

AnyConnect VPN電話故障排除 — IP電話、ASA和CUCM

目錄

[簡介](#)

[背景資訊](#)

[確認ASA上的VPN電話許可證](#)

[匯出受限和匯出非受限CUCM](#)

[ASA上的常見問題](#)

[ASA上使用的證書](#)

[ASA匯出和CUCM匯入的信任點/證書](#)

[ASA提供ECDSA自簽名證書，而不是配置的RSA證書](#)

[用於IP電話使用者身份驗證的外部資料庫](#)

[ASA證書和VPN電話信任清單之間的證書雜湊匹配](#)

[檢查SHA1雜湊](#)

[下載IP電話配置檔案](#)

[解碼雜湊](#)

[VPN負載平衡和IP電話](#)

[CSD和IP電話](#)

[ASA日誌](#)

[ASA調試](#)

[DAP規則](#)

[從DfltGrpPolicy或其他組繼承的值](#)

[支援的加密密碼](#)

[CUCM上的常見問題](#)

[VPN設定未應用於IP電話](#)

[憑證驗證方法](#)

[主機ID檢查](#)

[其他疑難排解](#)

[要在ASA中使用的日誌和調試](#)

[IP電話日誌](#)

[ASA日誌和IP電話日誌之間的相關問題](#)

[ASA日誌](#)

[電話日誌](#)

[Span到PC連線埠功能](#)

[通過VPN連線時的IP電話配置更改](#)

[續訂ASA SSL證書](#)

簡介

本文描述如何對使用安全套接字層(SSL)協定 (Cisco AnyConnect安全移動客戶端) 的IP電話進行故障排除，以便連線到用作VPN網關的Cisco Adaptive Security Appliance(ASA)，以及連線到用作語音伺服器的Cisco Unified Communications Manager(CUCM)。

有關帶VPN電話的AnyConnect的配置示例，請參閱以下文檔：

- [使用IP電話的SSLVPN配置示例](#)
- [使用證書身份驗證的AnyConnect VPN電話配置示例](#)

背景資訊

在通過IP電話部署SSL VPN之前，請確認您已滿足以下對於ASA的AnyConnect許可證和美國匯出受限版本的CUCM的初始要求。

確認ASA上的VPN電話許可證

VPN電話許可證在ASA中啟用該功能。若要確認可與AnyConnect連線的使用者數量（無論其是否為IP電話），請檢查AnyConnect Premium SSL許可證。請參閱[IP電話和移動VPN連線需要哪種ASA許可證？](#)瞭解更多詳情。

在ASA上，使用**show version**命令檢查功能是否已啟用。許可證名稱與ASA版本不同：

- ASA 8.0.x版：許可證名稱是Linksys電話的AnyConnect。
- ASA 8.2.x及更高版本：許可證名稱為AnyConnect for Cisco VPN Phone。

以下是ASA 8.0.x版的示例：

```
ASA5505(config)# show ver
```

```
Cisco Adaptive Security Appliance Software Version 8.0(5)
```

```
Device Manager Version 7.0(2)
<snip>
Licensed features for this platform:
VPN Peers : 10
WebVPN Peers : 2
AnyConnect for Linksys phone : Disabled
<snip>
This platform has a Base license.
```

以下是ASA 8.2.x及更高版本的示例：

```
ASA5520-C(config)# show ver

Cisco Adaptive Security Appliance Software Version 9.1(1)
Device Manager Version 7.1(1)
<snip>
Licensed features for this platform:
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
<snip>
This platform has an ASA 5520 VPN Plus license.
```

匯出受限和匯出非受限CUCM

您應該為VPN電話功能部署美國匯出限制版本的CUCM。

如果您使用美國匯出非受限版本的CUCM，請注意：

- 修改IP電話安全配置以禁用信令和媒體加密；其中包括VPN電話功能提供的加密。
- 無法通過匯入/匯出匯出VPN詳細資訊。
- 不顯示VPN配置檔案、VPN網關、VPN組和VPN功能配置的覈取方塊。

附註：一旦升級到美國出口限制版CUCM，您就不能以後升級至此軟體的美國出口限制版或執行此軟體的新安裝。

ASA上的常見問題

附註：您可以使用[Cisco CLI Analyzer](#)(僅供已註冊客戶使用)檢視show指令輸出的分析。使用debug指令之前，您還應先參閱[有關Debug指令](#)的重要資訊思科檔案。

ASA上使用的證書

在ASA上，您可以使用自簽名SSL證書、第三方SSL證書和萬用字元證書；其中任何一種方法都可以保護IP電話和ASA之間的通訊。

只能使用一個身份證書，因為每個介面只能分配一個證書。

對於第三方SSL證書，請在ASA中安裝完整的鏈結，並包括所有中間和根證書。

ASA匯出和CUCM匯入的信任點/證書

ASA在SSL協商期間向IP電話提供的證書必須從ASA匯出並匯入到CUCM。檢查分配給IP電話所連線的介面的信任點，以便知道從ASA匯出哪個證書。

使用show run ssl命令以驗證要匯出的信任點（證書）。有關詳細資訊，請參閱[帶證書身份驗證的AnyConnect VPN電話配置示例](#)。

附註：如果已將第三方證書部署到一個或多個ASA，則您需要從每個ASA匯出每個身份證書，然後將其作為phone-vpn-trust匯入到CUCM。

ASA提供ECDSA自簽名證書，而不是配置的RSA證書

發生此問題時，較新的型號電話無法連線，而較舊的型號電話沒有任何問題。以下是發生此問題時電話上的日誌：

```

VPNC: -protocol_handler: SSL dpd 30 sec from SG (enabled)
VPNC: -protocol_handler: connect: do_dtls_connect
VPNC: -do_dtls_connect: udp_connect
VPNC: -udp_connect: getsockname failed
VPNC: -udp_connect: binding sock to eth0 IP 63.85.30.39
VPNC: -udp_connect: getsockname failed
VPNC: -udp_connect: connecting to 63.85.30.34:443
VPNC: -udp_connect: connected to 63.85.30.34:443
VPNC: -do_dtls_connect: create_dtls_connection
VPNC: -create_dtls_connection: cipher list: AES256-SHA
VPNC: -create_dtls_connection: calling SSL_connect in non-block mode
VPNC: -dtls_state_cb: DTLS: SSL_connect: before/connect initialization
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 write client hello A
VPNC: -dtls_state_cb: DTLS: SSL_connect: DTLS1 read hello verify request A
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 write client hello A
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 flush data
VPNC: -dtls_state_cb: DTLS: write: alert: fatal:illegal parameter
VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status: 0x0 error: 0x0
VPNC: -alert_err: DTLS write alert: code 47, illegal parameter
VPNC: -create_dtls_connection: SSL_connect ret -1, error 1
VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
VPNC: -DTLS: SSL_connect: error:140920C5:SSL routines:SSL3_GET_SERVER_HELLO:
old session cipher not returned VPNC: -create_dtls_connection: DTLS setup failure, cleanup VPNC:
-do_dtls_connect: create_dtls_connection failed VPNC: -protocol_handler: connect:
do_dtls_connect failed VPNC: -protocol_handler: connect : err: SSL success DTLS fail

```

在9.4.1及更高版本中，SSL/TLS支援橢圓曲線加密。當支援橢圓曲線的SSL VPN客戶端（例如新的電話型號）連線到ASA時，會協商橢圓曲線密碼套件，並且ASA向SSL VPN客戶端提供橢圓曲線證書，即使對應的介面配置了基於RSA的信任點時也是如此。為了防止ASA呈現自簽名的SSL證書，管理員必須刪除通過**ssl cipher**命令對應的密碼套件。例如，對於使用RSA信任點配置的介面，管理員可以執行此命令，以便僅協商基於RSA的密碼：

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA"
```

實施思科錯誤ID [CSCuu02848](#)後，會優先考慮配置。始終使用顯式配置的證書。自簽名證書僅在沒有配置證書的情況下使用。

建議的客戶端密碼	僅限RSA證書	僅EC證書	兩個證書	無
僅限RSA密碼	使用RSA證書	使用RSA自簽名證書	使用RSA證書	使用RSA自簽名證書
	使用RSA密碼	使用RSA密碼	使用RSA密碼	使用RSA密碼
僅限EC密碼（稀有）	連線失敗	使用EC證書	使用EC證書	使用EC自簽名證書
		使用EC密碼	使用EC密碼	使用EC密碼
僅兩個密碼	使用RSA證書	使用EC證書	使用EC證書	使用EC自簽名證書
	使用RSA密碼	使用EC密碼	使用EC密碼	使用EC密碼

用於IP電話使用者身份驗證的外部資料庫

您可以使用外部資料庫對IP電話使用者進行身份驗證。輕型目錄訪問協定(LDAP)或遠端身份驗證撥入使用者服務(RADIUS)等協定可用於VPN電話使用者的身份驗證。

ASA證書和VPN電話信任清單之間的證書雜湊匹配

請記住，您必須下載分配到ASA SSL介面的證書，並在CUCM中將其上傳為Phone-VPN-Trust證書。不同情況可能會導致ASA提供的此證書的雜湊與CUCM伺服器生成的雜湊不匹配，並通過配置檔案推入VPN電話。

配置完成後，測試IP電話和ASA之間的VPN連線。如果連線繼續失敗，請檢查ASA證書的雜湊是否與IP電話預期的雜湊匹配：

1. 檢查ASA提供的安全雜湊演算法1(SHA1)雜湊。
2. 使用TFTP從CUCM下載IP電話配置檔案。
3. 解碼從十六進位制到基本64或從基本64到十六進位制的雜湊。

檢查SHA1雜湊

ASA在IP電話連線的介面上顯示使用`ssl trustpoint`命令應用的證書。要檢查此證書，請開啟瀏覽器（在本例中為Firefox），然後輸入電話應該連線的URL(`group-url`):

Page Info - https://10.198.16.140/+CSCOE+/logon.html?fcadbadd=1

General Media Permissions **Security**

Website Identity

Website: 10.198.16.140

Owner: This website does not supply ownership information.

Verified by: ASA Temporary Self Signed Certificate

2 View Certificate

Certificate Viewer: "ASA Temporary Self Signed Certificate"

General Details

Could not verify this certificate for unknown reasons.

Issued To

Common Name (CN)	ASA Temporary Self Signed Certificate
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	DF:F2:C4:50

Issued By

Common Name (CN)	ASA Temporary Self Signed Certificate
Organization (O)	ASA Temporary Self Signed Certificate
Organizational Unit (OU)	<Not Part Of Certificate>

Validity

Issued On	12/09/2012
Expires On	12/07/2022

Fingerprints

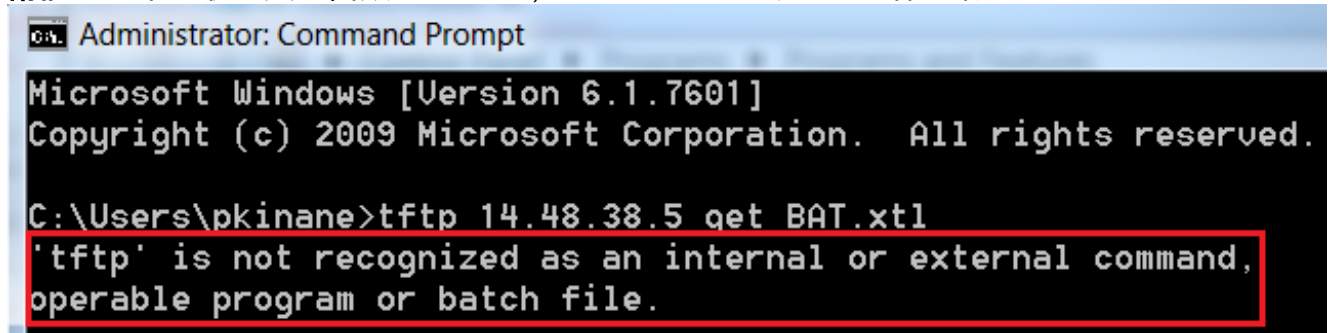
3 SHA1 Fingerprint	E5:7E:81:EA:99:54:C1:44:97:66:78:D0:E2:41:8C:DF:79:A9:31:76
MD5 Fingerprint	D7:10:78:FB:61:A2:F6:C2:01:07:6C:03:0E:17:EF:F9

下載IP電話配置檔案

從直接訪問CUCM的PC下載電話的TFTP配置檔案，以解決連線問題。有兩種下載方法：

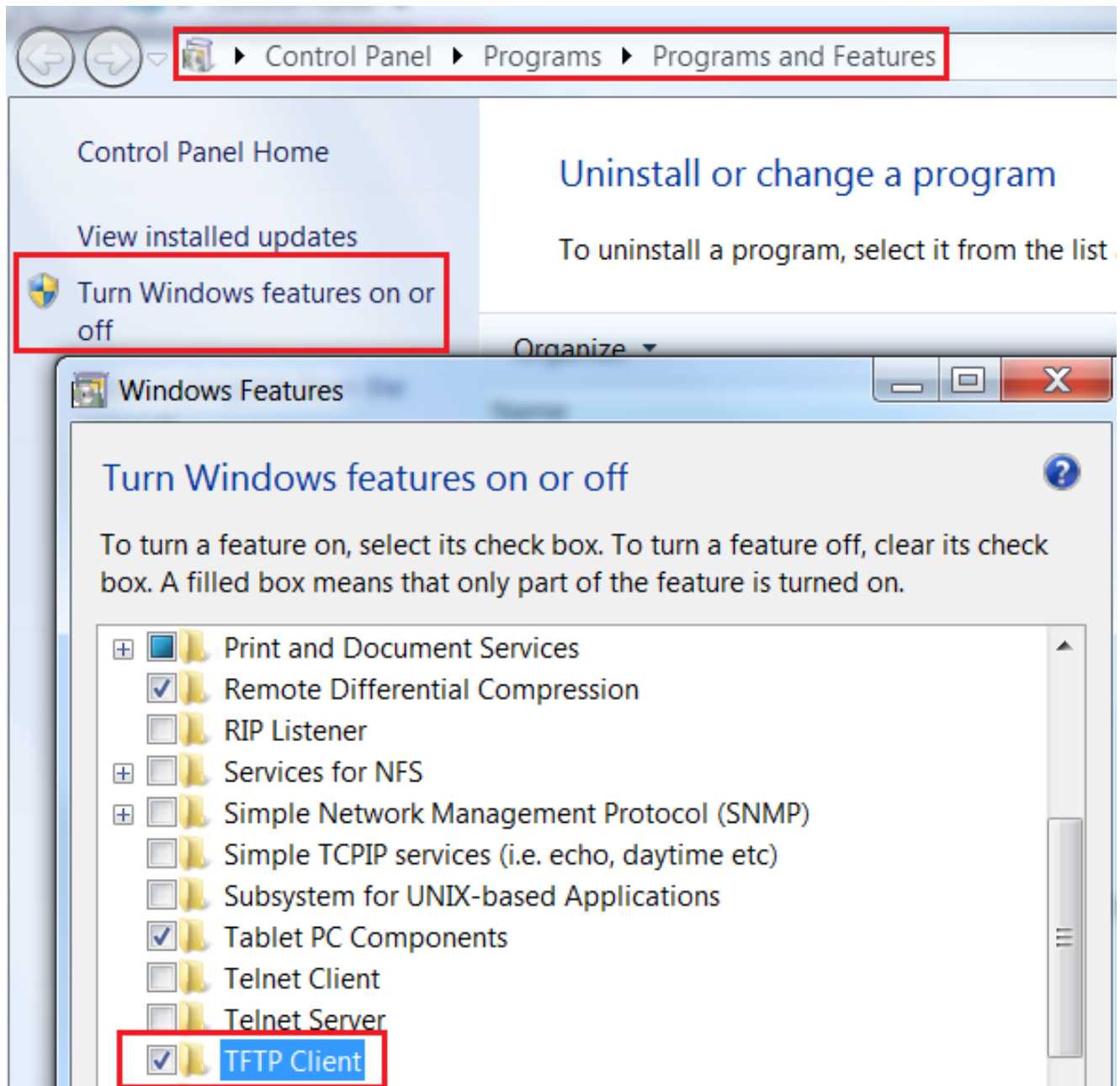
1. 在Windows中開啟CLI會話，並使用 `tftp -i <TFTP Server> GET SEP<Phone Mac Address>.cnf.xml` 命令。

附註：如果您收到與下面類似的錯誤，您應該確認已啟用TFTP客戶端功能。

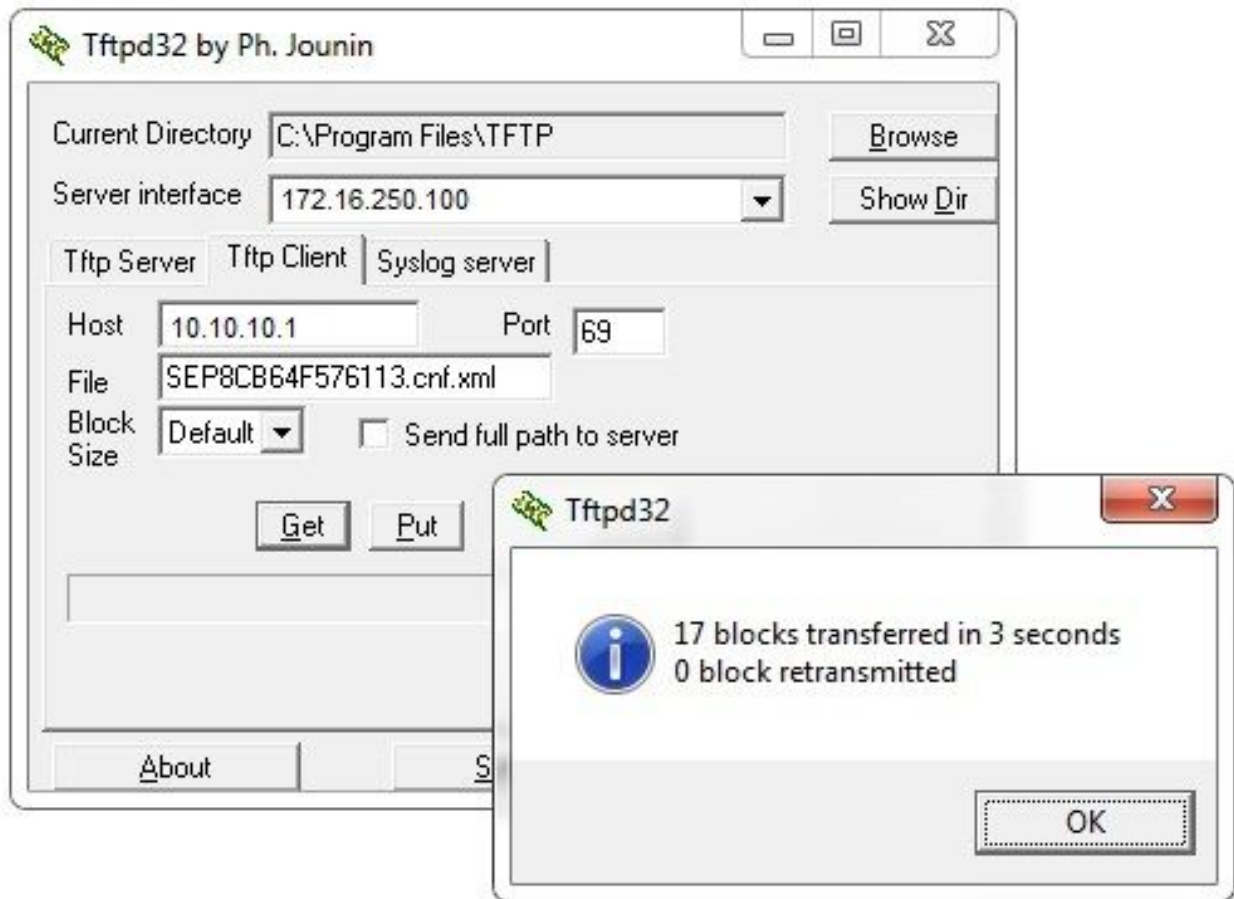


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\pkinane>tftp 14.48.38.5 get BAT.xml
'tftp' is not recognized as an internal or external command,
operable program or batch file.
```



2. 使用 [Tftpd32](#) 等應用程式下載檔案：



3. 下載檔案後，開啟XML並找到`vpnGroup`配置。此示例顯示要驗證的section和`certHash`:

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>0</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.198.16.140/VPNPhone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>

</credentials>
</vpnGroup>
```

解碼雜湊

確認兩個雜湊值匹配。瀏覽器以十六進位制格式顯示雜湊，而XML檔案使用base 64，因此將一種

格式轉換為另一種格式以確認匹配。有許多翻譯員；例如[TRANSLATOR](#)、[BINARY](#)。



附註：如果以前的雜湊值不匹配，則VPN電話不信任與ASA協商的連線，並且連線失敗。

VPN負載平衡和IP電話

VPN電話不支援負載平衡SSL VPN。VPN電話不執行真正的證書驗證，而是使用CUCM向下推送的雜湊來驗證伺服器。因為VPN負載平衡基本上是HTTP重定向，所以它要求電話驗證多個證書，從而導致失敗。VPN負載平衡失敗的症狀包括：

- 電話在伺服器之間交替，需要花費異常長的時間進行連線或最終出現故障。
- 電話日誌包含如下消息：

```
909: NOT 20:59:50.051721 VPNC: do_login: got login response
910: NOT 20:59:50.052581 VPNC: process_login: HTTP/1.0 302 Temporary moved
911: NOT 20:59:50.053221 VPNC: process_login: login code: 302 (redirected)
912: NOT 20:59:50.053823 VPNC: process_login: redirection indicated
913: NOT 20:59:50.054441 VPNC: process_login: new 'Location':
/+webvpn+/index.html
914: NOT 20:59:50.055141 VPNC: set_redirect_url: new URL
<https://xyz1.abc.com:443/+webvpn+/index.html>
```

CSD和IP電話

目前，IP電話不支援Cisco Secure Desktop(CSD)，並且在ASA中為隧道組或全域性啟用CSD時不會連線。

首先，確認ASA是否已啟用CSD。在ASA CLI中輸入**show run webvpn**命令：

```
ASA5510-F# show run webvpn
webvpn
enable outside
  csd image disk0:/csd_3.6.6210-k9.pkg
csd enable
anyconnect image disk0:/anyconnect-win-3.1.00495-k9.pkg 1
anyconnect enable
ASA5510-F#
```

要檢查IP電話連線期間的CSD問題，請檢查ASA中的日誌或調試。

ASA日誌

```
%ASA-4-724002: Group <VPNPhone> User <Phone> IP <172.6.250.9> WebVPN session not terminated. Cisco Secure Desktop was not running on the client's workstation.
```

ASA調試

```
debug webvpn anyconnect 255
<snip>
Tunnel Group: VPNPhone, Client Cert Auth Success.
WebVPN: CSD data not sent from client
http_remove_auth_handle(): handle 24 not found!
<snip>
```

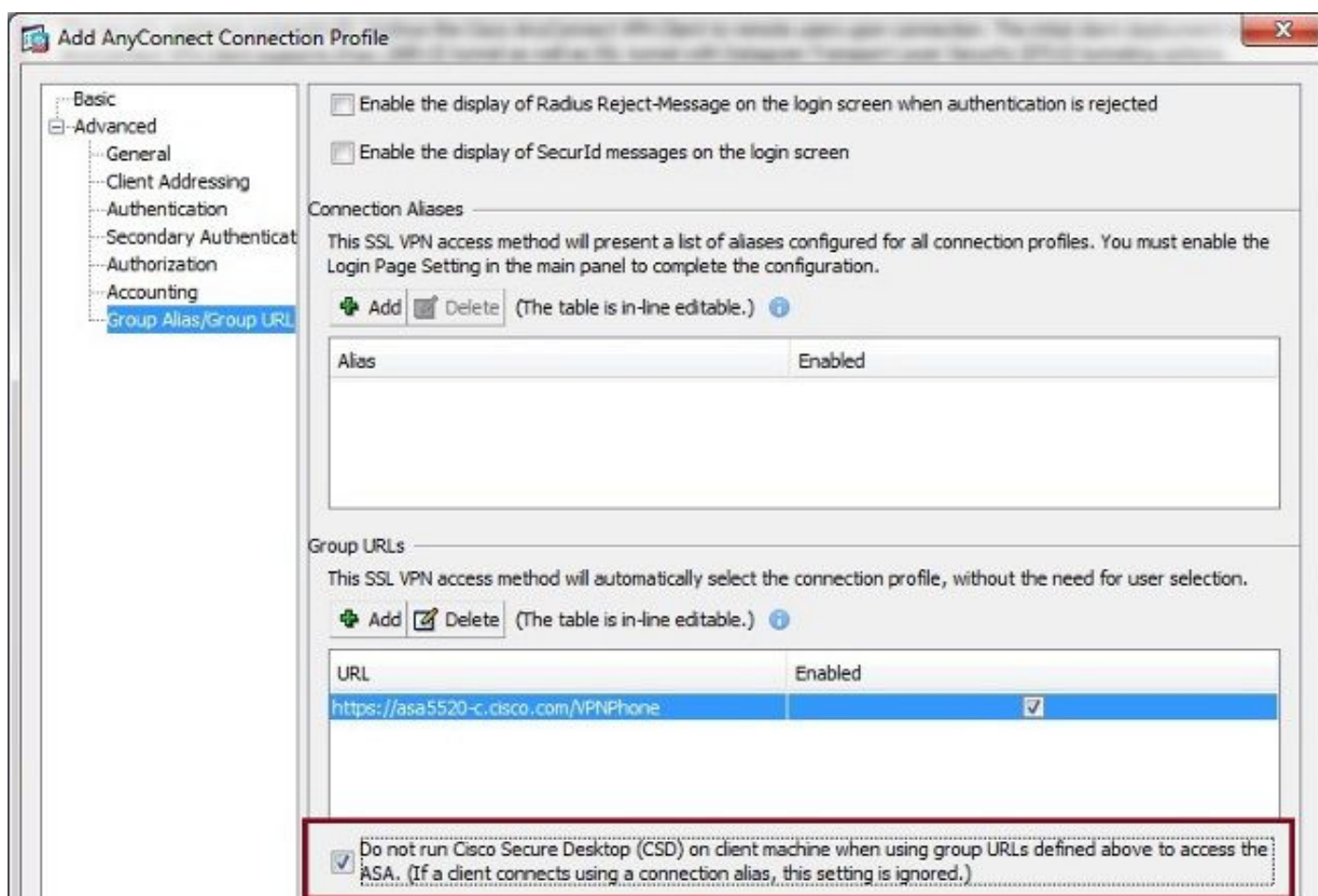
附註：在AnyConnect使用者負載較高的大型部署中，思科建議您不要啟用**debug webvpn anyconnect**。其輸出無法按IP地址過濾，因此可能會建立大量資訊。

在ASA 8.2及更高版本中，必須在tunnel-group的webvpn-attributes下應用**without-csd**命令：

```
tunnel-group VPNPhone webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/VPNPhone enable
without-csd
```

在ASA的早期版本中，這是不可能的，因此唯一的解決方法是全域性禁用CSD。

在思科自適應安全裝置管理器(ASDM)中，您可以禁用特定連線配置檔案的CSD，如下例所示：

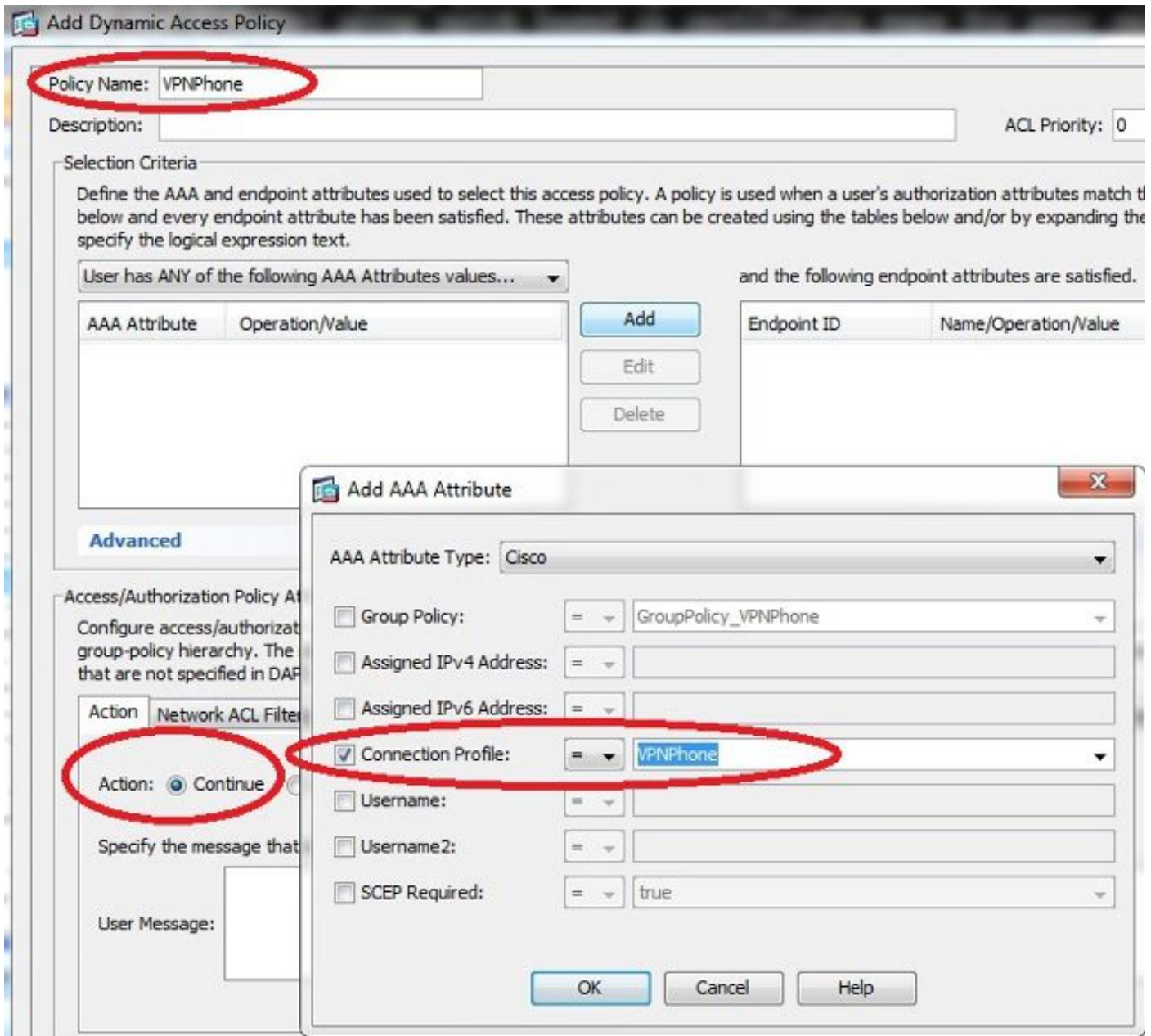


附註：使用group-url關閉CSD功能。

DAP規則

大多數部署不僅將IP電話連線到ASA，還連線不同型別的電腦(Microsoft、Linux、Mac OS)和流動裝置(Android、iOS)。因此，找到動態訪問策略(DAP)規則的現有配置是正常的，其中大多數情況下，DfltAccessPolicy下的預設操作是連線終止。

如果是這種情況，請為VPN電話建立單獨的DAP規則。使用特定引數 (如Connection Profile) ，並將操作設定為Continue:



如果沒有為IP電話建立特定DAP策略，則ASA會在DfltAccessPolicy下顯示命中和連線失敗：

```
%ASA-6-716038: Group <DfltGrpPolicy> User <CP-7962G-SEP8CB64F576113> IP <172.16.250.9> Authentication: successful, Session Type: WebVPN.
```

```
%ASA-7-734003: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9: Session
Attribute aaa.cisco.grouppolicy = GroupPolicy_VPNPhone
<snip>
%ASA-6-734001: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9,
Connection AnyConnect: The following DAP records were selected for this
connection: DfltAccessPolicy
%ASA-5-734002: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9: Connection
terminated by the following DAP records: DfltAccessPolicy
```

在操作設定為**Continue**的情況下，為IP電話建立特定DAP策略後，可以連線：

```
%ASA-7-746012: user-identity: Add IP-User mapping 10.10.10.10 -
LOCAL\CP-7962G-SEP8CB64F576113 Succeeded - VPN user
%ASA-4-722051: Group <GroupPolicy_VPNPhone> User <CP-7962G-SEP8CB64F576113> IP
<172.16.250.9> Address <10.10.10.10> assigned to session
%ASA-6-734001: DAP: User CP-7962G-SEP8CB64F576113, Addr 172.16.250.9, Connection
AnyConnect: The following DAP records were selected for this connection: VPNPhone
```

從DfltGrpPolicy或其他組繼承的值

在許多情況下，DfltGrpPolicy是使用多個選項設定的。預設情況下，除非在IP電話應使用的組策略中手動指定這些設定，否則將為IP電話會話繼承這些設定。

如果從DfltGrpPolicy繼承，可能會影響連線的某些引數包括：

- group-lock
- vpn-tunnel-protocol
- vpn-simultaneous-logins
- vpn過濾器

假定DfltGrpPolicy和GroupPolicy_VPNPhone中存在以下示例配置：

```
group-policy DfltGrpPolicy attributes
  vpn-simultaneous-logins 0
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-clientless
```

```
group-lock value DefaultWEBVPNGroup
vpn-filter value NO-TRAFFIC
```

```
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
default-domain value cisco.com
```

連線會繼承未在GroupPolicy_VPNPhone下明確指定的DfltGrpPolicy引數，並在連線期間將所有資訊推送到IP電話。

為了避免這種情況，請直接在組中手動指定所需的值：

```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
  vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
  vpn-filter none
default-domain value cisco.com
```

若要檢查DfltGrpPolicy的預設值，請使用show run all group-policy命令；此範例釐清輸出之間的差異：

```
ASA5510-F# show run group-policy DfltGrpPolicy
group-policy DfltGrpPolicy attributes
  dns-server value 10.198.29.20 10.198.29.21
  vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
  default-domain value cisco.com
ASA5510-F#
```

```
ASA5510-F# sh run all group-policy DfltGrpPolicy
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
banner none
wins-server none
dns-server value 10.198.29.20 10.198.29.21
dhcp-network-scope none
vpn-access-hours none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
ipv6-vpn-filter none
vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless
```

以下是通過ASDM的組策略繼承屬性的輸出：

The screenshot shows the configuration for 'DfltGrpPolicy'. The 'Banner', 'SCEP forwarding URL', 'Address Pools', and 'IPv6 Address Pools' fields are empty. Under 'More Options', 'Tunneling Protocols' has 'Clientless SSL VPN' and 'SSL VPN Client' checked. 'Filter' is set to '-- None --'. 'NAC Policy' is set to '-- None --'. 'Access Hours' is set to '-- Unrestricted --'. 'Simultaneous Logins' is set to '3'. 'Restrict access to VLAN' is set to '-- Unrestricted --'. 'Connection Profile (Tunnel Group) Lock' is set to '-- None --'. 'Maximum Connect Time' is set to 'Unlimited' minutes. 'Idle Timeout' is set to 'None' with a '30' minute value. 'On smart card removal' is set to 'Disconnect'.

The screenshot shows the configuration for 'VPNPhone'. All fields for 'Banner', 'SCEP forwarding URL', 'Address Pools', and 'IPv6 Address Pools' are set to 'Inherit'. Under 'More Options', 'Tunneling Protocols' has 'Inherit' checked, and 'Clientless SSL VPN' and 'SSL VPN Client' are unchecked. 'Filter', 'NAC Policy', 'Access Hours', 'Simultaneous Logins', 'Restrict access to VLAN', 'Connection Profile (Tunnel Group) Lock', 'Maximum Connect Time', 'Idle Timeout', and 'On smart card removal' are all set to 'Inherit'.

支援的加密密碼

使用7962G IP電話和韌體版本9.1.1測試的AnyConnect VPN電話僅支援兩個密碼，它們都是高級加密標準(AES):AES256-SHA和AES128-SHA。如果在ASA中未指定正確的密碼，連線將被拒絕，如ASA日誌所示：

```
%ASA-7-725010: Device supports the following 2 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:172.16.250.9/52684 proposes the following
2 cipher(s).
%ASA-7-725011: Cipher[1] : AES256-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725014: SSL lib error. Function: SSL3_GET_CLIENT_HELLO Reason: no
shared cipher
```

要確認ASA是否啟用了正確的密碼，請輸入show run all ssl和show ssl 命令：

```
ASA5510-F# show run all ssl
```



```
ssl server-version any
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point SSL outside
ASA5510-F#
```

```
ASA5510-F# show ssl
```

```
Accept connections using SSLv2, SSLv3 or TLSv1 and negotiate to SSLv3 or TLSv1
```

```
Start connections using SSLv3 and negotiate to SSLv3 or TLSv1
```

```
Enabled cipher order: rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
```

```
Disabled ciphers: des-sha1 rc4-md5 dhe-aes128-sha1 dhe-aes256-sha1 null-sha1
```

```
SSL trust-points:
```

```
outside interface: SSL
```

```
Certificate authentication is not enabled
```

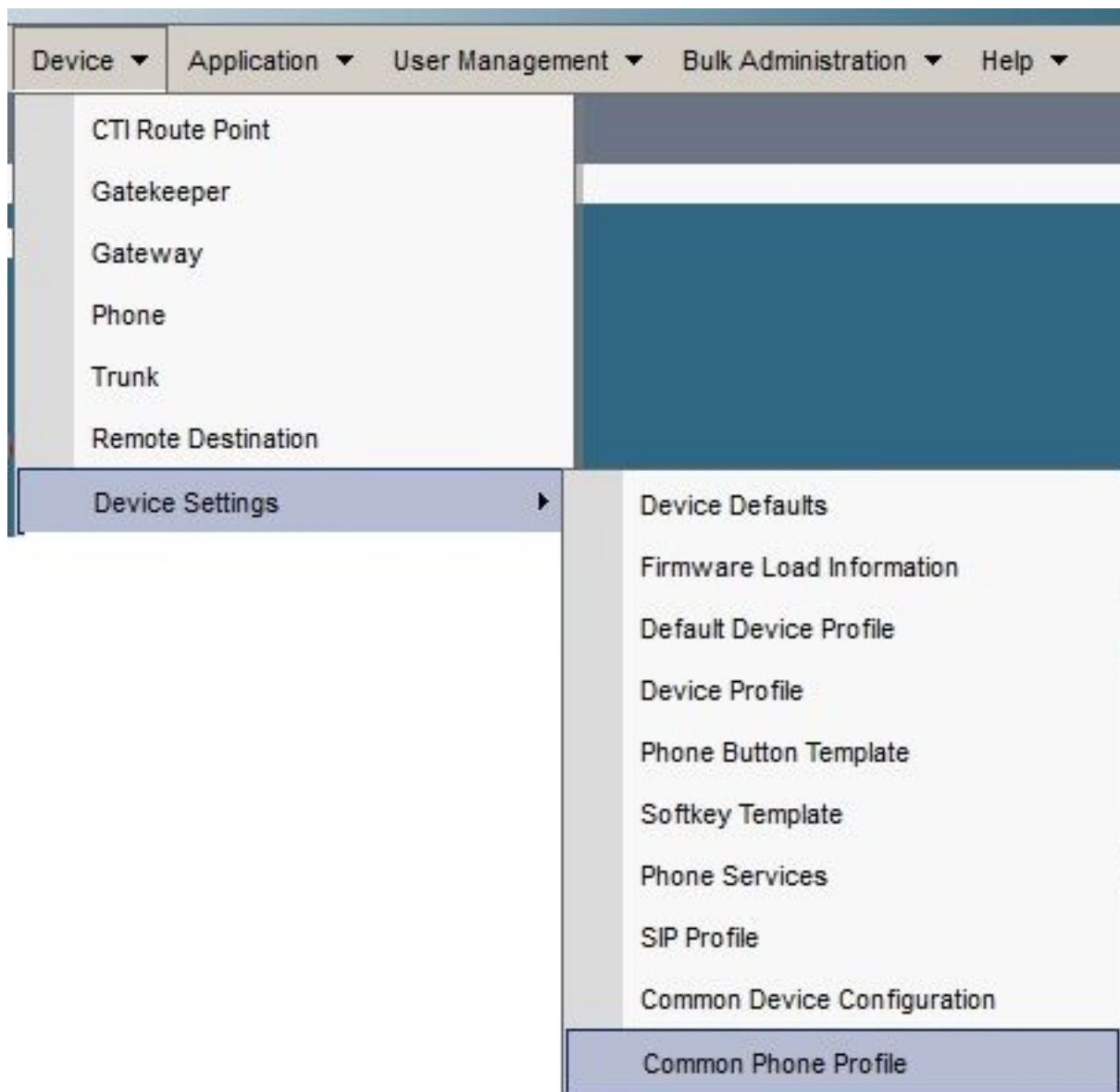
```
ASA5510-F#
```

CUCM上的常見問題

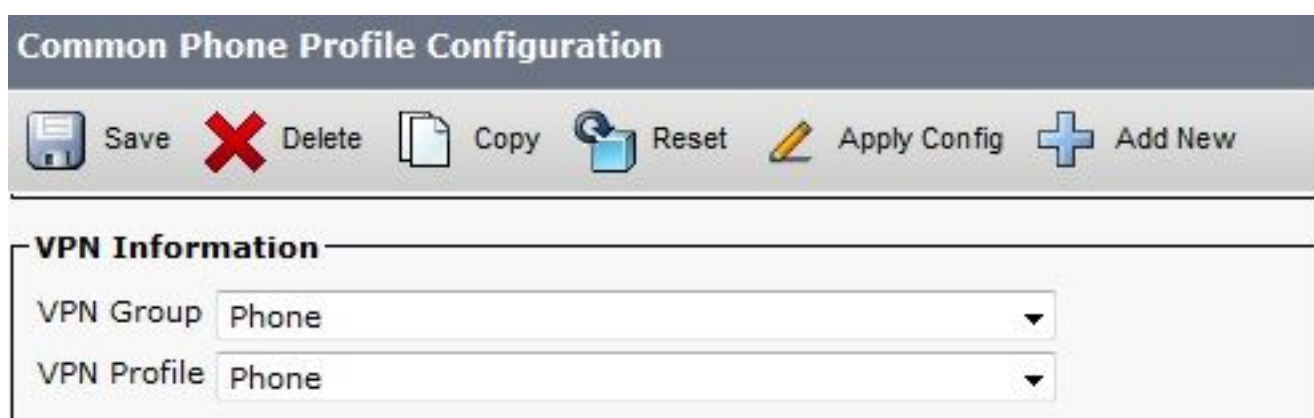
VPN設定未應用於IP電話

建立CUCM上的配置（網關、組和配置檔案）後，應用Common Phone Profile中的VPN設定：

1. 導覽至Device > Device Settings > Common Phone Profile。



2. 輸入VPN資訊：



3. 導航到Device > Phone，確認此配置檔案已分配給電話配置：



憑證驗證方法

為IP電話配置證書身份驗證的方法有兩種：製造商安裝證書(MIC)和本地有效證書(LSC)。請參閱[使用憑證驗證的AnyConnect VPN電話組態範例](#)，以選擇適用於您情況的最佳選項。

配置證書身份驗證時，從CUCM伺服器匯出證書（根CA）並將其匯入ASA：

1. 登入到CUCM。
2. 導航到**Unified OS Administration > Security > Certificate Management**。
3. 查詢證書頒發機構代理功能(CAPF)或Cisco_Manufacturing_CA;證書型別取決於您使用的是MIC證書驗證還是LSC證書驗證。
4. 將檔案下載到本地電腦。

下載檔案後，通過CLI或ASDM登入到ASA並將證書作為CA證書匯入。

Certificate List (1 - 21 of 21)		
Find Certificate List where File Name begins with <input type="text"/> Find Clear Filter + -		
Certificate Name	Certificate Type	.PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	CUCM85.pem
ipsec-trust	trust-certs	CUCM85.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem
TVS	certs	TVS.pem
CallManager-trust	trust-certs	Cisco Manufacturing CA.pem
CallManager-trust	trust-certs	CAP-RTP-001.pem
CallManager-trust	trust-certs	Cisco Root CA 2048.pem
CallManager-trust	trust-certs	CAPF-18cf046e.pem
CallManager-trust	trust-certs	CAP-RTP-002.pem

預設情況下，支援VPN的所有電話都預裝了MIC。7960和7940型號電話不附帶MIC，需要特殊的安裝過程，以便LSC安全地註冊。

最新的思科IP電話 (8811、8841、8851和8861) 包括由新的製造SHA2 CA簽名的MIC證書：

- CUCM版本10.5(1)包含並信任新的SHA2證書。
- 如果運行較早的CUCM版本，可能需要下載新的製造CA證書，並且：

將其上傳到CAPF-trust，以便電話可以通過CAPF進行身份驗證以獲取LSC。

如果要允許電話使用SIP 5061的MIC進行身份驗證，請將其上傳到CallManager-trust。

提示：如果CUCM當前運行的是較早版本，請按一下[此連結](#)以獲取SHA2 CA。

注意：思科建議您僅將MIC用於LSC安裝。思科支援LSC對與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户會自行承擔風險。如果MIC受到危害，思科不承擔任何責任。

預設情況下，如果電話中存在LSC，則無論電話中是否存在MIC，身份驗證都將使用LSC。如果電話中存在MIC和LSC，則身份驗證使用LSC。如果電話中不存在LSC，但存在MIC，則身份驗證使用MIC。

附註：請記住，對於證書身份驗證，您應從ASA匯出SSL證書並將其匯入CUCM。

主機ID檢查

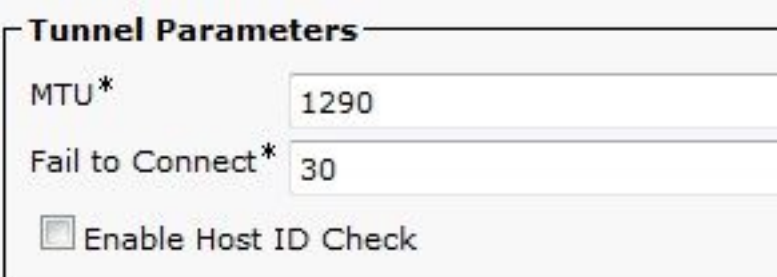
如果證書主題中的公用名稱(CN)與電話用於通過VPN連線到ASA的URL(group-url)不匹配，請禁用CUCM上的主機ID檢查或在ASA中使用與ASA上的該URL匹配的證書。

當ASA的SSL證書是萬用字元證書、SSL證書包含其他SAN（使用者替代名稱），或者使用IP地址而不是完全限定域名(FQDN)建立URL時，必須執行此操作。

以下是憑證的CN與電話嘗試連線的URL不符時IP電話記錄範例。

```
1231: NOT 07:07:32.445560 VPNC: DNS has wildcard, starting checks...
1232: ERR 07:07:32.446239 VPNC: Generic third level wildcards are not allowed,
stopping checks on host=(test.vpn.com) and dns=(*.vpn.com)
1233: NOT 07:07:32.446993 VPNC: hostID not found in subjectAltNames
1234: NOT 07:07:32.447703 VPNC: hostID not found in subject name
1235: ERR 07:07:32.448306 VPNC: hostIDCheck failed!!
```

要在CUCM中禁用主機ID檢查，請導航至Advanced Features > VPN > VPN Profile:



Tunnel Parameters

MTU* 1290

Fail to Connect* 30

Enable Host ID Check

其他疑難排解

要在ASA中使用的日誌和調試

在ASA上，您可以啟用以下調試和日誌以進行故障排除：

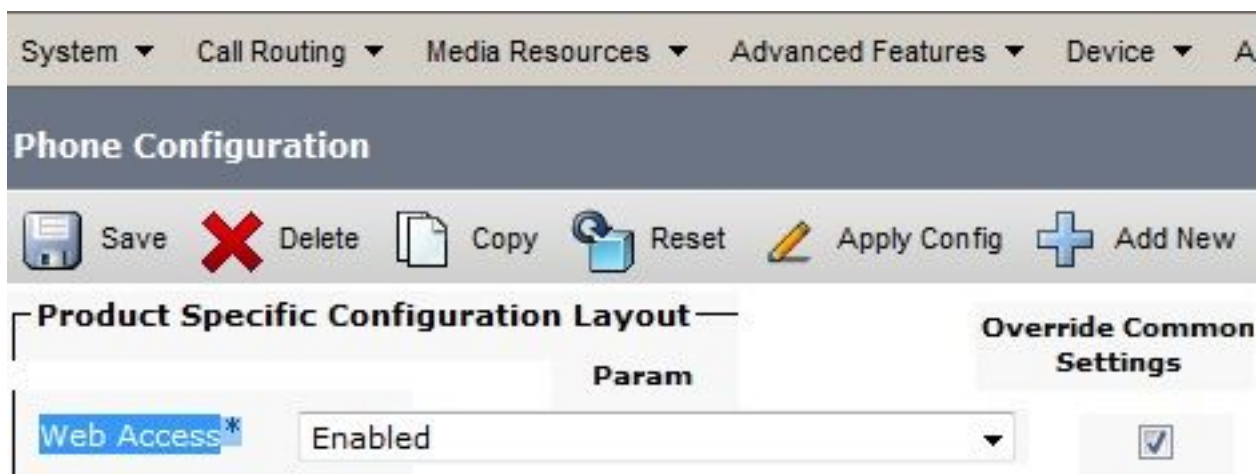
```
logging enable
logging buffer-size 1048576
logging buffered debugging

debug webvpn anyconnect 255
```

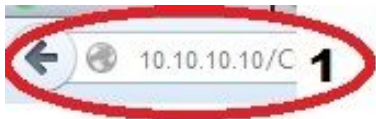
附註：在具有高負載AnyConnect使用者的大型部署中，思科建議您不要啟用debug webvpn anyconnect。其輸出無法按IP地址過濾，因此可能會建立大量資訊。

IP電話日誌

要訪問電話日誌，請啟用Web訪問功能。登入到CUCM，然後導航到**Device > Phone > Phone Configuration**。找到要啟用此功能的IP電話，並找到Web Access部分。將配置更改應用於IP電話：



啟用服務並重設電話以注入此新功能後，您可以在瀏覽器中存取IP電話記錄；從可以訪問該子網的電腦使用電話的IP地址。轉到控制檯日誌並檢查五個日誌檔案。由於電話會覆蓋這五個檔案，您必須檢查所有這些檔案，才能找到您尋找的資訊。



Console Logs

Cisco Unified IP Phone CP-7962G (SEP8CB64F576113)

Device Information

Network Configuration

Network Statistics

Ethernet Information

Access

Network

Device Logs

Console Logs

/FS/cache/fsck.fd0a.log

/FS/cache/fsck.f11a.log

/FS/cache/log181

/FS/cache/log182

3 /FS/cache/log178

/FS/cache/log179

/FS/cache/log180

ASA日誌和IP電話日誌之間的相關問題

以下示例說明如何關聯來自ASA和IP電話的日誌。在本示例中，ASA上的證書的雜湊與電話配置檔案上的證書的雜湊不匹配，因為ASA上的證書已替換為其他證書。

ASA日誌

```
%ASA-7-725012: Device chooses cipher : AES128-SHA for the SSL session with
client outside:172.16.250.9/50091
%ASA-7-725014: SSL lib error. Function: SSL3_READ_BYTES Reason: tlsv1 alert
unknown ca
%ASA-6-725006: Device failed SSL handshake with client outside:172.16.250.9/50091
```

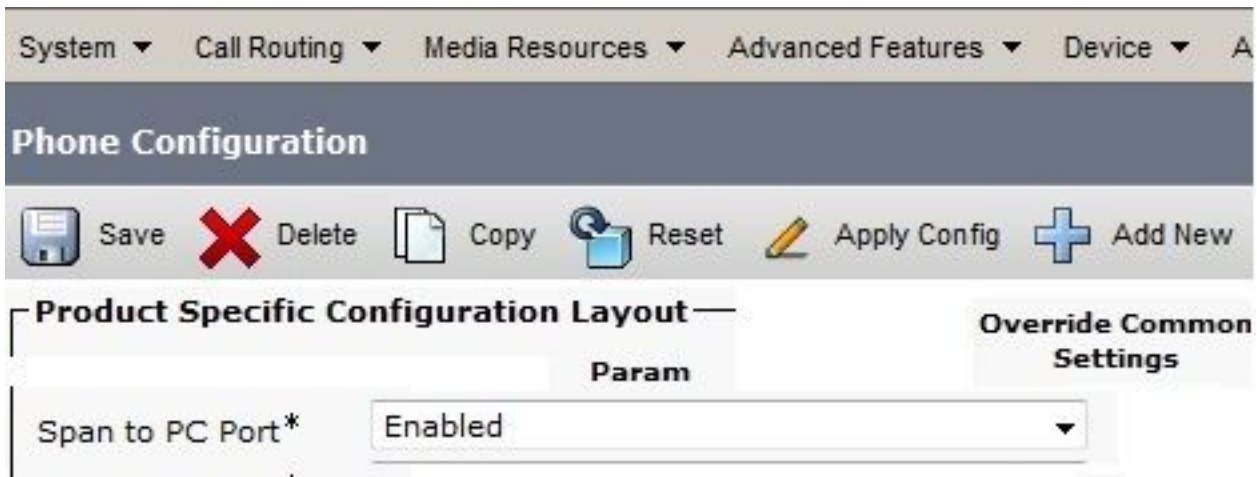
電話日誌

```
902: NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect
initialization
903: NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state
904: NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A
905: NOT 10:19:27.364687 VPNC: cert_vfy_cb: depth:1 of 1, subject:
</CN=10.198.16.140/unstructuredName=10.198.16.140>
906: NOT 10:19:27.365344 VPNC: cert_vfy_cb: depth:1 of 1, pre_err: 18 (self signed certificate)
907: NOT 10:19:27.368304 VPNC: cert_vfy_cb: peer cert saved: /tmp/leaf.crt
908: NOT 10:19:27.375718 SECD: Leaf cert hash = 1289B8A7AA9FFD84865E38939F3466A61B5608FC
909: ERR 10:19:27.376752 SECD: EROR:secLoadFile: file not found </tmp/issuer.crt>
910: ERR 10:19:27.377361 SECD: Unable to open file /tmp/issuer.crt
911: ERR 10:19:27.420205 VPNC: VPN cert chain verification failed, issuer certificate not found
and leaf not trusted
912: ERR 10:19:27.421467 VPNC: ssl_state_cb: TLSv1: write: alert: fatal:
unknown CA
913: ERR 10:19:27.422295 VPNC: alert_err: SSL write alert: code 48, unknown CA
914: ERR 10:19:27.423201 VPNC: create_ssl_connection: SSL_connect ret -1 error 1
915: ERR 10:19:27.423820 VPNC: SSL: SSL_connect: SSL_ERROR_SSL (error 1)
916: ERR 10:19:27.424541 VPNC: SSL: SSL_connect: error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
917: ERR 10:19:27.425156 VPNC: create_ssl_connection: SSL setup failure
918: ERR 10:19:27.426473 VPNC: do_login: create_ssl_connection failed
919: NOT 10:19:27.427334 VPNC: vpn_stop: de-activating vpn
920: NOT 10:19:27.428156 VPNC: vpn_set_auto: auto -> auto
921: NOT 10:19:27.428653 VPNC: vpn_set_active: activated -> de-activated
922: NOT 10:19:27.429187 VPNC: set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
923: NOT 10:19:27.429716 VPNC: set_login_state: VPNC : 1 (LoggingIn) --> 3
(LoginFailed)
924: NOT 10:19:27.430297 VPNC: vpnc_send_notify: notify type: 1 [LoginFailed]
925: NOT 10:19:27.430812 VPNC: vpnc_send_notify: notify code: 37
[SslAlertSrvrCert]
926: NOT 10:19:27.431331 VPNC: vpnc_send_notify: notify desc: [alert: Unknown
CA (server cert)]
927: NOT 10:19:27.431841 VPNC: vpnc_send_notify: sending signal 28 w/ value 13 to
pid 14
928: ERR 10:19:27.432467 VPNC: protocol_handler: login failed
```

Span到PC連線埠功能

您可以將電腦直接連線到電話。電話的後面板中有一個交換機埠。

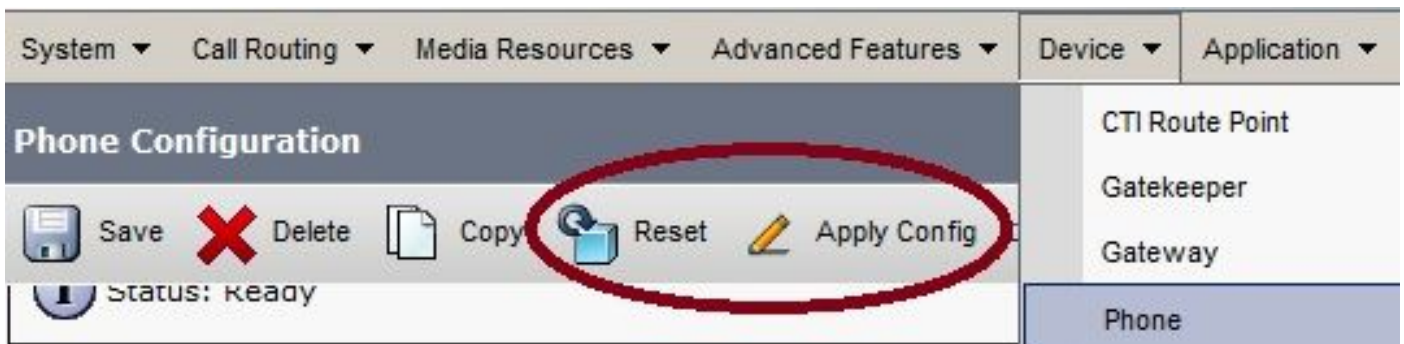
按照您以前的方式配置電話，在CUCM上啟用Span to PC Port並應用配置。電話開始將每個幀的副本傳送到PC。在混雜模式下使用Wireshark以捕獲流量進行分析。



通過VPN連線時的IP電話配置更改

一個常見問題是，在IP電話通過AnyConnect從網路外部連線時，是否可以修改VPN配置。答案為是，但您應該確認一些配置設定。

在CUCM中進行必要的更改，然後將更改應用到電話。有三種選項（應用配置、重置、重新啟動）可將新配置推送到電話。儘管所有三個選項都將VPN與電話和ASA斷開連線，但如果您使用證書身份驗證，則可以自動重新連線；如果您使用身份驗證、授權和記帳(AAA)，系統會再次提示您輸入憑據。



附註：當IP電話位於遠端端時，它通常從外部DHCP伺服器接收IP地址。要讓IP電話從CUCM接收新配置，應聯絡總部的TFTP伺服器。通常CUCM是同一個TFTP伺服器。

若要接收包含變更的組態檔，請確認電話中的網路設定中正確設定了TFTP伺服器的IP位址；要確認，請使用DHCP伺服器的選項150或手動設定電話上的TFTP。可以通過AnyConnect會話訪問此TFTP伺服器。

如果IP電話從本地DHCP伺服器接收TFTP伺服器，但該地址不正確，您可以使用備用TFTP伺服器選項來覆蓋DHCP伺服器提供的TFTP伺服器IP地址。以下程式說明如何應用備用TFTP伺服器：

1. 導覽至**Settings > Network Configuration > IPv4 Configuration**。
2. 滾動到「Alternate TFTP (備用TFTP)」選項。
3. 按電話的「Yes (是)」軟鍵使用其他TFTP伺服器；否則，請按「否」軟鍵。如果選項已鎖定，請按* * #解鎖該選項。
4. 按儲存軟鍵。
5. 在TFTP Server 1選項下應用備用TFTP伺服器。

直接在Web瀏覽器或電話選單中檢視狀態消息，以確認電話接收的資訊正確。如果通訊設定正確，您將看到如下消息：



The screenshot shows the Cisco Unified IP Phone interface. On the left, a navigation menu lists several options: Device Logs, Console Logs, Core Dumps, Status Messages (highlighted with a red oval), and Debug Display. The main area is titled 'Status Messages' and displays a list of system messages for the phone model CP-7962G (SEP8CB64F576113). The messages are as follows:

Time	Message
11:09:29	Trust List Updated
11:09:29	SEP8CB64F576113.cnf.xml.sgn
11:09:37	Trust List Updated
11:09:38	SEP8CB64F576113.cnf.xml.sgn
11:11:24	Trust List Updated
11:11:24	SEP8CB64F576113.cnf.xml.sgn
08:21:45	Trust List Updated
08:21:45	SEP8CB64F576113.cnf.xml.sgn
08:22:02	Trust List Updated
08:22:02	SEP8CB64F576113.cnf.xml.sgn

如果電話無法從TFTP伺服器檢索資訊，您將收到TFTP錯誤消息：

Status Messages

Cisco Unified IP Phone CP-7962G (SEP8CB64F578B2C)

11:51:10 Trust List Update Failed

11:51:10 TFTP Error : SEP8CB64F578B2C.cnf.xml.sgn

11:53:09 Trust List Update Failed

11:54:10 Trust List Update Failed

11:54:10 TFTP Timeout : SEP8CB64F578B2C.cnf.xml.sgn

11:54:31 TFTP Timeout : SEP8CB64F578B2C.cnf.xml.sgn

11:55:18 Trust List Update Failed

11:55:39 TFTP Timeout : SEP8CB64F578B2C.cnf.xml.sgn

11:58:00 Trust List Update Failed

11:58:00 TFTP Error : SEP8CB64F578B2C.cnf.xml.sgn

續訂ASA SSL證書

如果您的AnyConnect VPN電話設定功能正常，但ASA SSL證書即將過期，則不需要將所有IP電話都帶到主站點，以便向電話插入新的SSL證書；您可以在VPN連線時新增新證書。

如果您匯出或匯入了ASA的根CA證書而不是身份證書，並且希望在此續訂期間繼續使用同一供應商(CA)，則無需更改CUCM中的證書，因為它保持不變。但是，如果您使用了身份證書，則此過程是必需的；否則，ASA和IP電話之間的雜湊值不匹配，並且電話不信任該連線。

1. 在ASA上續訂證書。

附註：有關詳細資訊，請參閱[ASA 8.x:使用ASDM續訂並安裝SSL證書](#)。建立單獨的信任點，並在將證書應用到所有VPN IP電話之前，不要使用`ssl trustpoint <name> outside`命令應用此新證書。

2. 匯出新證書。
3. 將新證書作為Phone-VPN-Trust證書匯入CUCM。
附註：請注意[CSCuh19734](#)使用相同CN上傳證書將覆蓋電話 — VPN信任中的舊證書
4. 導航到CUCM中的VPN網關配置，然後應用新證書。現在，您有兩個憑證：即將到期的證書以及尚未應用於ASA的新證書。
5. 將此新配置應用於IP電話。導覽至**Apply Config > Reset > Restart**，以便通過VPN通道將新的組態變更注入到IP電話。確保所有IP電話都通過VPN連線，並且它們可以通過隧道到達TFTP伺服器。
6. 使用TFTP檢查狀態消息和配置檔案，以確認IP電話已收到包含更改的配置檔案。
7. 在ASA中應用新的SSL信任點，並替換舊證書。

附註：如果ASA SSL證書已過期，並且IP電話無法通過AnyConnect連線；您可以將更改（如新的ASA證書雜湊）推送到IP電話。手動將IP電話中的TFTP設定為公共IP地址，以便IP電話可以從那裡檢索資訊。使用公共TFTP伺服器託管配置檔案；例如，在ASA上建立埠轉發並將流量重定向到內部TFTP伺服器。