AnyConnect VPN電話連線到Cisco IOS路由器配置示例

目錄

簡介

本文檔介紹如何配置Cisco IOS®路由器和呼叫管理器裝置，以便思科IP電話建立與Cisco IOS路由器的VPN連線。需要使用以下VPN連線來保護與以下兩種客戶端身份驗證方法之一的通訊：

- 身份驗證、授權和記帳(AAA)伺服器或本地資料庫
- 電話證書

必要條件

需求

本文件沒有特定需求。

採用元件

本文件中的資訊是以下列硬體與軟體版本為依據：

- Cisco IOS 15.1(2)T或更高版本
- 功能集/許可證：適用於Cisco IOS整合式服務路由器(ISR)-G2的通用（資料和安全與UC）
- 功能集/許可證：Cisco IOS ISR的高級安全
- 思科統一通訊管理器(CUCM)版本8.0.1.100000-4或更高版本
- IP電話版本9.0(2)SR1S — 精簡型通話控制通訊協定(SCCP)或更新版本

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 Phone Feature List > Generate a new report > Feature:虛擬私人網路。

此組態範例中使用的版本包括：

- Cisco IOS路由器版本15.1(4)M4
- 通話管理員版本8.5.1.10000-26
- IP電話版本9.1(1)SR1S

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。

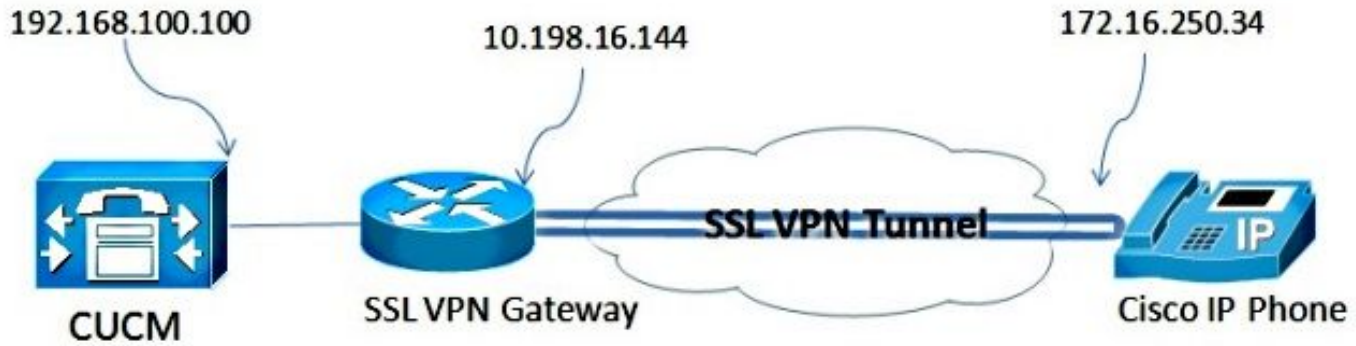
設定

本節介紹設定本檔案中所述功能所需的資訊。

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更多資訊。

網路拓撲

本文檔中使用的拓撲包括一台Cisco IP電話、用作安全套接字層(SSL)VPN網關的Cisco IOS路由器以及用作語音網關的CUCM。



SSL VPN伺服器配置

本節介紹如何配置Cisco IOS頭端以允許入站SSL VPN連線。

常見配置步驟

1. 生成長度為1024位元組的Rivest-Shamir-Adleman(RSA)金鑰：

```
<#root>

Router(config)#

crypto key generate rsa general-keys label SSL modulus 1024
```

2. 為自簽名證書建立信任點，並附加SSL RSA金鑰:

```
<#root>

Router(config)#

crypto pki trustpoint server-certificate


 enrollment selfsigned
 usage ssl-server
 serial-number
 subject-name CN=10.198.16.144
 revocation-check none
 rsakeypair SSL
```

3. 配置信任點後，使用以下命令註冊自簽名證書：

```
<#root>

Router(config)#

crypto pki enroll

server-certificate


% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

4. 在頭端啟用正確的AnyConnect軟體包。電話本身不會下載此程式包。但是，如果沒有軟體包，VPN隧道無法建立。建議使用Cisco.com上提供的最新客戶端軟體版本。本示例使用3.1.3103版。

在舊版Cisco IOS中，以下命令可啟用封包：

```
<#root>

Router(config)#

webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
```

但是最新Cisco IOS版本中的命令如下：

```
<#root>

Router(config)#

crypto vpn anyconnect flash:/webvpn/anyconnect-win-
3.1.03103-k9.pkg sequence 1
```

5. 配置VPN網關。WebVPN網關用於終止來自使用者的SSL連線。

```
webvpn gateway SSL
ip address 10.198.16.144 port 443
 ssl encryption 3des-sha1 aes-sha1
 http-redirect port 80
 ssl trustpoint server-certificate
 inservice
```

附註：此處使用的IP地址必須與電話所連線的介面位於同一子網中，或者網關需要直接從路由器上的介面獲得。閘道也用於定義路由器使用哪個憑證來向使用者端驗證其自身。

---

6. 定義在客戶端連線時用於分配IP地址的本地池：

```
ip local pool ap_phonevpn 192.168.100.1 192.168.100.254
```

使用AAA驗證的組態

本節介紹配置AAA伺服器或本地資料庫以對您的電話進行身份驗證所需的命令。如果計畫對電話使用僅證書身份驗證，請繼續下一部分。

配置使用者資料庫

路由器的本地資料庫或外部AAA伺服器可用於身份驗證：

- 要配置本地資料庫，請輸入：

```
aaa new-model
aaa authentication login SSL local
username phones password 0 phones
```

- 若要將遠端AAA RADIUS伺服器設定為驗證，請輸入：

```
aaa new-model
aaa authentication login SSL group radius
radius-server host 192.168.100.200 auth-port 1812 acct-port 1813
radius-server key cisco
```

配置虛擬情景和組策略

虛擬環境用於定義管理VPN連線的屬性，例如：

- 連線時要使用的URL
- 分配客戶端地址時要使用的池
- 使用哪種身份驗證方法

以下命令是對客戶端使用AAA身份驗證的上下文示例：

```
webvpn context SSL
 aaa authenticate list SSL
 gateway SSL domain SSLPhones
 !
 ssl authenticate verify all
 inservice
 !
 policy group phones
  functions svc-enabled
  svc address-pool "ap_phonevpn" netmask 255.255.255.0
  svc keep-client-installed
 default-group-policy phones
```

使用IP電話本地重要證書(LSC)配置客戶端身份驗證

本節介紹為電話配置基於證書的客戶端身份驗證所需的命令。但是，要執行此操作，需要瞭解各種型別的電話證書：

- 製造商安裝證書(MIC) — 所有7941、7961和新型Cisco IP電話都包含MIC。MIC是由思科憑證授權單位(CA)簽署的2,048位金鑰憑證。 為了使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。由於此證書是由製造商本身提供的（如名稱中所示），因此建議不要將此證書用於客戶端身份驗證。
- 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。這是更安全的方法（相對於使用MIC）。

注意：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。為使用MIC進行傳輸層安全(TLS)驗證或用於任何其他目的而配置Cisco IP電話的客戶自行承擔風險。

在此配置示例中，LSC用於驗證電話。

提示：連線您的電話的最安全方法是使用雙重身份驗證，這種身份驗證結合了證書和AAA身份驗證。如果將用於每個虛擬上下文的命令組合到一個虛擬上下文下，則可以進行配置。

配置信任點以驗證客戶端證書

路由器必須安裝CAPF證書才能從IP電話驗證LSC。若要取得該憑證並將其安裝到路由器上，請完成以下步驟：

1. 轉到CUCM作業系統(OS)管理網頁。
2. 選擇Security > Certificate Management。

附註：此位置可能根據CUCM版本而更改。

---

3. 找到標有CAPF的憑證，並下載.pem檔案。將其另存為.txt檔案
4. 擷取憑證後，在路由器上建立一個新的信任點，並使用CAPF驗證信任點，如此處所示。當系統提示輸入base-64編碼的CA憑證時，選擇並貼上下載的.pem檔案中的文字以及BEGIN和END行。
<#root>

```
Router(config)#

crypto pki trustpoint CAPF


 enrollment terminal
 authorization username subjectname commonname
 revocation-check none
Router(config)#

crypto pki authenticate CAPF


Router(config)#
```

```
 quit
```

需注意的事項：

- 註冊方法是終端，因為必須在路由器上手動安裝證書。
- 需要使用authorization username命令才能告訴路由器在客戶端建立連線時用作使用者名稱的裝置。在這種情況下，會使用公用名(CN)。
- 需要禁用吊銷檢查，因為電話證書沒有定義證書吊銷清單(CRL)。因此，除非禁用此功能，否則連線將失敗，並且公開金鑰基礎結構(PKI)調試將顯示以下輸出：

```
<#root>

Jun 17 21:49:46.695: CRYPTO_PKI: (A0076)

 Starting CRL revocation check


Jun 17 21:49:46.695: CRYPTO_PKI:

Matching CRL not found


Jun 17 21:49:46.695: CRYPTO_PKI: (A0076)

 CDP does not exist. Use SCEP to
query CRL.


Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076)

Certificate validation failed
```

配置虛擬情景和組策略

此部分的組態與之前使用的組態類似，但兩處除外：

- 驗證方法
- 上下文用於驗證電話的信任點

命令如下所示：

```
webvpn context SSL
 gateway SSL domain SSLPhones
 authentication certificate
```

```
ca trustpoint CAPF
!
ssl authenticate verify all
inservice
!
policy group phones
functions svc-enabled
svc address-pool "ap_phonevpn" netmask 255.255.255.0
svc keep-client-installed
default-group-policy phones
```

Call Manager配置

本節介紹Call Manager的配置步驟。

將自簽名證書或身份證書從路由器匯出到CUCM

要從路由器匯出證書並將證書作為Phone-VPN-Trust證書匯入到Call Manager，請完成以下步驟：

1. 檢查用於SSL的證書。

   <#root>

   ```
   Router#
   ```

   show webvpn gateway SSL

   ```
   SSL Trustpoint: server-certificate
   ```

2. 匯出證書。

   <#root>

   ```
   Router(config)#
   ```

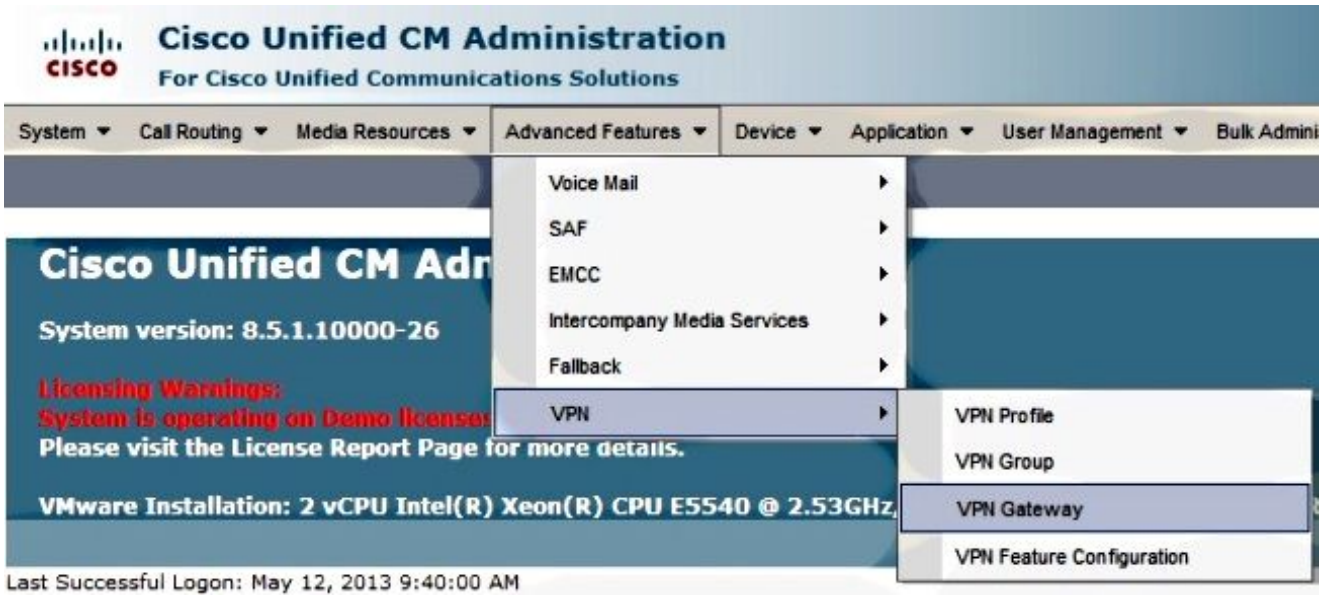
   crypto pki export server-certificate pem terminal

   ```
   The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
   -----BEGIN CERTIFICATE-----

   <output removed>

   -----END CERTIFICATE-----
   ```

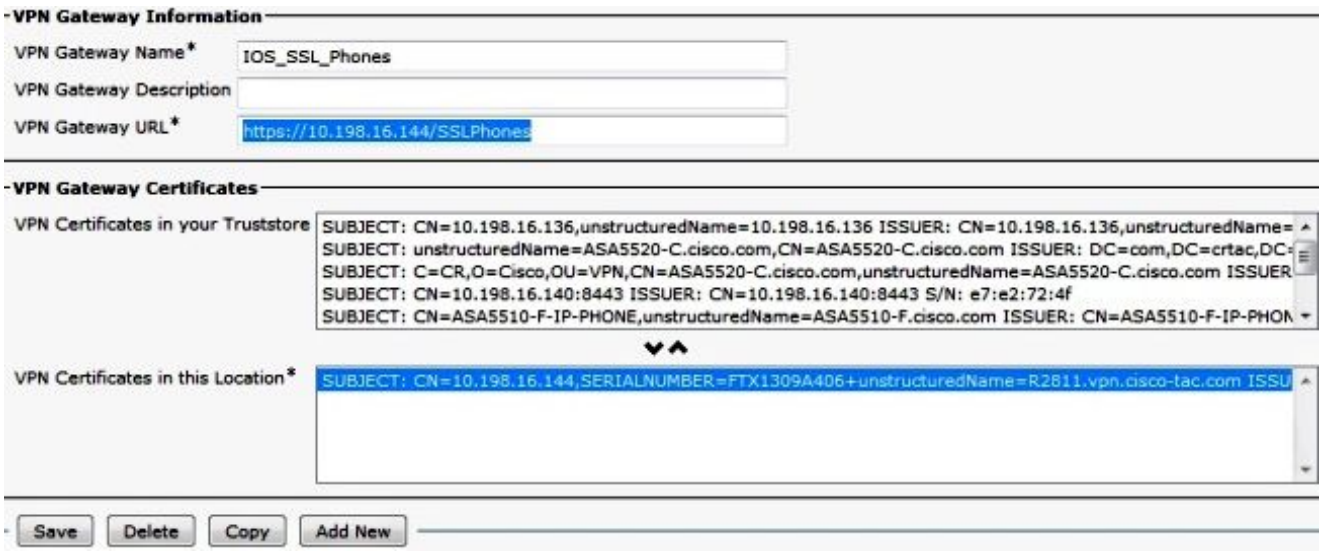
3. 從終端複製文字並將其另存為.pem文件。
4. 登入到Call Manager，然後選擇Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust以上傳在上一步中儲存的證書檔案。

在CUCM中配置VPN網關、組和配置檔案

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

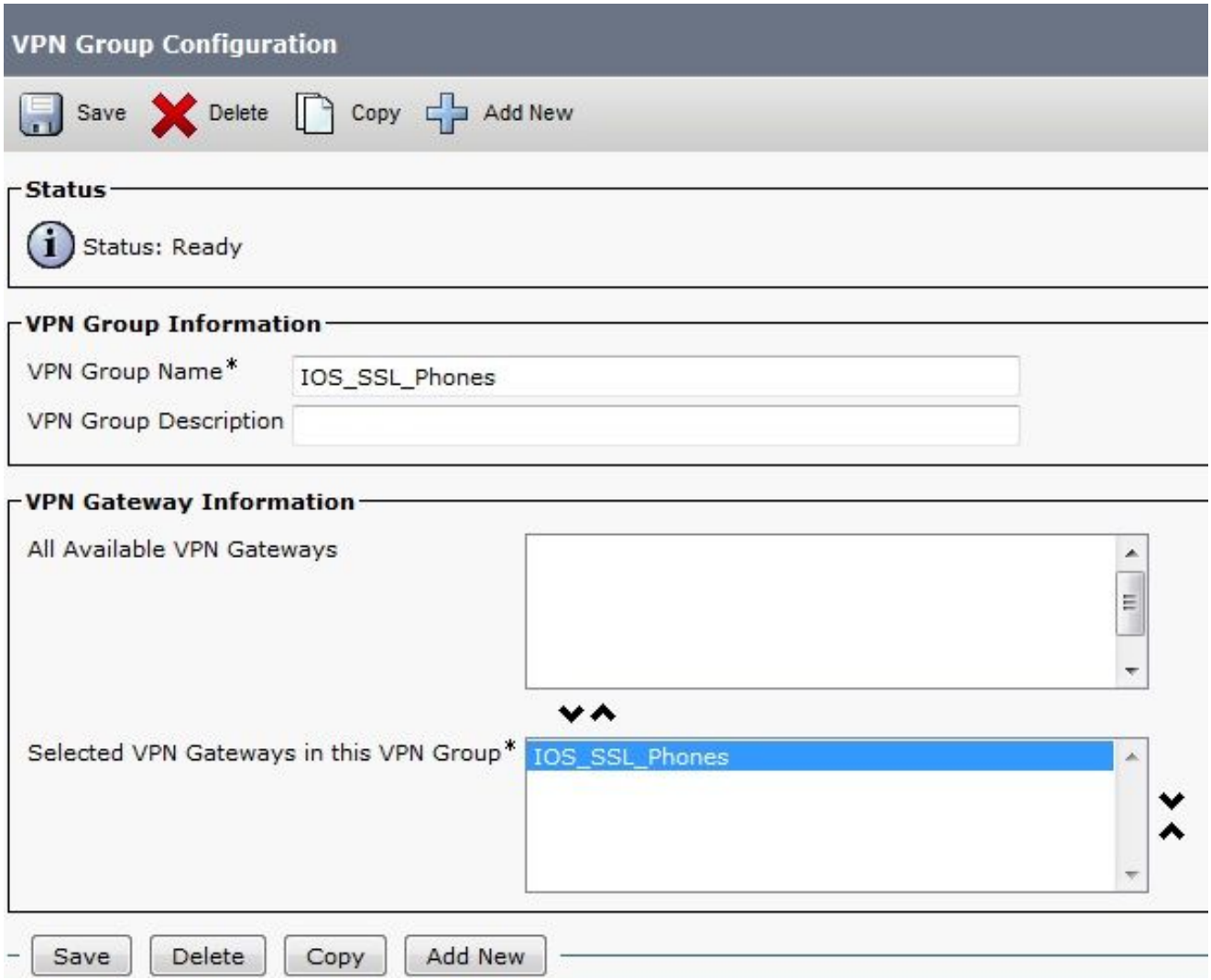


3. 在VPN網關配置視窗中，完成以下步驟：
   - 在VPN Gateway Name欄位中，輸入名稱。此名稱可以是任意名稱。
   - 在VPN Gateway Description欄位中，輸入說明（可選）。
   - 在VPN Gateway URL欄位中，輸入路由器上定義的group-URL。
   - 在此位置的VPN證書欄位中，選擇之前上傳到Call Manager的證書，以便將其從信任儲存移動到此位置。

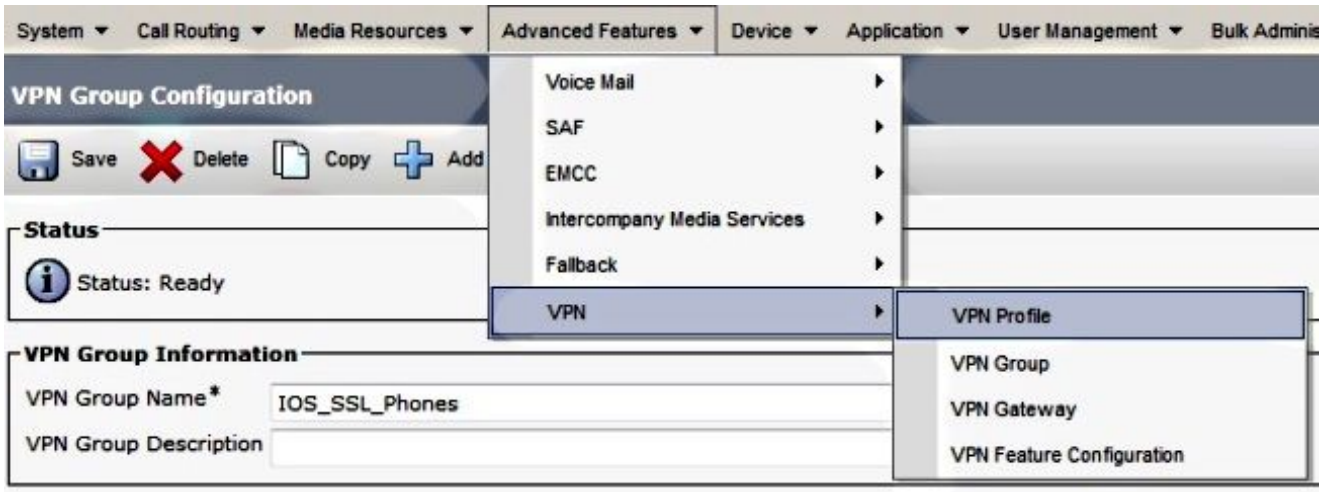


4. 從選單欄中選擇Advanced Features > VPN > VPN Group。

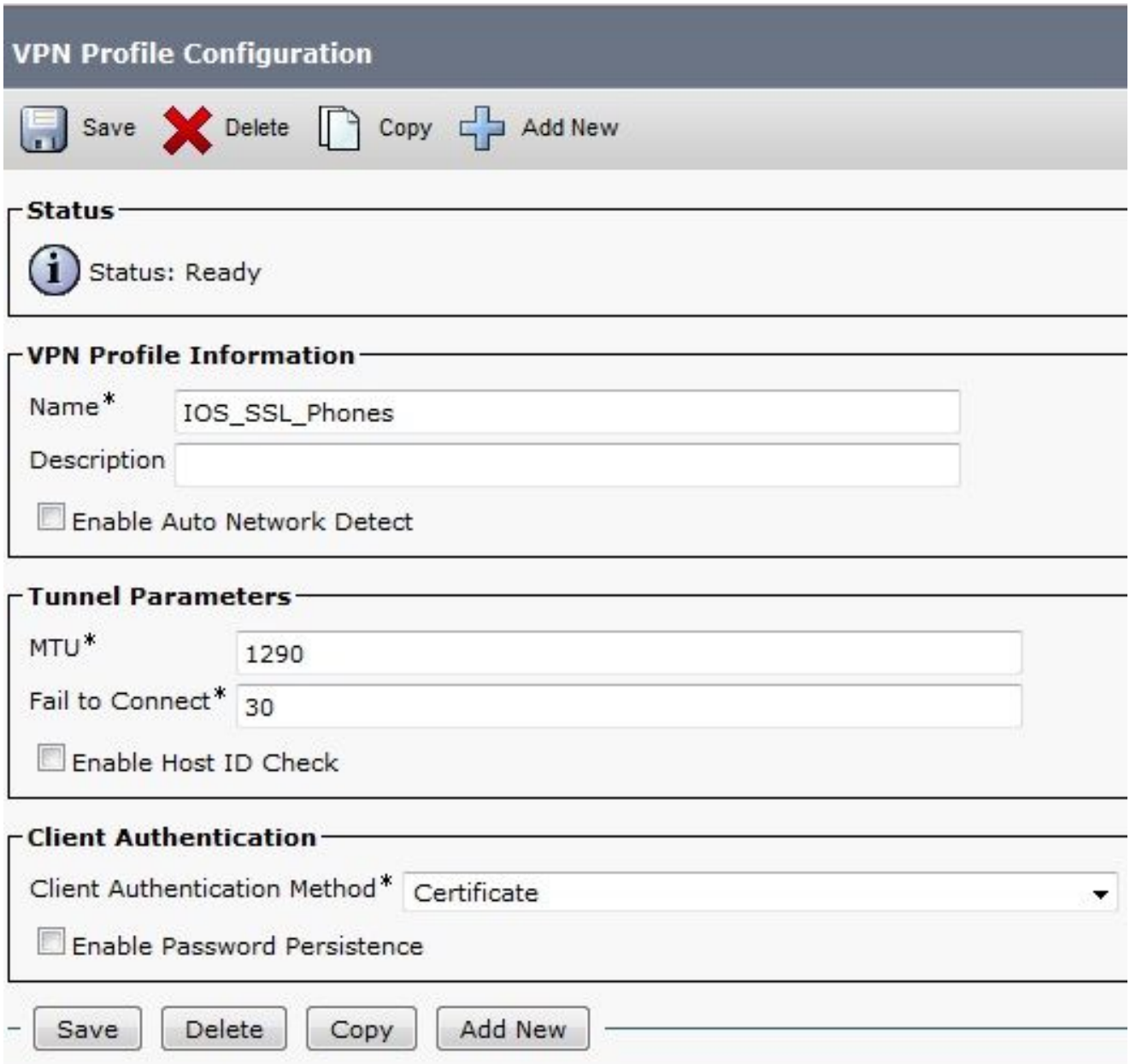
5. 在All Available VPN Gateways欄位中，選擇之前定義的VPN Gateway。點選向下箭頭將所選網關移動到此VPN組欄位中的Selected VPN Gateways（選定VPN網關）。



6. 在選單欄中，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。



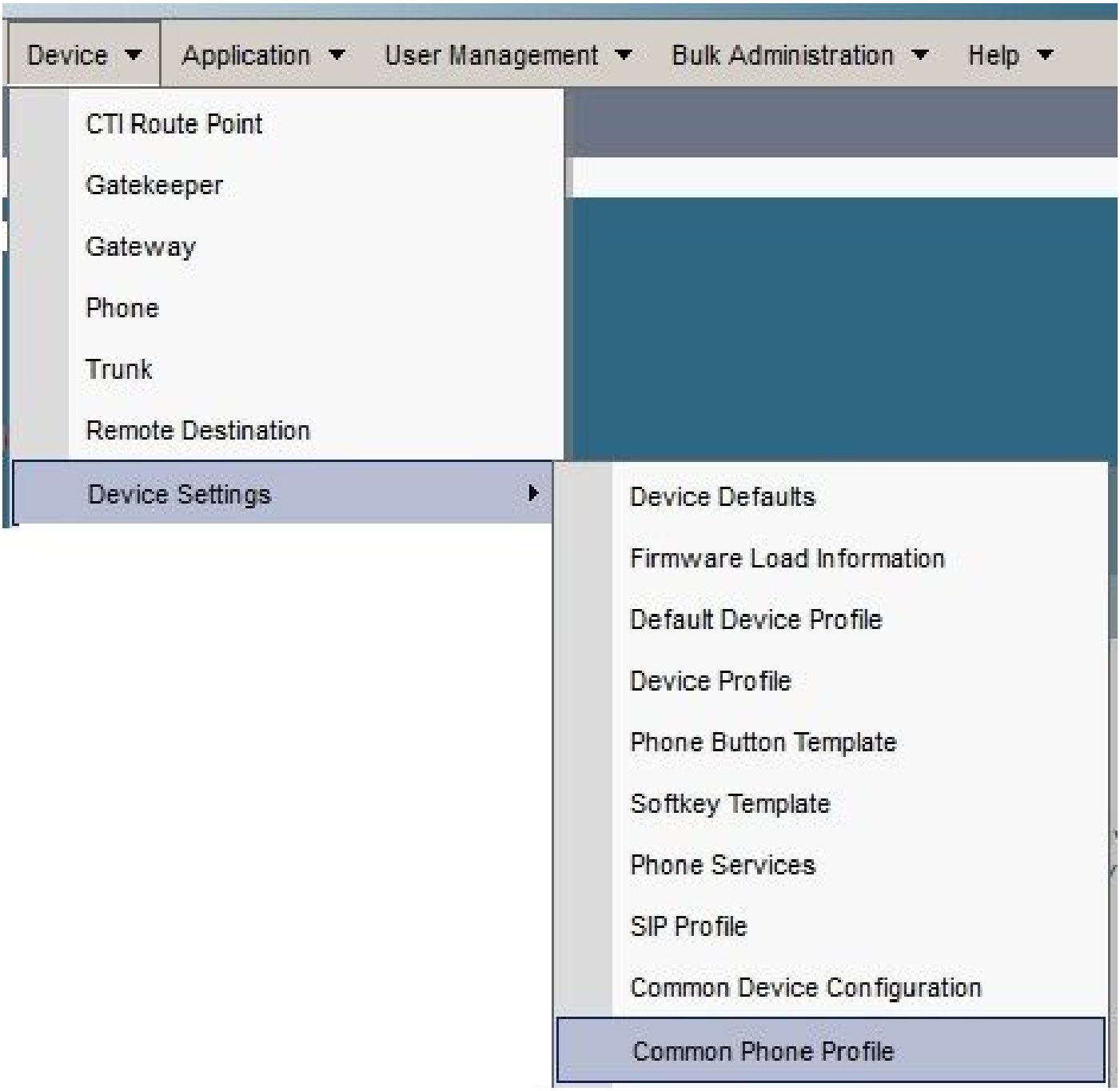
- 啟用自動網路檢測：如果啟用，VPN電話ping TFTP伺服器。如果沒有收到響應，它將

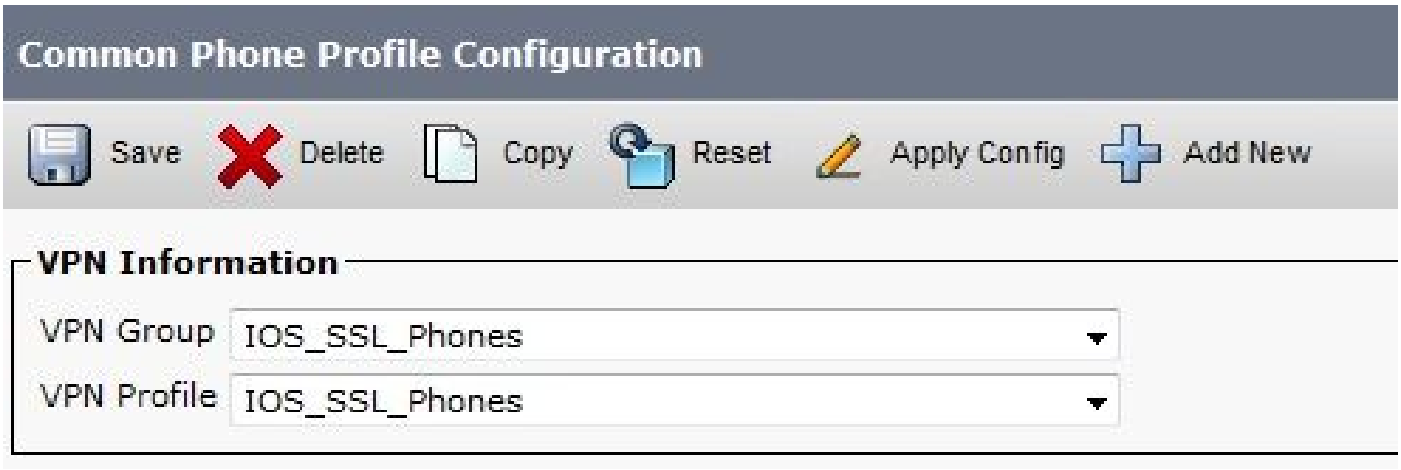
自動發起VPN連線。

- 啟用主機ID檢查：如果啟用，VPN電話會將VPN網關URL的完全限定域名(FQDN)與證書的CN/儲存區域網路(SAN)進行比較。如果這些專案不匹配或使用星號(*)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。

將組和配置檔案應用於具有通用電話配置檔案的IP電話

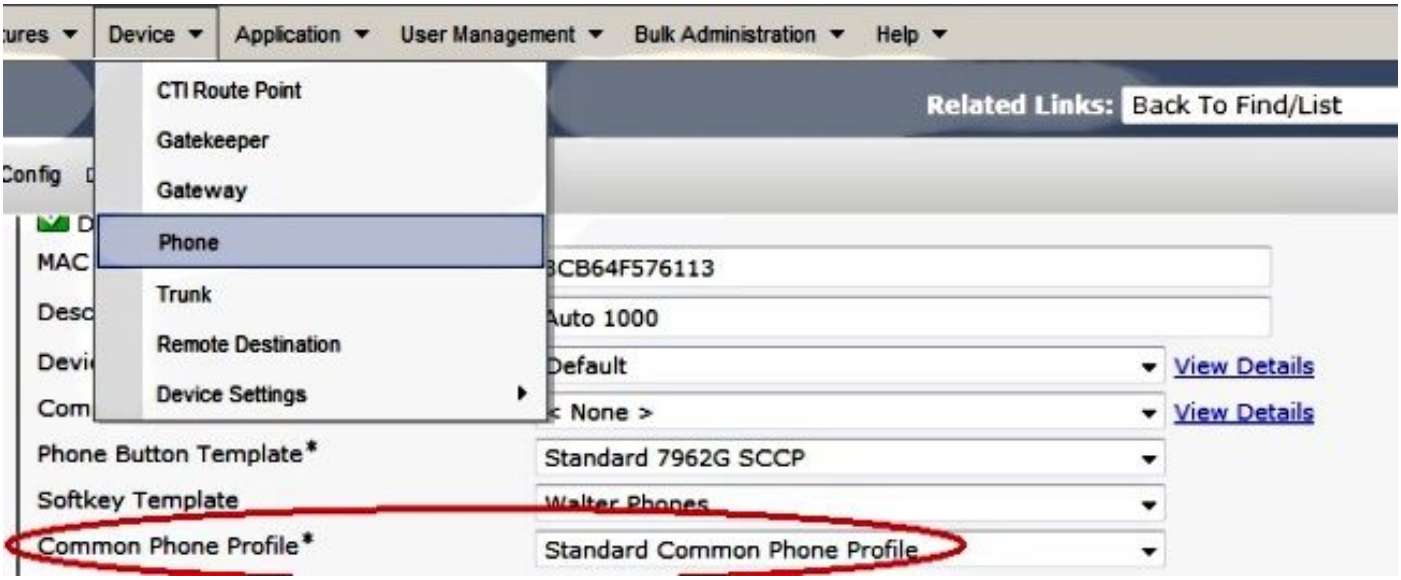
在Common Phone Profile Configuration視窗中，按一下Apply Config以應用新的VPN配置。您可以使用標準的通用電話配置檔案或建立新配置檔案。





將常用電話配置檔案應用於IP電話

如果為特定電話/使用者建立了新配置檔案，請導航到電話配置視窗。在Common Phone Profile欄位中，選擇Standard Common Phone配置檔案。



在Cisco IP電話上安裝本地重要證書(LSC)

以下指南可用於在Cisco IP電話上安裝本地重要證書。 僅當使用LSC進行身份驗證時，才需要執行此步驟。 使用製造商安裝的證書(MIC)或使用者名稱和密碼進行身份驗證不需要安裝LSC。

將CUCM集群安全模式設定為「非安全」的電話上安裝LSC。

再次將電話註冊到Call Manager，以便下載新配置

這是組態過程中的最後一步。

驗證

路由器驗證

為了檢查路由器中VPN會話的統計資訊，可以使用以下命令，並檢查使用者名稱和證書身份驗證的輸出之間的差異（突出顯示）：

對於使用者名稱/密碼身份驗證：

<#root>

```
Router#

show webvpn session user phones context SSL


Session Type      : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username          :

phones

               Num Connection : 1
Public IP         : 172.16.250.34        VRF Name       : None
Context           : SSL                  Policy Group   : SSLPhones
Last-Used         : 00:00:29             Created        : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : SSL                  MTU Size       : 1290
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 10.10.10.1           Netmask        : 255.255.255.0
Rx IP Packets     : 106                  Tx IP Packets  : 145
CSTP Started      : 00:11:15             Last-Received  : 00:00:29
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Client Ports      : 51534
DTLS Port         : 52768
Router#

Router#

show webvpn session context all


WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used

phones

             172.16.250.34              1         00:30:38  00:00:20
```

對於證書身份驗證：

<#root>

```
Router#

show webvpn session user SEP8CB64F578B2C context all
```

```
Session Type      : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username          :
```

SEP8CB64F578B2C

```
      Num Connection : 1
Public IP         : 172.16.250.34        VRF Name       : None
```

CA Trustpoint : CAPF

```
Context           : SSL                  Policy Group   :
Last-Used         : 00:00:08             Created        : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : SSL                  MTU Size       : 1290
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 10.10.10.2           Netmask        : 255.255.255.0
Rx IP Packets     : 152                  Tx IP Packets  : 156
CSTP Started      : 00:06:44             Last-Received  : 00:00:08
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Client Ports      : 50122
DTLS Port         : 52932


Router#
```

show webvpn session context all

```
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
```

SEP8CB64F578B2C

```
    172.16.250.34              1         3d04h     00:00:16
```

CUCM驗證

確認IP電話已註冊到Call Manager，且其分配地址由路由器提供給SSL連線。

疑難排解

SSL VPN伺服器上的調試

<#root>

```
Router#
```

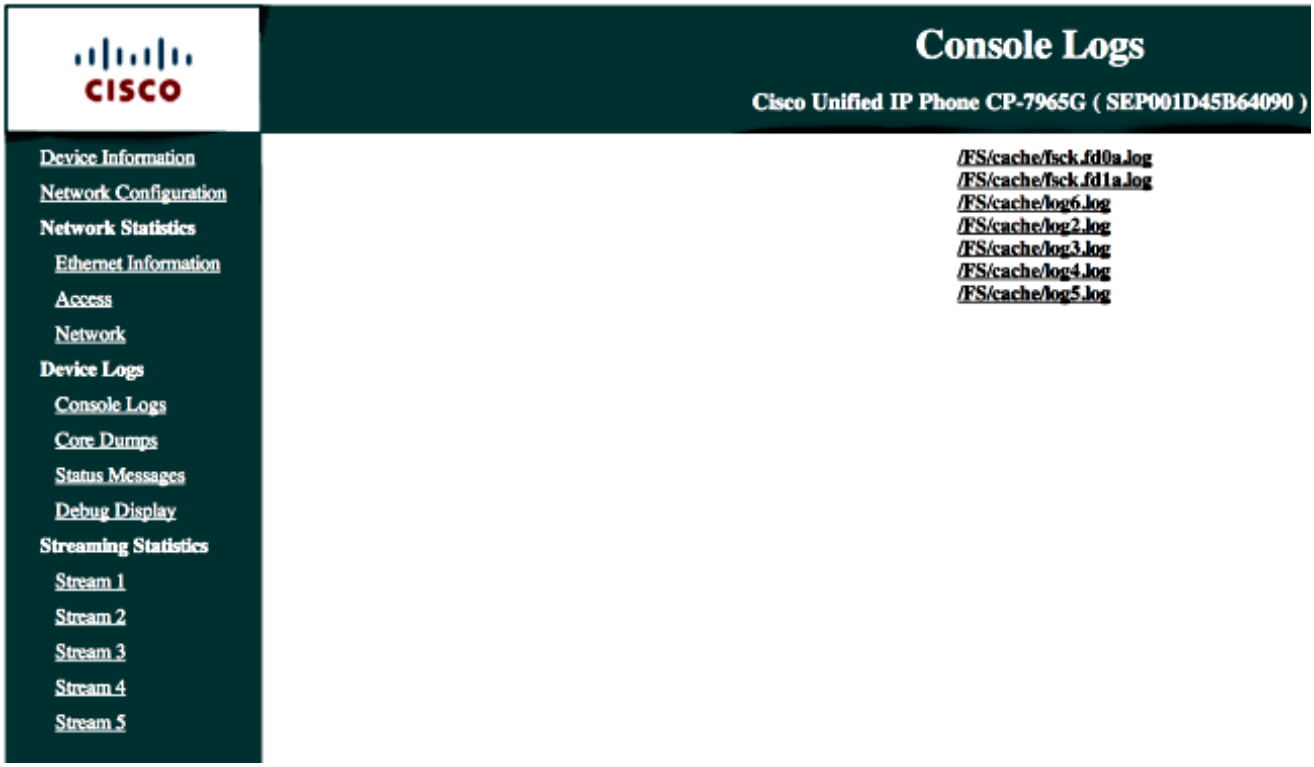
show debug

```
WebVPN Subsystem:
 WebVPN (verbose) debugging is on
 WebVPN HTTP debugging is on
 WebVPN AAA debugging is on
 WebVPN tunnel debugging is on
 WebVPN Tunnel Events debugging is on
 WebVPN Tunnel Errors debugging is on
 Webvpn Tunnel Packets debugging is on


PKI:
 Crypto PKI Msg debugging is on
 Crypto PKI Trans debugging is on
 Crypto PKI Validation Path debugging is on
```

電話調試

1. 從CUCM導航到Device > Phone。
2. 在裝置配置頁面上，將Web Access設定為Enabled。
3. 按一下「Save」，然後按一下「Apply Config」。

4. 在瀏覽器中，輸入電話的IP地址，然後從左側選單中選擇Console Logs。



5. 下載所有/FS/cache/log*.log文件。控制檯日誌檔案包含有關電話無法連線到VPN的原因的資訊。

相關錯誤

思科漏洞ID CSCty46387（僅限註冊使用者），IOS SSLVPN:將上下文設定為預設上下文的增強功能
思科漏洞ID CSCty46436（僅限註冊使用者），IOS SSLVPN:增強客戶端證書驗證行為

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）。