

配置VPN電話並對其進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[ASA配置](#)

[CUCM配置](#)

[疑難排解](#)

[要收集的資料](#)

[常見問題](#)

[更新ASA自簽名身份證書](#)

[ASA選擇橢圓曲線\(EC\)密碼](#)

[DTLS連線失敗](#)

[證書更新後電話無法連線到ASA](#)

[電話無法通過DNS解析ASA URL](#)

[電話不啟用VPN](#)

[電話註冊但無法顯示呼叫歷史記錄](#)

[相關資訊](#)

簡介

本文檔介紹如何配置Cisco IP電話和Cisco Unified Communications Manager的VPN電話功能並對其進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合通訊管理員(CUCM)
- 思科調適型安全裝置(ASA)
- AnyConnect虛擬私人網路(VPN)
- Cisco IP電話

採用元件

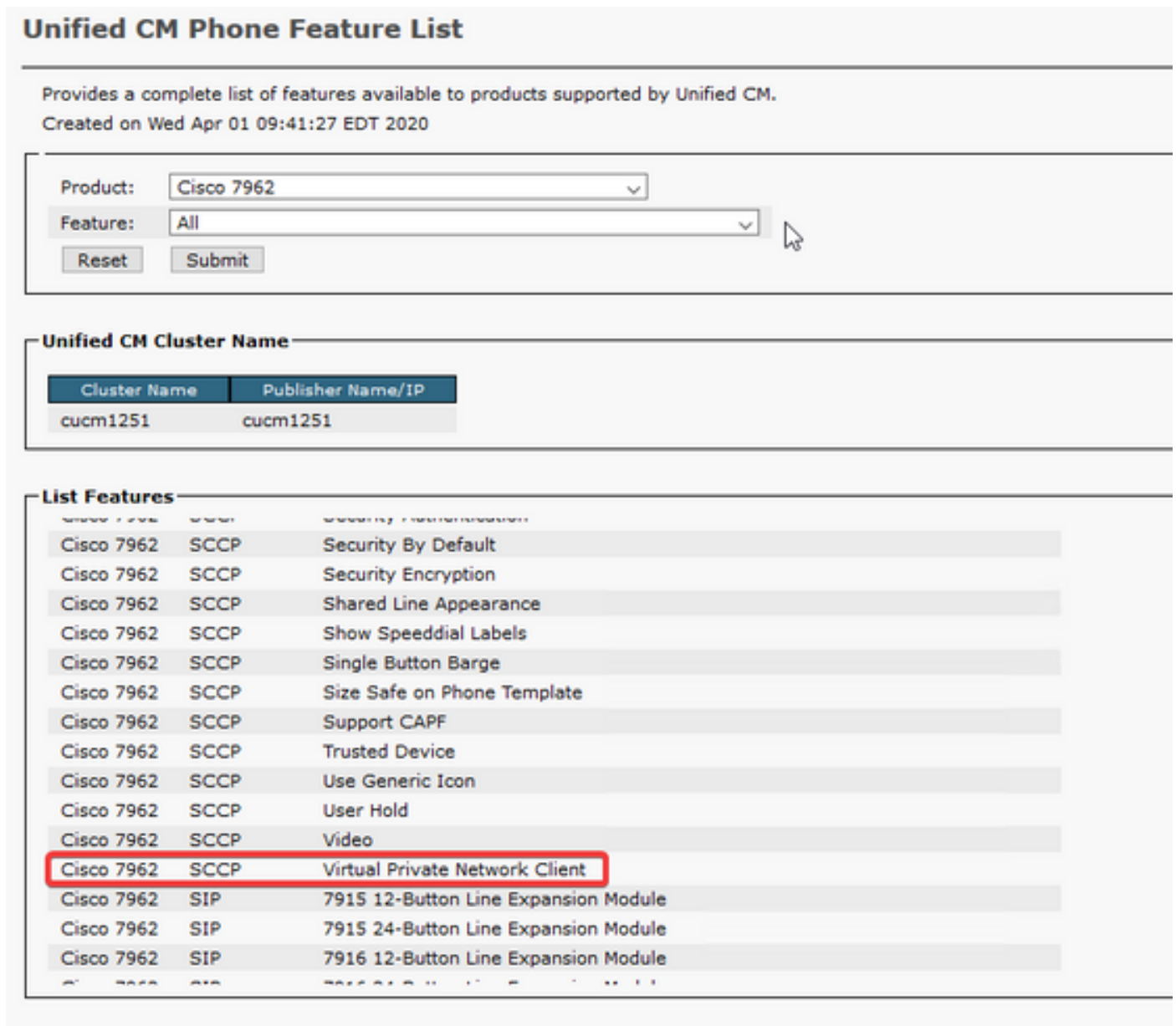
- 8861 14-0-1-0101-145
- ASAv 9.12(2)9

- CUCM 11.5.1.21900-40

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。

背景資訊

本文中的測試環境包括8861、ASA和CUCM 11.5.1，但您可以使用這些產品的許多不同變體。您必須檢查CUCM上的電話功能清單，以確保您的電話型號支援VPN功能。要使用電話功能清單，請在瀏覽器中訪問CUCM發佈者並導航至**Cisco Unified Reporting > Unified CM電話功能清單**。生成新報告，然後在下拉選單中選擇您的電話型號。接下來，您需要搜尋「List Features（列出功能）」部分以找到虛擬專用網路客戶端，如下圖所示：



Unified CM Phone Feature List

Provides a complete list of features available to products supported by Unified CM.
Created on Wed Apr 01 09:41:27 EDT 2020

Product: Cisco 7962
Feature: All
Reset Submit

Unified CM Cluster Name

Cluster Name	Publisher Name/IP
cucm1251	cucm1251

List Features

Product	Protocol	Feature Name
Cisco 7962	SCCP	Security By Default
Cisco 7962	SCCP	Security Encryption
Cisco 7962	SCCP	Shared Line Appearance
Cisco 7962	SCCP	Show Speeddial Labels
Cisco 7962	SCCP	Single Button Barge
Cisco 7962	SCCP	Size Safe on Phone Template
Cisco 7962	SCCP	Support CAPF
Cisco 7962	SCCP	Trusted Device
Cisco 7962	SCCP	Use Generic Icon
Cisco 7962	SCCP	User Hold
Cisco 7962	SCCP	Video
Cisco 7962	SCCP	Virtual Private Network Client
Cisco 7962	SIP	7915 12-Button Line Expansion Module
Cisco 7962	SIP	7915 24-Button Line Expansion Module
Cisco 7962	SIP	7916 12-Button Line Expansion Module

設定

VPN電話要求您在ASA和CUCM上有正確的配置。您可以先從任一產品開始，但本文檔首先介紹ASA配置。

ASA配置

步驟1.驗證ASA的許可是否支援適用於VPN電話的AnyConnect。 ASA上的show version命令可用於驗證是否已啟用適用於Cisco VPN電話的Anyconnect，如以下代碼片斷所示：

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

如果未啟用此功能，您需要與許可證團隊合作以獲得相應的許可證。 確認您的ASA支援VPN電話後，即可開始配置。

附註：配置部分中所有帶下劃線的專案都是可以更改的可配置名稱。 這些名稱大多會在配置中的其他位置引用，因此請務必記住您在這些部分（組策略、隧道組等）中使用的名稱，因為以後需要這些名稱。

步驟2.為VPN客戶端建立IP地址池。 這與DHCP池類似，因為IP電話連線到ASA時，它會收到來自此池的IP地址。 可以使用以下命令在ASA上建立池：

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0
```

此外，如果您偏好不同的網路或子網掩碼，則也可以更改。 建立池後，您需要配置組策略（ASA和IP電話之間的連線的一組引數）：

```
group-policy vpn-phone-policy internal
```

```
group-policy vpn-phone-policy 屬性
```

```
split-tunnel-policy tunnelall
```

```
vpn-tunnel-protocol ssl-client
```

步驟3.如果AnyConnect尚未啟用，則需要啟用它。 為此，您需要知道外部介面的名稱。 通常，此介面命名為**outside**（如代碼片斷所示），但它可以配置，因此請確保您具有正確的介面。運行show ip以檢視介面清單：

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
```

```
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

在此環境中，外部介面命名為**outside**，因此這些命令在該介面上啟用AnyConnect。

webvpn

```
enable outside
anyconnect enable
```

步驟4.配置新隧道組，以將之前建立的組策略應用到連線到特定URL的任何客戶端。請注意在代碼片段的第三行和第四行中引用您先前建立的IP地址池和組策略的名稱。如果修改了IP地址池或組策略的名稱，則需要使用修改後的名稱替換不正確的值：

```
tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
    address-pool vpn-phone-pool
    default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attributes
    驗證憑證
    group-url https://asav.sckiewer.lab/phone enable
```

您可以使用IP位址，而不是**group-url**的名稱。如果電話無權訪問可以解析ASA的完全限定域名(FQDN)的DNS伺服器，通常會發生這種情況。此外，您還可以看到此範例使用基於憑證的驗證。您也可以選擇使用使用者名稱/密碼身份驗證，但ASA上的其他要求不屬於本文檔的範圍。

在本例中，DNS伺服器具有A記錄**asav.sckiewer.lab - 172.16.1.250**，您可以從**show ip**輸出中看到，172.16.1.250是在名為**outside**的介面上配置的。因此配置如下：

```
crypto ca trustpoint asa-identity-cert
```

```
    註冊自我
```

```
    subject-name CN=asav.sckiewer.lab
```

```
crypto ca enroll asa-identity-cert
```

```
ssl trust-point asa-identity-cert outside
```

需要注意幾點：

1. 已建立一個名為**asa-identity-cert**的新信任點，並且已對其應用主題名稱。這將導致從此信任點生成的證書使用指定的使用者名稱
2. 接下來，「**crypto ca enroll asa-identity-cert**」命令允許ASA生成自簽名證書並將其儲存到該信任點
3. 最後，ASA將信任點中的證書提供給連線到外部介面的任何裝置

步驟5.建立必要的信任點以允許ASA信任IP電話的證書。首先，您需要確定IP電話是使用製造商安裝證書(MIC)還是使用本地有效證書(LSC)。預設情況下，所有電話均使用其MIC進行安全連線，除非其上安裝了LSC。在CUCM 11.5.1及更高版本中，您可以運行位於**Unified CM Administration > Device > Phone**的搜尋，以檢視是否安裝了LSC，而較舊版本的CUCM需要實際檢查每台電話上的安全設定。在CUCM 11.5.1中，請注意您需要將過濾器（或更改預設過濾器）新增到**LSC Issued By**。在**LSC Issued By**列中具有**NA**的裝置會使用MIC，因為它們未安裝LSC。

Phone	Device Name(Usa) *	Description	Extension	Owner User ID	LSC Status	LSC Expires	LSC Issued By	LSC Issuer Expires By	CAPF Auth String	Device P
	BCTAAAAAAAAAAAA				None	NA	NA	NA		SIP
	SEF3ED185528E	Auto 3010	3010		None	NA	NA	NA		SIP
	SEPSG124085CE	Auto 3006	43780		None	NA	NA	NA		SIP
	SEPSG3E18F2786	Auto 3009	3009		Troubleshoot Success	02/17/2025	CAPF-09992bf	06/01/2024		SIP
	SEDA849C33A3C	Auto 3013	3013		None	NA	NA	NA		SIP
	WCCX_7886	INITIAL_INBOUND_CCG-1			None	NA	NA	NA		SCCP

如果您的電話看起來與影象中突出顯示的電話類似，則需要將CUCM Publisher的CAPF證書上傳到ASA，以便ASA驗證電話證書以進行安全連線。如果您要使用未安裝LSC的裝置，則需要將思科製造證書上傳到ASA。這些證書可在CUCM Publisher的Cisco Unified OS Administration > Security > Certificate Management中找到：

附註：您可以看到這些證書中有一些位於多個信任儲存中（CallManager-trust和CAPF-trust）。只要確保選擇具有這些確切名稱的信任庫，就可以從哪個信任庫下載證書。

- Cisco_Root_CA_2048 < MIC SHA-1根
- Cisco_Manufacturing_CA < MIC SHA-1中繼
- Cisco_Root_CA_M2 < MIC SHA-256根
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256中繼
- 來自CUCM發佈者< LSC的CAPF

Certificate *	Common Name	Type	Distribution	Issued By
CAPF	CAPF-bf1846f2	Self-signed	CAPF-bf1846f2	CAPF-bf1846f2

關於MIC，較舊的電話型號（如79xx和99xx系列）使用SHA-1證書鏈，而較新的電話型號（如88xx系列）使用SHA-256證書鏈。您的電話使用的證書鏈需要上傳到ASA。

一旦您擁有所需的證書，您就可以使用以下工具建立信任點：

`crypto ca trustpoint cert1`

註冊終端

`crypto ca authenticate cert1`

第一個命令建立名為cert1的信任點，`crypto ca authenticate`命令允許您將base64編碼的證書貼上到CLI中。您可以根據需要多次運行這些命令，以便在ASA上獲取適當的信任點，但請確保為每個證書使用新的信任點名稱。

步驟6.發出以下命令獲取ASA身份證書的副本：

`crypto ca export asa-identity-cert identity-certificate`

這會匯出名為asa-identity-cert的信任點的身份證書。請務必調整名稱，使其與您在步驟4中建立的信任點匹配。

以下是ASA的完整實驗配置：

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
    split-tunnel-policy tunnelall
    vpn-tunnel-protocol ssl-client

webvpn
    enable outside
    anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
    address-pool vpn-phone-pool
    default-group-policy vpn-phone-policy

tunnel-group vpn-phone-group webvpn-attributes
    authentication certificate
    group-url https://asav.sckiewer.lab/phone enable

ssl trust-point asa-identity-cert outside
```

此時，ASA配置已完成，您可以繼續配置CUCM。 您需要具有剛收集的ASA證書的副本以及在 tunnel-group 部分配置的URL。

CUCM配置

步驟1.在CUCM上，導航到Cisco Unified OS Administration > Security > Certificate Management，然後以phone-vpn-trust身份上傳ASA證書。

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR

Status

1 records found

Certificate List (1 - 1 of 1)

Find Certificate List where Certificate begins with phone-vpn Find Clear Filter + -

Certificate	Common Name	Type
Phone-VPN-trust	asav.sckiewer.lab	Self-signed

Generate Self-signed Upload Certificate/Certificate chain Download CTL Generate CSR




步驟2.完成此操作後，導航到Cisco Unified CM管理>高級功能> VPN > VPN配置檔案，然後建立新的配置檔案。 此部分沒有正確或錯誤，瞭解每個設定的用途非常重要。

1. 啟用Auto Network Detect — 啟用此功能後，電話會在通電時對TFTP伺服器執行ping操作。如果收到對此ping的響應，則不會啟用VPN。如果電話未收到對此ping的響應，則會啟用VPN。啟用此設定後，無法手動啟用VPN。
2. 主機ID檢查 — 啟用此功能時，電話會從其配置檔案(本文檔中使用了


<https://asav.sckiewer.lab/phone>)中檢查VPN URL，並確保主機名或FQDN與ASA提供的證書中的公用名(CN)或SAN條目匹配。

3. **Authentication Method** — 控制用於連線到ASA的身份驗證方法的型別。在本文檔的配置示例中，使用基於證書的身份驗證。
4. **密碼持續性** — 如果此選項處於啟用狀態，客戶端的密碼將儲存在電話中，直到嘗試登入失敗、客戶端手動清除密碼或電話重置。

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

Save Delete Copy Add New

步驟3.接下來，導覽至Cisco Unified CM Administration > Advanced Features > VPN > VPN Gateway。您需要確保VPN網關URL與ASA配置匹配，並將證書從頂部框移動到底部框，如下圖所示：

VPN Gateway Configuration

Save

Status
 Status: Ready

VPN Gateway Information
 VPN Gateway Name* asav.sckiewer.lab
 VPN Gateway Description
 VPN Gateway URL* https://asav.sckiewer.lab/phone

VPN Gateway Certificates
 VPN Certificates in your Truststore
 VPN Certificates in this Location* SUBJECT: 2.5.4.5=#130b394144563639334c50454c+1.2.840.113549.1.9.2=#160d73636b69657765722d4153417

步驟4.儲存後，您需要導航到Cisco Unified CM管理>高級功能> VPN > VPN組，並將您建立的網關移動到「在此VPN組中選定的VPN網關」框中：

VPN Group Configuration

Save

Status
 Status: Ready

VPN Group Information
 VPN Group Name* asav.sckiewer.lab
 VPN Group Description

VPN Gateway Information
 All Available VPN Gateways
 Selected VPN Gateways in this VPN Group: asav.sckiewer.lab

步驟5.現在已配置VPN設定，您需要導航到Cisco Unified CM管理> Device > Device Settings > Common Phone Profile。在此，您必須複製所需的VPN電話使用的配置檔案，重新命名它，然後選擇您的VPN組和VPN配置檔案，然後儲存新配置檔案：

Common Phone Profile Configuration



Save

Status



Status: Ready

Common Phone Profile Information

Name*	<input type="text" value="Standard Common Phone Profile - VPN_Auto-On"/>
Description	<input type="text" value="Standard Common Phone Profile - VPN_Auto-On"/>
Local Phone Unlock Password	<input type="text"/>
DND Option*	<input type="text" value="Ringer Off"/>
DND Incoming Call Alert*	<input type="text" value="Beep Only"/>
Feature Control Policy	<input type="text" value="< None >"/>
Wi-Fi Hotspot Profile	<input type="text" value="< None >"/> View Details

Enable End User Access to Phone Background Image Setting

Secure Shell Information

Secure Shell User	<input type="text"/>
Secure Shell Password	<input type="text"/>

Phone Personalization Information

Phone Personalization*	<input type="text" value="Default"/>
Always Use Prime Line*	<input type="text" value="Default"/>
Always Use Prime Line for Voice Message*	<input type="text" value="Default"/>
Services Provisioning*	<input type="text" value="Default"/>

VPN Information

VPN Group	<input type="text" value="VPN_Group_1"/>
VPN Profile	<input type="text" value="VPN_Profile"/>

步驟6。最後，您需要將此新配置檔案應用到您的電話，然後在電話處於內部網路時重置電話。這樣，電話就可以接收所有這些新配置，例如ASA證書雜湊和VPN URL。

附註：測試電話之前，您需要確保電話配置有「備用TFTP」伺服器。由於ASA不為電話提供選項150，因此需要在電話上手動配置TFTP IP。

步驟7.測試VPN電話並驗證其能否成功連線到ASA並進行註冊。您可以使用`show vpn-sessiondb anyconnect`:

```
sckiewer-ASAv# show vpn-sessiondb anyconnect
Session Type: AnyConnect
Username      : CP-8841-SEP682C7B40B5CE
Index        : 3
Assigned IP   : 10.10.1.131      Public IP    : 192.168.1.52
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption    : AnyConnect-Parent: (1)AES256 SSL-Tunnel: (1)AES256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 4275771          Bytes Rx     : 32476192
Group Policy  : VPN-Phone        Tunnel Group : VPN-Phone
Login Time    : 01:07:39 UTC Fri Mar 27 2020
Duration      : 4d 1h:56m:42s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A              VLAN         : none
Audt Sess ID  : 0e3051fa000030005e7d51db
Security Grp  : none
```

疑難排解

要收集的資料

為了對VPN電話問題進行故障排除，建議使用以下資料：

- ASA調試：logging buffered debuglogging debug-tracedebug crypto ca transactions 255debug crypto ca messages 255debug crypto ca 255debug webvpn 255debug webvpn anyconnect 255
- 電話控制檯日誌(如果電話支援，則為PRT — 此處提供更多[資訊](#))

在啟用調試後重現問題後，您可以使用此命令檢視輸出，因為debug輸出始終包含711001:

顯示日誌 | i 711001

常見問題

附註：在本節中，日誌片段來自8861電話，因為它是部署為VPN電話的較常見電話系列之一。請記住，其他型號可以在日誌中寫入不同的資訊。

更新ASA自簽名身份證書

在ASA身份證書到期之前，需要生成新證書並將其推送到電話。為了在不影響VPN電話的情況下完成此操作，請使用以下過程：

步驟1.為新身份證書建立新的信任點：

```
crypto ca trustpoint asa-identity-cert-2
```

註冊自我

```
subject-name CN=asav.sckiewer.lab
```

crypto ca enroll asa-identity-cert-2

步驟2.此時，您將會有用於ASA的新身份證書，但尚未在任何介面上使用。 您需要匯出此新證書並將其上傳到CUCM:

crypto ca export asa-identity-cert-2 identity-certificate

步驟3.一旦您擁有新的身份證書，請將其以Cisco Unified OS Administration > Security > Certificate Management > Upload上的phone-VPN-trust形式上傳到您的CUCM節點之一。

附註：當前的phone-VPN信任證書將只存在於最初上傳到的CUCM節點上（不會自動傳播到其他節點，如某些證書）。 如果CUCM版本受[CSCuo58506](#)影響，則必須將新的ASA證書上傳到其他節點。

步驟4.將新證書上傳到群集中的任何節點後，在CUCM發佈伺服器上導航到Cisco Unified CM管理 >高級功能> VPN > VPN網關

步驟5.選擇適當的網關。

步驟6.選擇頂部框（這是您剛剛上傳的證書）中的證書，然後選擇向下箭頭將其移至底部（這允許TFTP將該證書新增到VPN電話的配置檔案中）並選擇「儲存」。

步驟7.完成後，重置所有VPN電話。 在此過程的此刻，ASA仍顯示舊證書，因此電話可以連線，但電話獲取的新配置檔案包含新證書和舊證書。

步驟8.現在您可以將新證書應用到ASA。 為此，您需要新信任點的名稱和外部介面的名稱，然後使用以下資訊運行此命令：

ssl trust-point asa-identity-cert-2 outside

附註：您可以在瀏覽器中導航到webvpn URL以驗證ASA是否顯示新證書。 由於外部電話必須能夠公開訪問該地址，因此您的PC也可以訪問該地址。 然後，您可以檢查ASA提供給您的瀏覽器的證書，並確認它是新證書。

步驟9.將ASA配置為使用新證書後，重置測試電話並驗證其是否能夠連線到ASA並進行註冊。 如果電話成功註冊，則您可以重置所有電話並驗證它們是否能夠連線到ASA並進行註冊。 這是推薦的過程，因為證書更改後，連線到ASA的電話保持連線。 如果首先在一部電話上測試證書更新，則可以降低配置問題影響大量電話的風險。 如果第一個VPN電話無法連線到ASA，則可以從電話和/或ASA收集日誌，以便在其他電話保持連線時進行故障排除。

步驟10.驗證電話能夠連線並註冊新證書後，即可從CUCM中刪除舊證書。

ASA選擇橢圓曲線(EC)密碼

自9.4(x)起，ASA支援橢圓曲線(EC)加密技術，因此在ASA升級到9.4(x)或更高版本後，經常可以看到以前工作的VPN電話出現故障。 出現這種情況的原因是ASA現在在與較新的電話型號進行TLS握手期間選擇EC密碼。 通常，有一個RSA證書與電話所連線的介面相關聯，因為以前的ASA版本不支援EC。 此時，由於ASA已選擇EC密碼，因此它無法使用RSA證書進行連線，因此它生成並傳送電話臨時自簽名證書，該證書是使用EC演算法而不是RSA建立的。 由於電話無法識別此臨時證書，因此連線失敗。 您可以在88xx電話日誌中驗證這一點。

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
```

電話日誌顯示，ASA為此連線選擇了一個EC密碼，因為「新密碼」行包含導致連線失敗的EC密碼。

在選擇了AES的情況下，您會看到：

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-
SHA:AES128-SHA
```

有關此問題的詳細資訊，請參閱[CSCuu02848](#)。

此問題的解決方法是針對您的電話使用的TLS版本，禁用ASA上的EC密碼。有關每種電話型號支援的TLS版本的更多資訊，請訪問以下網址：

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

Version	Phone Models			
	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware
 ** With 12.5 firmware

<https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf>

一旦您知道您的環境中哪些TLS版本相關，您就可以在ASA上運行以下命令來禁用這些版本的EC密碼：

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
```

請記住，IP電話預設使用DTLS（資料包傳輸層安全），因此您需要為DTLS運行密碼語句，並為您的電話運行相關TLS版本。此外，重要的是要瞭解這些更改是ASA上的全域性更改，因此它們阻止

使用這些TLS版本的任何其他AnyConnect客戶端協商EC密碼。

DTLS連線失敗

在某些情況下，VPN電話無法使用DTLS建立與ASA的連線。如果電話嘗試使用DTLS但失敗，則電話會繼續反複嘗試DTLS，未成功，因為它知道啟用了DTLS您將在88xx電話日誌中看到以下內容：

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
fatal:illegal parameter
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000
status: 0x0 error: 0x0
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal
parameter
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1,
error 1
3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL
routines:ssl3_get_server_hello:old session cipher not returned
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,
cleanup
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
warning:close notify
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect
failed
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success
DTLS fail
```

這可能是由於ASA選擇橢圓曲線(EC)密碼部分中提到的相同問題造成的，因此您必須確保為DTLS禁用了EC密碼。除此之外，您可以完全禁用DTLS，從而迫使VPN電話改用TLS。這不是理想的，因為這意味著所有流量都將使用TCP而不是UDP，這會增加一些開銷。但是，在某些情況下，這是一個好的測試，因為它至少可以確認大多數配置都正常，並且此問題特定於DTLS。如果您想進行測試，最好在組策略級別進行測試，因為管理員通常對VPN電話使用唯一的組策略，因此我們可以在不影響其他客戶端的情況下測試更改。

group-policy vpn-phone-policy屬性

webvpn

anyconnect ssl dtls none

另一個可能會阻止DTLS連線成功的常見配置問題是如果電話無法使用相同的密碼建立TLS和DTLS連線。日誌摘錄示例：

```
##### TLS Ciphers Offered
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA

##### DTLS Ciphers Offered
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA

##### DTLS connection failure
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093,
to abort connect
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase
```

您可以在代碼片段的首行中看到TLS密碼。選擇兩端支援的最安全選項（日誌不顯示選擇，但您可以推斷日誌片段至少為AES-256）。您還可以看到唯一提供的DTLS密碼是AES128。由於選定的

TLS密碼不可用於DTLS，連線失敗。此場景中的修復方案是確保ASA配置允許對TLS和DTLS使用相同的密碼。

證書更新後電話無法連線到ASA

在CUCM上以phone-vpn-trust身份上傳新的ASA身份證書非常重要，這樣電話才能獲取該新證書的雜湊。如果未遵循此過程，則在更新後以及下次VPN電話嘗試連線到ASA時，電話會收到其不信任的證書，因此連線失敗。這有時會在ASA證書更新後的幾天或幾週內發生，因為證書更改時電話不會斷開。只要ASA繼續從電話接收keepalive，VPN隧道就會保持運行。因此，如果您已確認ASA證書已更新，但新證書未首先放在CUCM上，則有兩個選項：

1. 如果舊ASA身份證書仍然有效，請將ASA恢復為舊證書，然後按照本文檔中提供的過程更新證書。如果已經生成了新證書，則可以跳過證書生成部分。
2. 如果舊ASA身份證書已過期，您需要將新ASA證書上傳到CUCM並將電話帶回內部網路，以接收帶有新證書雜湊的更新配置檔案。

電話無法通過DNS解析ASA URL

在某些情況下，管理員使用主機名而不是IP地址配置VPN URL。完成此操作後，電話需要有一個DNS伺服器才能將該名稱解析為IP地址。在代碼片段中，您可以看到電話嘗試用其兩個DNS伺服器（192.168.1.1和192.168.1.2）解析名稱，但沒有收到響應。30秒後，電話將列印「DnsLookupErr：」

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

這通常表示以下情況之一：

1. 電話的DNS伺服器無效
2. 電話沒有通過DHCP接收DNS伺服器，或者沒有手動配置

要解決此問題，有兩種方法：

1. 檢查電話上的配置，確保電話在外部時從DHCP伺服器接收DNS伺服器，和/或驗證電話的

DNS伺服器是否可以解析ASA配置中使用的名稱

2. 將ASA配置中的URL和CUCM更改為IP地址，以便不需要DNS

電話不啟用VPN

如本文檔前面所述，自動網路檢測導致電話ping TFTP伺服器並檢查響應。如果電話位於內部網路上，則不使用VPN即可訪問TFTP伺服器，因此當電話收到對ping的響應時，它不會啟用VPN。當電話不在內部網路時，ping會失敗，因此電話將啟用VPN並連線到ASA。請記住，客戶端的家庭網路可能不會配置為通過DHCP為電話提供選項150，而ASA也不能提供選項150，因此「備用TFTP」是VPN電話的一項要求。

在日誌中，您需要驗證以下幾點：

1. 電話ping CUCM TFTP伺服器IP嗎？
2. 電話是否收到對ping的響應？
3. 電話在未收到對ping的響應後是否啟用VPN？

必須按此順序檢視這些專案。在電話ping錯誤的IP並接收響應的情況下，在ASA上啟用調試毫無意義，因為電話不會啟用VPN。按以下順序驗證這3項內容，以便防止不必要的日誌分析。如果ping失敗，且之後啟用了VPN，您將在88xx電話日誌中看到以下內容：

```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

電話註冊但無法顯示呼叫歷史記錄

確認電話已啟用備用TFTP並配置了正確的TFTP IP。VPN電話需要備用TFTP，因為ASA無法提供選項150。

相關資訊

- [技術支援與文件 - Cisco Systems](#)