

# 在ASA上使用證書身份驗證配置AnyConnect VPN電話

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[電話證書型別](#)

[設定](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

## 簡介

本文檔提供配置示例，說明如何配置自適應安全裝置(ASA)和CallManager裝置，為在Cisco IP電話上運行的AnyConnect客戶端提供證書身份驗證。完成此配置後，思科IP電話可以建立到ASA的VPN連線，利用證書來保護通訊。

## 必要條件

### 需求

嘗試此組態之前，請確保符合以下要求：

- AnyConnect Premium SSL許可證
- 適用於Cisco VPN的AnyConnect電話許可證

根據ASA版本，您會看到ASA 8.0.x版的「適用於Linksys電話的AnyConnect」或ASA 8.2.x版或更高版本的「適用於Cisco VPN電話的AnyConnect」。

### 採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ASA - 8.0(4)版或更高版本

- IP電話型號 — 7942 / 7962 / 7945 / 7965 / 7975
- 電話 — 8961 / 9951 / 9971 , 帶9.1(1)版韌體
- Phone - 9.0(2)SR1S版 — Skinny Call Control Protocol(SCCP)或更高版本
- 思科統一通訊管理器(CUCM)- 8.0.1.10000-4版或更高版本

此組態範例中使用的版本包括：

- ASA 9.1(1)版
- CallManager — 版本8.5.1.10000-26

有關CUCM版本中受支援電話的完整清單，請完成以下步驟：

1. 開啟此URL:<https://<CUCM Server IP Address>:8443/cucreports/systemReports.do>
2. 選擇**Unified CM電話功能清單>生成新報告>功能：虛擬私人網路。**

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

## 慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

## 電話證書型別

思科在電話中使用以下憑證型別：

- 製造商安裝證書(MIC) — 所有7941、7961和較新型號Cisco IP電話都包含MIC。MIC是由思科憑證授權單位(CA)簽署的2048位金鑰憑證。如果存在MIC，則無需安裝本地有效證書(LSC)。為了讓CUCM信任MIC證書，它在其證書信任儲存中使用預安裝的CA證書CAP-RTP-001、CAP-RTP-002和Cisco\_Manufacturing\_CA。
- LSC — 在配置裝置安全模式進行身份驗證或加密後，LSC會保護CUCM和電話之間的連線。LSC擁有思科IP電話的公鑰，該公鑰由CUCM證書授權代理功能(CAPF)私鑰簽名。這是首選方法（與使用MIC相反），因為只允許管理員手動調配的Cisco IP電話下載和驗證CTL檔案。**附註：**由於安全風險增加，Cisco建議僅將MIC用於LSC安裝，而不是繼續使用。將Cisco IP電話配置為使用MIC進行傳輸層安全(TLS)驗證或用於任何其他目的的客戶需要自行承擔風險。

## 設定

本節提供用於設定本文件中所述功能的資訊。

**附註：**使用[命令查詢工具](#)(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

## 組態

本檔案將說明以下組態：

- ASA配置
- CallManager配置

- CallManager上的VPN配置
- IP電話上的證書安裝

## ASA配置

ASA的配置與將AnyConnect客戶端電腦連線到ASA時的配置幾乎相同。但是，以下限制適用：

- 隧道組必須具有group-url。此URL將在CM中的VPN網關URL下配置。
- 組策略不得包含拆分隧道。

此配置使用先前在ASA裝置的安全套接字層(SSL)信任點中配置和安裝的ASA (自簽名或第三方)證書。如需詳細資訊，請參閱以下檔案：

- [配置數位證書](#)
- [ASA 8.x手動安裝第三方供應商證書以用於WebVPN配置示例](#)
- [ASA 8.x:使用AnyConnect VPN客戶端使用自簽名證書的VPN訪問配置示例](#)

ASA的相關配置為：

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client

tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable

ssl trust-point SSL outside
```

## CallManager配置

若要從ASA匯出證書並將證書作為Phone-VPN-Trust證書匯入CallManager，請完成以下步驟：

1. 向CUCM註冊生成的證書。
2. 檢查用於SSL的證書。

```
ASA(config)#show run ssl
ssl trust-point SSL outside
```

3. 匯出證書。

```
ASA(config)#crypto ca export SSL identity-certificate
```

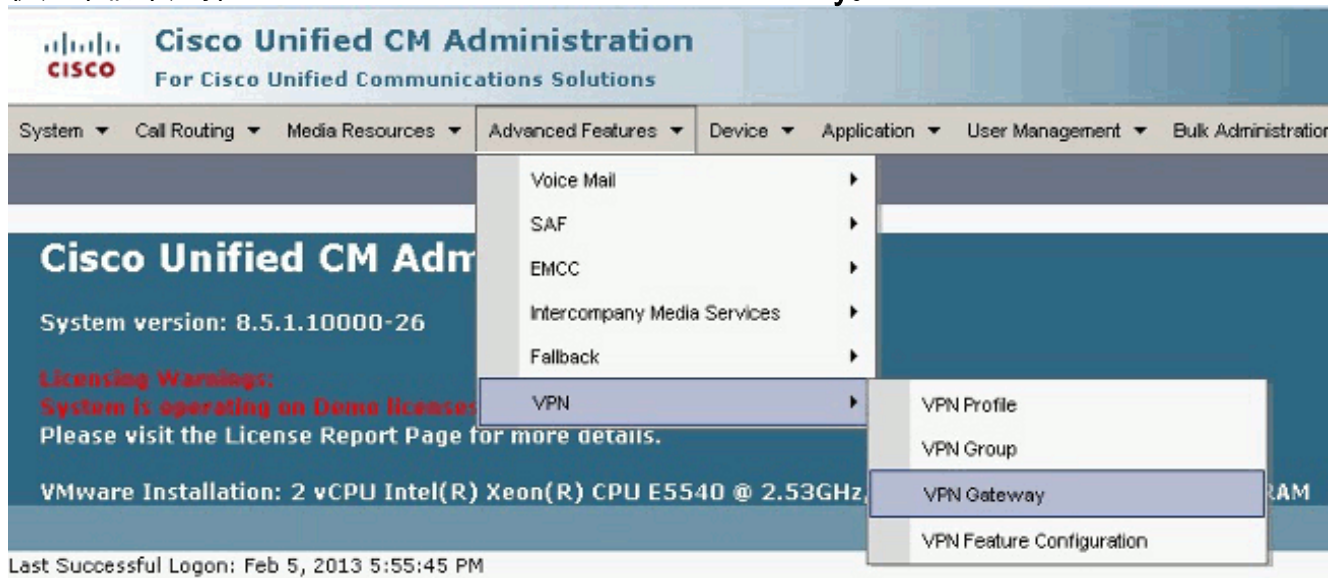
Privacy Enhanced Mail(PEM)編碼的身份證書如下：

```
-----BEGIN CERTIFICATE-----ZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUxFjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysjZ+MawKBx8Zk69SW4AR
FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jcl5vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZhOlV9xOpR7BFpZdlyFyzwAPkoB1l
-----END CERTIFICATE-----
```

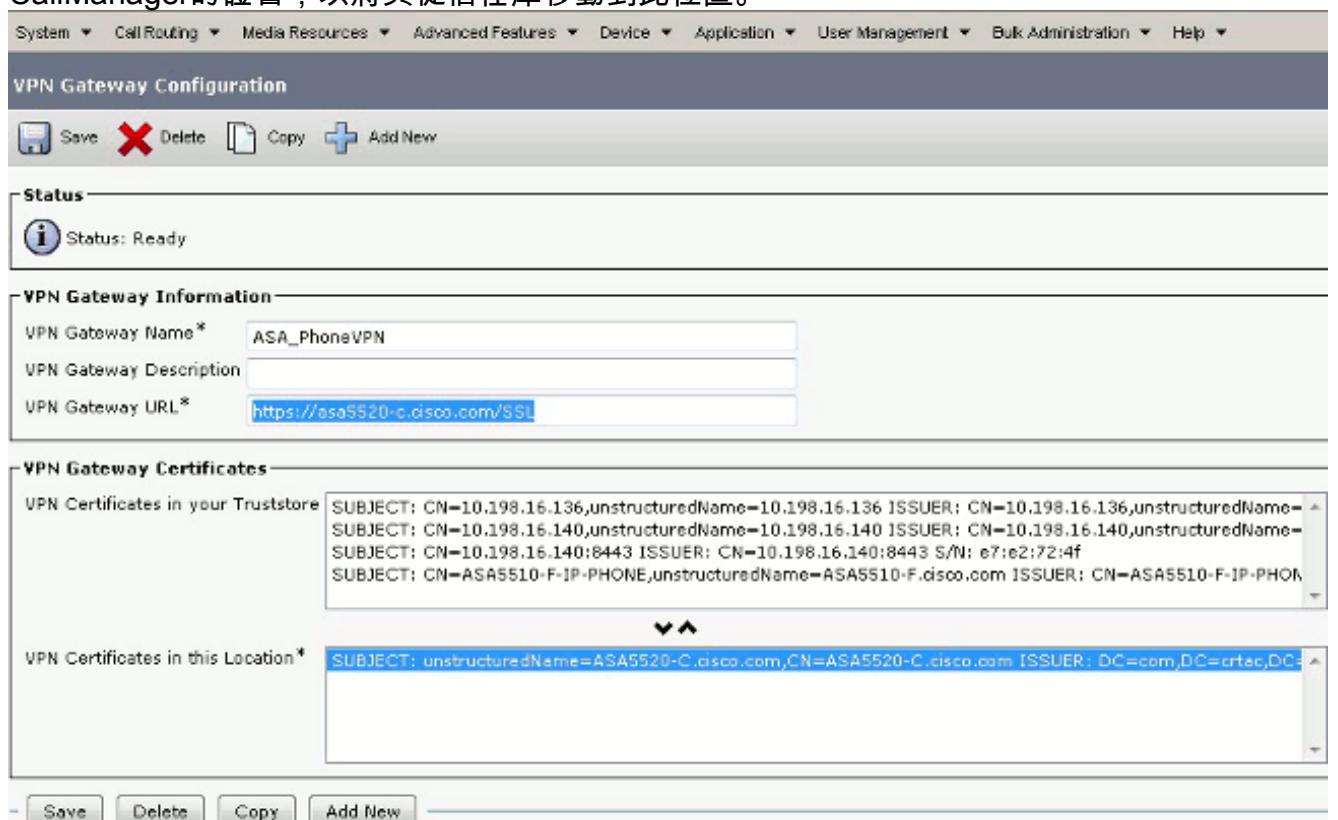
4. 從終端複製文字並將其另存為.pem檔案。
5. 登入到CallManager並選擇Unified OS Administration > Security > Certificate Management >

Upload Certificate > Select Phone-VPN-trust以上步驟中儲存的證書檔案進行上傳。  
CallManager上的VPN配置

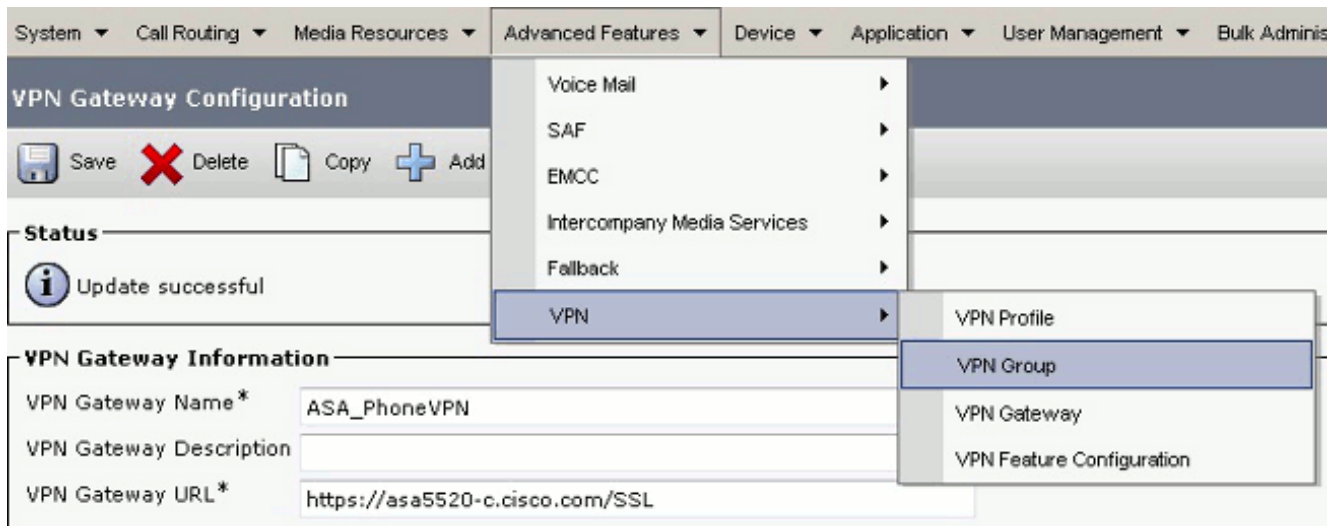
1. 導航到Cisco Unified CM Administration。
2. 從選單欄中選擇Advanced Features > VPN > VPN Gateway。



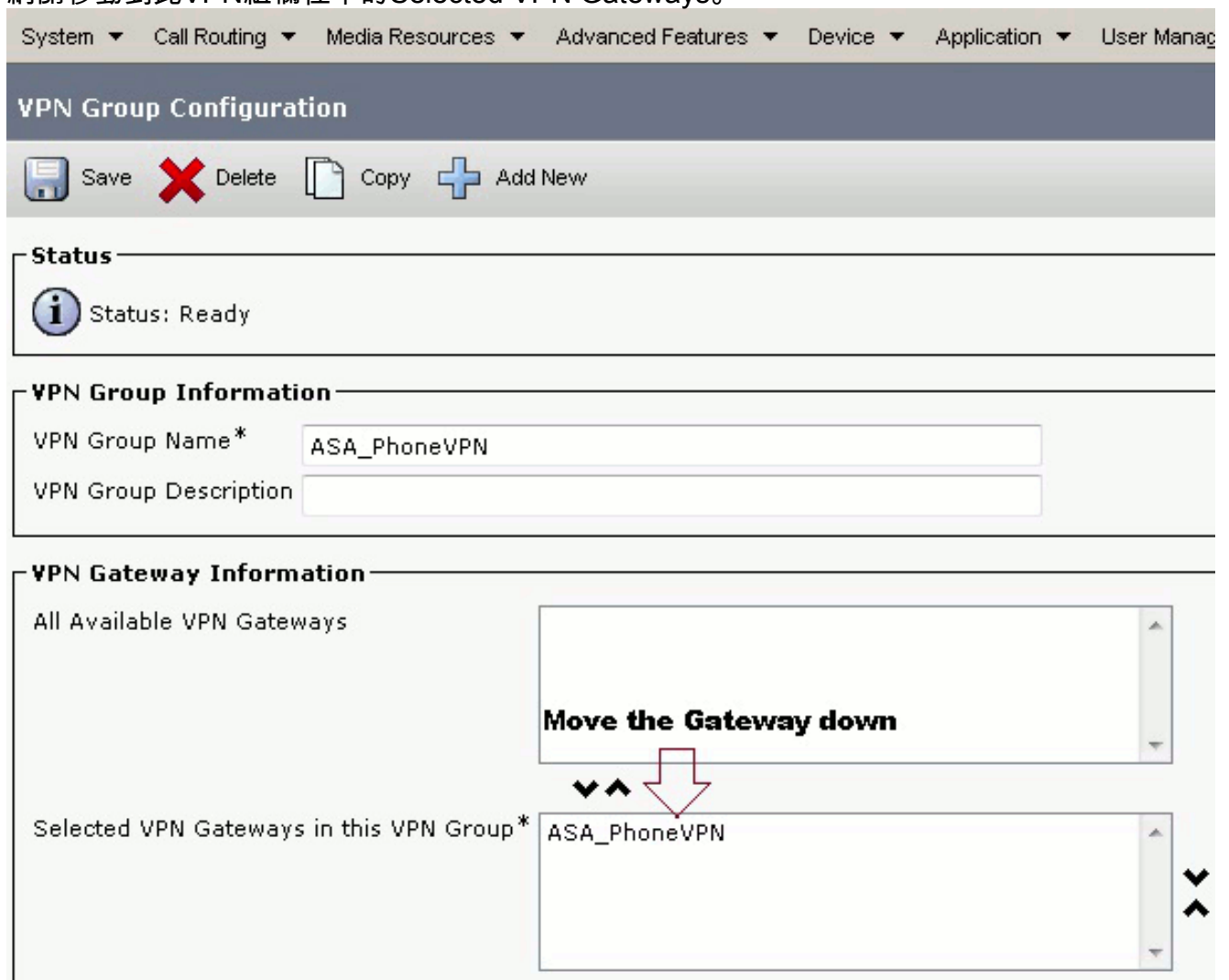
3. 在VPN網關配置視窗中，完成以下步驟：在VPN Gateway Name欄位中，輸入名稱。可以是任何名稱。在VPN Gateway Description欄位中，輸入說明（可選）。在VPN Gateway URL欄位中，輸入在ASA上定義的group-url。在此位置中的VPN證書欄位中，選擇之前上傳到CallManager的證書，以將其從信任庫移動到此位置。



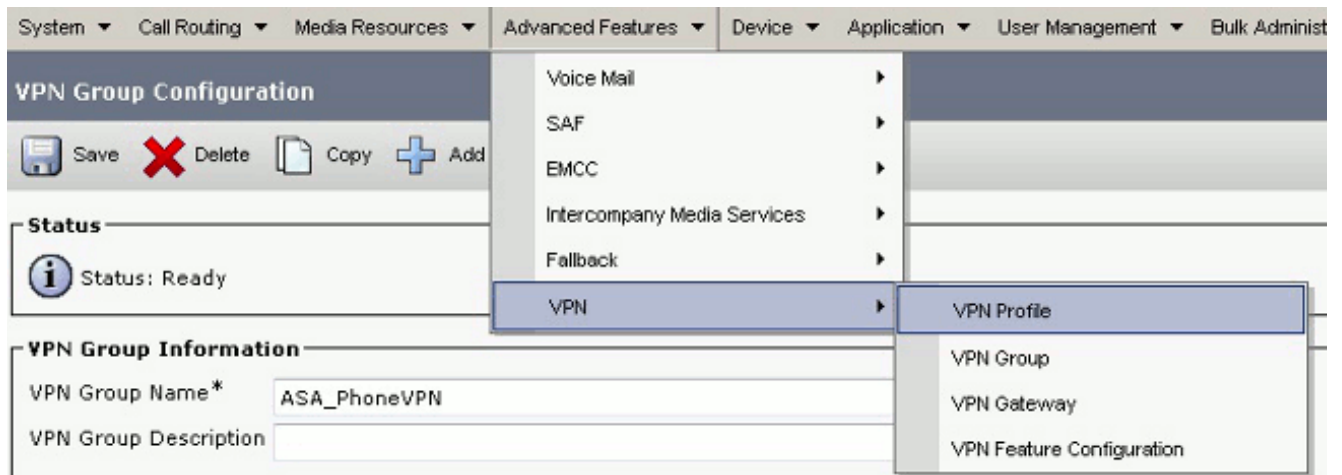
4. 從選單欄中選擇Advanced Features > VPN > VPN Group。



5. 在All Available VPN Gateways欄位中，選擇先前定義的VPN Gateway。點選向下箭頭將所選網關移動到此VPN組欄位中的Selected VPN Gateways。



6. 從選單欄中選擇Advanced Features > VPN > VPN Profile。



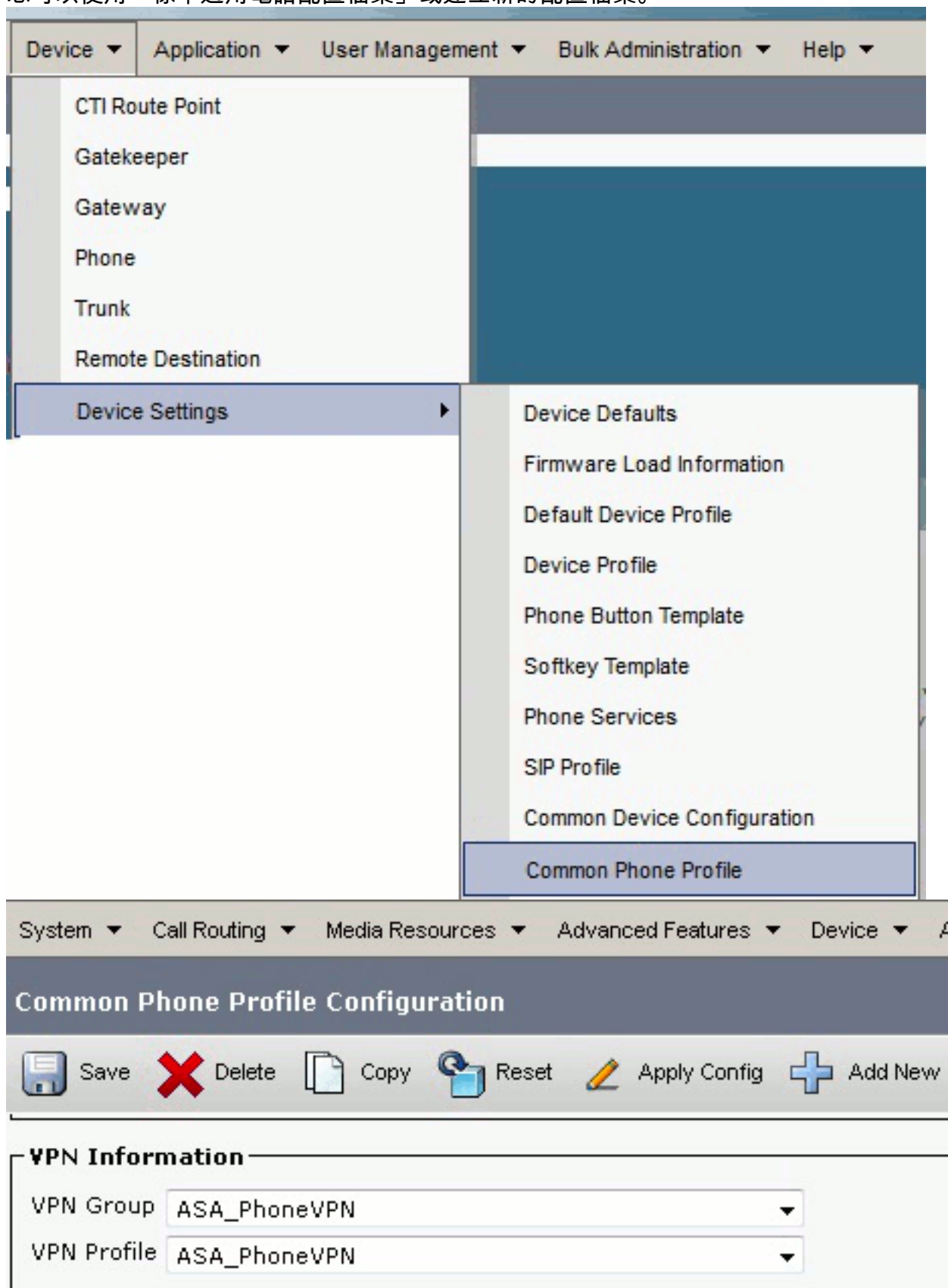
7. 要配置VPN配置檔案，請填寫所有標有星號(\*)的欄位。

**啟用自動網路檢測：**如果啟用，VPN電話ping TFTP伺服器，如果未收到響應，則自動發起VPN連線。**啟用主機ID檢查：**如果啟用，VPN電話會將VPN網關URL的FQDN與證書的CN/SAN進行比較。如果客戶端不匹配或使用帶有星號(\*)的萬用字元證書，則客戶端無法連線。**啟用密碼永續性：**這允許VPN電話快取下次VPN嘗試的使用者名稱和密碼。

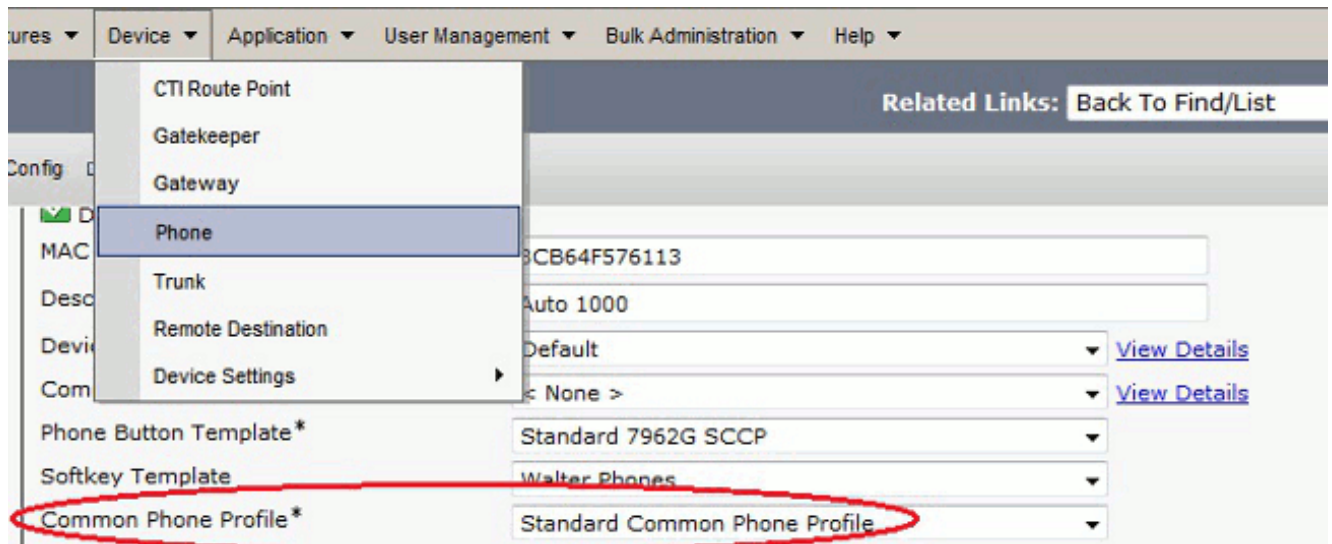
8. 在Common Phone Profile Configuration視窗中，按一下**Apply Config**以應用新的VPN配置。



您可以使用「標準通用電話配置檔案」或建立新的配置檔案。



9. 如果您為特定電話/使用者建立了新配置檔案，請轉到「電話配置」視窗。在Common Phone Profile欄位中，選擇Standard Common Phone Profile。



10. 再次向CallManager註冊電話，以便下載新配置。

### 證書身份驗證配置





要配置證書身份驗證，請在CallManager和ASA中完成以下步驟：

1. 從選單欄中選擇**Advanced Features > VPN > VPN Profile**。
2. 確認Client Authentication Method欄位已設定為**Certificate**。




System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

## VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

---

**Status**

 Status: Ready

---

**VPN Profile Information**

Name\*

Description

Enable Auto Network Detect

---

**Tunnel Parameters**

MTU\*

Fail to Connect\*

Enable Host ID Check



---

**Client Authentication**

Client Authentication Method\*

Enable Password Persistence

- 登入到CallManager。從選單欄中選擇Unified OS Administration > Security > Certificate Management > Find。
- 匯出所選證書身份驗證方法的正確證書：MIC:Cisco\_Manufacturing\_CA — 使用MIC驗證IP電話

Find Certificate List where File Name ▾ begins with ▾  Find Clear Filter  

Certificate Name	Certificate Type	.PEM File
tomcat	certs	<a href="#">tomcat.pem</a>
ipsec	certs	<a href="#">ipsec.pem</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>
ipsec-trust	trust-certs	<a href="#">CUCM85.pem</a>
CallManager	certs	<a href="#">CallManager.pem</a>
CAPF	certs	<a href="#">CAPF.pem</a>
TVS	certs	<a href="#">TVS.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-001.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco Root CA 2048.pem</a>
CallManager-trust	trust-certs	<a href="#">CAPF-18cf046e.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-002.pem</a>

LSC:思科憑證授權代理功能(CAPF) — 使用LSC驗證IP電話

Certificate Name	Certificate Type	.PEM File	.DER File
tomcat	certs	<a href="#">tomcat.pem</a>	<a href="#">tomcat.der</a>
ipsecc	certs	<a href="#">ipsecc.pem</a>	<a href="#">ipsecc.der</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
ipsecc-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
CallManager	certs	<a href="#">CallManager.pem</a>	<a href="#">CallManager.der</a>
CAPF	certs	<a href="#">CAPF.pem</a>	<a href="#">CAPF.der</a>
TVS	certs	<a href="#">TVS.pem</a>	<a href="#">TVS.der</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>	

- 查詢證書 ( Cisco\_Manufacturing\_CA或CAPF )。下載.pem檔案並另存為.txt檔案
- 在ASA上建立新的信任點，並使用以前儲存的證書驗證信任點。當系統提示您輸入base-64編碼的CA憑證時，請選擇並貼上下載的.pem檔案中的文字以及BEGIN和END行。範例如下：

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#
```

```
<base-64 encoded CA certificate>
```

```
quit
```

- 確認隧道組上的身份驗證已設定為證書身份驗證。

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

## IP電話上的證書安裝

IP電話可以與MIC或LSC一起使用，但每個證書的配置過程不同。

## MIC安裝

預設情況下，支援VPN的所有電話都預裝了MIC。7960和7940電話不附帶MIC，並且需要特殊的安裝步驟才能使LSC安全地註冊。

**附註：**思科建議您僅將MIC用於LSC安裝。Cisco支援LSC對CUCM的TLS連線進行身份驗證。由於MIC根證書可能受到危害，因此將電話配置為使用MIC進行TLS驗證或用於任何其他目的的客戶會自行承擔風險。如果MIC受到危害，思科不承擔任何責任。

## LSC安裝

- 在CUCM上啟用CAPF服務。
- 啟用CAPF服務後，分配電話說明以在CUCM中生成LSC。登入到Cisco Unified CM管理並選擇**Device > Phone**。選擇您配置的電話。
- 在「Certificate Authority Proxy Function(CAPF)Information(證書頒發機構代理功能(CAPF)資訊)」部分，確保所有設定都正確無誤，並且操作已設定為未來的日期。

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Size (Bits)\*

Operation Completes By     (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

4. 如果身份驗證模式設定為空字串或現有證書，則無需執行進一步的操作。
5. 如果身份驗證模式設定為字串，請在電話控制檯中手動選擇 **Settings > Security Configuration > \*\*# > LSC > Update**。

## 驗證

使用本節內容，確認您的組態是否正常運作。

### ASA驗證

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : CP-7962G-SEPXXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 57.1
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Encryption : AES128 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Dst Port : 443
```



- Cisco錯誤ID [CSCuj71475](#),IP電話VPN所需的手動TFTP條目
- 思科錯誤ID [CSCum10683](#) , 未記錄未接、已撥或已接呼叫的IP電話

## 相關資訊

- [技術支援與文件 - Cisco Systems](#)