

# Probleemoplossing voor AnyConnect VPN-telefoon - IP-telefoons, ASA en CUCM

## Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Licentie voor VPN-telefoon bevestigen op ASA](#)

[Beperkte uitvoer en onbeperkte CUCM-export](#)

[Gemeenschappelijke kwesties inzake de ASA](#)

[Certificaten voor gebruik op de ASA](#)

[Trustpoint/certificaat voor ASA-export en CUCM-import](#)

[ASA presenteert ECDSA zelfondertekend certificaat in plaats van ingesteld RSA-certificaat](#)

[Externe database voor verificatie van IP-telefoongebruikers](#)

[Overeenkomsten tussen ASA-certificaat en VPN-telefoonvertrouwenslijst met certificaten](#)

[SHA1-hash controleren](#)

[Configuratie-bestand IP-telefoon downloaden](#)

[De hash decoderen](#)

[VPN-taakverdeling en IP-telefoons](#)

[CSD- en IP-telefoons](#)

[ASA-kaarten](#)

[ASA Debugs](#)

[DAP-regels](#)

[Geëvenaarde waarden van DfltGrpPolicy of andere groepen](#)

[Ondersteunde encryptie-cips](#)

[Gemeenschappelijke problemen met betrekking tot het UCM](#)

[VPN-instellingen niet toegepast op IP-telefoon](#)

[Verificatiemethode voor certificaten](#)

[Controleren van host-ID](#)

[Aanvullende probleemoplossing](#)

[Aanmelden en onderhoud voor gebruik in de ASA](#)

[Vastlegging IP-telefoon](#)

[Gelijkaardige kwesties tussen ASA logboek en IP telefoonlijsten](#)

[ASA-kaarten](#)

[Telefoonvastlegging](#)

[Centrifugeren naar PC-poortfunctie](#)

[Configuratie van IP-telefoon verandert terwijl u met VPN verbonden bent](#)

[Verlengen van het ASA SSL-certificaat](#)

## Inleiding

Dit document beschrijft hoe problemen met IP-telefoons worden opgelost die het Secure Socket Layer (SSL)-protocol (Cisco AnyConnect Secure Mobility Client) gebruiken om verbinding te maken met een Cisco adaptieve security applicatie (ASA) die als VPN-gateway wordt gebruikt en om verbinding te maken met een Cisco Unified Communications Manager (CUCM) die als spraakserver wordt gebruikt.

Raadpleeg voor configuratievoorbeelden van AnyConnect met VPN-telefoons deze documenten:

- [Configuratievoorbeeld van SSLVPN met IP-telefoons](#)
- [AnyConnect VPN-telefoon met configuratievoorbeeld voor certificaatverificatie](#)

## Achtergrondinformatie

Voordat u SSL VPN met IP-telefoons implementeert, moet u bevestigen dat u aan deze eerste vereisten voor AnyConnect-licenties voor de ASA en voor de U.S.-versie met exportbeperkingen van de CUCM hebt voldaan.

### Licentie voor VPN-telefoon bevestigen op ASA

De VPN telefoonlicentie maakt de functie in de ASA mogelijk. Controleer de AnyConnect Premium SSL-licentie om het aantal gebruikers te bevestigen dat verbinding kan maken met AnyConnect (of het een IP-telefoon is). Raadpleeg [welke ASA-licentie er nodig is voor IP-telefoon- en mobiele VPN-verbindingen?](#) voor nadere bijzonderheden .

In de ASA, gebruik de opdracht **show versie** om te controleren of de optie is ingeschakeld. De licentiernaam verschilt van de ASA release:

- ASA release 8.0.x: licentiernaam is AnyConnect voor Linksys-telefoon.
- ASA release 8.2.x en later: De licentiernaam is AnyConnect voor Cisco VPN-telefoon.

Hier is een voorbeeld voor ASA release 8.0.x:

```
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.
```

Hier is een voorbeeld voor ASA release 8.2.x en later:

```
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.
```

## Beperkte uitvoer en onbeperkte CUCM-export

U dient een Amerikaanse versie van CUCM met exportbeperkingen voor de VPN-telefoonfunctie in te voeren.

Als u een onbeperkte versie van CUCM uit de V.S. gebruikt, let dan op:

- IP-telefoonbeveiligingsconfiguraties worden gewijzigd om signalering en mediaconcentratie uit te schakelen; dit omvat encryptie die door de de telefoonfunctie van VPN wordt verstrekt.
- U kunt VPN-gegevens niet exporteren door Importeren/Exporteren.
- De vinkjes voor VPN-profiel, VPN-gateway, VPN-groep en VPN-functieknop worden niet weergegeven.

Opmerking: Nadat u hebt geupgrade naar de Amerikaanse versie van CUCM voor onbeperkte export, kunt u niet later upgraden naar de Amerikaanse versie van deze software of deze opnieuw installeren.

## Gemeenschappelijke kwesties inzake de ASA

Opmerking: U kunt de [Cisco CLI Analyzer](#) gebruiken (alleen [geregistreerde](#) klanten) om een analyse van **show** opdrachtoutput te bekijken. U dient ook te verwijzen naar de [Belangrijke informatie over Debug Commands](#) Cisco-document voordat u **debug**-opdrachten gebruikt.

### Certificaten voor gebruik op de ASA

Op de ASA, kunt u zelfgetekende SSL certificaten, derdenSSL certificaten, en wildkaartcertificaten gebruiken; een van deze beveiligingen de communicatie tussen de IP-telefoon en de ASA.

Er kan slechts één identiteitsbewijs worden gebruikt omdat aan elke interface slechts één certificaat kan worden toegewezen.

Voor SSL-certificaten van derden, installeert u de volledige keten in de ASA en omvat u alle intermediaire en wortelcertificaten.

### Trustpoint/certificaat voor ASA-export en CUCM-import

Het certificaat dat de ASA tijdens de SSL-onderhandeling aan de IP-telefoon presenteert moet vanuit de ASA worden geëxporteerd en in de CUCM worden geïmporteerd. Controleer het trustpunt toegewezen aan de interface waaraan de IP telefoons verbinden om te weten welk certificaat om van de ASA te exporteren is.

Gebruik de opdracht **Show run ssl** om het te exporteren trustpunt (certificaat) te controleren. Raadpleeg [AnyConnect VPN-telefoon met voorbeeld voor de configuratie van de certificaatverificatie](#) voor meer informatie.

Opmerking: Als u een certificaat van derden aan een of meer ASA's hebt uitgevoerd, moet u elk Identity Certificaat van elke ASA exporteren en dan importeren naar de CUCM als telefoon-VPN-trust.

## ASA presenteert ECDSA zelfondertekend certificaat in plaats van ingesteld RSA-certificaat

Wanneer dit probleem zich voordoet, kunnen nieuwere modeltelefoons geen verbinding maken, terwijl de oudere modeltelefoons geen problemen ervaren. Hier zijn de blogs op de telefoon als dit probleem zich voordoet:

```
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
```

In versies 9.4.1 en later wordt de elliptische bocht cryptografie ondersteund voor SSL/TLS. Wanneer een elliptische bocht-Geschiedt SSL VPN client zoals een nieuw telefoonmodel met de ASA verbonden is, wordt de elliptische reeks van het curve-algoritme onderhandeld en de ASA presenteert de SSL VPN client met een elliptisch bocht certificaat, zelfs wanneer de interface die correspondeert met een op RSA gebaseerd betrouwbaarheidspunt wordt gevormd. Om te voorkomen dat de ASA een zelf-ondertekend SSL-certificaat kan indienen, moet de beheerder de algoritme verwijderen die via de opdracht **ssl algoritme** overeenkomen. Bijvoorbeeld, voor een interface die met een RSA vertrouwen punt wordt gevormd, kan de beheerder deze opdracht

uitvoeren zodat slechts op RSA gebaseerde ciphers worden overeengekomen:

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

Dankzij de implementatie van Cisco bug-ID [CSCu02848](#) krijgt de configuratie prioriteit. Er worden altijd expliciet gedefinieerde certificaten gebruikt. Zelfgetekende certificaten worden alleen gebruikt bij gebrek aan een bepaald certificaat.

<b>Voorgestelde clientdecs</b>	<b>Alleen RSA Cert</b>	<b>Alleen EC-sigitaal</b>	<b>Beide certificeringen</b>	<b>None</b>
<b>Alleen RSA-cifen</b>	Gebruikt RSA-cert Gebruikt RSA-ciphers	Gebruikt RSA zelfgetekende cert Gebruikt RSA-ciphers	Gebruikt RSA-cert Gebruikt RSA-ciphers	Gebruikt RSA zelfgetekende cert Gebruikt RSA-ciphers
<b>Enkel EG-civilen (zelden)</b>	<b>Verbinding met verbroken</b>	Gebruik van EC-cert Gebruik van EG-cifers	Gebruik van EC-cert Gebruik van EG-cifers	Gebruikt zelfgetekende van de EG Gebruik van EG-cifers
<b>Alleen civils</b>	Gebruikt RSA-cert Gebruikt RSA-ciphers	Gebruik van EC-cert Gebruik van EG-cifers	Gebruik van EC-cert Gebruik van EG-cifers	Gebruikt zelfgetekende van de EG Gebruik van EG-cifers

## Externe database voor verificatie van IP-telefoongebruikers

U kunt een externe database gebruiken om IP-telefoongebruikers te authenticeren. Protocollen zoals het Lichtgewicht Directory Access Protocol (LDAP) of RADIUS-Dial in User Service (RADIUS) kunnen worden gebruikt voor verificatie van VPN-telefoongebruikers.

## Overeenkomsten tussen ASA-certificaat en VPN-telefoonvertrouwenslijst met certificaten

Onthoud dat u het certificaat moet downloaden dat aan de ASA SSL-interface is toegewezen en het als een Phone-VPN-Trust Document in CUCM uploaden. Andere omstandigheden kunnen de hash voor dit certificaat dat door de ASA wordt aangeboden veroorzaken om de hash niet aan te passen die de CUCM server genereert en naar de VPN-telefoon door het configuratiebestand duwt.

Zodra de configuratie is voltooid, test u de VPN-verbinding tussen de IP-telefoon en de ASA. Als de verbinding blijft mislukken, controleer of de hash van het ASA-certificaat overeenkomt met de hash van de IP-telefoon:

1. Controleer het Secure Hash Algorithm 1 (SHA1), dat door de ASA is voorgesteld.
2. Gebruik TFTP om het IP-telefoonconfiguratiebestand in de CUCM te downloaden.
3. Ontdek de hash van hexadecimaal tot basis 64 of van basis 64 tot hexadecimaal.

### SHA1-hash controleren

ASA presenteert het certificaat dat wordt toegepast met de opdracht **ssl trustpoint** op de interface waarmee de IP-telefoon wordt verbonden. Om dit certificaat te controleren, open de browser (in dit voorbeeld, Firefox), en voer de URL (group-url) in waar de telefoons zouden moeten verbinden:

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

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**

<b>3</b> 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

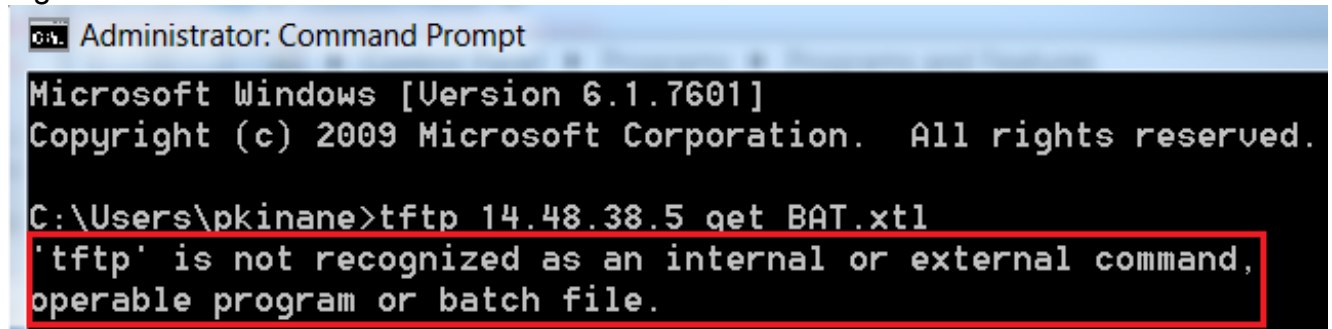
## Configuratie-bestand IP-telefoon downloaden

Van een PC met directe toegang tot CUCM, download het TFTP configuratiebestand voor de telefoon met verbindingskwesaties. Twee downloadmethoden zijn:



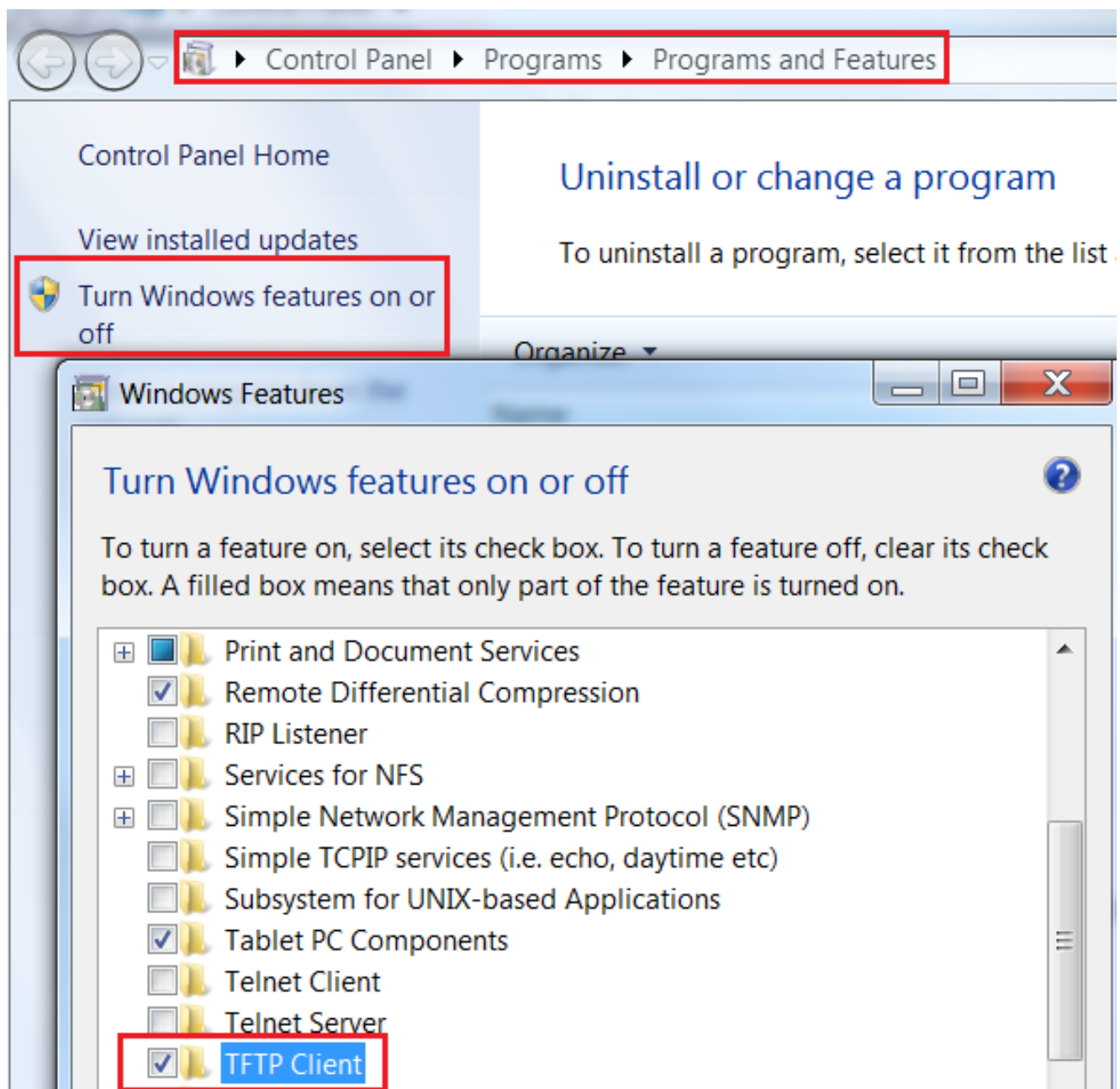
1. Open een CLI-sessie in Windows, en gebruik de opdracht `ftp -i <TFTP Server> GET SEP<Phone Mac Address>.cnf.xml`.

Opmerking: Als u een fout ontvangt die vergelijkbaar is met de onderstaande, dient u te bevestigen dat de TFTP-clientfunctie is ingeschakeld.

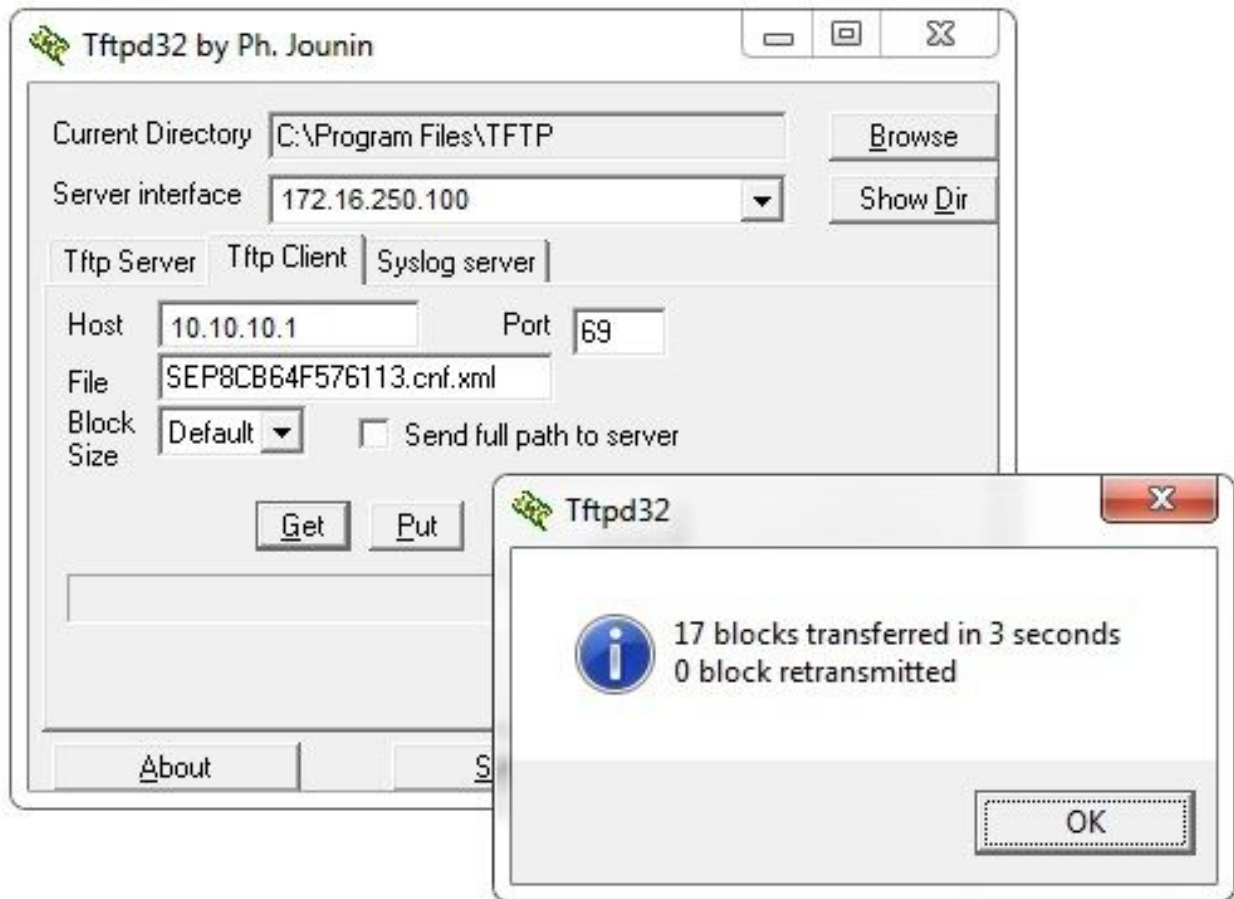


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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. Gebruik een toepassing zoals [Tftpd32](#) om het bestand te downloaden:



3. Zodra het bestand is gedownload, opent u het XML en vindt u de *vpnGroup* configuratie. Dit voorbeeld toont het gedeelte en de te controleren *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>
```

## De hash decoderen

Bevestig dat beide waarden overeenkomen. De browser presenteert de hash in hexadecimaal formaat, terwijl het XML bestand basis 64 gebruikt, dus converteert het ene formaat naar het andere om de match te bevestigen. Er zijn veel vertalers beschikbaar. een voorbeeld is de [TRANSLATOR, BINARY](#).



Opmerking: Als de vorige hash-waarde niet overeenkomt, vertrouwt de VPN-telefoon niet op de verbinding die met de ASA is onderhandeld en de verbinding mislukt.

## VPN-taakverdeling en IP-telefoons

Laden-gebalanceerde SSL VPN wordt niet ondersteund voor VPN-telefoons. VPN-telefoons voeren geen echte certificatie uit maar gebruiken in plaats daarvan hashes die door de CUCM zijn ingedrukt om de servers te valideren. Omdat het in evenwicht brengen van VPN is in wezen een HTTP-omleiding, vereist het de telefoons om meerdere certificaten te valideren, wat tot mislukking leidt. Symptomen van een fout in taakverdeling van VPN zijn:

- De telefoon wisselt tussen servers en duurt uitzonderlijk lang om te verbinden of uiteindelijk mislukt.
- De telefoonlogs bevatten berichten zoals deze:

```
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- en IP-telefoons

Op dit moment ondersteunen IP-telefoons niet de Cisco Secure Desktop (CSD) en verbinden ze zich niet wanneer CSD is ingeschakeld voor een tunnelgroep of mondiaal in de ASA.

Bevestig eerst of de ASA CSD heeft ingeschakeld. Voer de **show run webVPN** opdracht in in de ASA CLI:

```
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#
```

Controleer de logbestanden of debugs in de ASA om CSD-emissies tijdens een IP-telefoonverbinding te controleren.

## ASA-kaarten

```
%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 Debugs

```
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>
```

Opmerking: In een grote plaatsing met een hoge lading gebruikers AnyConnect, adviseert Cisco dat u geen **web om het even welke verbinding** kunt zuiveren. De output kan niet door IP adres worden gefilterd, dus kan er een grote hoeveelheid informatie worden gecreëerd.

In ASA versies 8.2 en later, moet u de **zonder-csd** opdracht toepassen onder de webvpn-eigenschappen van de tunnelgroep:

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

In eerdere versies van de ASA was dit niet mogelijk, dus de enige oplossing was om de CSD wereldwijd uit te schakelen.

In de Cisco Adaptieve Security Devices Manager (ASDM) kunt u CSD voor een specifiek verbindingsprofiel uitschakelen zoals in dit voorbeeld:

The screenshot shows the 'Add AnyConnect Connection Profile' window in Cisco ASDM. The left sidebar has 'Group Alias/Group URL' selected. The main area has two sections: 'Connection Aliases' and 'Group URLs'. The 'Group URLs' section contains a table with one entry:

URL	Enabled
https://asa5520-c.cisco.com/VPNPhone	<input checked="" type="checkbox"/>

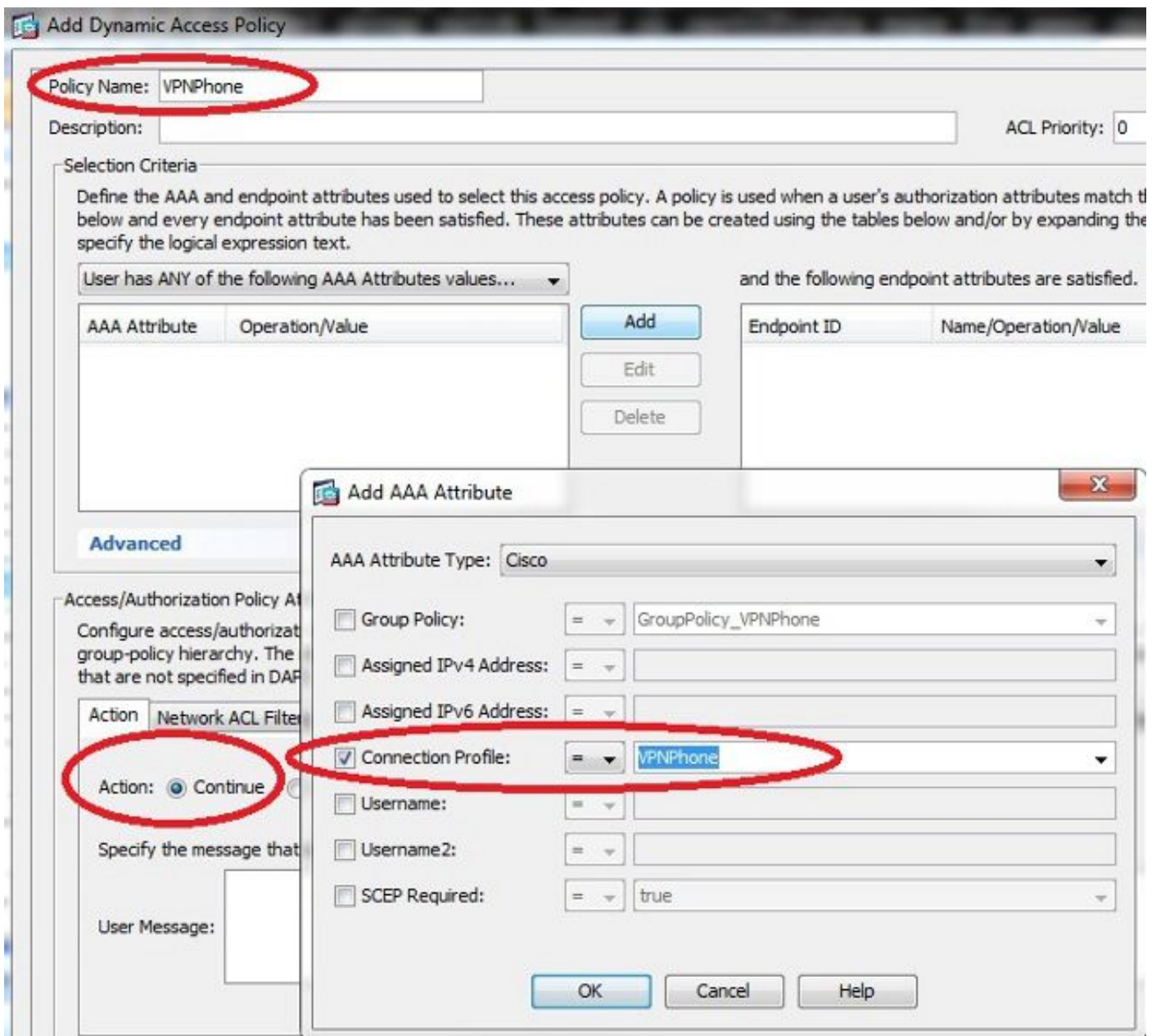
At the bottom of the window, a checkbox is checked with the following text: 'Do not run Cisco Secure Desktop (CSD) on client machine when using group URLs defined above to access the ASA. (If a client connects using a connection alias, this setting is ignored.)'

Opmerking: Gebruik een groepsregel om de CSD-functie uit te schakelen.

## DAP-regels

De meeste implementaties verbinden niet alleen IP-telefoons met de ASA maar verbinden ook verschillende typen machines (Microsoft, Linux, Mac OS) en mobiele apparaten (Android, iOS). Om deze reden is het normaal om een bestaande configuratie van Dynamic Access Policy (DAP) regels te vinden, waar de Default Action onder het DfltAccessPolicy meestal eindigt met de verbinding.

Als dit probleem zich voordoet, maakt u een afzonderlijke DAP-regel voor de VPN-telefoons. Gebruik een specifieke parameter, zoals het verbindingsprofiel, en stel de actie in om **door te gaan**:



Als u geen specifiek DAP-beleid voor IP-telefoons maakt, toont de ASA een hit onder DfltAccessPolicy en een defecte verbinding:

```
%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
```

Zodra u een specifiek DAP beleid voor de IP telefoons creëert met de actie die wordt ingesteld op

Doorgaan, kunt u verbinding maken:

```
%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
```

## Geëvenaarde waarden van DfltGrpPolicy of andere groepen

In veel gevallen is het DfltGrpPolicy opgezet met verschillende opties. Standaard worden deze instellingen geërfd voor de IP-telefoonsessie tenzij ze handmatig worden ingesteld in het groepsbeleid dat door de IP-telefoon moet worden gebruikt.

Sommige parameters die de verbinding zouden kunnen beïnvloeden als ze van DfltGrpPolicy geërfd zijn:

- groepsslot
- VPN-tunnelprotocol
- VPN-simultane logins
- VPN-filter

Stel dat u deze voorbeeldconfiguratie in DfltGrpPolicy en de GroupPolicy\_VPNPhone heeft:

```
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
```



De verbinding erft de parameters van DfltGrpPolicy die niet expliciet werden gespecificeerd onder de telefoon GroupPolicy\_VPN en drukt alle informatie naar de IP-telefoon tijdens de verbinding.

Specificeer daartoe handmatig de waarde(s) die u rechtstreeks in de groep nodig hebt:

```
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
```

Om de standaardwaarden van DfltGrpPolicy te controleren, gebruikt u de opdracht **show run-beleid**. dit voorbeeld verduidelijkt het verschil tussen de output :

```
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
```

Hier is de output van de groep-beleid erfgenaam door de ASDM:

Name:	DRIGrpPolicy
Banner:	
SCP forwarding URL:	
Address Pools:	
IPv6 Address Pools:	
<b>More Options</b>	
Tunneling Protocols:	<input checked="" type="checkbox"/> Clientless SSL VPN <input checked="" type="checkbox"/> SSL VPN Client
Filter:	-- None --
NAC Policy:	-- None --
Access Hours:	-- Unrestricted --
Simultaneous Logins:	3
Restrict access to VLAN:	-- Unrestricted --
Connection Profile (Tunnel Group) Lock:	-- None --
Maximum Connect Time:	<input checked="" type="checkbox"/> Unlimited <input type="text"/> minutes
Idle Timeout:	<input type="checkbox"/> None <input type="text" value="30"/> minutes
On smart card removal:	<input checked="" type="radio"/> Disconnect <input type="radio"/> Keep the connection

Name:	VPNPhone
Banner:	<input checked="" type="checkbox"/> Inherit
SCP forwarding URL:	<input checked="" type="checkbox"/> Inherit
Address Pools:	<input checked="" type="checkbox"/> Inherit
IPv6 Address Pools:	<input checked="" type="checkbox"/> Inherit
<b>More Options</b>	
Tunneling Protocols:	<input checked="" type="checkbox"/> Inherit <input type="checkbox"/> Clientless SSL VPN <input type="checkbox"/> SSL VPN Client
Filter:	<input checked="" type="checkbox"/> Inherit
NAC Policy:	<input checked="" type="checkbox"/> Inherit
Access Hours:	<input checked="" type="checkbox"/> Inherit
Simultaneous Logins:	<input checked="" type="checkbox"/> Inherit
Restrict access to VLAN:	<input checked="" type="checkbox"/> Inherit
Connection Profile (Tunnel Group) Lock:	<input checked="" type="checkbox"/> Inherit
Maximum Connect Time:	<input checked="" type="checkbox"/> Inherit <input type="checkbox"/> Unlimited <input type="text"/> minutes
Idle Timeout:	<input checked="" type="checkbox"/> Inherit <input type="checkbox"/> None <input type="text"/> minutes
On smart card removal:	<input checked="" type="checkbox"/> Inherit <input type="radio"/> Disconnect <input type="radio"/> Keep the connection

## Ondersteunde encryptie-cips

Een AnyConnect VPN-telefoon met 7962G IP-telefoon en firmware versie 9.1.1 ondersteunt slechts twee telefoons, die beide Advanced Encryption Standard (AES) zijn: AES256-SHA en AES128-SHA. Als de juiste lettertypen niet in de ASA zijn gespecificeerd, wordt de verbinding geweigerd, zoals in het ASA-logboek wordt getoond:

```
%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
```

Om te bevestigen of de ASA de juiste toegelaten ciphers heeft, stel de **show in de run alle ssl** en **show ssl** opdrachten:

```
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

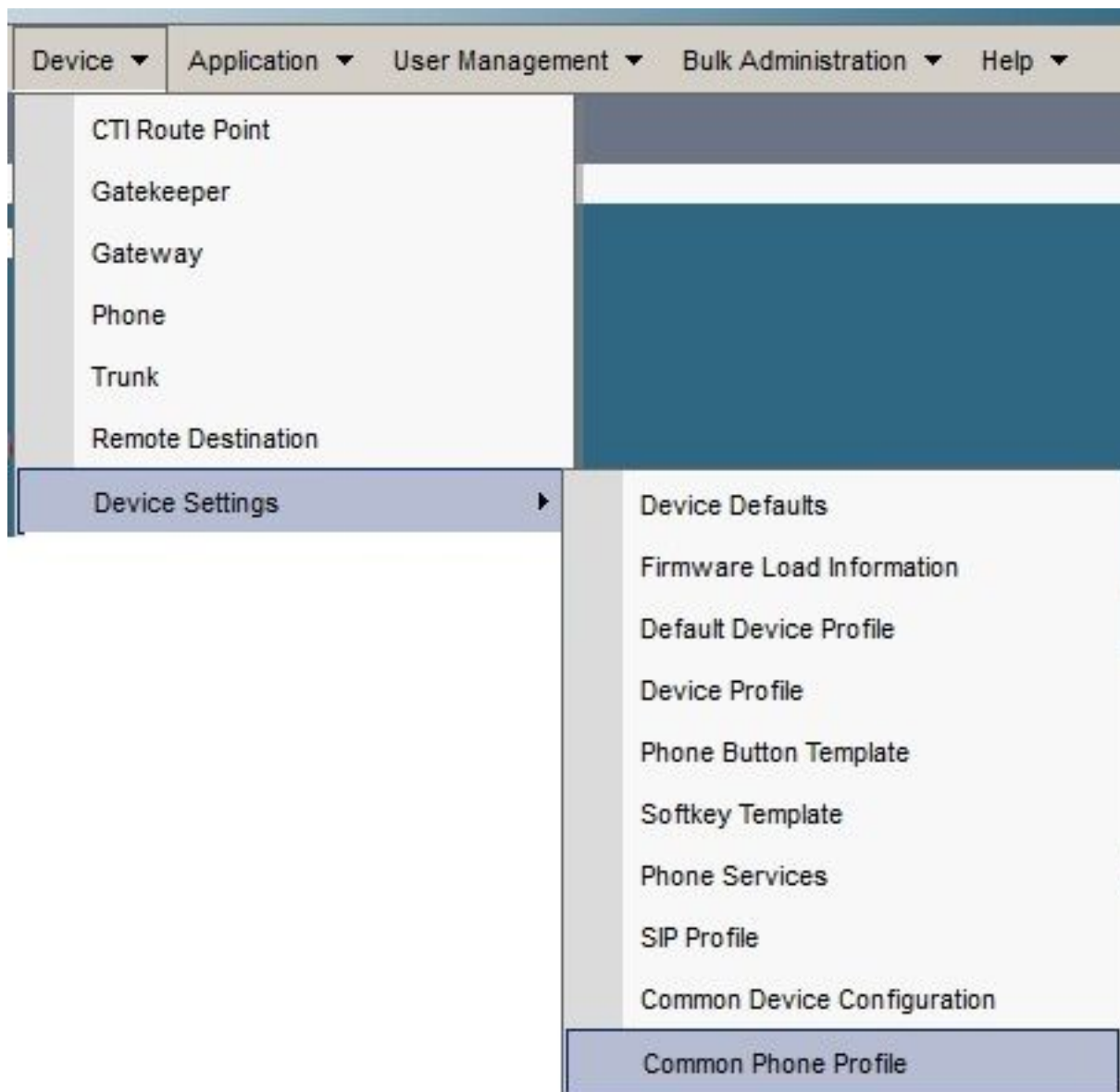
ASA5510-F#

## Gemeenschappelijke problemen met betrekking tot het UCM

### VPN-instellingen niet toegepast op IP-telefoon

Nadat de configuratie op CUCM is gemaakt (Gateway, Group en Profile), passen u de VPN-instellingen in het Common Phone Profile toe:

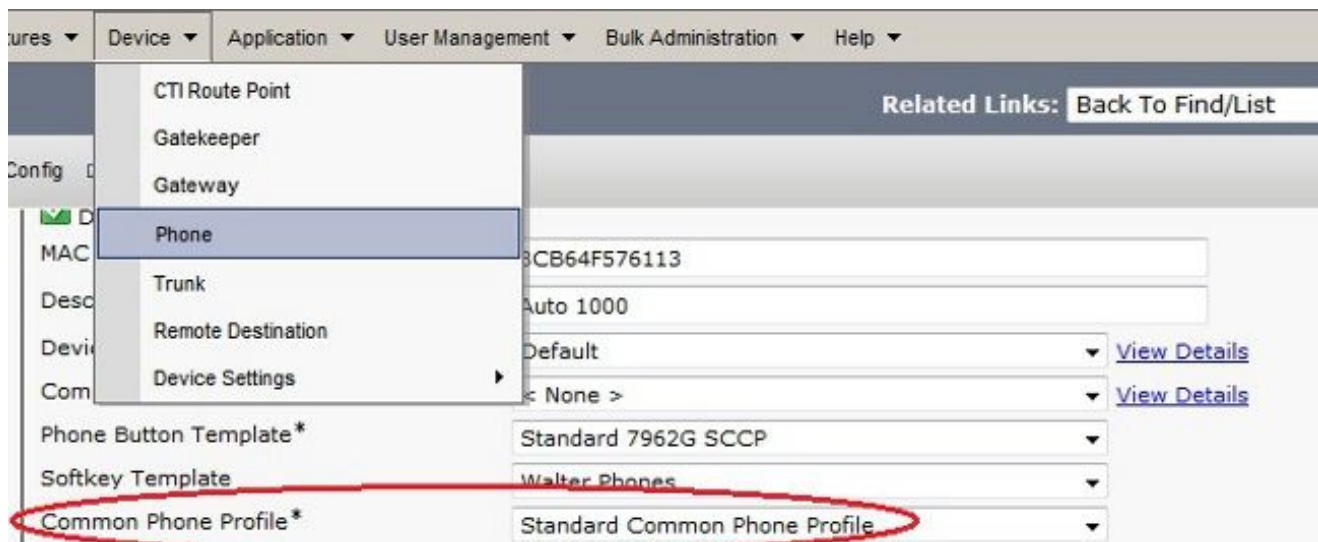
1. navigeren naar **apparaat > Apparaatinstellingen > Gemeenschappelijk telefoonprofiel**.



2. Voer de VPN-informatie in:

A screenshot of the 'Common Phone Profile Configuration' page. The page title is 'Common Phone Profile Configuration'. Below the title is a toolbar with icons for 'Save', 'Delete', 'Copy', 'Reset', 'Apply Config', and 'Add New'. The 'VPN Information' section is highlighted and contains two dropdown menus: 'VPN Group' and 'VPN Profile', both of which are currently set to 'Phone'.

3. Navigeren naar **apparaat > telefoon** en bevestigen dat dit profiel aan de telefoonconfiguratie is toegewezen:



## Verificatiemethode voor certificaten

Er zijn twee manieren om certificatie voor IP telefoons te configureren: Geïnstalleerd certificaat (MIC) en lokaal belangrijk certificaat (LSC). Raadpleeg [AnyConnect VPN-telefoon](#) met [Configuratievoorbeeld](#) van [certificaatverificatie](#) om de beste optie voor uw situatie te kiezen.

Wanneer u certificatie-verificatie configureren exporteert u het certificaat of de certificaten (Root CA) vanaf de CUCM-server en importeert u deze naar de ASA:

1. Meld u aan bij de CUCM.
2. Navigeer naar **Unified OS-beheer > Beveiliging > certificaatbeheer**.
3. Vind de Proxy-functie (CAPF) van de certificaatinstantie of Cisco\_Manufacturing\_CA; het type certificaat hangt af van de vraag of u MIC of LSC certificatie gebruikte.
4. Download het bestand naar de lokale computer.

Nadat de bestanden zijn gedownload, logt u in bij de ASA via de CLI of ASDM en importeert u het certificaat als CA-certificaat.

Certificate List (1 - 21 of 21)		
Find Certificate List where File Name begins with <input type="text"/> Find Clear Filter <input type="button" value="+"/> <input type="button" value="-"/>		
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>

Standaard worden alle telefoons die VPN ondersteunen vooraf geladen met MIC's. De 7960- en 7940-modeltelefoons hebben geen MIC en vereisen een speciale installatieprocedure zodat de LSC zich veilig kan registreren.

De nieuwste Cisco IP-telefoons (8811, 8841, 8851 en 8861) bevatten MIC-certificaten die door de nieuwe Manufacturing SHA2 CA2 zijn ondertekend:

- De CUCM versie 10.5(1) bevat en vertrouwt de nieuwe SHA2-certificaten.
- Als u een eerdere CUCM-versie gebruikt, moet u het nieuwe CA-certificaat downloaden en:

Upload het naar het CAPF-vertrouwen zodat de telefoons met CAPF voor authentiek kunnen verklaren om een LSC te verkrijgen.

Upload het naar het CallManager-vertrouwen als u de telefoons met een MIC voor SIP 5061 wilt kunnen authentiek verklaren.

**Tip:** Klik op [deze link](#) om de SHA2 CA te verkrijgen als de CUCM momenteel een eerdere versie draait.

**Voorzichtig:** Cisco raadt u aan MICs alleen te gebruiken voor LSC-installatie. Cisco ondersteunt LSC's voor verificatie van de TLS-verbinding met de CUCM. Omdat de MIC wortelcertificaten kunnen worden gecompromitteerd, doen klanten die telefoons configureren om MICs te gebruiken voor TLS authenticatie of voor enig ander doel dit op hun eigen risico. Cisco is niet aansprakelijk als de MIC's gecompromitteerd zijn.

Standaard gebruikt een LSC als er een LSC in de telefoon is, de verificatie de LSC, ongeacht of er een MIC in de telefoon aanwezig is. Als er een MIC en LSC in de telefoon bestaan, gebruikt de authenticatie de LSC. Als er geen LSC in de telefoon bestaat maar er wel een MIC bestaat, gebruikt de authenticatie het MIC.

Opmerking: Vergeet niet dat u voor certificatie het SSL-certificaat van de ASA moest exporteren en het naar de CUCM moest importeren.

## Controleren van host-ID

Als de gezamenlijke naam (CN) in het onderwerp van het certificaat niet overeenkomt met de URL (group-url), worden de telefoons gebruikt om via VPN met de ASA te verbinden, schakelt u de Host ID Check op CUCM uit of gebruikt u een certificaat in de ASA dat overeenkomt met die URL op de ASA.

Dit is nodig wanneer het SSL-certificaat van de ASA een jokercertificaat is, het SSL-certificaat een ander SAN bevat (Onderwerp Alternatieve Naam) of de URL met het IP-adres is gemaakt in plaats van de volledig gekwalificeerde domeinnaam (FQDN).

Dit is een voorbeeld van een IP-telefoonlog wanneer de GN van het certificaat niet overeenkomt met de URL die de telefoon probeert te bereiken.

```
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!!
```

Als u de controle van de Host ID in het CUCM wilt uitschakelen, navigeer dan naar **geavanceerde functies > VPN > VPN-profiel**:

**Tunnel Parameters**

MTU*	1290
Fail to Connect*	30
<input type="checkbox"/> Enable Host ID Check	

## Aanvullende probleemoplossing

### Aanmelden en onderhoud voor gebruik in de ASA

Op de ASA, kunt u deze debugs en logboeken voor het oplossen van problemen toelaten:

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

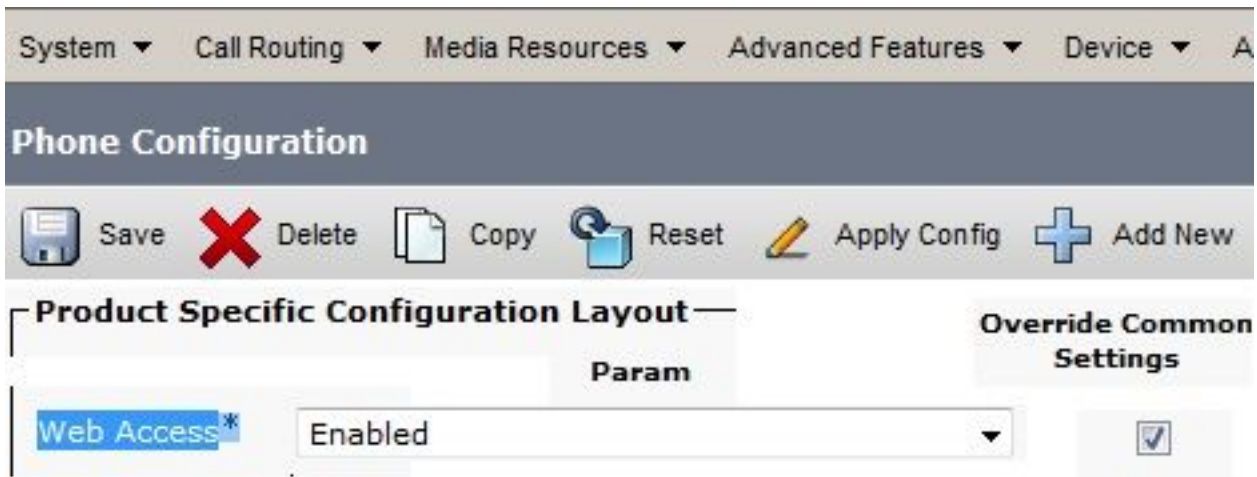
debug webvpn anyconnect 255
```

Opmerking: In een grote plaatsing met een hoge lading gebruikers AnyConnect, adviseert Cisco dat u **WebVpnh** niet toelaat **om overal verbinding te maken**. De output kan niet door IP adres worden gefilterd, dus kan er een grote hoeveelheid informatie worden gecreëerd.

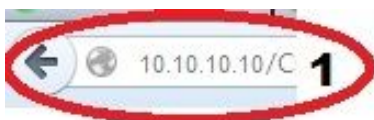
### Vastlegging IP-telefoon

U hebt toegang tot de telefoonbestanden door deze functie in te schakelen. Meld u aan bij CUCM en navigeer naar **apparaat > telefoon > telefoonconfiguratie**. Vind de IP-telefoon waarop u deze optie wilt activeren en vind de sectie voor webtoegang. Pas de configuratieveranderingen op de IP-telefoon toe:





Nadat u de service hebt ingeschakeld en de telefoon hebt gereset om deze nieuwe functie te injecteren, hebt u toegang tot IP-telefoonbestanden in de browser; gebruik het IP adres van de telefoon van een computer met toegang tot die subnet. Ga naar de console logbestanden en controleer de vijf logbestanden. Omdat de telefoon de vijf bestanden overschrijft, moet je al deze bestanden controleren om de informatie te vinden die je zoekt.



## 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](#)

Gelijkaardige kwesties tussen ASA logboek en IP telefoonlijsten

Dit is een voorbeeld van hoe de logbestanden van de ASA en de IP-telefoon met elkaar te verbinden. In dit voorbeeld komt de hash van het certificaat op de ASA niet overeen met de hash van het certificaat op het configuratiebestand van de telefoon omdat het certificaat op de ASA vervangen werd door een ander certificaat.

## ASA-kaarten

```
%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
```

## Telefoonvastlegging

```
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)]

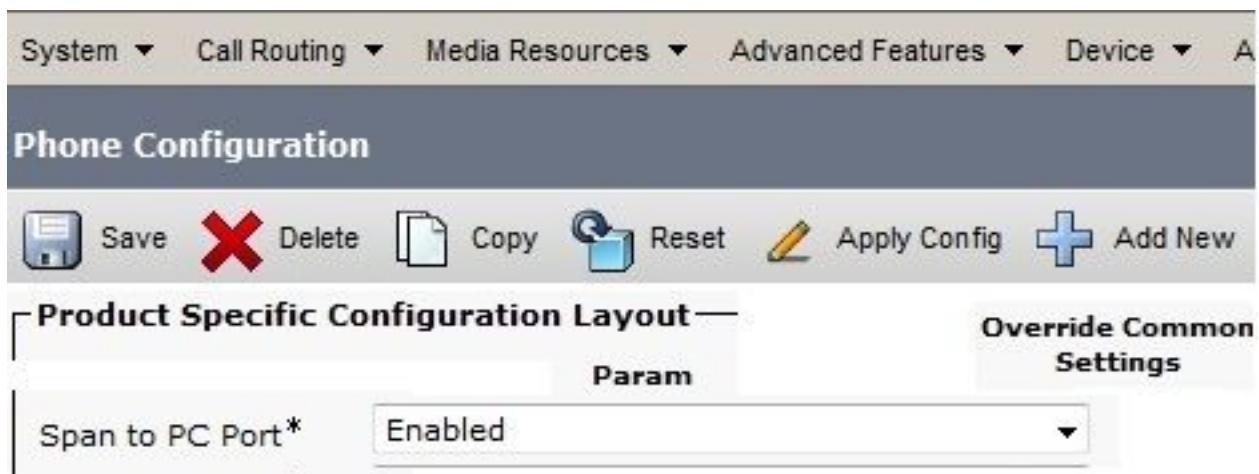
927: NOT 10:19:27.431841 VPNC: vpnc\_send\_notify: sending signal 28 w/ value 13 to pid 14

928: ERR 10:19:27.432467 VPNC: protocol\_handler: login failed

## Centrifugeren naar PC-poortfunctie

U kunt een computer rechtstreeks aan een telefoon aansluiten. De telefoon heeft een wisselpoort in het achtervliegtuig.

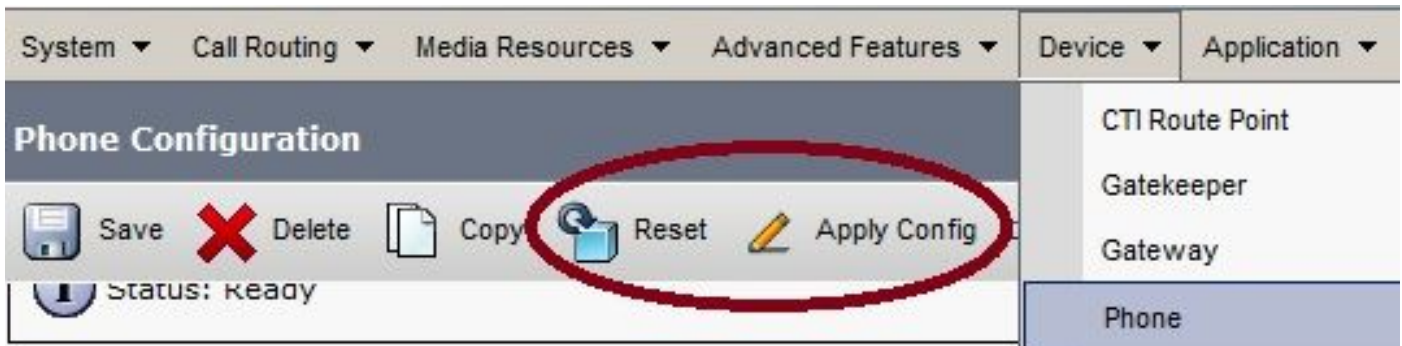
Configureer de telefoon zoals u eerder hebt gedaan, schakelt u de Spanning in de PC-poort op de CUCM in en past u de configuratie toe. De telefoon stuurt een kopie van elk frame naar de PC. Gebruik Wireshark in veelbelovende modus om verkeer voor analyse vast te leggen.



## Configuratie van IP-telefoon verandert terwijl u met VPN verbonden bent

Een veel voorkomende vraag is of u de VPN-configuratie kunt wijzigen terwijl de IP-telefoon door AnyConnect uit het netwerk wordt aangesloten. Het antwoord is ja, maar u zou bepaalde configuratie instellingen moeten bevestigen.

Breng de gewenste wijzigingen aan in het CUCM en pas vervolgens de wijzigingen aan de telefoon toe. Er zijn drie opties (Toepassen, Config, Reset, Restart) om de nieuwe configuratie aan de telefoon te drukken. Hoewel alle drie de opties VPN van de telefoon en de ASA scheiden, kunt u automatisch opnieuw verbinden als u certificatie gebruikt; Als u Verificatie, autorisatie en accounting (AAA) gebruikt, wordt u opnieuw gevraagd om uw aanmeldingsgegevens.



Opmerking: Wanneer de IP-telefoon in de afstandsrij is, ontvangt het normaal een IP-adres van een externe DHCP-server. Voor de IP-telefoon om de nieuwe configuratie van CUCM te ontvangen, zou deze de TFTP-server in het hoofdkantoor moeten benaderen. Normaal is CUCM dezelfde TFTP-server.

Om de configuratiebestanden met de veranderingen te ontvangen, moet u bevestigen dat het IP-adres voor de TFTP-server correct is ingesteld in de netwerkinstellingen in de telefoon; Gebruik voor bevestiging optie 150 van de server van DHCP of stel het TFTP handmatig in op de telefoon. Deze TFTP-server is toegankelijk via een AnyConnect-sessie.

Als de IP-telefoon de TFTP-server van een lokale DHCP-server ontvangt maar dat adres niet correct is, kunt u de alternatieve TFTP-serveroptie gebruiken om het IP-adres van de TFTP-server te omzeilen dat door de DHCP-server is opgegeven. Deze procedure beschrijft hoe de alternatieve TFTP-server moet worden toegepast:

1. Navigeer in op **instellingen > Netwerkconfiguratie > IPv4-configuratie**.
2. Scrollt naar de alternatieve TFTP-optie.
3. Druk op Ja softkey voor de telefoon om een alternatieve TFTP server te gebruiken; anders drukt u op de toets No. Als de optie vergrendeld is, drukt u op \* # om deze te ontgrendelen.
4. Druk op de knop Opslaan.
5. Pas de Alternate TFTP Server onder de optie TFTP Server 1 toe.

Bekijk de statusberichten in de webbrowser of in de telefoonmenu's direct om te bevestigen dat de telefoon de juiste informatie ontvangt. Als de communicatie correct is ingesteld, ziet u berichten als deze:



# Status Messages

Cisco Unified IP Phone CP-7962G ( SEP8CB64F576113 )

## Device Logs

[Console Logs](#)

[Core Dumps](#)

[Status Messages](#)

[Debug Display](#)

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

Als de telefoon de informatie van de server van TFTP niet kan terugkrijgen, ontvangt u TFTP foutmeldingen:

# 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**

## Verlengen van het ASA SSL-certificaat

Als u een functionele AnyConnect VPN-telefooninstelling hebt, maar uw ASA SSL-certificaat binnenkort verloopt, hoeft u alle IP-telefoons niet naar de hoofdsite te brengen om de nieuwe SSL-certificaten aan de telefoon te injecteren. u kunt de nieuwe certificaten toevoegen terwijl VPN is verbonden.

Als u het CA-certificaat van de ASA hebt geëxporteerd of geïmporteerd in plaats van het identiteitsbewijs en als u tijdens deze vernieuwing dezelfde verkoper (CA) wilt blijven gebruiken, hoeft u het certificaat niet in de UCM te wijzigen, omdat dit hetzelfde blijft. Maar als u het identiteitsbewijs gebruikt, is deze procedure nodig. anders komt de hashwaarde tussen de ASA en IP telefoon niet overeen en wordt de verbinding niet vertrouwd door de telefoon.

1. Verleng het certificaat op de ASA.

Opmerking: Raadpleeg voor meer informatie [ASA 8.x: Verleng en Installeer het SSL-](#)

[certificaat met ASDM](#). Maak een afzonderlijk trustpunt en pas dit nieuwe certificaat niet toe met het **ssl vertrouwen <name> buiten** commando totdat u het certificaat op alle VPN-telefoons hebt toegepast.

2. Exporteren van het nieuwe certificaat.
3. Importeer het nieuwe certificaat aan de CUCM als Phone-VPN-Trust certificaat.  
Opmerking: Let op dat [CSCuh19734 uploadcerts met dezelfde GN die oude cert in Phone-VPN-trust zullen overschrijven](#)
4. Navigeer naar de VPN Gateway Configuration in het CUCM en pas het nieuwe certificaat toe. U hebt nu beide certificaten: het certificaat dat op het punt staat te vervallen en het nieuwe certificaat dat nog niet op de ASA is toegepast.
5. Pas deze nieuwe configuratie op de IP-telefoon toe. Navigeren in om **Config > Beginwaarden > Herstart** toe **te passen** om de nieuwe configuratieveranderingen in de IP-telefoon door de VPN-tunnel te injecteren. Zorg ervoor dat alle IP-telefoons via VPN zijn aangesloten en dat ze de TFTP-server via de tunnel kunnen bereiken.
6. Gebruik TFTP om de statusberichten en het configuratiebestand te controleren om te bevestigen dat de IP-telefoon het configuratiebestand met de wijzigingen heeft ontvangen.
7. Pas het nieuwe SSL Trustpoint in de ASA toe en vervang het oude certificaat.

Opmerking: Als het ASA SSL-certificaat al is verlopen en de IP-telefoons niet via AnyConnect kunnen worden aangesloten, u kunt de wijzigingen (zoals de nieuwe ASA-certificaathash) naar de IP-telefoon duwen. Stel het TFTP in de IP-telefoon handmatig in op een openbaar IP-adres, zodat de IP-telefoon de informatie vanuit deze telefoon kan ophalen. Gebruik een openbare TFTP-server om het configuratiebestand te ontvangen. een voorbeeld is een Port Forwarding op de ASA te creëren en het verkeer opnieuw te richten naar de interne TFTP server.