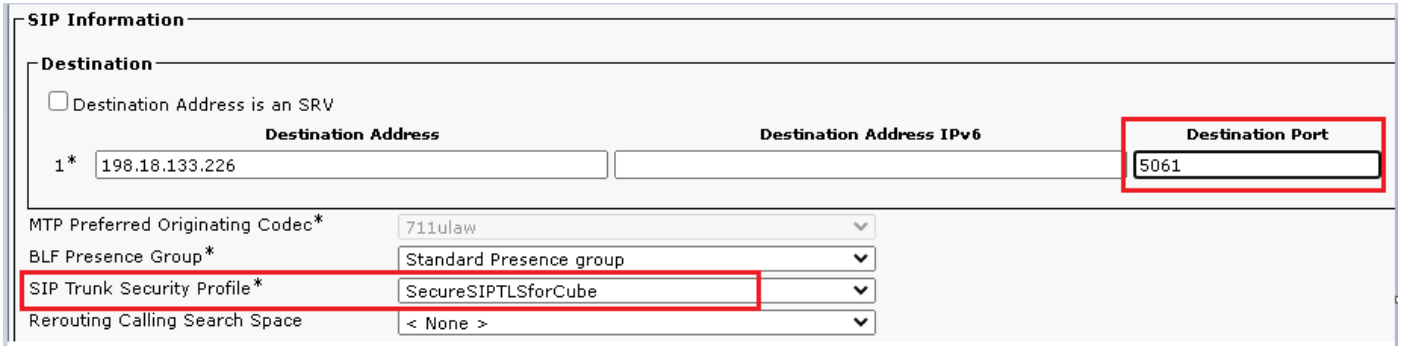
步驟：

1. 在CUCM管理頁面上，導航至 Device > Trunk.

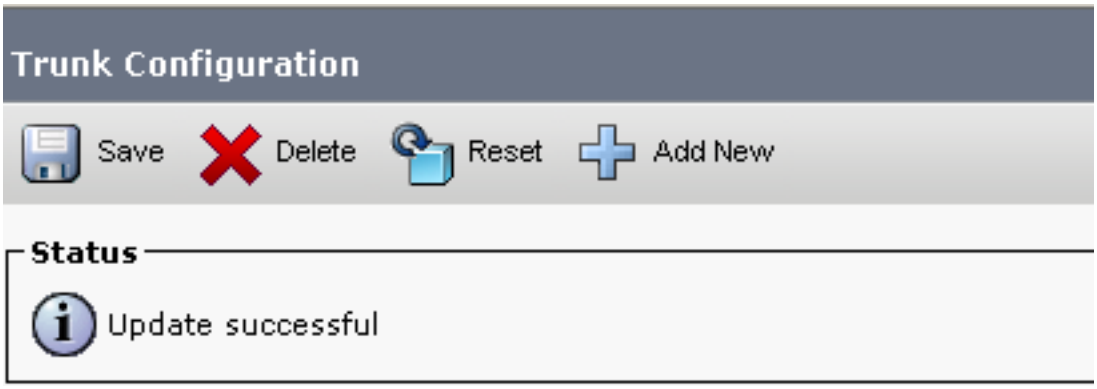


2. 搜尋CUBE中繼。在本示例中，CUBE中繼名稱是 vCube . 按一下 **Find**.

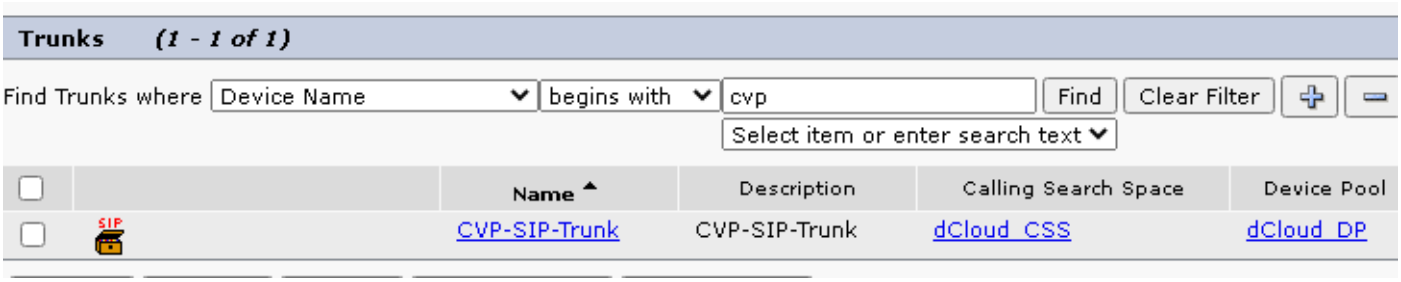
3. 按一下vCUBE以開啟vCUBE中繼配置頁。
4. 向下滾動到 SIP Information 部分，並更改 Destination Port 成長至 5061.
5. 變更 SIP Trunk Security Profile 成長至 SecureSIPTLSForCube.



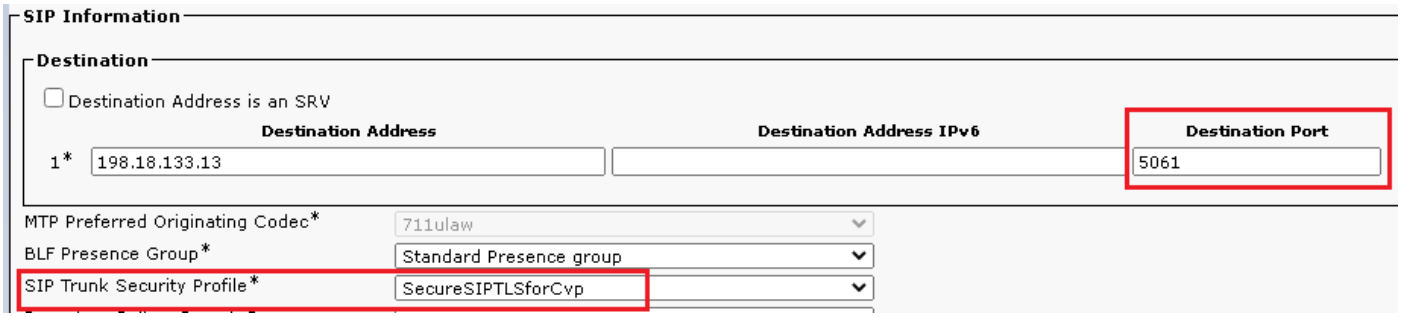
6. 按一下 Save 然後 Rest 以 Save 並應用更改。



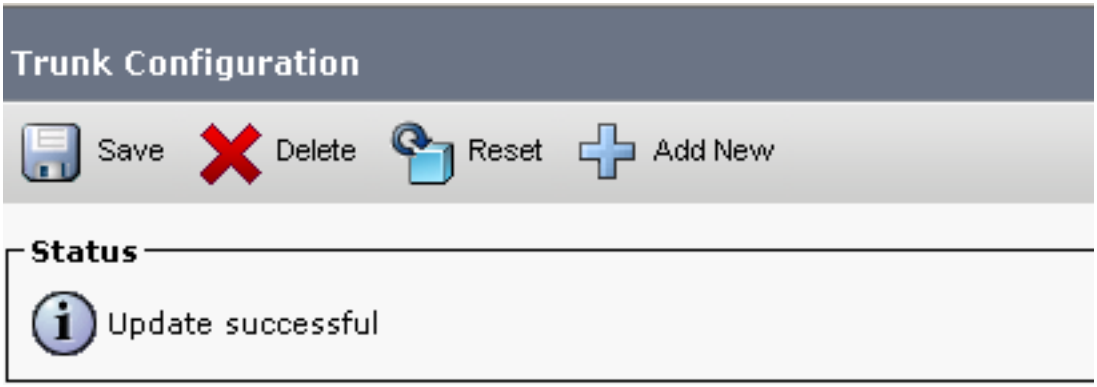
7. 導航至 Device > Trunk，並搜尋CVP中繼。在本示例中，CVP中繼名稱是 cvp-SIP-Trunk．按一下 **Find**.



8. 按一下 CVP-SIP-Trunk 以開啟CVP中繼配置頁面。
9. 向下滾動到 SIP Information 小節和更改 Destination Port 成長至 5061．
10. 變更 SIP Trunk Security Profile 成長至 SecureSIPTLSForCvp.



11. 按一下 Save 然後 Rest 以 save 並應用更改。



安全代理與CUCM的裝置通訊

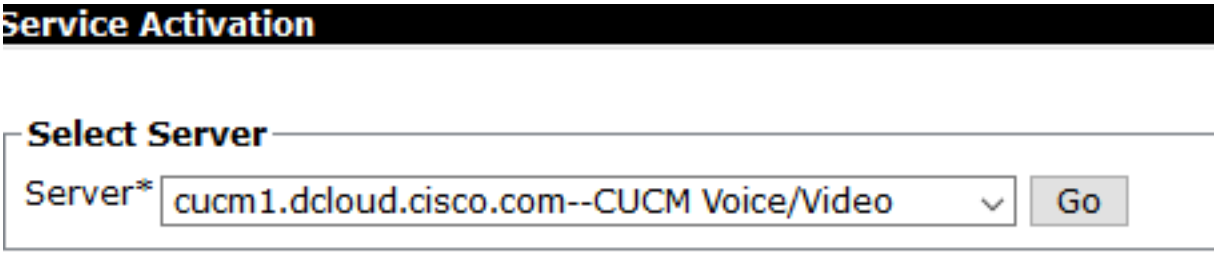
要為裝置啟用安全功能，必須安裝本地重要證書(LSC)並為該裝置分配安全配置檔案。LSC擁有端點

的公鑰，該公鑰由憑證授權代理功能(CAPF)私鑰簽署。預設情況下，它不會安裝在電話上。

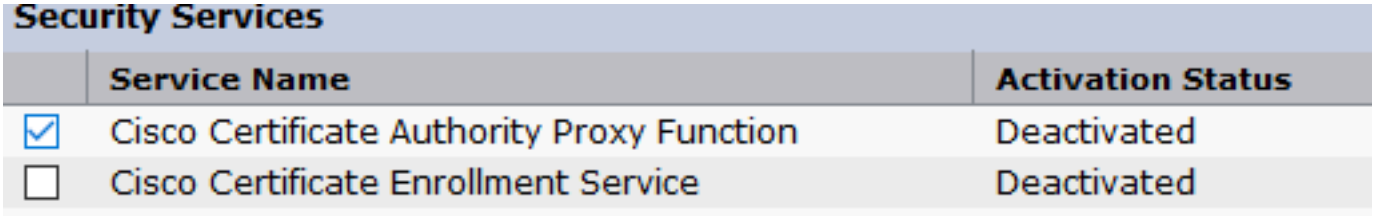
步驟：

1. 登入到 Cisco Unified Serviceability Interface.
2. 導航至 Tools > Service Activation.

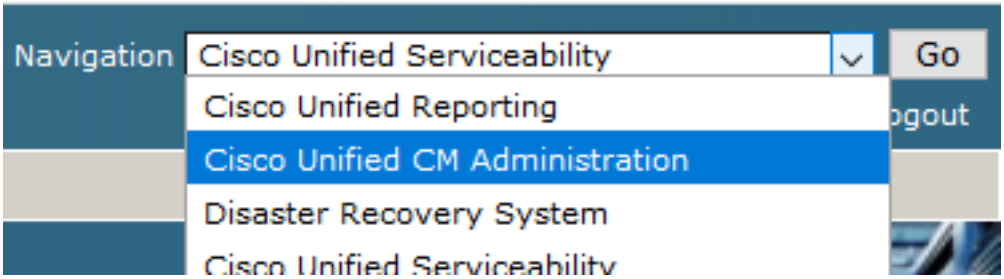
3. 選擇CUCM伺服器並按一下 Go .



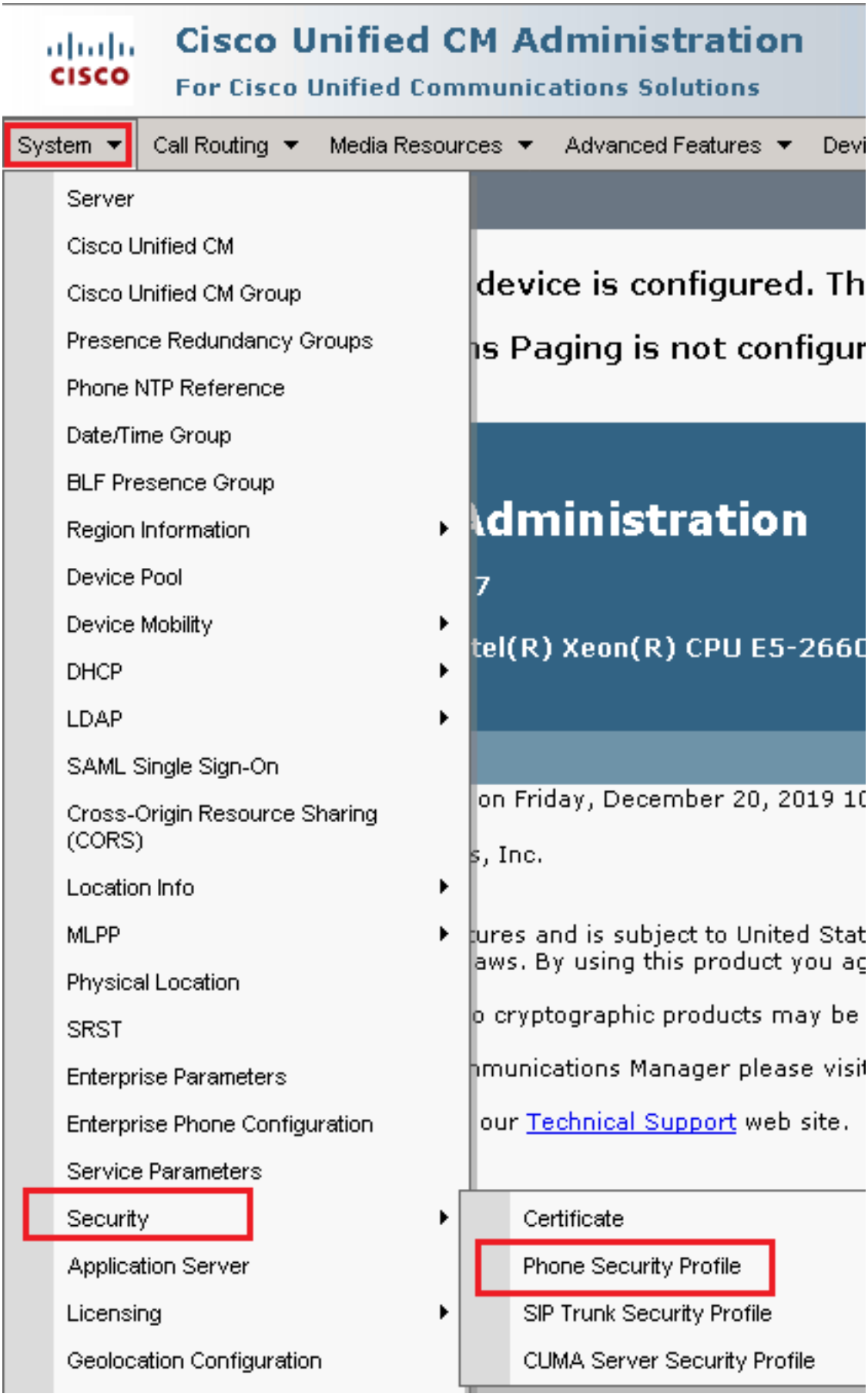
4. 支票 Cisco Certificate Authority Proxy Function 然後按一下 Save 啟用服務。按一下 Ok 確認。



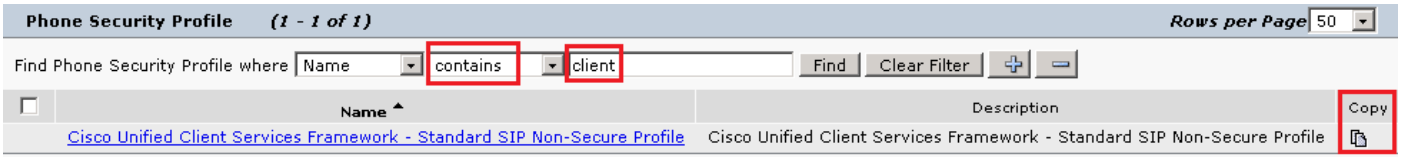
5. 確保服務已啟用，然後導航至 Cisco Unified CM Administration.



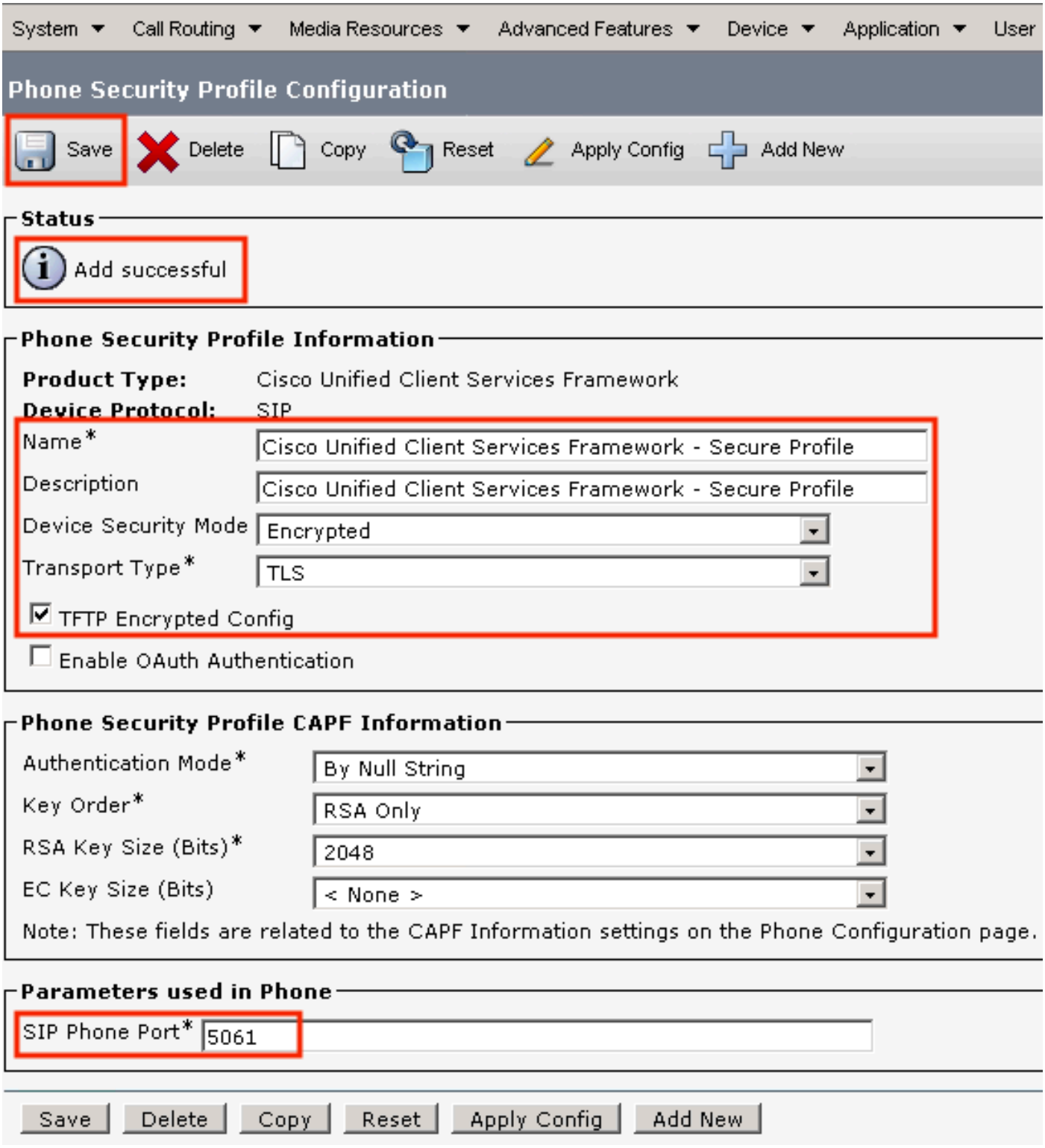
6. 成功登入到CUCM管理後，導航至 System > Security > Phone Security Profile 為代理裝置建立裝置安全配置檔案。



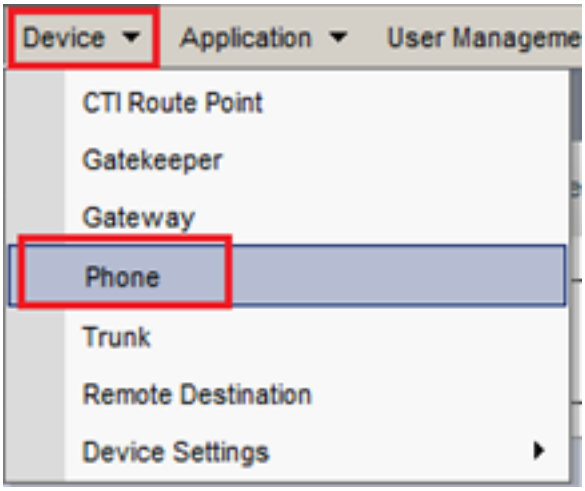
7. 查詢與您的代理裝置型別對應的安全配置檔案。在此示例中，使用的是軟體電話，因此選擇 Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile。按一下 Copy 以便複製此配置檔案。



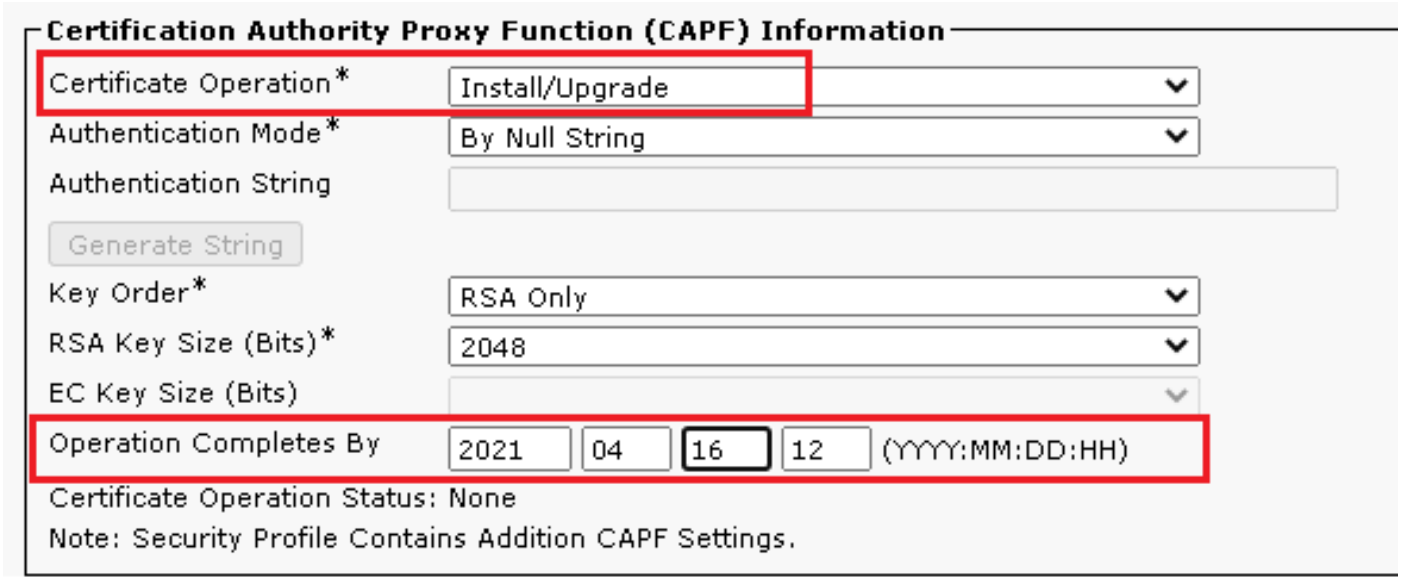
8. 將配置檔案重新命名為 Cisco Unified Client Services Framework - Secure Profile，更改此圖中所示的引數，然後按一下 Save 在頁面的左上角。



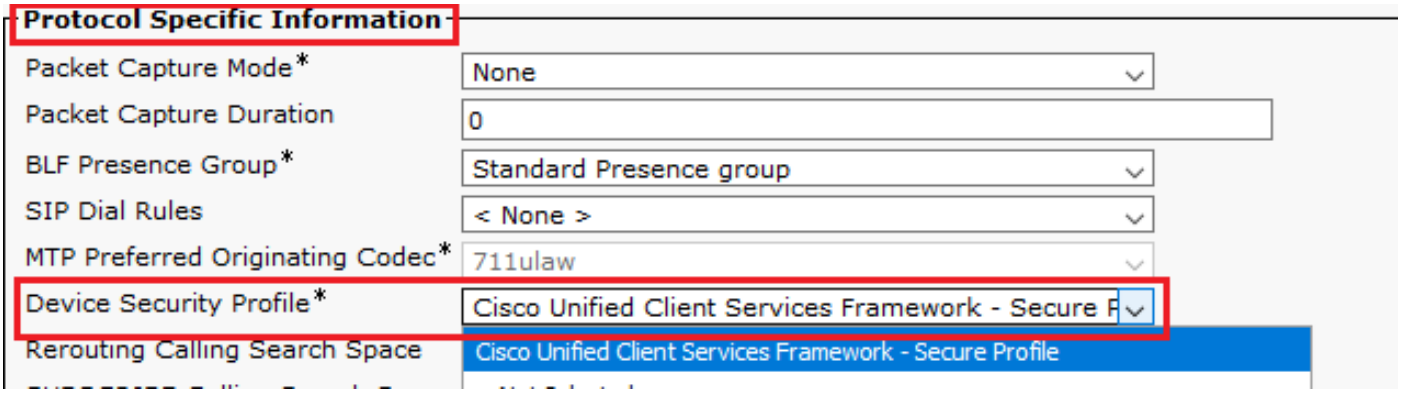
9. 成功建立電話裝置配置檔案後，導航至 Device > Phone.



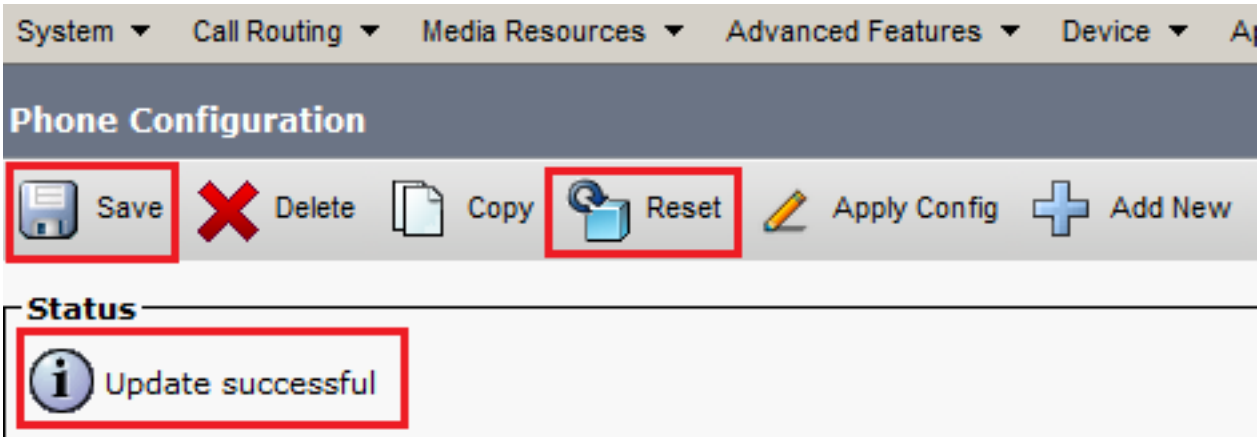
10. 按一下 Find 要列出所有可用電話，請按一下座席電話。
11. 座席電話配置頁面開啟。尋找 Certification Authority Proxy Function (CAPF) Information 部分。要安裝 LSC，請設定 Certificate Operation 成長至 Install/Upgrade 和 Operation Completes by 到任何未來的日子。



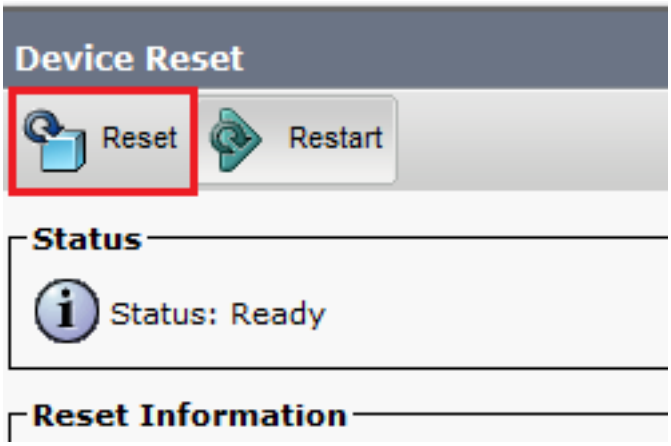
12. 尋找 Protocol Specific Information 部分。變更 Device Security Profile 成長至 Cisco Unified Client Services Framework – Secure Profile.



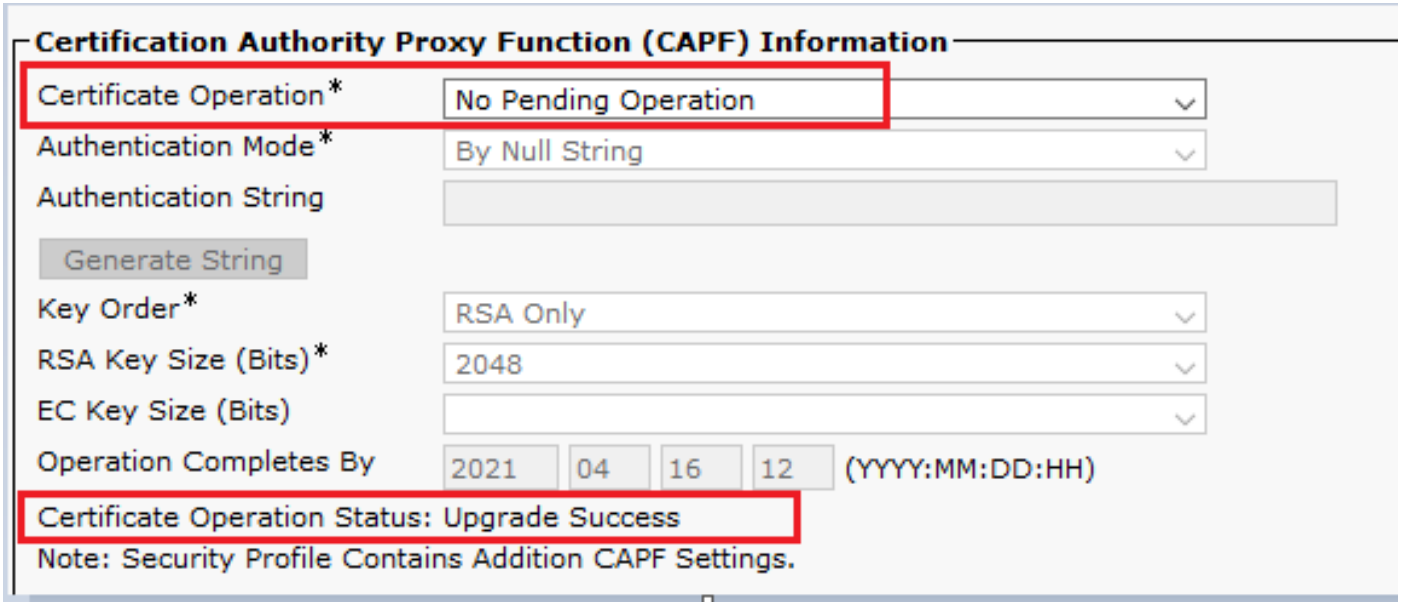
13. 按一下 Save 在頁面的左上角。確保更改已成功儲存，然後按一下 Reset.



14. 此時將開啟一個彈出視窗，按一下 Reset 確認操作。



15. 代理裝置再次向CUCM註冊後，請刷新當前頁面並驗證LSC是否安裝成功。支票 Certification Authority Proxy Function (CAPF) Information 部分， Certificate Operation 必須設定為 No Pending Operation,和 Certificate Operation Status 設定為 Upgrade Success．

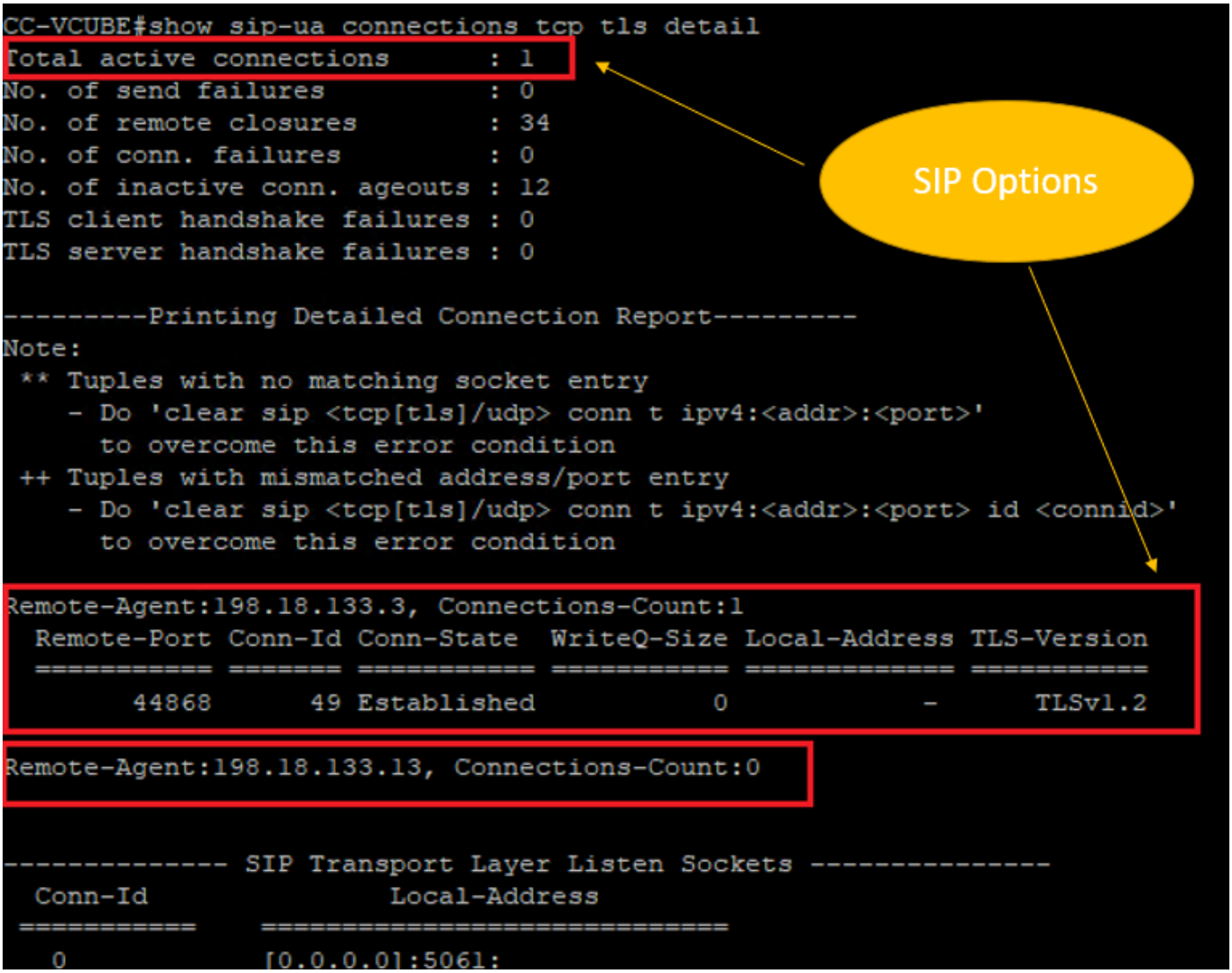


16. 請參閱步驟。7-13，以保護要用於通過CUCM保護SIP的其他代理裝置。

驗證

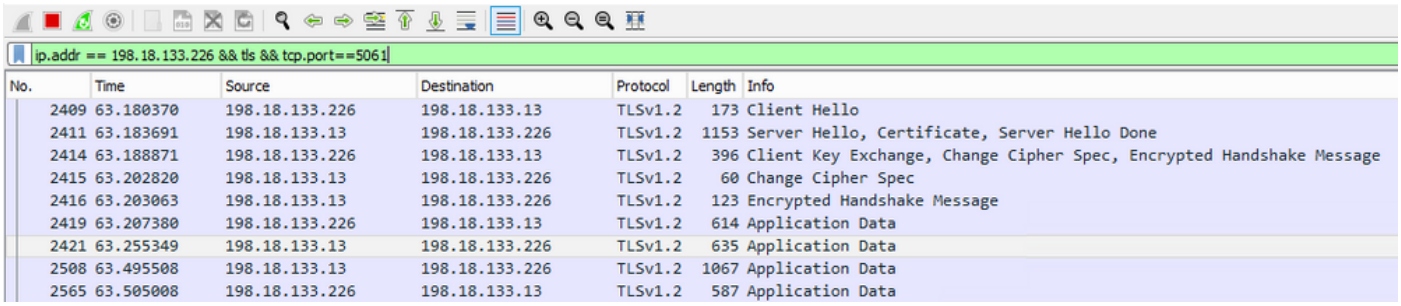
要驗證SIP信令是否正確安全，請執行以下步驟：

1. 開啟與vCUBE的SSH會話，運行命令 show sip-ua connections tcp tls detail ，並確認當前未與CVP(198.18.133.13)建立TLS連線。



注意：此時，在CUCM(198.18.133.3)上僅啟用一個具有CUCM的SIP選項的活動TLS會話。如果未啟用SIP選項，則不存在SIP TLS連線。

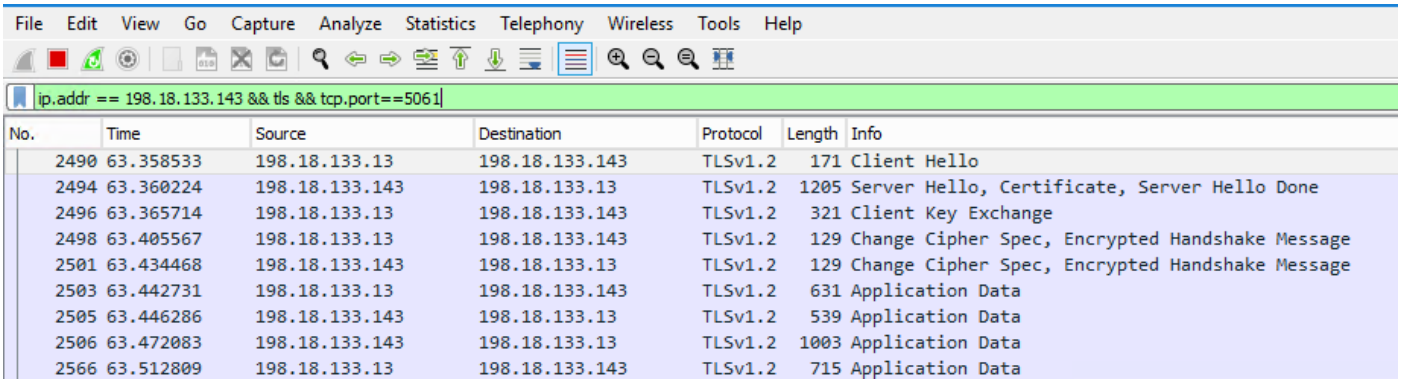
2. 登入到CVP並啟動Wireshark。
3. 向聯絡中心號碼發出測試呼叫。
4. 導航到CVP會話；在Wireshark上，運行此過濾器以使用CUBE檢查SIP信令：
   ip.addr == 198.18.133.226 && tls && tcp.port==5061



檢查：是否已建立SIP over TLS連線？如果是，則輸出確認CVP和CUBE之間的SIP訊號是安全的。

5.檢查CVP和CVVB之間的SIP TLS連線。在同一Wireshark會話中，運行此過濾器：

ip.addr == 198.18.133.143 && tls && tcp.port==5061



檢查：是否已建立SIP over TLS連線？如果是，則輸出確認CVP和CVVB之間的SIP訊號是安全的。

6.您還可以通過CUBE驗證與CVP的SIP TLS連線。導航到vCUBE SSH會話，然後運行此命令以檢查安全sip訊號：

show sip-ua connections tcp tls detail

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= ========== ========== ============= ===========
        38896       2 Established          0             -      TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= ========== ========== ============= ===========
         5061       3 Established          0             -      TLSv1.2


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id                Local-Address
 ===========    ================================
   0             [0.0.0.0]:5061:
```

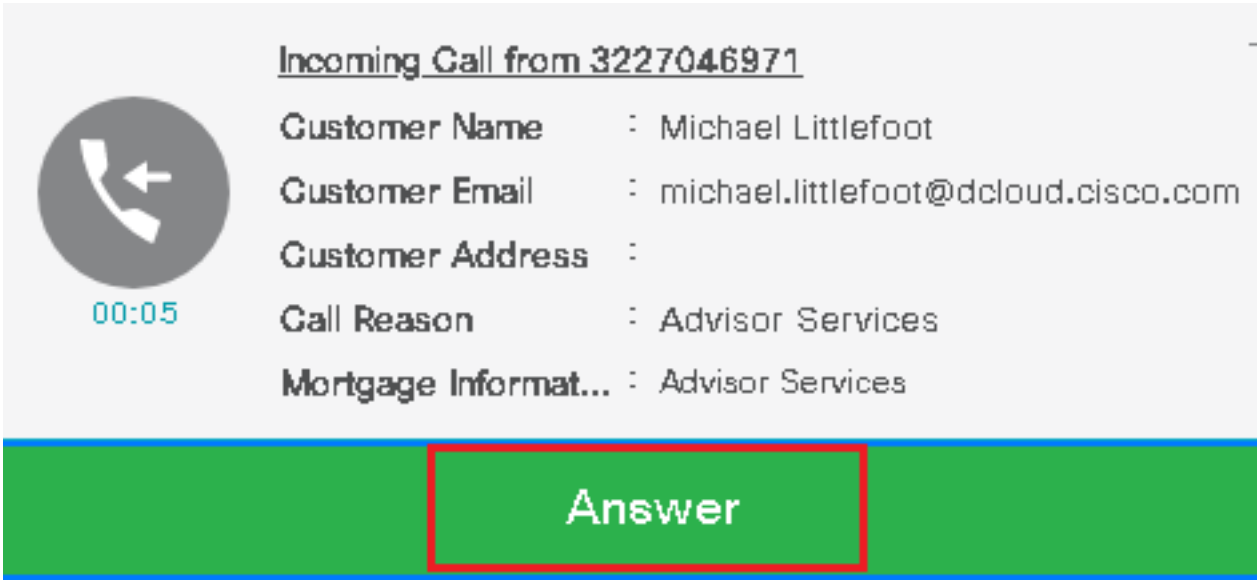
檢查:SIP over TLS是否與CVP建立連線？如果是，則輸出確認CVP和CUBE之間的SIP訊號是安全的。

7.此時，呼叫處於活動狀態，並且您聽到「通話等待音樂」(MOH)，因為沒有可以應答呼叫的座席。

8.使座席可以應答呼叫。

.

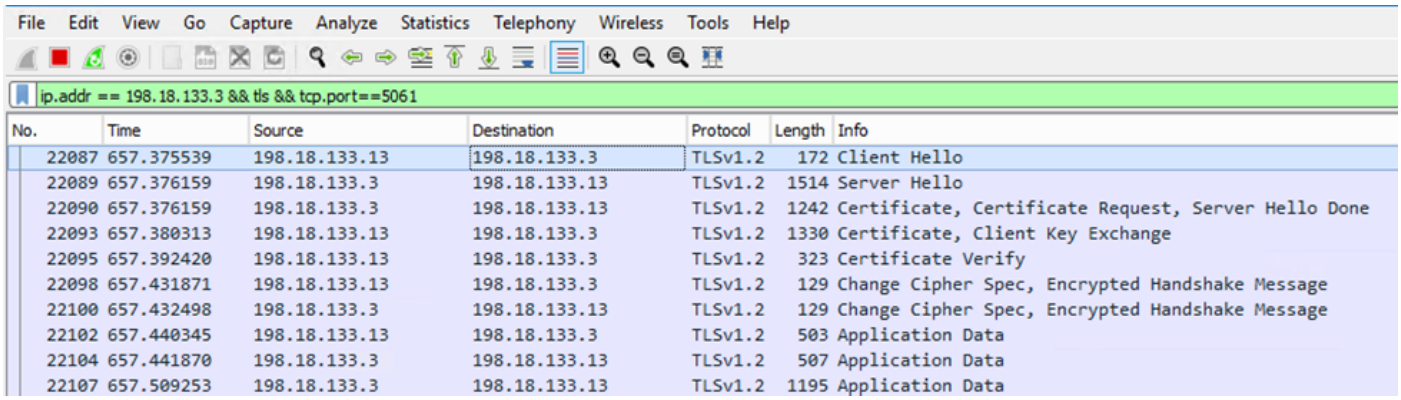
9.座席將被保留，並且呼叫將被轉接給他/她。按一下 Answer 來接電話。



10.呼叫連線到座席。

11.為了驗證CVP和CUCM之間的SIP訊號，請導航到CVP會話，然後在Wireshark中運行此過濾器：

ip.addr == 198.18.133.3 && tls && tcp.port==5061



> **檢查**：是否所有與CUCM(198.18.133.3)的SIP通訊均通過TLS?如果是，則輸出確認CVP和CUCM之間的SIP訊號是安全的。

疑難排解

如果未建立TLS，請在CUBE上運行以下命令以啟用debug TLS進行故障排除：

- Debug ssl openssl errors
- Debug ssl openssl msg
- Debug ssl openssl states

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。