在Contact Center Enterprise中配置安全RTP

目錄

簡介

本文描述如何在Contact Center Enterprise(CCE)中保護即時傳輸協定(SRTP)流量的綜合呼叫流。

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。

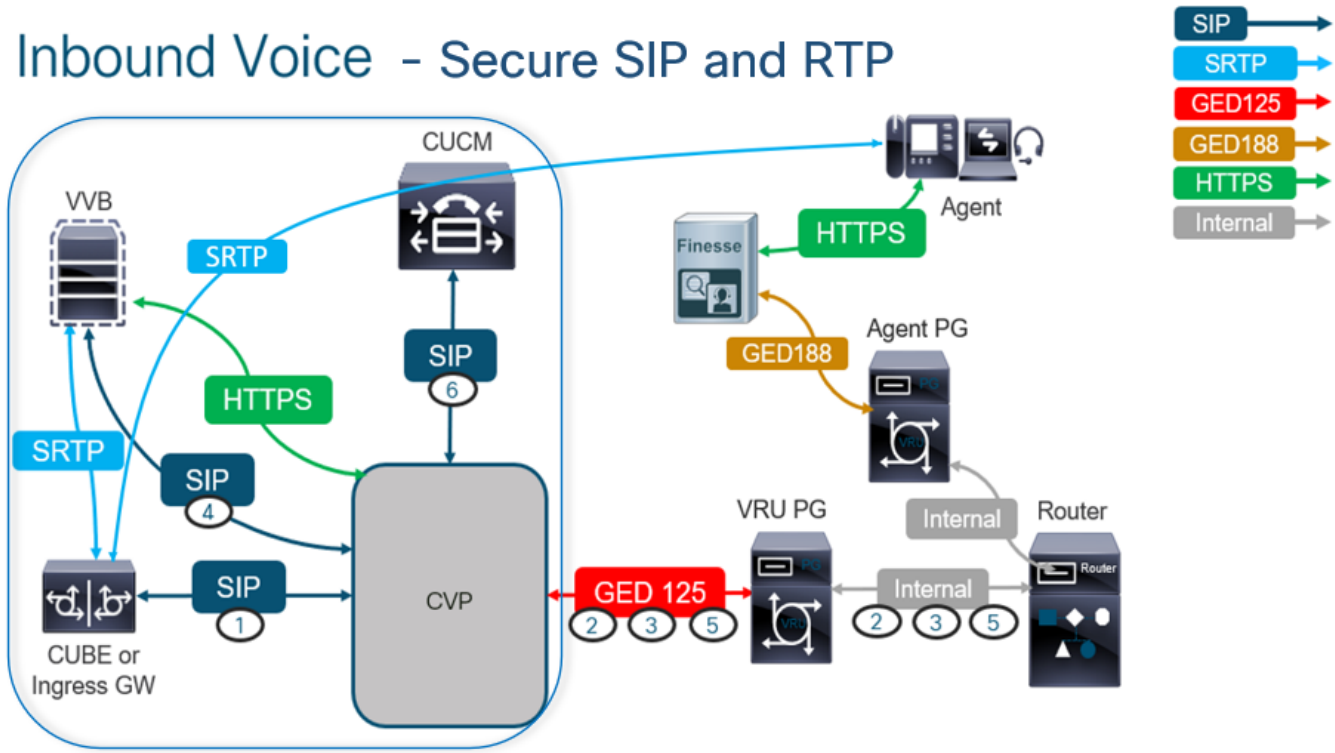
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

）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

> **注意**：在聯絡中心綜合呼叫流程中，為了啟用安全RTP，必須啟用安全SIP訊號。因此，本文檔中的配置同時啟用安全SIP和SRTP。

下圖顯示了在聯絡中心綜合呼叫流程中參與SIP訊號和RTP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上啟動配置。接下來，配置CVP、CVVB和CUCM。



任務1:CUBE安全配置

在本任務中，您將CUBE配置為保護SIP協定消息和RTP。

必需的配置：

- 為SIP UA配置預設信任點
- 修改撥號對等體以使用TLS和SRTP

步驟：

1. 開啟到CUBE的SSH會話。
2. 運行這些命令以使SIP堆疊使用CUBE的CA證書。CUBE建立從/到CUCM(198.18.133.3)和CVP(198.18.133.13)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 srtp exit

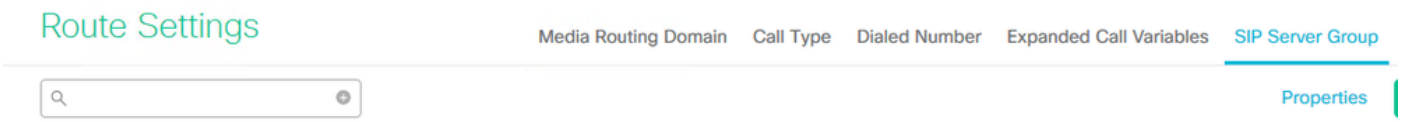
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#SRTP
CC-VCUBE(config-dial-peer)#exit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

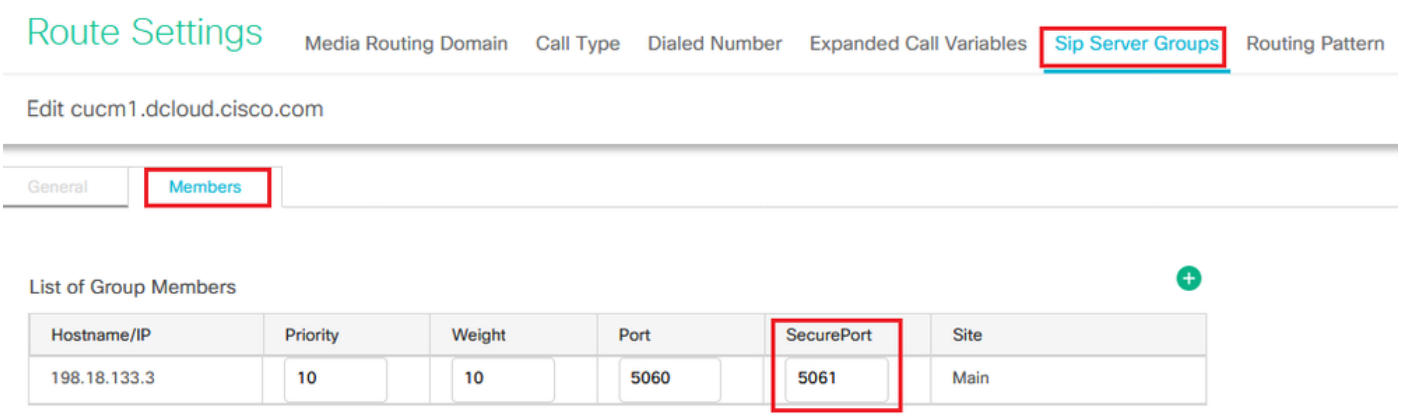
1. 登入 UCCE Web Administration.
2. 導航至 Call Settings > Route Settings > SIP Server Group.



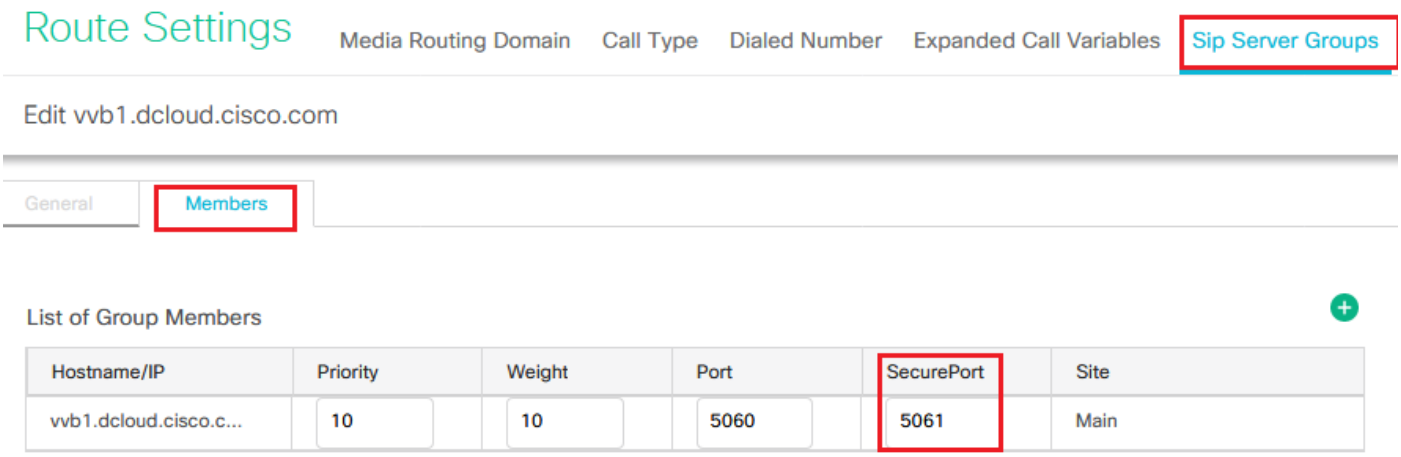
根據您的配置，您已為CUCM、CVVB和CUBE配置了SIP伺服器組。您需要將所有安全SIP埠設定為5061。 在此示例中，使用以下SIP伺服器組：

- 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 顯示SIP伺服器組配置詳細資訊的頁籤。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，設定 **SecurePort** 成長至 5061 然後按一下 Save.

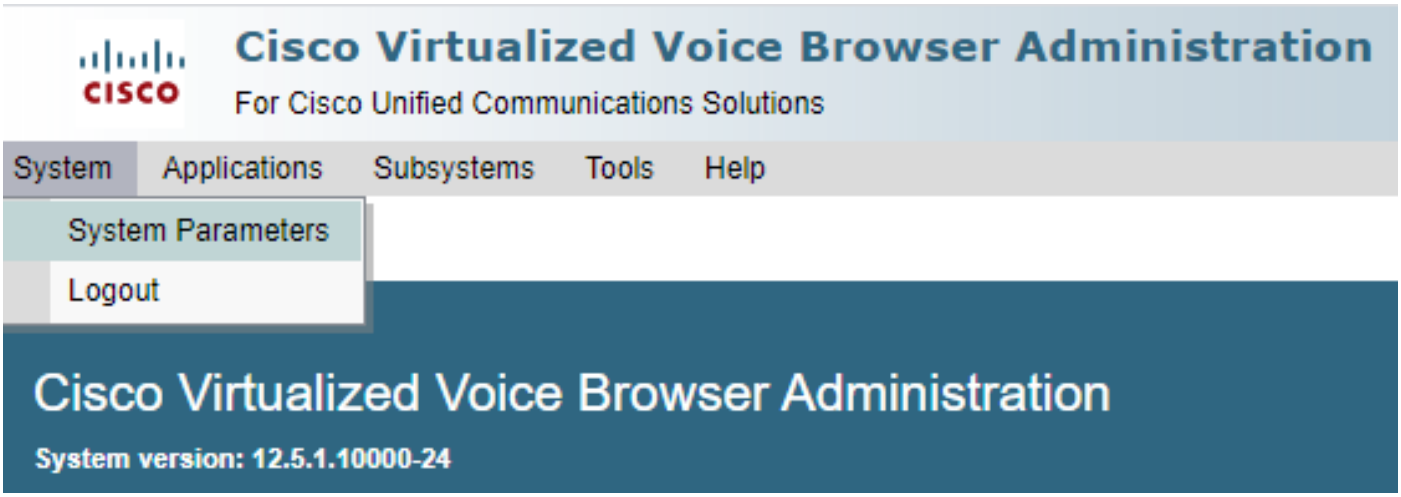


任務3:CVVB安全配置

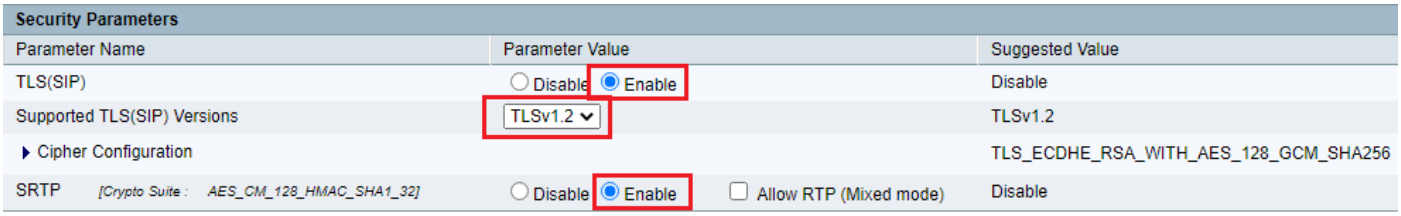
在此任務中，配置CVVB以保護SIP協定消息(SIP TLS)和SRTP。

步驟：

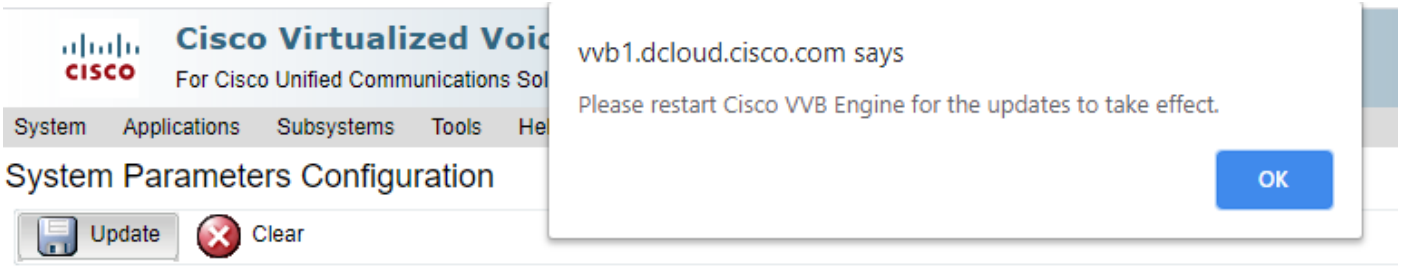
1. 開啟 Cisco VVB Admin 頁面。
2. 導航至 System > System Parameters.



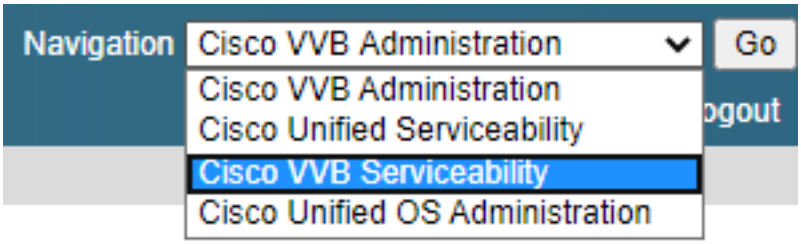
3. 在 Security Parameters 部分，選擇 Enable 對於 TLS (SIP) .保留 Supported TLS(SIP) version as TLSv1.2 選擇 Enable 對於 SRTP.



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

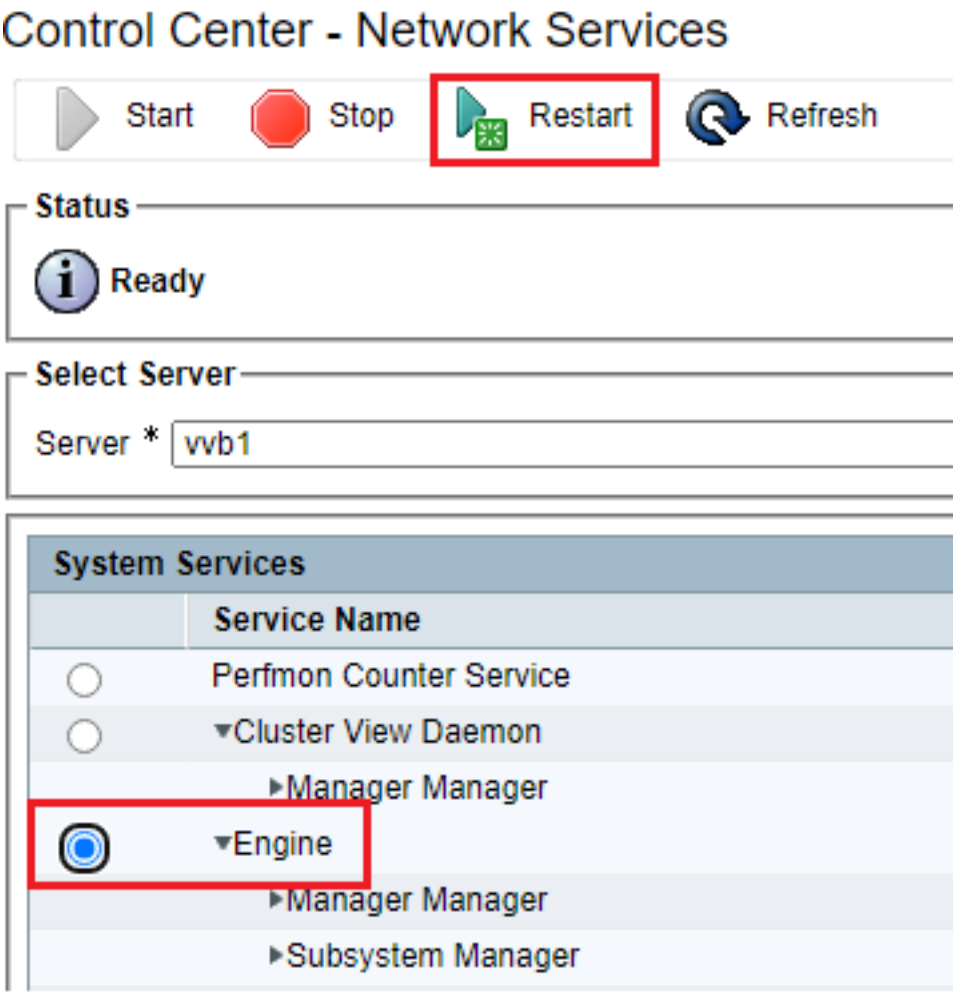


5. 這些更改需要重新啟動Cisco VVB引擎。要重新啟動VVB引擎，請導航至 Cisco VVB Serviceability ，然後按一下 **Go**.



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消息和RTP，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中繼並啟用SRTP
- 安全代理與CUCM的裝置通訊

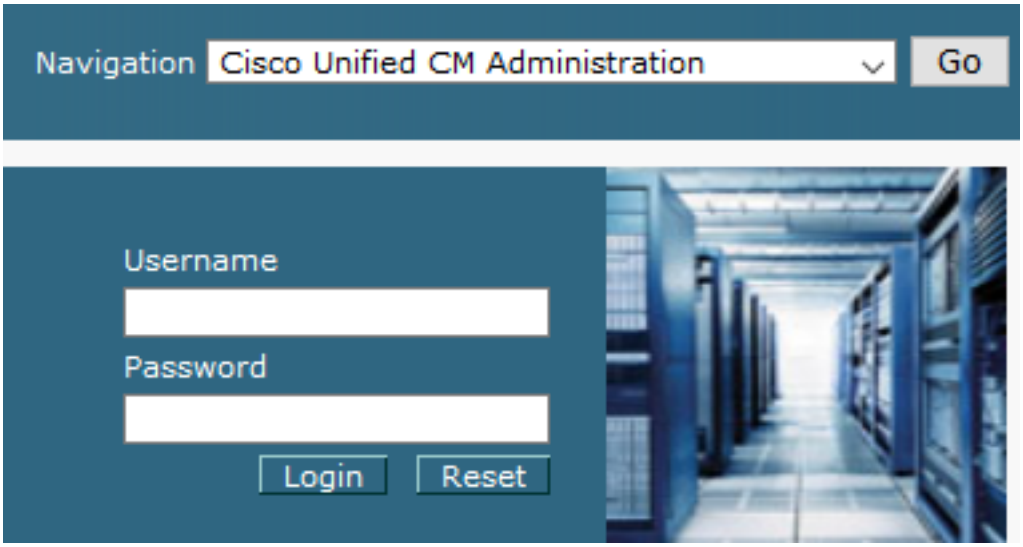
將CUCM安全模式設定為混合模式

CUCM支援兩種安全模式：

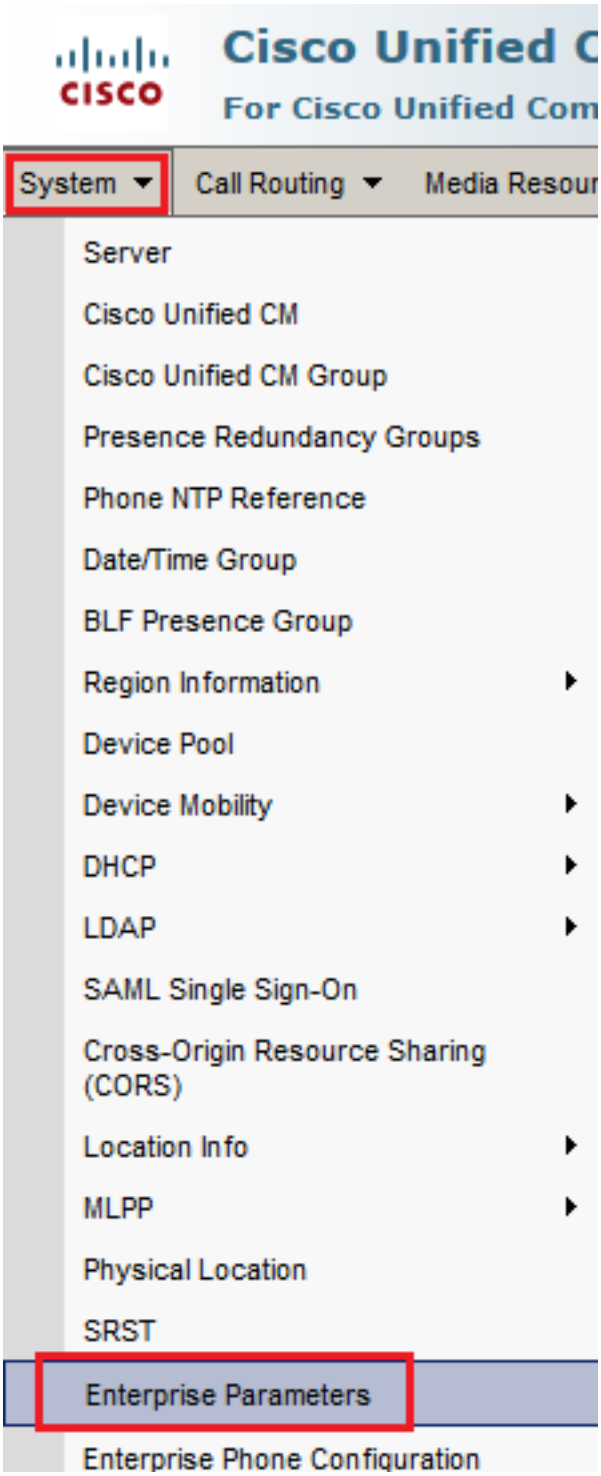
- 非安全模式（預設模式）
- 混合模式（安全模式）

步驟：

1. 登入到CUCM管理介面。



2. 登入到CUCM時，您可以導航到 System > Enterprise Parameters.

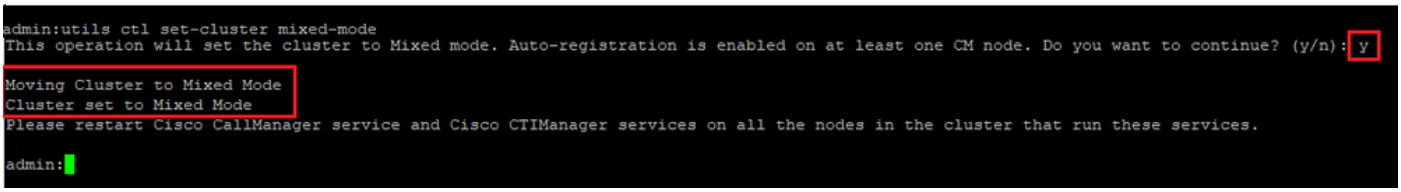


3. 在 Security Parameters 部分，檢查是否 Cluster Security Mode 設定為 0.

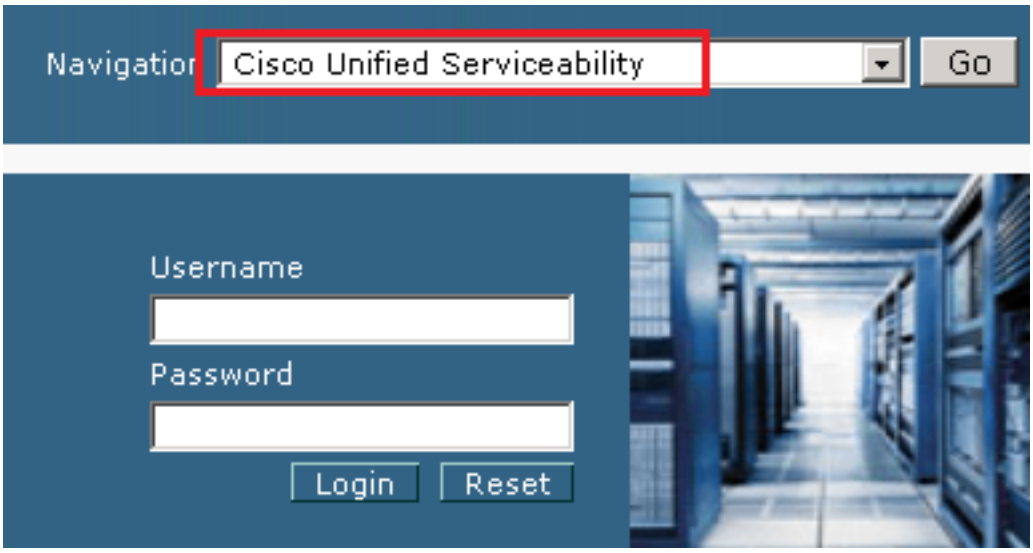
4. 如果「群集安全模式」設定為0，則表示群集安全模式設定為非安全。您需要從CLI啟用混合模式。
5. 開啟與CUCM的SSH會話。
6. 通過SSH成功登入到CUCM後，請運行以下命令：

utils ctl set-cluster mixed-mode

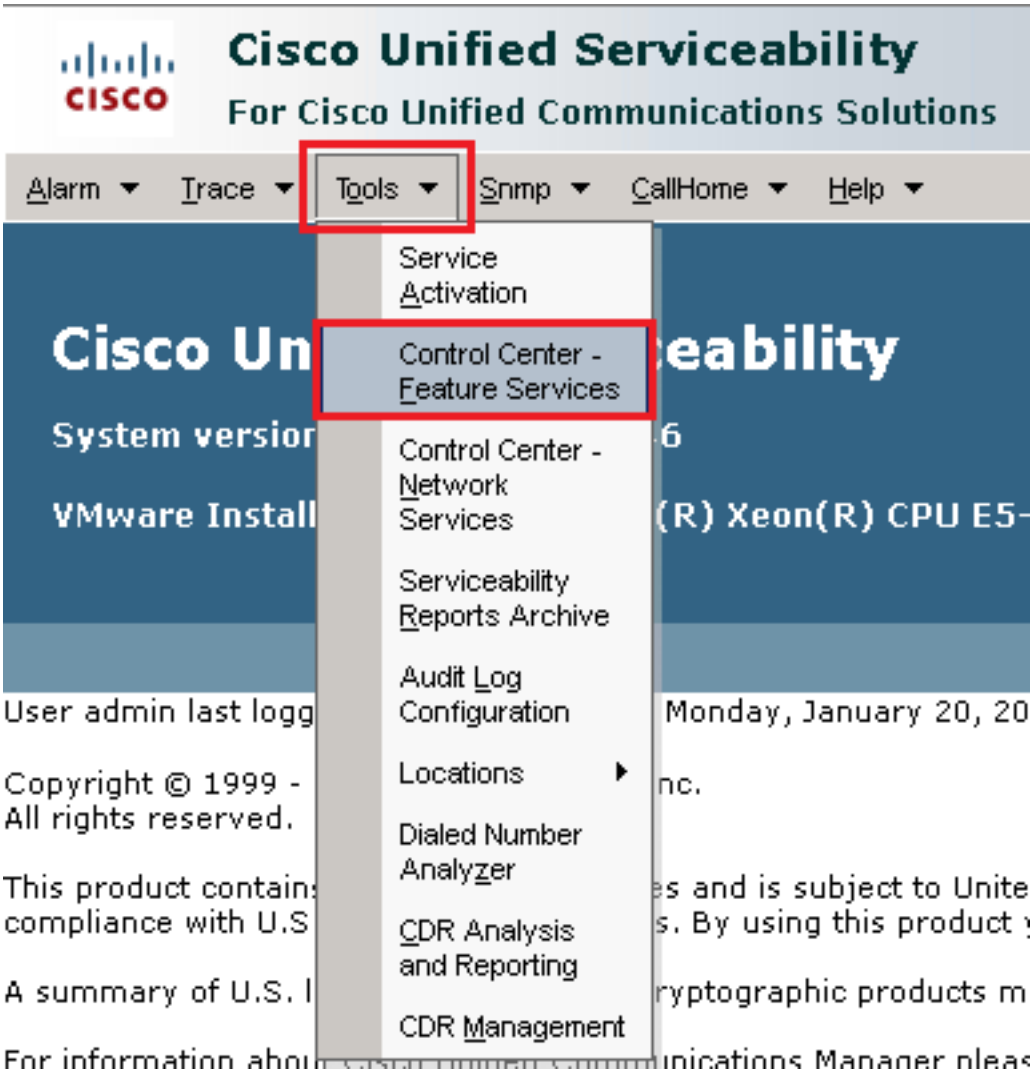
7. 類型 y 然後按一下 Enter 當系統提示時。此命令將群集安全模式設定為混合模式。



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**.

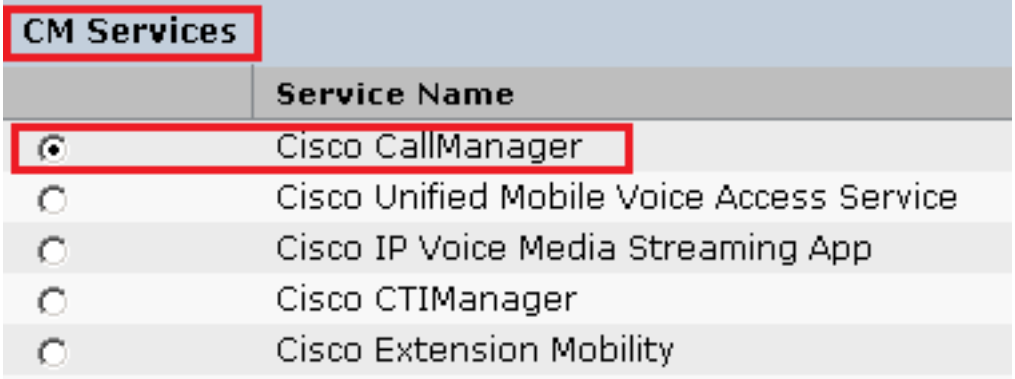


10. 成功登入後，導航至 Tools > Control Center – Feature Services.

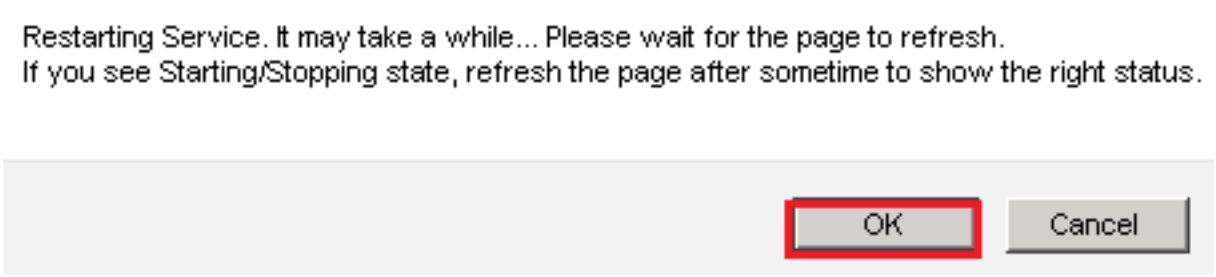


11. 選擇伺服器，然後按一下 Go.

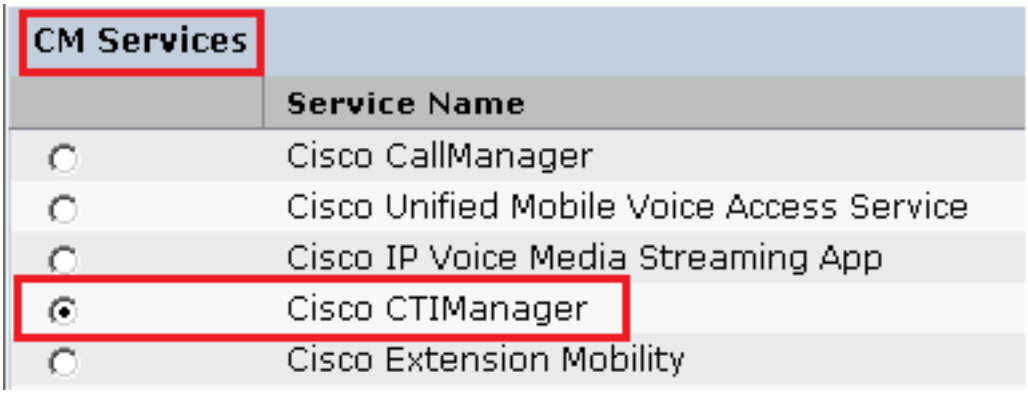
12. 在CM服務下，選擇 Cisco CallManager ，然後按一下 Restart 按鈕。



13. 確認彈出消息，然後按一下 OK.等待服務成功重新啟動。



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



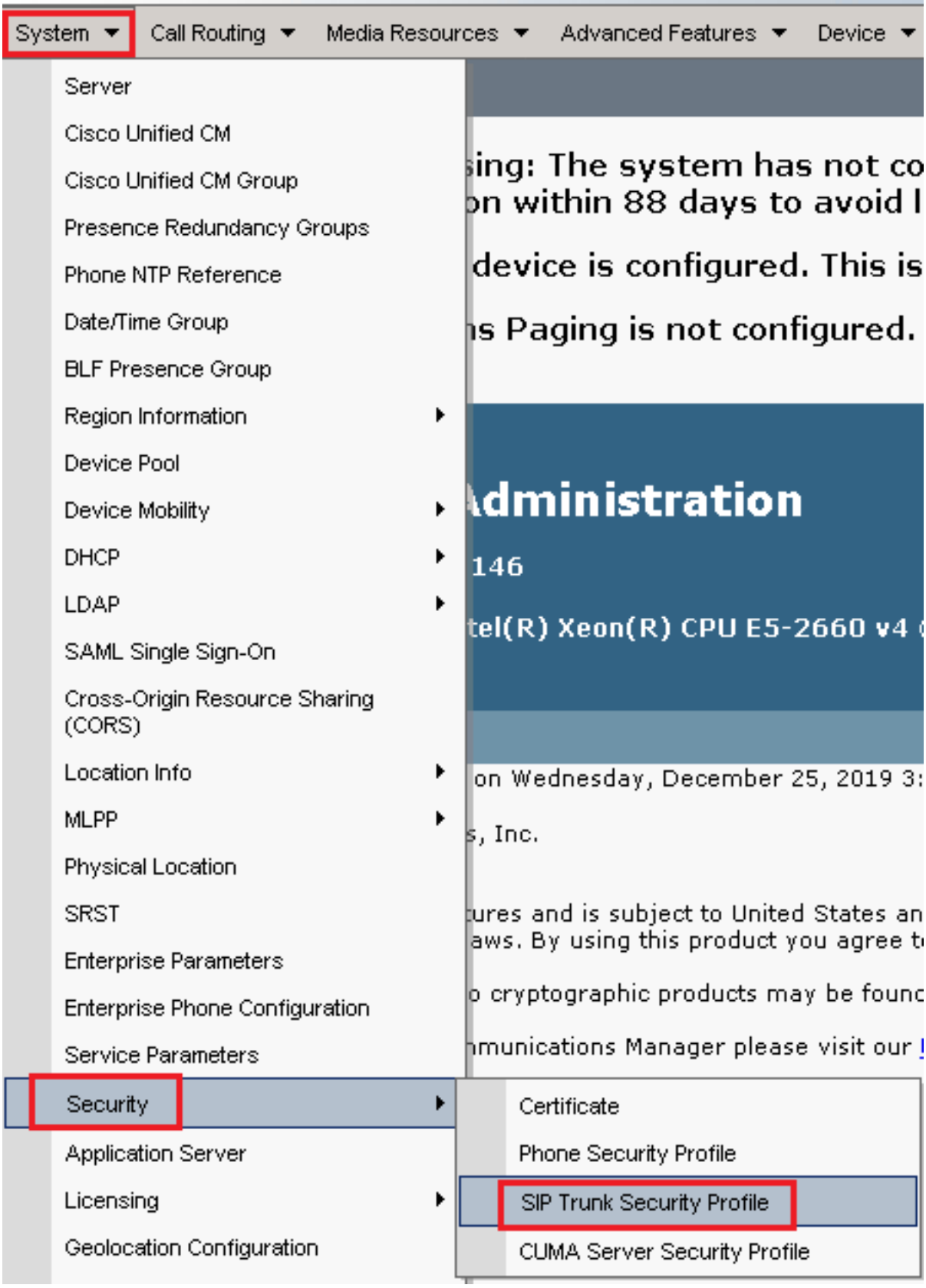
15. 確認彈出消息，然後按一下 OK.等待服務成功重新啟動。

16. 成功重新啟動服務後，若要驗證群集安全模式是否設定為混合模式，請按照步驟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

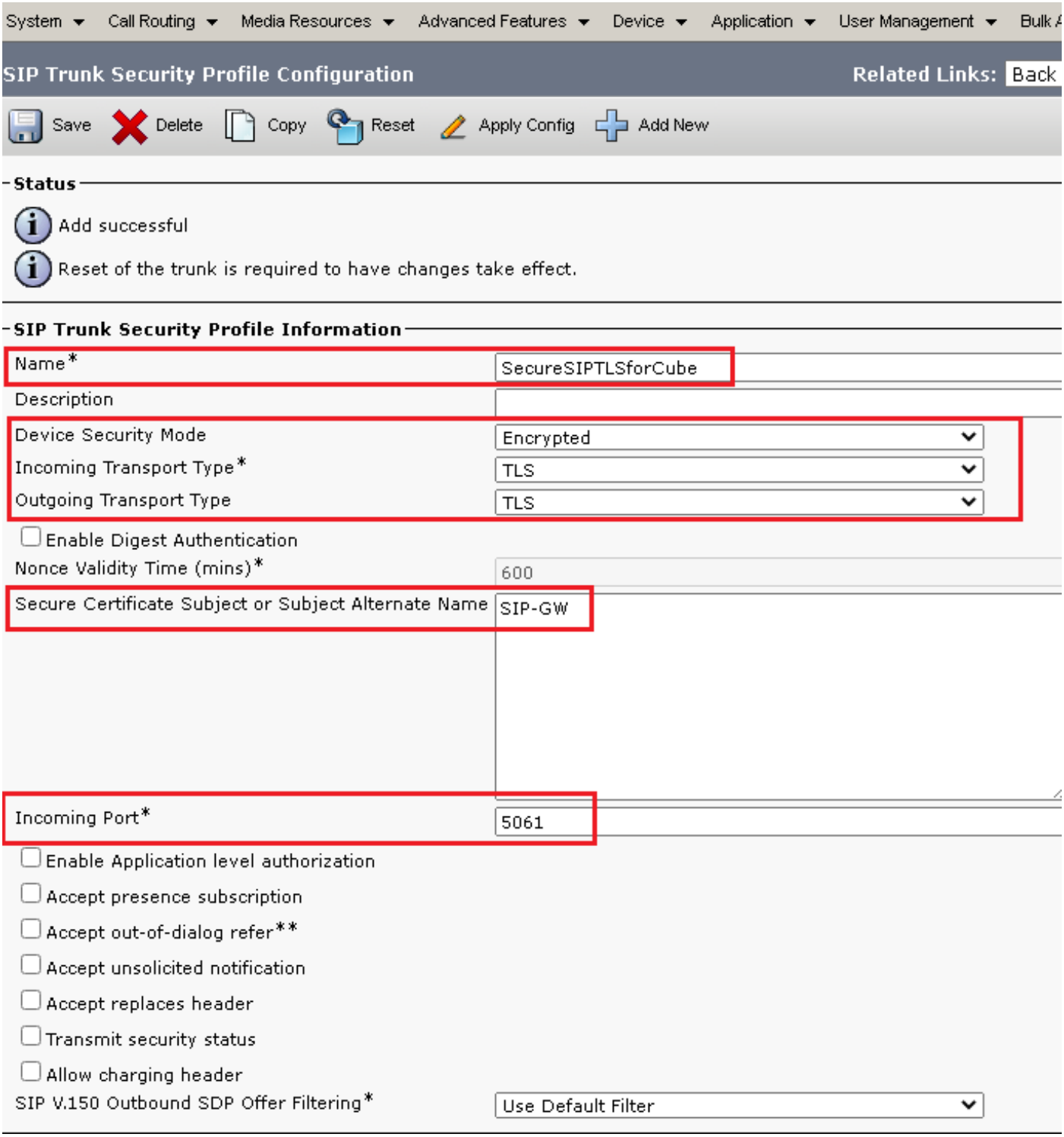
步驟：

1. 登入到CUCM管理介面。
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**新增新配置檔案。

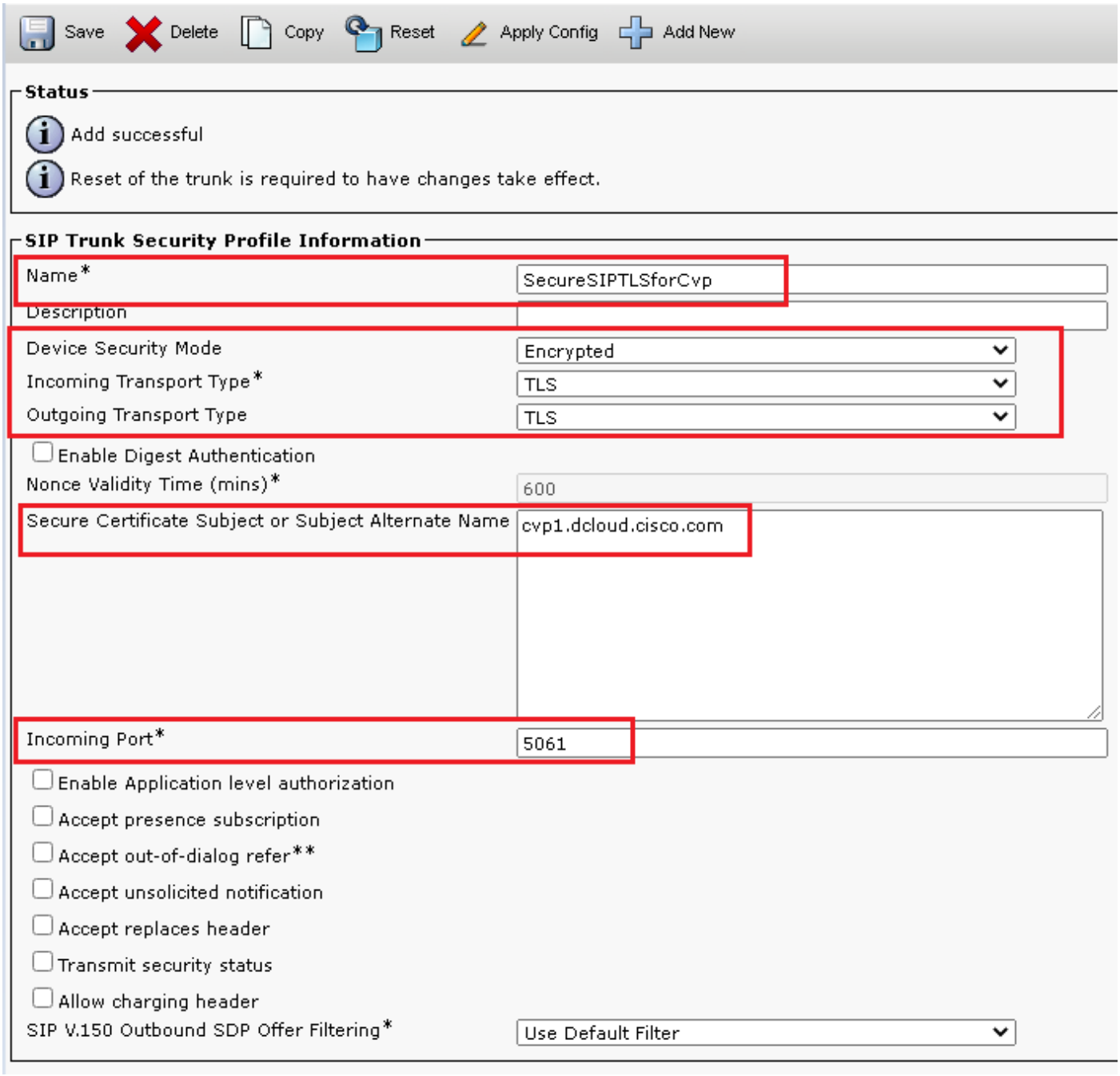
4. 設定 SIP Trunk Security Profile 作為此影象，然後按一下 Save 在頁面左下角。



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。

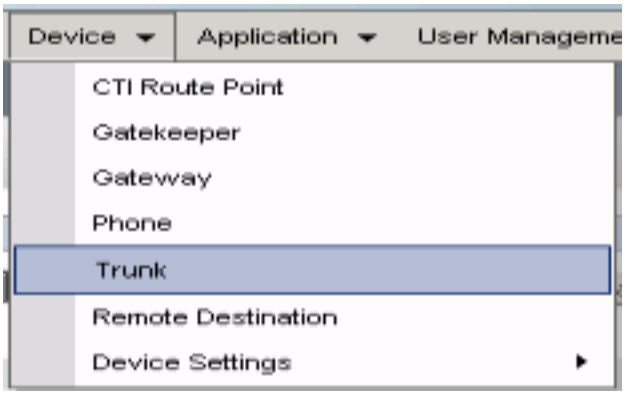
6.按一下 Copy 按鈕並更改 Name 成長至 SecureSipTLSforCVP.變更 Secure Certificate Subject CVP呼叫伺服器證書的CN，因為它必須匹配。按一下 **Save** 按鈕。



將SIP中繼安全配置檔案關聯到各自的SIP中繼並啟用SRTP

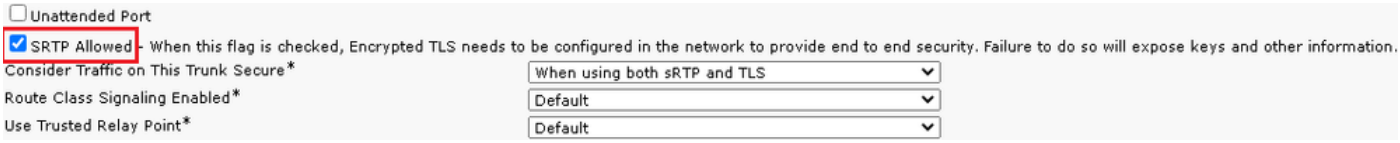
步驟：

1. 在CUCM管理頁面上，導航至 Device > Trunk.

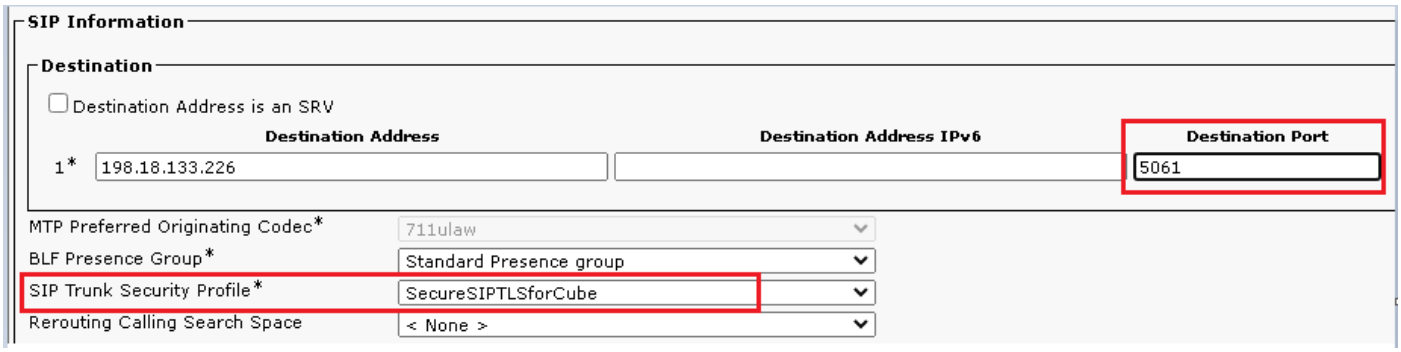


2. 搜尋CUBE中繼。在本示例中，CUBE中繼名稱是 vCube ，然後按一下 Find.

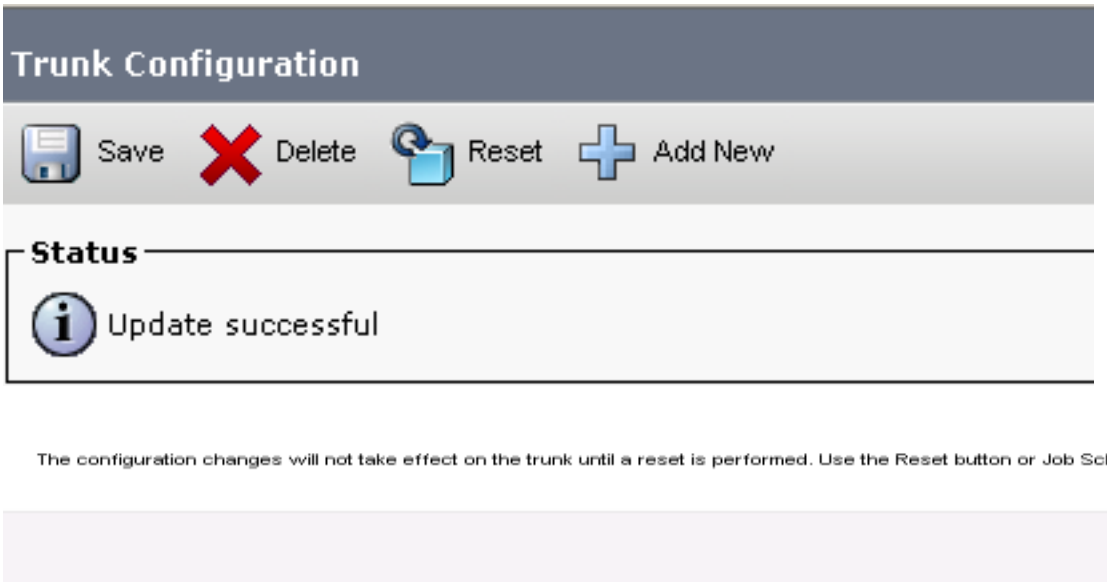
3. 按一下 vCUBE 開啟vCUBE中繼配置頁。
4. 在 Device Information 部分，請檢查 SRTP Allowed 覈取方塊，以便啟用SRTP。



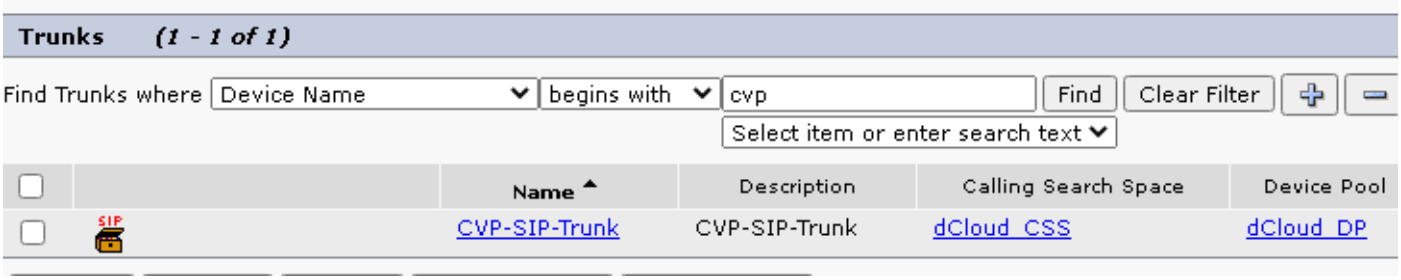
5. 向下滾動到 SIP Information 部分，並更改 Destination Port 成長至 5061.
6. 變更 SIP Trunk Security Profile 成長至 SecureSIPTLSForCube.



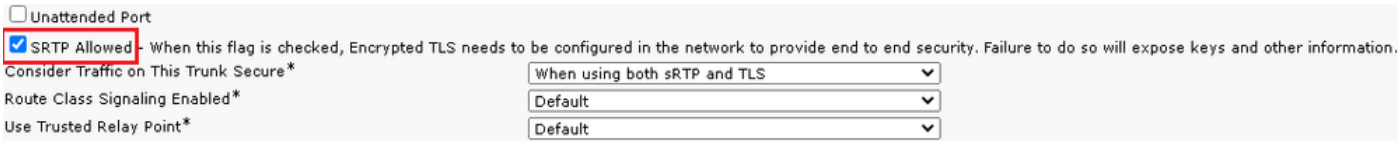
7. 按一下 Save 然後 Rest 成長至 save 並應用更改。



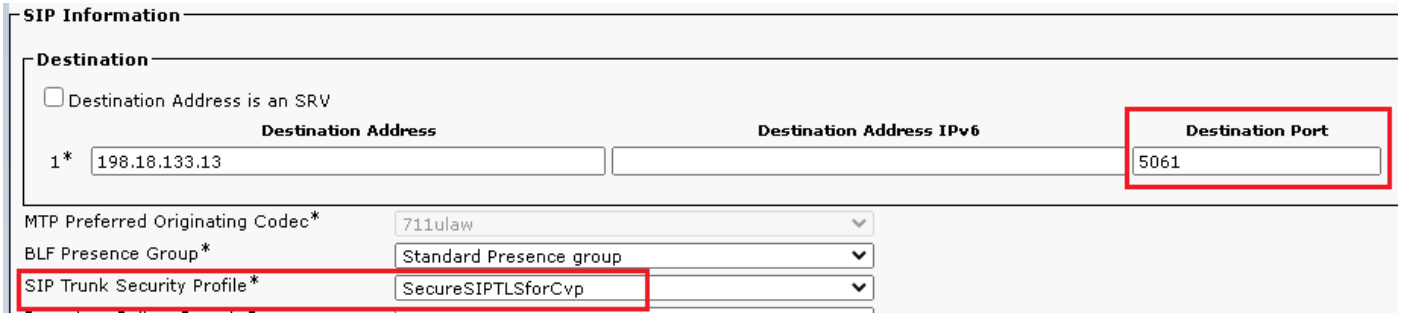
8. 導航至 Device > Trunk，搜尋CVP中繼，在此示例中，CVP中繼名稱為 cvp-SIP-Trunk.按一下 Find.



9. 按一下 CVP-SIP-Trunk 開啟CVP中繼配置頁面。
10. 在 Device Information 部分，檢查 SRTP Allowed 覈取方塊，以便啟用SRTP。



11. 向下滾動到 SIP Information 部分，更改 Destination Port 成長至 5061.
12. 變更 SIP Trunk Security Profile 成長至 SecureSIPTLSForCvp.



13. 按一下 Save 然後 Rest 成長至 save 並應用更改。

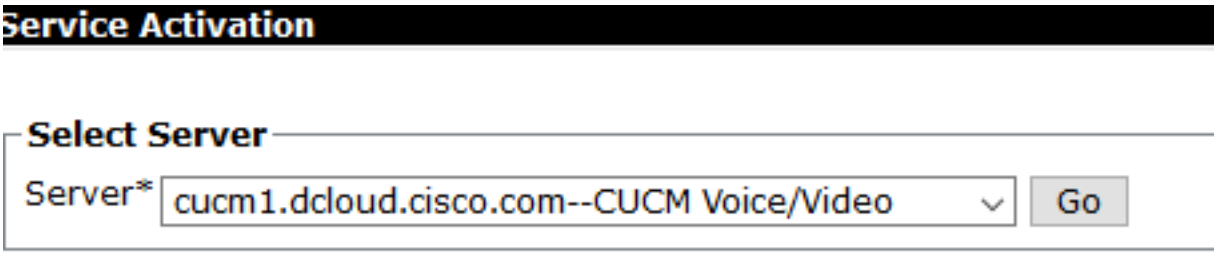
安全代理與CUCM的裝置通訊

要為裝置啟用安全功能，必須安裝本地重要證書(LSC)並將安全配置檔案分配給該裝置。LSC擁有終端的公鑰，該公鑰由CUCM CAPF私鑰簽名。預設情況下，它不會安裝在電話上。

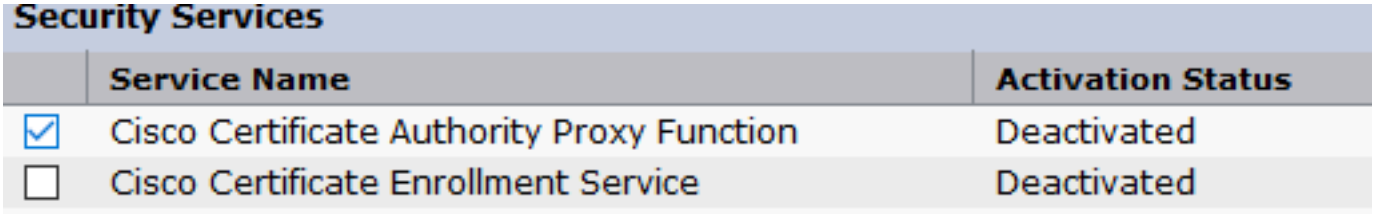
步驟：

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

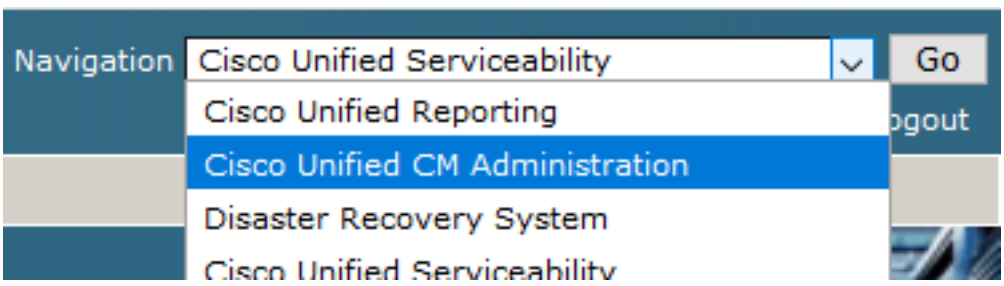
3. 選擇CUCM伺服器並按一下 Go.



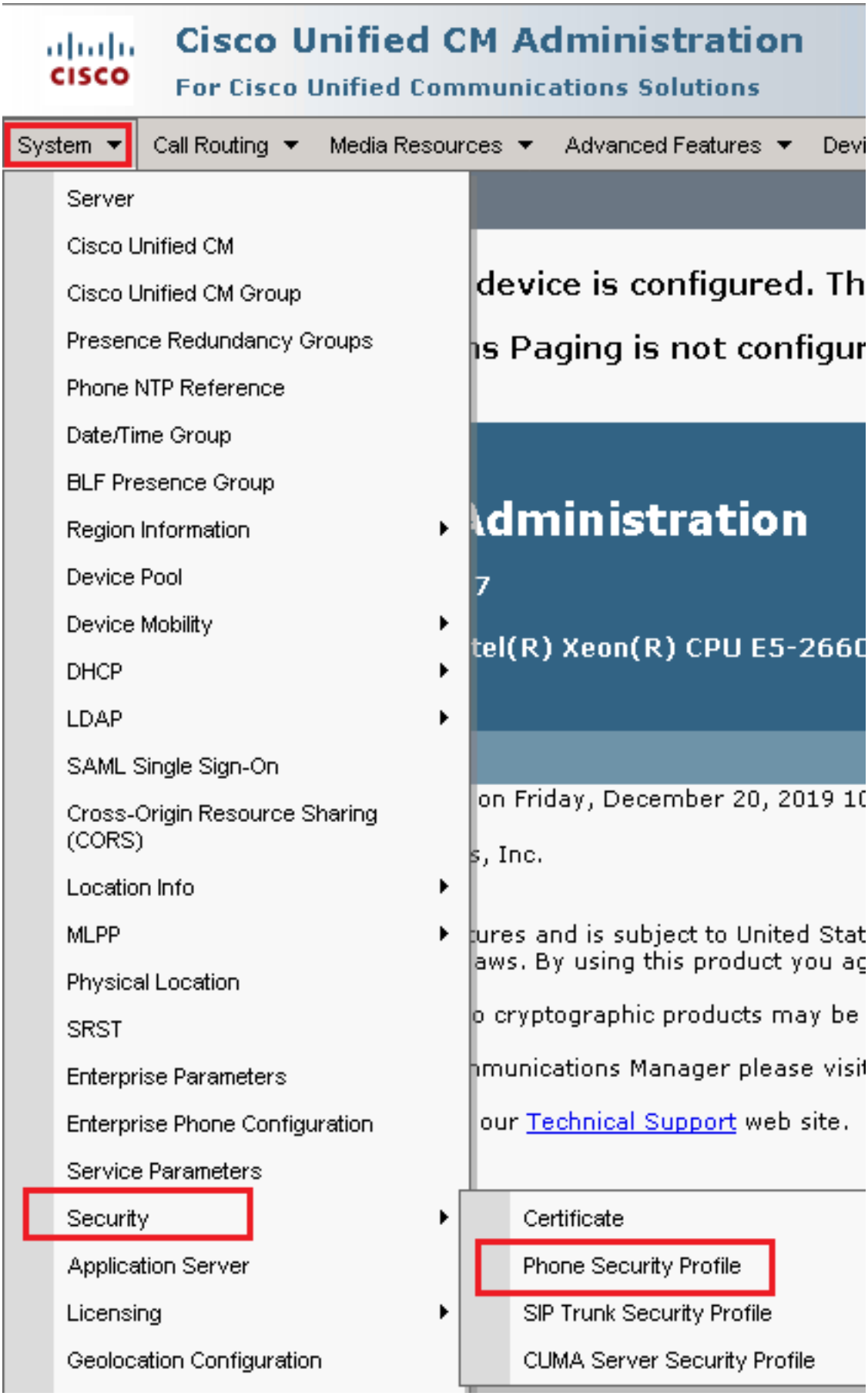
4. 支票 Cisco Certificate Authority Proxy Function 然後按一下 Save 啟用服務。按一下 Ok 確認。



5. 確保服務已啟用，然後導航至CUCM管理。



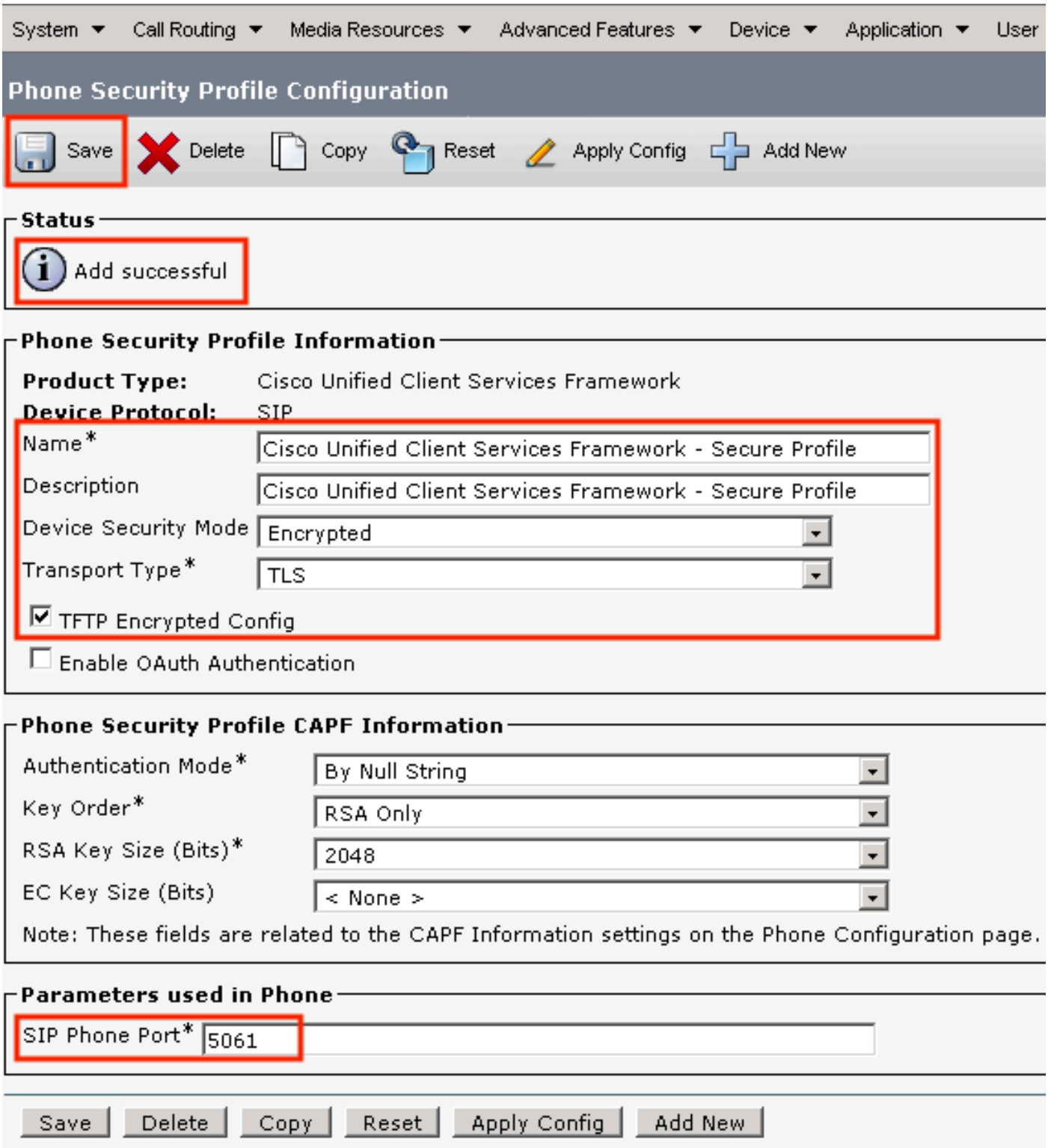
6. 成功登入到CUCM管理後，導航至 System > Security > Phone Security Profile 為代理裝置建立裝置安全配置檔案。



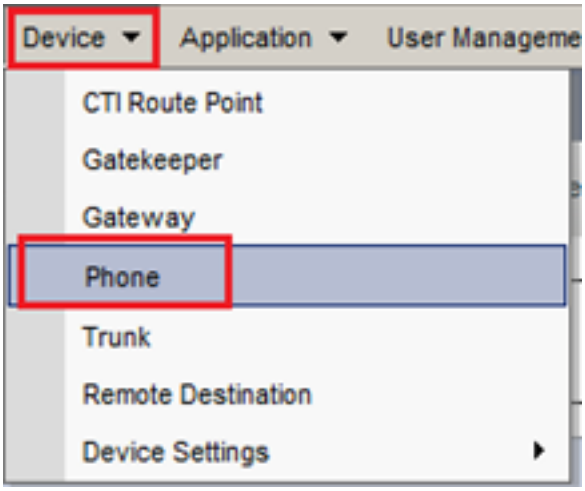
7. 查詢與您的代理裝置型別對應的安全配置檔案。在此示例中，使用的是軟體電話，因此選擇

Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile. 按一下「複製」圖示 以便複製此配置檔案。

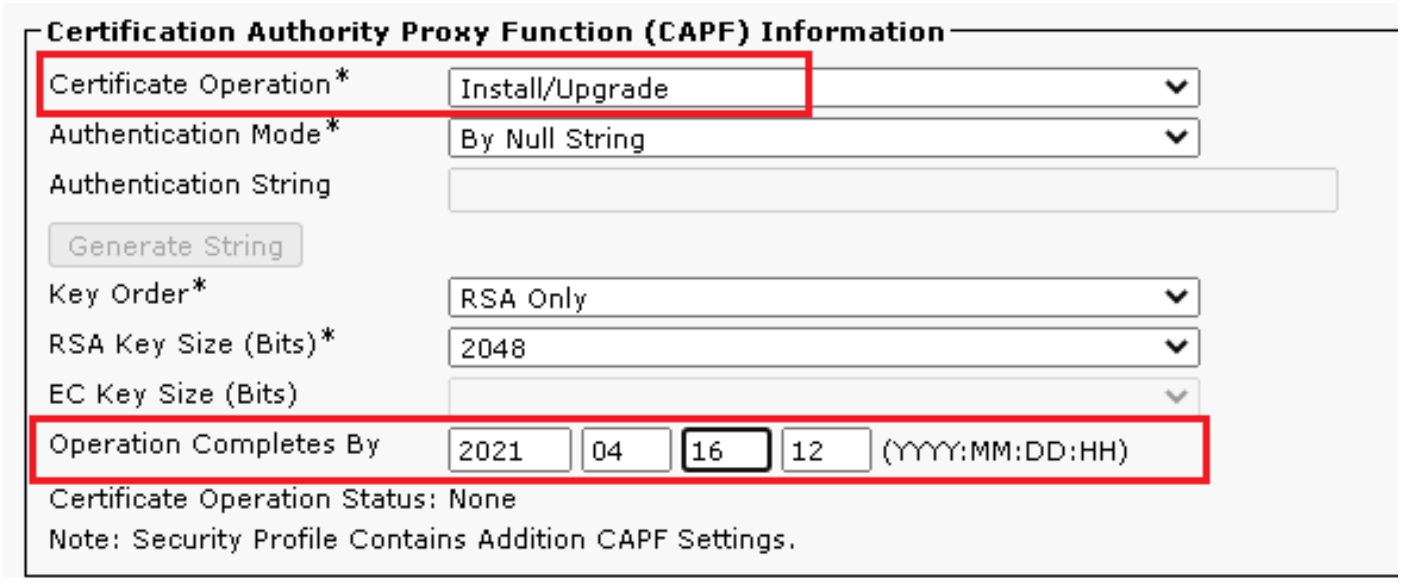
8. 將配置檔案重新命名為 Cisco Unified Client Services Framework - Secure Profile. 思更改此影象中的引數，然後按一下 Save 在頁面的左上角。



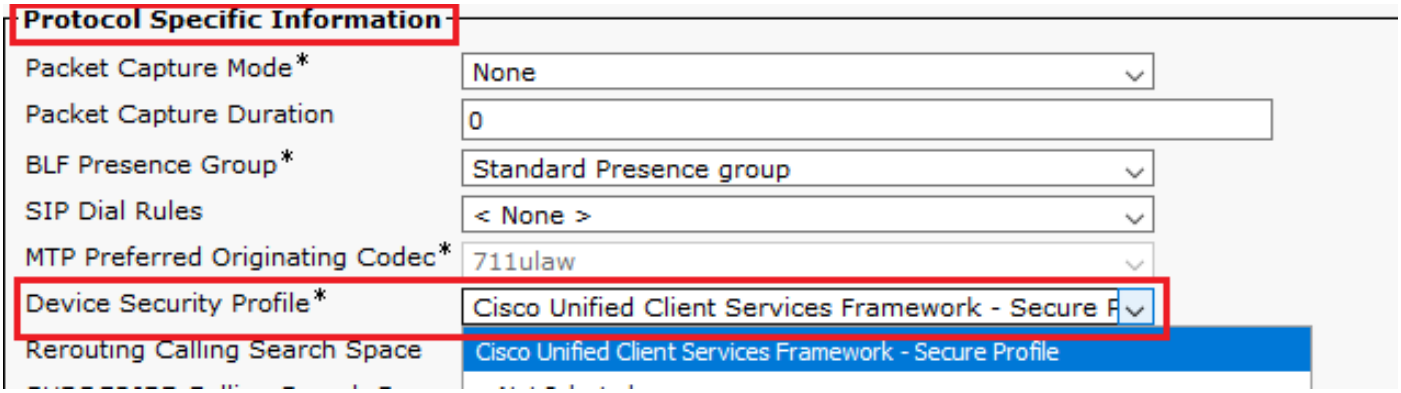
9. 成功建立電話裝置配置檔案後，導航至 Device > Phone.



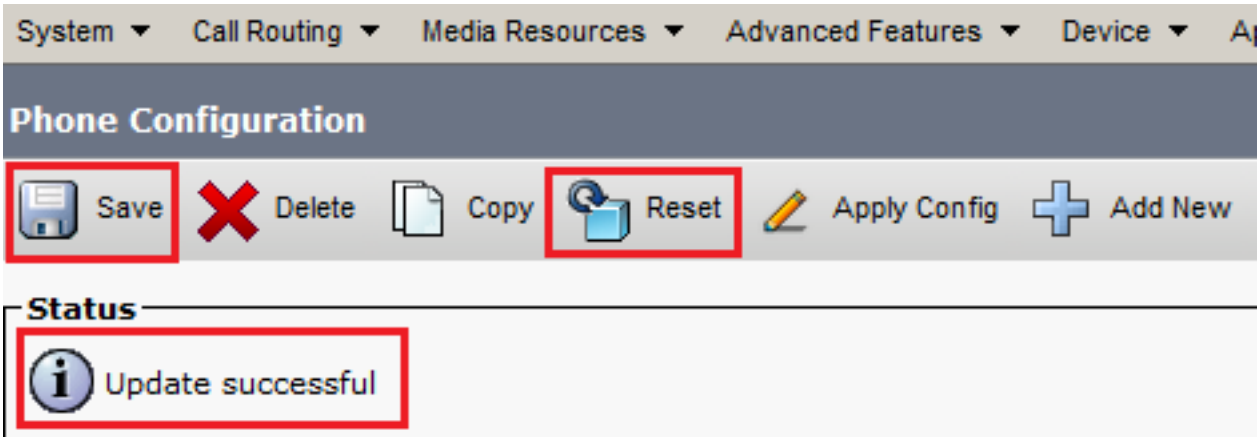
10. 按一下 Find 要列出所有可用電話，請按一下座席電話。
11. 座席電話配置頁面開啟。尋找 Certification Authority Proxy Function (CAPF) Information 部分。要安裝 LSC，請設定 Certificate Operation 成長至 Install/Upgrade 和 Operation Completes by 到任何未來的日子。



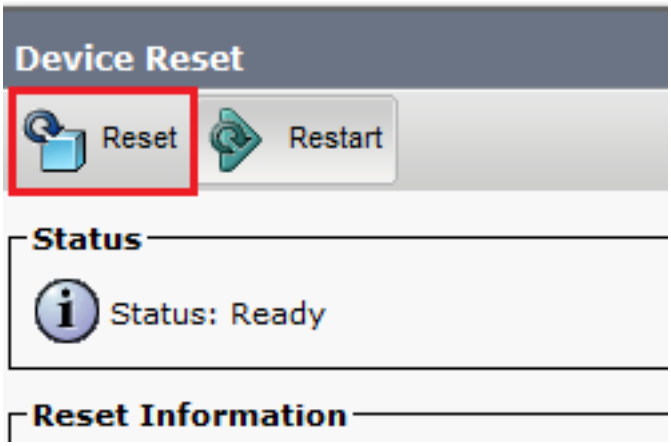
12. 尋找 Protocol Specific Information 分割槽並更改 Device Security Profile 成長至 Cisco Unified Client Services Framework – Secure Profile.



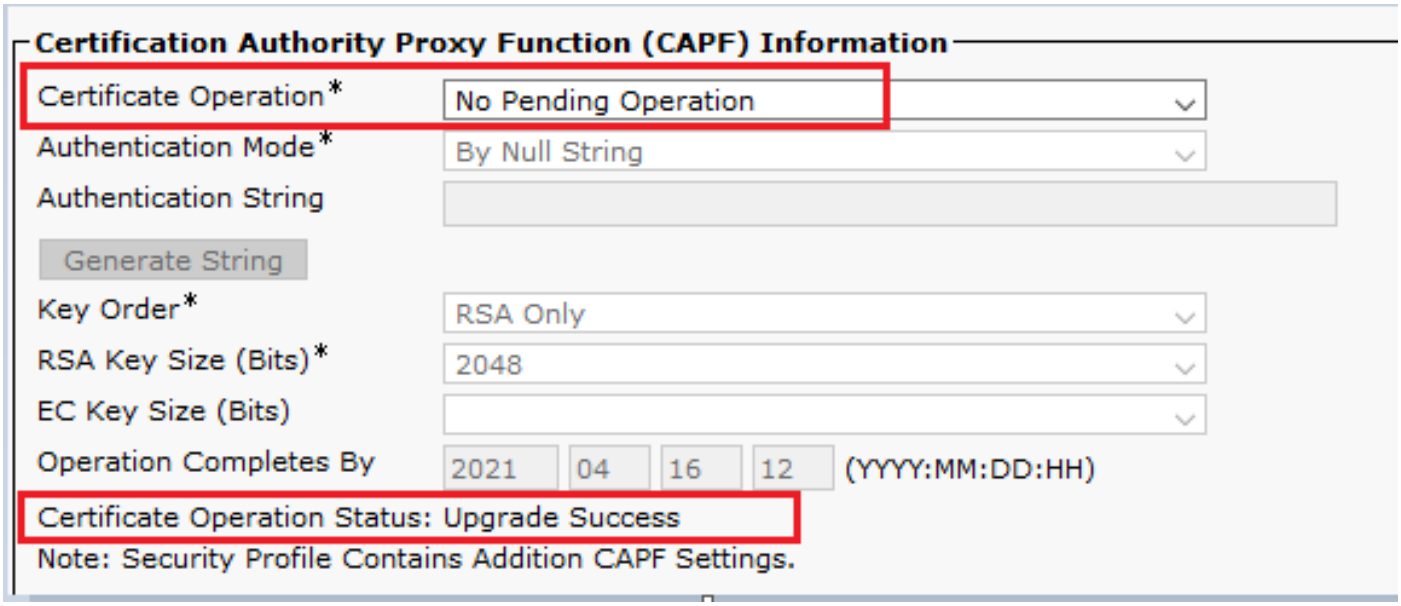
13. 按一下 Save 在頁面的左上角。確保更改已成功儲存，然後按一下 Reset.



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. 請參閱步驟中的相同步驟。7 - 13，保護您想在CUCM中使用安全SIP和RTP的其他代理裝置。

驗證

為了驗證RTP是否正確受到保護，請執行以下步驟：

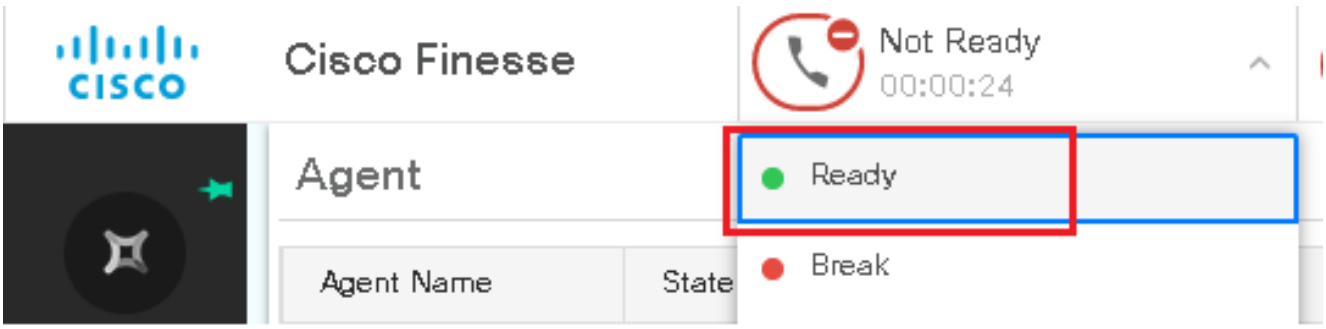
1. 向聯絡中心發出測試呼叫，並監聽IVR提示。
2. 同時，開啟到vCUBE的SSH會話，並運行以下命令：
   show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
 dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:4865626844c25f248e19a95a65b0ad50
 RemoteUUID:674ECD1639ED7A710000ABF910000178
 VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 active
 dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.143:25346 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No IC
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:674ECD1639ED7A710000ABF910000178
 RemoteUUID:4865626844c25f248e19a95a65b0ad50
 VRF:
```

提示：檢查SRTP是否為 on 在CUBE和VVB之間(198.18.133.143)。如果是，這可以確認CUBE和VVB之間的RTP流量是安全的。

3. 使座席可以應答呼叫。

.

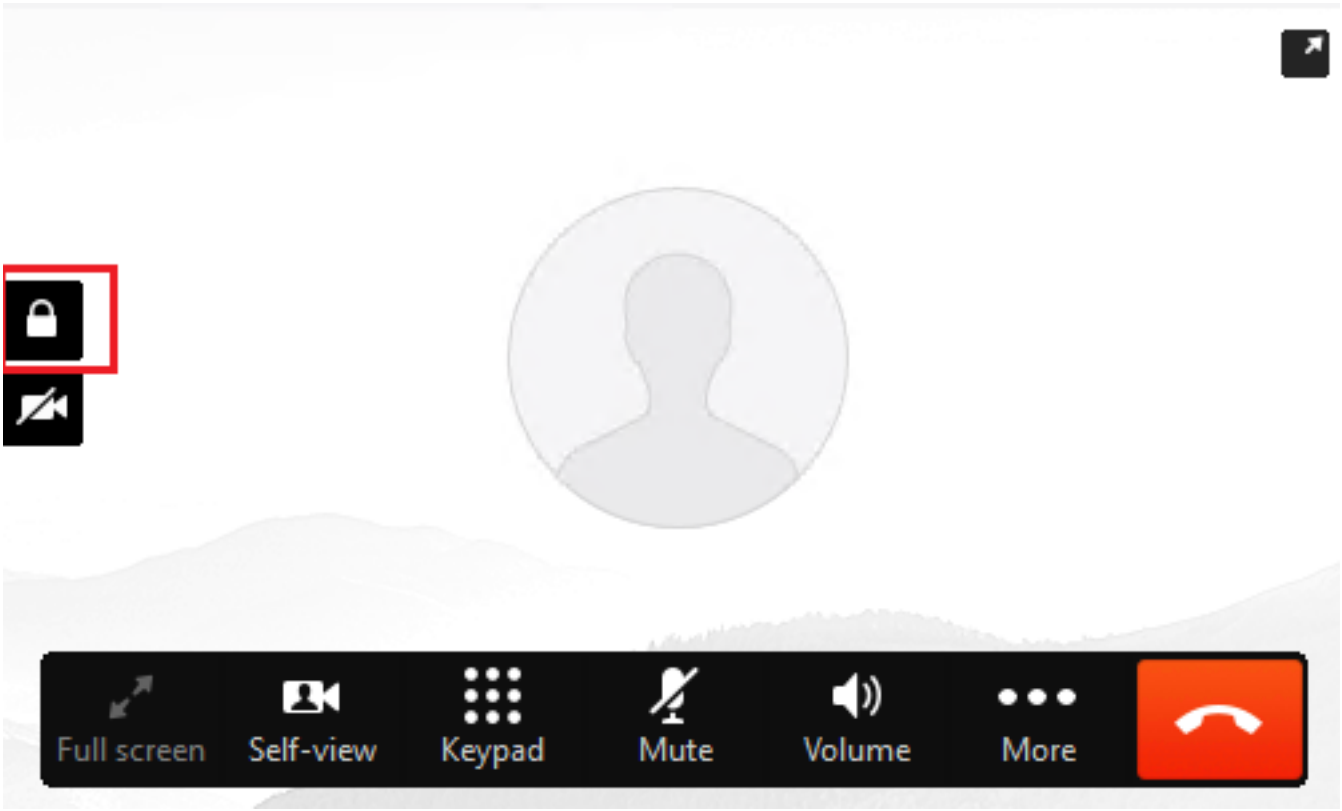


4. 座席將被保留，呼叫將被路由至座席。接聽電話。
5. 呼叫連線到座席。返回vCUBE SSH會話，並運行以下命令：
   show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 connected
 dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:4865626844c25f248e19a95a65b0ad50
 RemoteUUID:00003e7000105000a000005056a06cb8
 VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 connected
 dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 IP 198.18.133.75:24648 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
 media inactive detected:n media contrl rcvd:n/a timestamp:n/a
 long duration call detected:n long duration call duration:n/a timestamp:n/a
 LostPacketRate:0.00 OutOfOrderRate:0.00
 LocalUUID:00003e7000105000a000005056a06cb8
 RemoteUUID:4865626844c25f248e19a95a65b0ad50
 VRF:
```

提示：檢查SRTP是否為 on 在CUBE和座席的電話(198.18.133.75)之間切換。如果是，這可以確認CUBE和代理之間的RTP流量是安全的。

6. 此外，一旦呼叫被連線，安全鎖就會顯示在代理裝置上.這也確認了RTP流量是安全的。



要驗證SIP訊號是否正確安全，請參閱配置安全SIP信令文章。

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）。