

Fehlerbehebung bei AnyConnect VPN-Telefonen - IP-Telefone, ASA und CUCM

Inhalt

[Einführung](#)

[Hintergrundinformationen](#)

[VPN-Telefonlizenz auf ASA bestätigen](#)

[Eingeschränkter Export und uneingeschränkter Export von CUCM](#)

[Häufige Probleme bei der ASA](#)

[Zertifikate zur Verwendung auf der ASA](#)

[Trustpoint/Zertifikat für ASA-Export und CUCM-Import](#)

[ASA stellt anstelle des konfigurierten RSA-Zertifikats ein selbstsigniertes ECDSA-Zertifikat vor.](#)

[Externe Datenbank für die Authentifizierung von IP-Telefonbenutzern](#)

[Zertifikats-Hash stimmt zwischen ASA-Zertifikat und VPN-TelefonTrust-Liste überein](#)

[SHA1-Hash überprüfen](#)

[Konfigurationsdatei für das IP-Telefon herunterladen](#)

[Dekodieren des Hashs](#)

[VPN-Lastenausgleich und IP-Telefone](#)

[CSD und IP-Telefone](#)

[ASA-Protokolle](#)

[ASA-Debugger](#)

[DAP-Regeln](#)

[Von DfltGrpPolicy oder anderen Gruppen geerbte Werte](#)

[Unterstützte Verschlüsselungs-Chiffren](#)

[Häufige Probleme beim CUCM](#)

[VPN-Einstellungen auf IP-Telefon nicht angewendet](#)

[Authentifizierungsmethode für Zertifikate](#)

[Host-ID-Prüfung](#)

[Zusätzliche Fehlerbehebung](#)

[Protokolle und zu verwendende Debugger in der ASA](#)

[IP-Telefonprotokolle](#)

[Korrelierung von Problemen zwischen ASA-Protokollen und IP-Telefonprotokollen](#)

[ASA-Protokolle](#)

[Telefonprotokolle](#)

[Span-Funktion für PC-Port](#)

[Änderungen bei der Konfiguration von IP-Telefonen bei Verbindung über VPN](#)

[Verlängerung des ASA SSL-Zertifikats](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie Probleme mit IP-Telefonen beheben können, die das Secure Sockets Layer (SSL)-Protokoll (Cisco AnyConnect Secure Mobility Client) verwenden, um eine Verbindung zu einer Cisco Adaptive Security Appliance (ASA) herzustellen, die als VPN-Gateway verwendet wird, und um eine Verbindung zu einem Cisco Unified Communications Manager (CUCM) herzustellen, der als Sprachserver verwendet wird.

Konfigurationsbeispiele für AnyConnect mit VPN-Telefonen finden Sie in den folgenden Dokumenten:

- [Konfigurationsbeispiel für SSL VPN mit IP-Telefonen](#)
- [Konfigurationsbeispiel für ein AnyConnect VPN-Telefon mit Zertifikatsauthentifizierung](#)

Hintergrundinformationen

Bevor Sie SSL VPN mit IP-Telefonen bereitstellen, stellen Sie sicher, dass Sie diese ursprünglichen Anforderungen für AnyConnect-Lizenzen für die ASA und für die exportbeschränkte Version des CUCM in den USA erfüllt haben.

VPN-Telefonlizenz auf ASA bestätigen

Die VPN-Telefonlizenz aktiviert die Funktion in der ASA. Um die Anzahl der Benutzer zu überprüfen, die eine Verbindung mit AnyConnect herstellen können (unabhängig davon, ob es sich um ein IP-Telefon handelt oder nicht), überprüfen Sie die AnyConnect Premium SSL-Lizenz. Weitere Informationen finden Sie unter [Welche ASA-Lizenz ist für IP-Telefon- und mobile VPN-Verbindungen erforderlich?](#) für weitere Informationen.

Verwenden Sie auf der ASA den Befehl **show version**, um zu überprüfen, ob die Funktion aktiviert ist. Der Lizenzname unterscheidet sich von der ASA-Version:

- ASA Version 8.0.x: Der Name der Lizenz ist AnyConnect für das Linksys-Telefon.
- ASA Version 8.2.x und höher: Der Lizenzname ist AnyConnect für Cisco VPN Phone.

Hier ein Beispiel für ASA Version 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 ein Beispiel für ASA-Versionen 8.2.x und höher:

```
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.
```

Eingeschränkter Export und uneingeschränkter Export von CUCM

Für die VPN-Telefonfunktion sollten Sie eine exportbeschränkte Version von CUCM in den USA bereitstellen.

Wenn Sie eine uneingeschränkte Version von CUCM in den USA exportieren, beachten Sie Folgendes:

- Sicherheitskonfigurationen für IP-Telefone werden geändert, um Signalisierung und Medienverschlüsselung zu deaktivieren. Dazu gehört auch die Verschlüsselung durch die VPN-Telefonfunktion.
- VPN-Details können nicht über Import/Export exportiert werden.

- Die Kontrollkästchen für VPN Profile, VPN Gateway, VPN Group und VPN Feature Configuration werden nicht angezeigt.

Hinweis: Wenn Sie ein Upgrade auf die uneingeschränkte CUCM-Version für die USA durchführen, können Sie zu einem späteren Zeitpunkt kein Upgrade auf die exportbeschränkte Version dieser Software durchführen oder eine Neuinstallation durchführen.

Häufige Probleme bei der ASA

Hinweis: Sie können den [Cisco CLI Analyzer](#) (nur [registrierte](#) Kunden) verwenden, um eine Analyse der **angezeigten** Befehlsausgaben anzuzeigen. Vor der Verwendung von **Debug-**Befehlen sollten Sie auch das Cisco Dokument [Wichtige Informationen über Debug-Befehle](#) lesen.

Zertifikate zur Verwendung auf der ASA

Auf der ASA können Sie selbst signierte SSL-Zertifikate, SSL-Zertifikate von Drittanbietern und Platzhalterzertifikate verwenden. All diese Elemente schützen die Kommunikation zwischen dem IP-Telefon und der ASA.

Es kann nur ein Identitätszertifikat verwendet werden, da jeder Schnittstelle nur ein Zertifikat zugewiesen werden kann.

Installieren Sie bei SSL-Zertifikaten von Drittanbietern die gesamte Kette in der ASA, und fügen Sie alle Zwischen- und Root-Zertifikate ein.

Trustpoint/Zertifikat für ASA-Export und CUCM-Import

Das Zertifikat, das die ASA dem IP-Telefon während der SSL-Aushandlung vorlegt, muss von der

ASA exportiert und in den CUCM importiert werden. Überprüfen Sie den Trustpoint, der der Schnittstelle zugewiesen ist, mit der die IP-Telefone verbunden sind, um zu erfahren, welches Zertifikat von der ASA exportiert werden soll.

Verwenden Sie den Befehl **show run ssl**, um den zu exportierenden Trustpoint (Zertifikat) zu überprüfen. Weitere Informationen finden Sie im [Konfigurationsbeispiel für das AnyConnect VPN-Telefon mit Zertifikatsauthentifizierung](#).

Hinweis: Wenn Sie ein Zertifikat eines Drittanbieters für eine oder mehrere ASAs bereitgestellt haben, müssen Sie jedes Identitätszertifikat von jeder ASA exportieren und anschließend als "phone-vpn-trust" in den CUCM importieren.

ASA stellt anstelle des konfigurierten RSA-Zertifikats ein selbstsigniertes ECDSA-Zertifikat vor.

Wenn dieses Problem auftritt, können neuere Modelltelefone keine Verbindung herstellen, während bei den älteren Modelltelefonen keine Probleme auftreten. Im Folgenden sind die Protokolle am Telefon aufgeführt, wenn dieses Problem auftritt:

```
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 Version 9.4.1 und höher wird die Verschlüsselung der elliptischen Kurve für SSL/TLS unterstützt. Wenn ein SSL VPN-Client mit elliptischer Kurve (z. B. ein neues Telefonmodell) mit der ASA verbunden wird, wird die Verschlüsselungssuite mit elliptischer Kurve ausgehandelt, und die ASA stellt dem SSL VPN-Client ein Zertifikat mit elliptischer Kurve zur Verfügung, selbst wenn die Schnittstelle, die mit einem RSA-basierten Trustpoint konfiguriert ist, konfiguriert ist. Um zu verhindern, dass die ASA ein selbstsigniertes SSL-Zertifikat anzeigt, muss der Administrator die Verschlüsselungssuiten entfernen, die über den Befehl **ssl cipher** entsprechen. Bei einer Schnittstelle, die mit einem RSA-Trustpoint konfiguriert ist, kann der Administrator diesen Befehl ausführen, sodass nur RSA-basierte Chiffren ausgehandelt werden:

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

Bei der Implementierung der Cisco Bug-ID [CSCuu02848](#) wird der Konfiguration Priorität eingeräumt. Explizit konfigurierte Zertifikate werden immer verwendet. Selbstsignierte Zertifikate werden nur verwendet, wenn kein konfiguriertes Zertifikat vorhanden ist.

Vorgeschlagene Client-Chips	Nur RSA-Zertifikat	Nur EC Cert	Beide Zertifizierungen	Keine
Nur RSA-Chiffren	Verwendet RSA-Zertifikat Verwendet RSA-Chiffren	Verwendet selbst signierte RSA-Zertifikate Verwendet RSA-Chiffren	Verwendet RSA-Zertifikat Verwendet RSA-Chiffren	Verwendet selbst signierte RSA-Zertifikate Verwendet RSA-Chiffren
Nur EC-Chiffren (selten)	Verbindung fehlgeschlagen	Verwendet EC-Zertifikat Verwendet EC-Chiffren	Verwendet EC-Zertifikat Verwendet EC-Chiffren	Verwendet selbst signierte EC-Zertifikate Verwendet EC-Chiffren
Nur beide Ciphers	Verwendet RSA-Zertifikat Verwendet RSA-Chiffren	Verwendet EC-Zertifikat Verwendet EC-Chiffren	Verwendet EC-Zertifikat Verwendet EC-Chiffren	Verwendet selbst signierte EC-Zertifikate Verwendet EC-Chiffren

Externe Datenbank für die Authentifizierung von IP-Telefonbenutzern

Sie können eine externe Datenbank verwenden, um IP-Telefonbenutzer zu authentifizieren. Protokolle wie das Lightweight Directory Access Protocol (LDAP) oder RADIUS (Remote Authentication Dial In User Service) können für die Authentifizierung von VPN-Telefonbenutzern verwendet werden.

Zertifikats-Hash stimmt zwischen ASA-Zertifikat und VPN-TelefonTrust-Liste überein

Denken Sie daran, dass Sie das Zertifikat herunterladen müssen, das der ASA SSL-Schnittstelle zugewiesen ist, und es als Telefon-VPN-Trust-Zertifikat in CUCM hochladen müssen.

Unterschiedliche Umstände können dazu führen, dass der Hash für dieses von der ASA präsentierte Zertifikat nicht mit dem Hash übereinstimmt, den der CUCM-Server generiert und über die Konfigurationsdatei an das VPN-Telefon übermittelt.

Nachdem die Konfiguration abgeschlossen ist, testen Sie die VPN-Verbindung zwischen dem IP-Telefon und der ASA. Wenn die Verbindung weiterhin fehlschlägt, überprüfen Sie, ob der Hash des ASA-Zertifikats mit dem Hash übereinstimmt, den das IP-Telefon erwartet:

1. Überprüfen Sie den SHA1-Hash (Secure Hash Algorithm 1) der ASA.
2. Verwenden Sie TFTP, um die Konfigurationsdatei für das IP-Telefon vom CUCM herunterzuladen.
3. Dekodieren Sie den Hash von hexadezimal auf Base 64 oder von Base 64 auf hexadezimal.

SHA1-Hash überprüfen

Die ASA präsentiert das Zertifikat, das mit dem Befehl **ssl trustpoint** auf der Schnittstelle angewendet wird, mit der das IP-Telefon verbunden ist. Um dieses Zertifikat zu überprüfen, öffnen Sie den Browser (in diesem Beispiel Firefox), und geben Sie die URL (group-url) ein, mit der die Telefone eine Verbindung herstellen sollen:

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

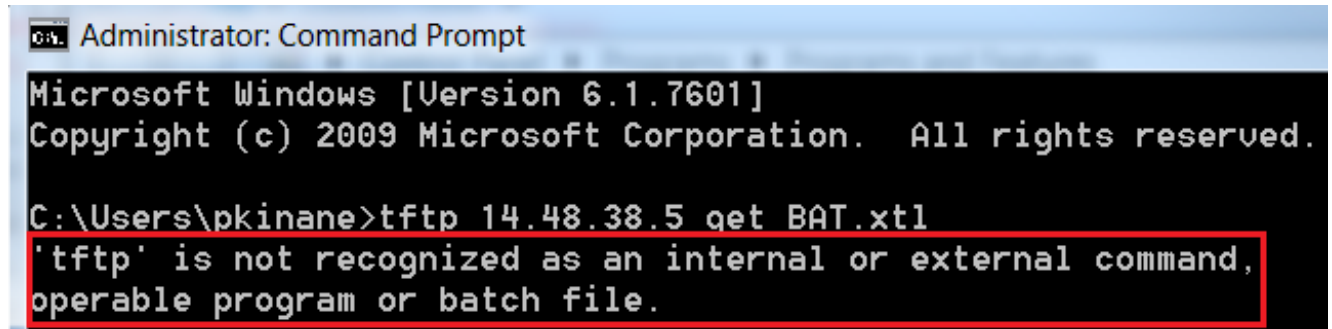
3 SHA1 Fingerprint	E5:7E:81:EA:99:54:C1:44:97:66:78:D0:E2:41:8C:DF:79:A9:31:76
MD5 Fingerprint	D7:10:78:FB:61:A2:F6:C2:01:07:6C:03:0E:17:EF:F9

Konfigurationsdatei für das IP-Telefon herunterladen

Laden Sie von einem PC mit direktem Zugriff auf den CUCM die TFTP-Konfigurationsdatei für das Telefon mit Verbindungsproblemen herunter. Es gibt zwei Downloadmethoden:

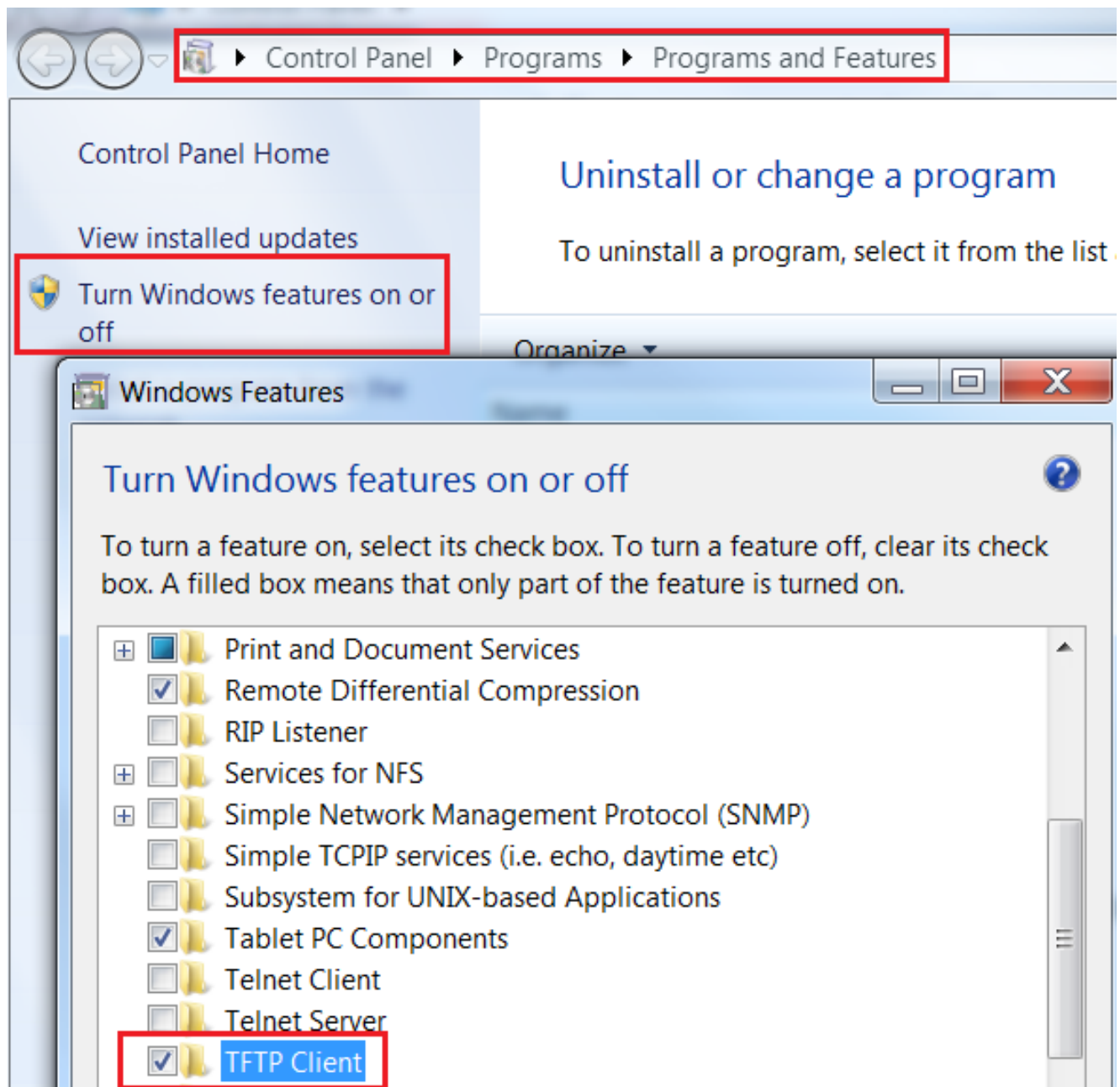
1. Öffnen Sie in Windows eine CLI-Sitzung, und verwenden Sie den Befehl `tftp -i <TFTP-Server> GET SEP<Phone Mac Address>.cnf.xml`.

Hinweis: Wenn Sie einen Fehler wie den unten angegebenen erhalten, sollten Sie bestätigen, dass die TFTP-Client-Funktion aktiviert ist.

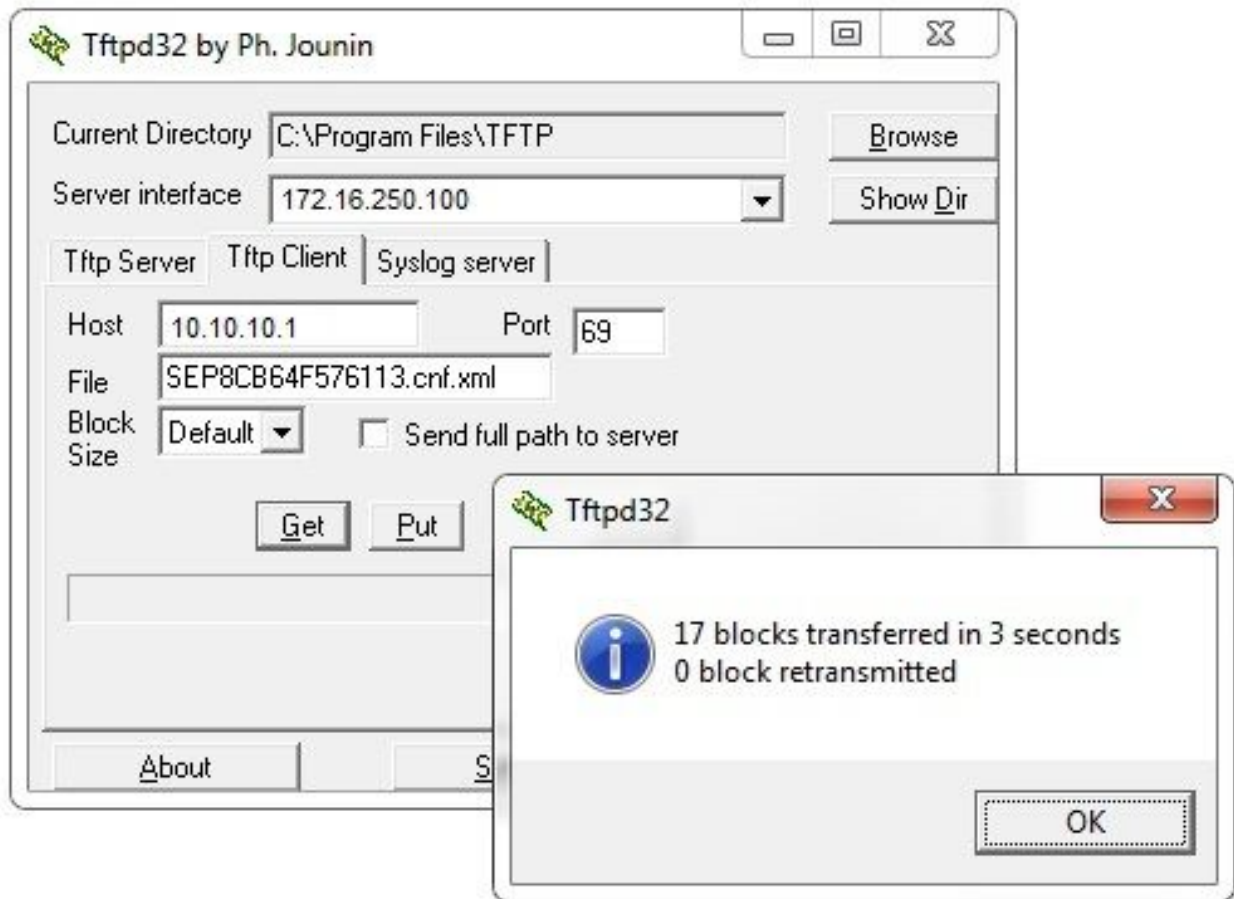


```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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



2. Verwenden Sie eine Anwendung wie [Tftpd32](#), um die Datei herunterzuladen:



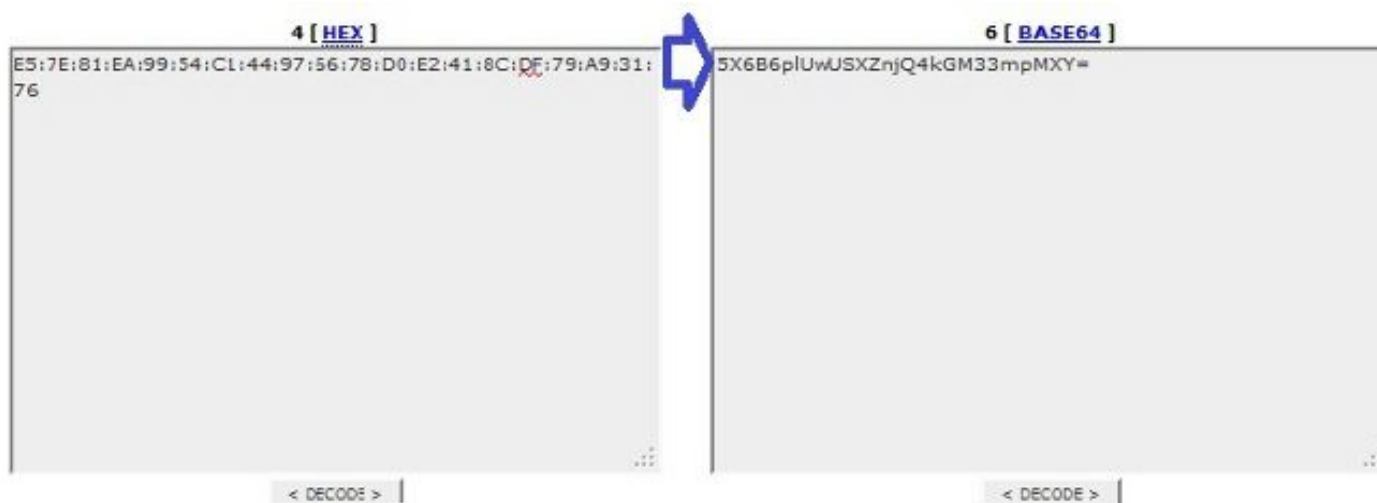
3. Öffnen Sie nach dem Herunterladen der Datei die XML-Datei, und suchen Sie die *vpnGroup*-Konfiguration. In diesem Beispiel werden der Abschnitt und der zu überprüfende *certHash* veranschaulicht:

```
<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>
```

Dekodieren des Hashs

Bestätigen Sie, dass beide Hashwerte übereinstimmen. Der Browser stellt den Hash im hexadezimalen Format dar, während die XML-Datei Base 64 verwendet. Konvertieren Sie daher ein Format in das andere, um die Übereinstimmung zu bestätigen. Es stehen viele Übersetzer zur Verfügung. Ein Beispiel ist der [TRANSLATOR, BINARY](#).



Hinweis: Wenn der vorherige Hash-Wert nicht übereinstimmt, vertraut das VPN-Telefon nicht der Verbindung, die mit der ASA ausgehandelt wird, und die Verbindung schlägt fehl.

VPN-Lastenausgleich und IP-Telefone

SSL VPN mit Lastausgleich wird für VPN-Telefone nicht unterstützt. VPN-Telefone führen keine echte Zertifikatsvalidierung durch, sondern verwenden Hashes, die vom CUCM zur Validierung der Server nach unten gedrückt werden. Da der VPN-Lastenausgleich grundsätzlich eine HTTP-Umleitung ist, müssen die Telefone mehrere Zertifikate validieren, was zu einem Ausfall führt. Symptome eines VPN-Lastenausgleichs:

- Das Telefon wechselt zwischen den Servern und es dauert außerordentlich lange, bis eine Verbindung hergestellt wird oder ausfällt.
- Die Telefonprotokolle enthalten Meldungen wie die folgenden:

```
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 und IP-Telefone

Derzeit unterstützen IP-Telefone nicht den Cisco Secure Desktop (CSD) und stellen keine Verbindung her, wenn der CSD für Tunnelgruppen oder global in der ASA aktiviert ist.

Überprüfen Sie zunächst, ob der ASA-CSD aktiviert ist. Geben Sie den Befehl **show run webvpn** in der ASA-CLI ein:

```
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#
```

Um CSD-Probleme während einer IP-Telefonverbindung zu überprüfen, überprüfen Sie die Protokolle oder das Debuggen in der ASA.

ASA-Protokolle

```
%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-Debugger

```
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>

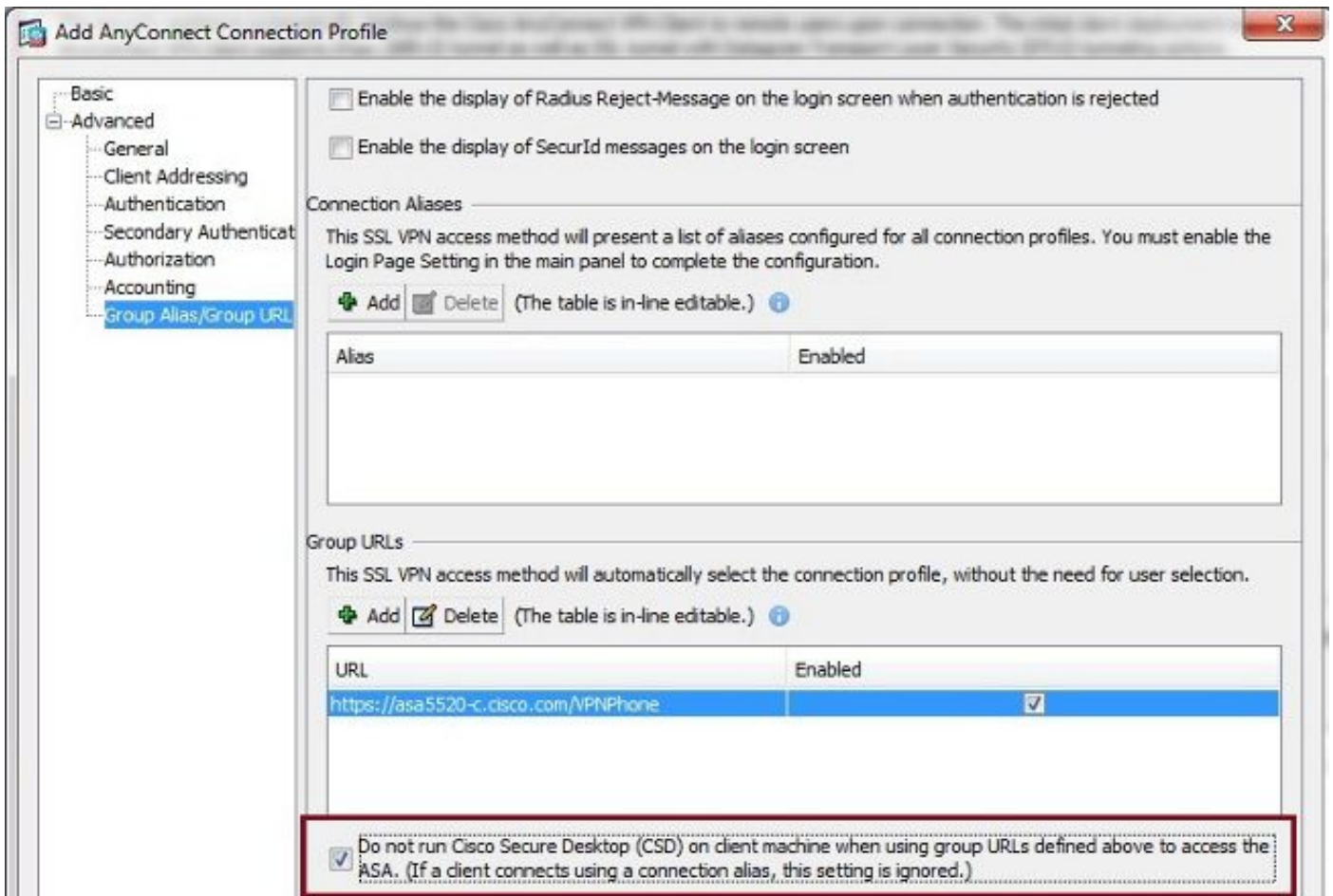
Hinweis: In einer umfangreichen Bereitstellung mit einer hohen Anzahl an AnyConnect-Benutzern empfiehlt Cisco, das **Debug-Webvpn anyconnect** nicht zu aktivieren. Die Ausgabe kann nicht nach IP-Adresse gefiltert werden, sodass möglicherweise eine große Menge an Informationen erstellt wird.

In ASA Version 8.2 und höher müssen Sie den Befehl **ohne CSD** unter den webvpn-Attributen der Tunnelgruppe anwenden:

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

In früheren Versionen der ASA war dies nicht möglich, sodass die einzige Lösung darin bestand, den CSD global zu deaktivieren.

Im Cisco Adaptive Security Device Manager (ASDM) können Sie den CSD für ein bestimmtes Verbindungsprofil deaktivieren, wie in diesem Beispiel gezeigt:

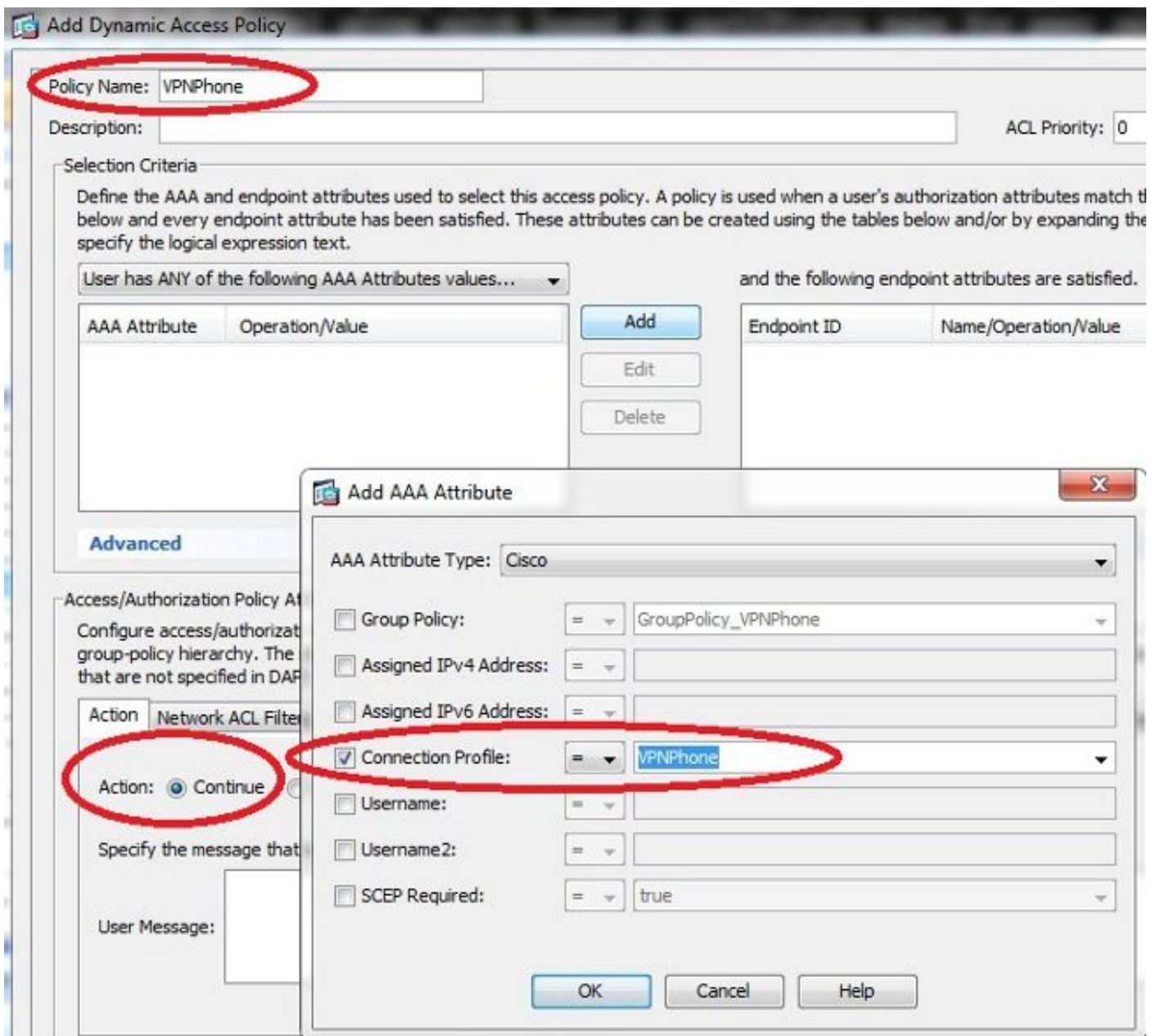


Hinweis: Verwenden Sie eine Gruppen-URL, um die CSD-Funktion zu deaktivieren.

DAP-Regeln

In den meisten Bereitstellungen werden nicht nur IP-Telefone mit der ASA verbunden, sondern auch verschiedene Gerätetypen (Microsoft, Linux, Mac OS) und mobile Geräte (Android, iOS) miteinander verbunden. Aus diesem Grund ist es normal, eine vorhandene Konfiguration von Dynamic Access Policy (DAP)-Regeln zu finden, bei der die Standardaktion unter der DfltAccessPolicy in der Regel die Beendigung der Verbindung ist.

In diesem Fall erstellen Sie eine separate DAP-Regel für die VPN-Telefone. Verwenden Sie einen bestimmten Parameter, z. B. das Verbindungsprofil, und legen Sie die Aktion auf **Weiter fest**:



Wenn Sie keine spezifische DAP-Richtlinie für IP-Telefone erstellen, zeigt die ASA einen Treffer unter der DfltAccessPolicy und eine fehlgeschlagene Verbindung an:

```
%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
```

Nachdem Sie eine bestimmte DAP-Richtlinie für die IP-Telefone erstellt haben, deren Aktion auf

Weiter eingestellt ist, können Sie Folgendes verbinden:

```
%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
```

Von DfltGrpPolicy oder anderen Gruppen geerbte Werte

In vielen Fällen ist die DfltGrpPolicy mit mehreren Optionen eingerichtet. Standardmäßig werden diese Einstellungen für die IP-Telefonsitzung übernommen, es sei denn, sie werden manuell in der Gruppenrichtlinie festgelegt, die das IP-Telefon verwenden soll.

Folgende Parameter können sich auf die Verbindung auswirken, wenn sie von der DfltGrpPolicy geerbt werden:

- Gruppensperre
- VPN-Tunnel-Protokoll
- VPN-Simultanmeldungen
- VPN-Filter

Angenommen, Sie haben diese Beispielkonfiguration in der DfltGrpPolicy und im GroupPolicy_VPNPhone:

```
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
```


Die Verbindung erbt die Parameter aus der DfltGrpPolicy, die nicht explizit unter dem GroupPolicy_VPNPhone angegeben wurden, und leitet alle Informationen während der Verbindung an das IP-Telefon weiter.

Um dies zu vermeiden, müssen Sie die Werte manuell direkt in der Gruppe angeben:

```
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
```

Um die Standardwerte der DfltGrpPolicy zu überprüfen, verwenden Sie den Befehl **show run all group policy (Alle Gruppenrichtlinien anzeigen)**. In diesem Beispiel wird der Unterschied zwischen den Outputs klargestellt:

```
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
```

Im Folgenden finden Sie die Ergebnisse der Gruppenrichtlinien, die Attribute über das ASDM erben:

Name:	DRIGrPolicy
Banner:	
SCEP forwarding URL:	
Address Pools:	
IPv6 Address Pools:	
More Options	
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
SCEP forwarding URL:	<input checked="" type="checkbox"/> Inherit
Address Pools:	<input checked="" type="checkbox"/> Inherit
IPv6 Address Pools:	<input checked="" type="checkbox"/> Inherit
More Options	
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

Unterstützte Verschlüsselungs-Chiffren

Ein mit dem 7962G IP-Telefon und der Firmware Version 9.1.1 getestetes AnyConnect VPN-Telefon unterstützt nur zwei Chiffren, die beide Advanced Encryption Standard (AES) sind: AES256-SHA und AES128-SHA. Wenn die richtigen Chiffren nicht in der ASA angegeben sind, wird die Verbindung abgelehnt, wie im ASA-Protokoll gezeigt:

```
%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
```

Um zu überprüfen, ob die ASA die richtigen Chiffren aktiviert hat, geben Sie den Befehl **show run all ssl** ein und **show ssl**-Befehle ein:

```
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
```

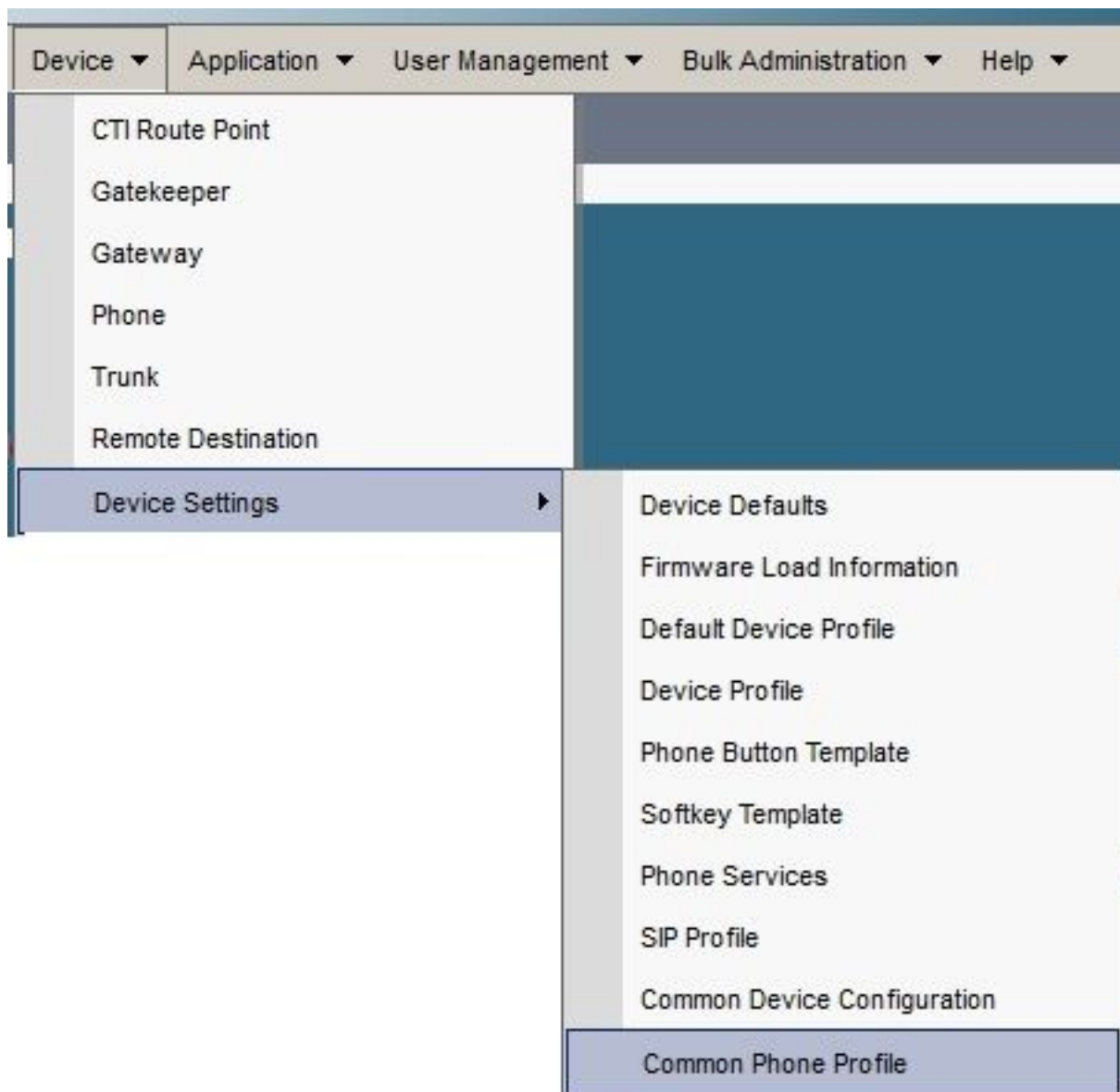
```
ASA5510-F#
```

Häufige Probleme beim CUCM

VPN-Einstellungen auf IP-Telefon nicht angewendet

Nachdem die Konfiguration auf dem CUCM erstellt wurde (Gateway, Gruppe und Profil), übernehmen Sie die VPN-Einstellungen im allgemeinen Telefonprofil:

1. Navigieren Sie zu **Gerät > Geräteeinstellungen > Allgemeines Telefonprofil**.



2. Geben Sie die VPN-Informationen ein:

The screenshot shows the 'Common Phone Profile Configuration' page. At the top, there is a title bar with the text 'Common Phone Profile Configuration'. Below the title bar is a toolbar with several icons and labels: 'Save' (floppy disk icon), 'Delete' (red X icon), 'Copy' (document icon), 'Reset' (circular arrow icon), 'Apply Config' (pencil icon), and 'Add New' (plus sign icon). Below the toolbar is a section titled 'VPN Information'. This section contains two dropdown menus. The first dropdown menu is labeled 'VPN Group' and has 'Phone' selected. The second dropdown menu is labeled 'VPN Profile' and also has 'Phone' selected.

3. Navigieren Sie zu **Gerät > Telefon**, und bestätigen Sie, dass dieses Profil der Telefonkonfiguration zugewiesen ist:



Authentifizierungsmethode für Zertifikate

Es gibt zwei Möglichkeiten, die Zertifikatauthentifizierung für IP-Telefone zu konfigurieren: Vom Hersteller installiertes Zertifikat (MIC) und lokales Zertifikat (LSC). Informationen zur Auswahl der besten Option für Ihre Situation finden Sie unter [Konfigurationsbeispiel für AnyConnect VPN-Telefon mit Zertifikatsauthentifizierung](#).

Wenn Sie die Zertifikatsauthentifizierung konfigurieren, exportieren Sie die Zertifikate (Stammzertifizierungsstelle) vom CUCM-Server, und importieren Sie sie in die ASA:

1. Melden Sie sich beim CUCM an.
2. Navigieren Sie zu **Unified OS Administration > Security > Certificate Management**.
3. Suchen Sie die Certificate Authority Proxy Function (CAPF) oder Cisco_Manufacturing_CA. Der Zertifikatstyp hängt davon ab, ob Sie die MIC- oder LSC-Zertifikatauthentifizierung verwendet haben.
4. Laden Sie die Datei auf den lokalen Computer herunter.

Melden Sie sich nach dem Herunterladen der Dateien über die CLI oder ASDM bei der ASA an, und importieren Sie das Zertifikat als Zertifizierungsstellenzertifikat.

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	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

Standardmäßig sind alle Telefone, die VPN unterstützen, mit MICs vorinstalliert. Die Telefone der Modelle 7960 und 7940 verfügen nicht über ein MIC und erfordern ein spezielles Installationsverfahren, damit das LSC sicher registriert werden kann.

Die neuesten Cisco IP-Telefone (8811, 8841, 8851 und 8861) umfassen MIC-Zertifikate, die von der neuen Manufacturing SHA2 CA signiert werden:

- Die CUCM-Version 10.5(1) enthält die neuen SHA2-Zertifikate und vertraut diesen.
- Wenn Sie eine ältere CUCM-Version ausführen, müssen Sie möglicherweise das neue Zertifikat für die Zertifizierungsstelle für die Fertigung herunterladen und:

Laden Sie sie in die CAPF-trust-Datei hoch, damit die Telefone sich mit CAPF authentifizieren können, um ein LSC zu erhalten.

Laden Sie sie in CallManager-trust hoch, wenn Sie die Authentifizierung der Telefone mit einem MIC für SIP 5061 zulassen möchten.

Tipp: Klicken Sie auf [diesen Link](#), um die SHA2-CA abzurufen, wenn der CUCM derzeit eine ältere Version ausführt.

Vorsicht: Cisco empfiehlt, MICs nur für die LSC-Installation zu verwenden. Cisco unterstützt LSCs für die Authentifizierung der TLS-Verbindung mit dem CUCM. Da die MIC-Root-Zertifikate kompromittiert werden können, können Kunden, die Telefone so konfigurieren, dass sie MICs für die TLS-Authentifizierung oder für andere Zwecke verwenden, dies auf eigenes Risiko tun. Cisco übernimmt keine Haftung, wenn die MICs kompromittiert werden.

Wenn auf dem Telefon ein LSC vorhanden ist, verwendet die Authentifizierung standardmäßig das LSC, unabhängig davon, ob ein MIC auf dem Telefon vorhanden ist. Wenn ein MIC und ein LSC auf dem Telefon vorhanden sind, verwendet die Authentifizierung das LSC. Wenn ein LSC im Telefon nicht vorhanden ist, aber ein MIC vorhanden ist, verwendet die Authentifizierung das MIC.

Hinweis: Beachten Sie, dass Sie für die Zertifikatsauthentifizierung das SSL-Zertifikat von der ASA exportieren und in den CUCM importieren sollten.

Host-ID-Prüfung

Wenn der gebräuchliche Name (CN) im Betreff des Zertifikats nicht mit der URL (group-url) übereinstimmt, die die Telefone für die Verbindung mit der ASA über das VPN verwenden, deaktivieren Sie die Host-ID-Prüfung auf dem CUCM, oder verwenden Sie ein Zertifikat in der ASA, das dieser URL auf der ASA entspricht.

Dies ist erforderlich, wenn das SSL-Zertifikat der ASA ein Platzhalterzertifikat ist, das SSL-Zertifikat ein anderes SAN (Subject Alternative Name) enthält oder die URL mit der IP-Adresse statt mit dem vollqualifizierten Domännennamen (FQDN) erstellt wurde.

Dies ist ein Beispiel für ein IP-Telefonprotokoll, wenn der CN des Zertifikats nicht mit der URL übereinstimmt, die das Telefon zu erreichen versucht.

```
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!!
```

Um den Check der Host-ID im CUCM zu deaktivieren, navigieren Sie zu **Erweiterte Funktionen > VPN > VPN Profile:**

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

Zusätzliche Fehlerbehebung

Protokolle und zu verwendende Debugger in der ASA

Auf der ASA können Sie diese Debug- und Protokolldateien für die Fehlerbehebung aktivieren:

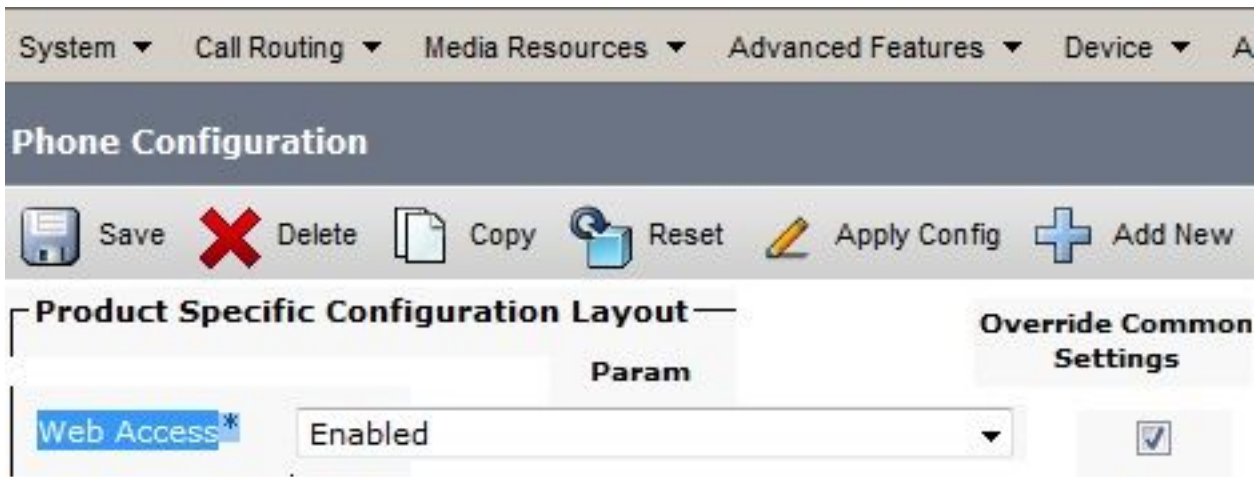
```
logging enable
logging buffer-size 1048576
logging buffered debugging

debug webvpn anyconnect 255
```

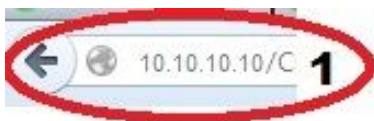
Hinweis: In einer umfangreichen Bereitstellung mit einer hohen Anzahl an AnyConnect-Benutzern empfiehlt Cisco, das **Debug-Webvpn anyconnect** nicht zu aktivieren. Die Ausgabe kann nicht nach IP-Adresse gefiltert werden, sodass möglicherweise eine große Menge an Informationen erstellt wird.

IP-Telefonprotokolle

Um auf die Telefonprotokolle zuzugreifen, aktivieren Sie die Webzugriffsfunktion. Melden Sie sich beim CUCM an, und navigieren Sie zu **Gerät > Telefon > Telefonkonfiguration**. Suchen Sie das IP-Telefon, auf dem Sie diese Funktion aktivieren möchten, und suchen Sie nach dem Abschnitt für den Webzugriff. Anwenden der Konfigurationsänderungen auf das IP-Telefon:



Sobald Sie den Dienst aktiviert und das Telefon zurückgesetzt haben, um diese neue Funktion einzufügen, können Sie im Browser auf IP-Telefonprotokolle zugreifen. verwenden Sie die IP-Adresse des Telefons von einem Computer mit Zugriff auf dieses Subnetz. Rufen Sie die Konsolenprotokolle auf, und überprüfen Sie die fünf Protokolldateien. Da das Telefon die fünf Dateien überschreibt, müssen Sie alle diese Dateien überprüfen, um die gesuchten Informationen zu finden.



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.fd1a.log](#)

[/FS/cache/log181](#)

[/FS/cache/log182](#)

3 [/FS/cache/log178](#)

[/FS/cache/log179](#)

[/FS/cache/log180](#)

Korrelierung von Problemen zwischen ASA-Protokollen und IP-Telefonprotokollen

Dies ist ein Beispiel dafür, wie die Protokolle von ASA und IP-Telefon korreliert werden. In diesem Beispiel stimmt der Hash des Zertifikats auf der ASA nicht mit dem Hash des Zertifikats in der Konfigurationsdatei des Telefons überein, da das Zertifikat auf der ASA durch ein anderes Zertifikat ersetzt wurde.

ASA-Protokolle

```
%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
```

Telefonprotokolle

```
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)]

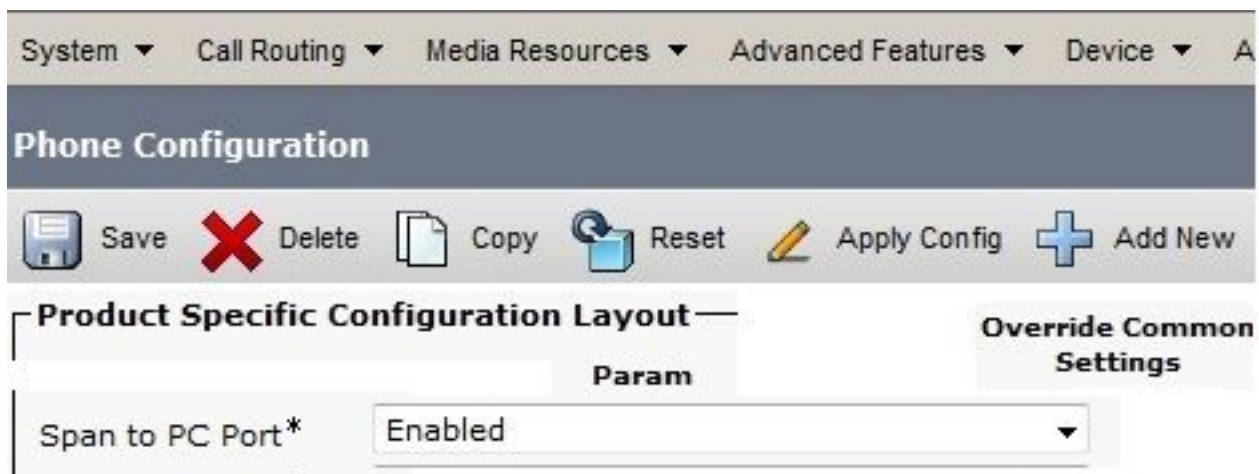
927: NOT 10:19:27.431841 VPNC: vpnc_send_notify: sending signal 28 w/ value 13 to pid 14

928: ERR 10:19:27.432467 VPNC: protocol_handler: login failed

Span-Funktion für PC-Port

Sie können einen Computer direkt an ein Telefon anschließen. Das Telefon verfügt über einen Switch-Port auf der Rückwandplatine.

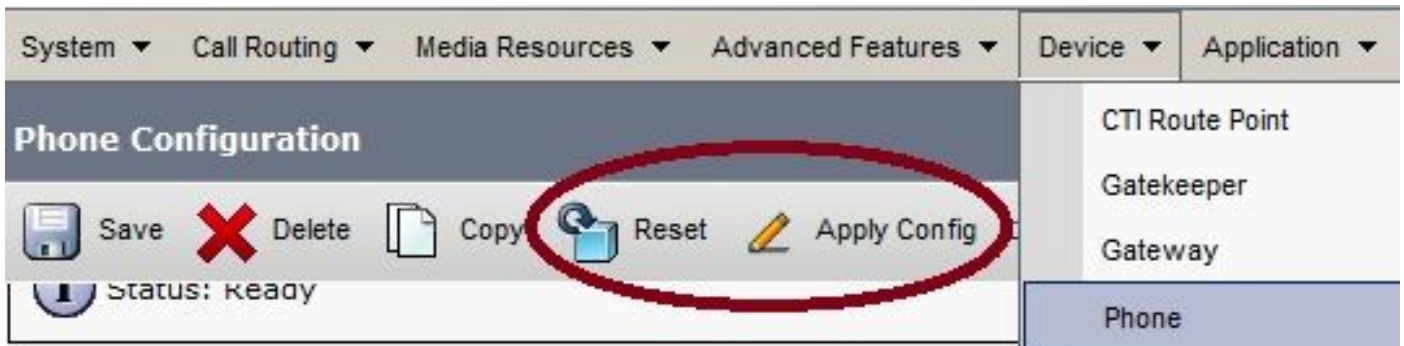
Konfigurieren Sie das Telefon wie zuvor, aktivieren Sie den Port Span to PC auf dem CUCM, und wenden Sie die Konfiguration an. Das Telefon sendet eine Kopie jedes Frames an den PC. Verwenden Sie Wireshark im Promiscuous-Modus, um Datenverkehr zur Analyse zu erfassen.



Änderungen bei der Konfiguration von IP-Telefonen bei Verbindung über VPN

Eine häufige Frage ist, ob Sie die VPN-Konfiguration ändern können, während das IP-Telefon über AnyConnect aus dem Netzwerk verbunden ist. Die Antwort lautet Ja, aber Sie sollten einige Konfigurationseinstellungen bestätigen.

Nehmen Sie die erforderlichen Änderungen am CUCM vor, und wenden Sie die Änderungen dann auf das Telefon an. Es gibt drei Optionen (Apply Config, Reset, Restart), um die neue Konfiguration auf das Telefon zu übertragen. Obwohl alle drei Optionen das VPN vom Telefon und der ASA trennen, können Sie die Verbindung automatisch wieder herstellen, wenn Sie die Zertifikatsauthentifizierung verwenden. Wenn Sie Authentication, Authorization, and Accounting (AAA) verwenden, werden Sie erneut zur Eingabe Ihrer Anmeldeinformationen aufgefordert.



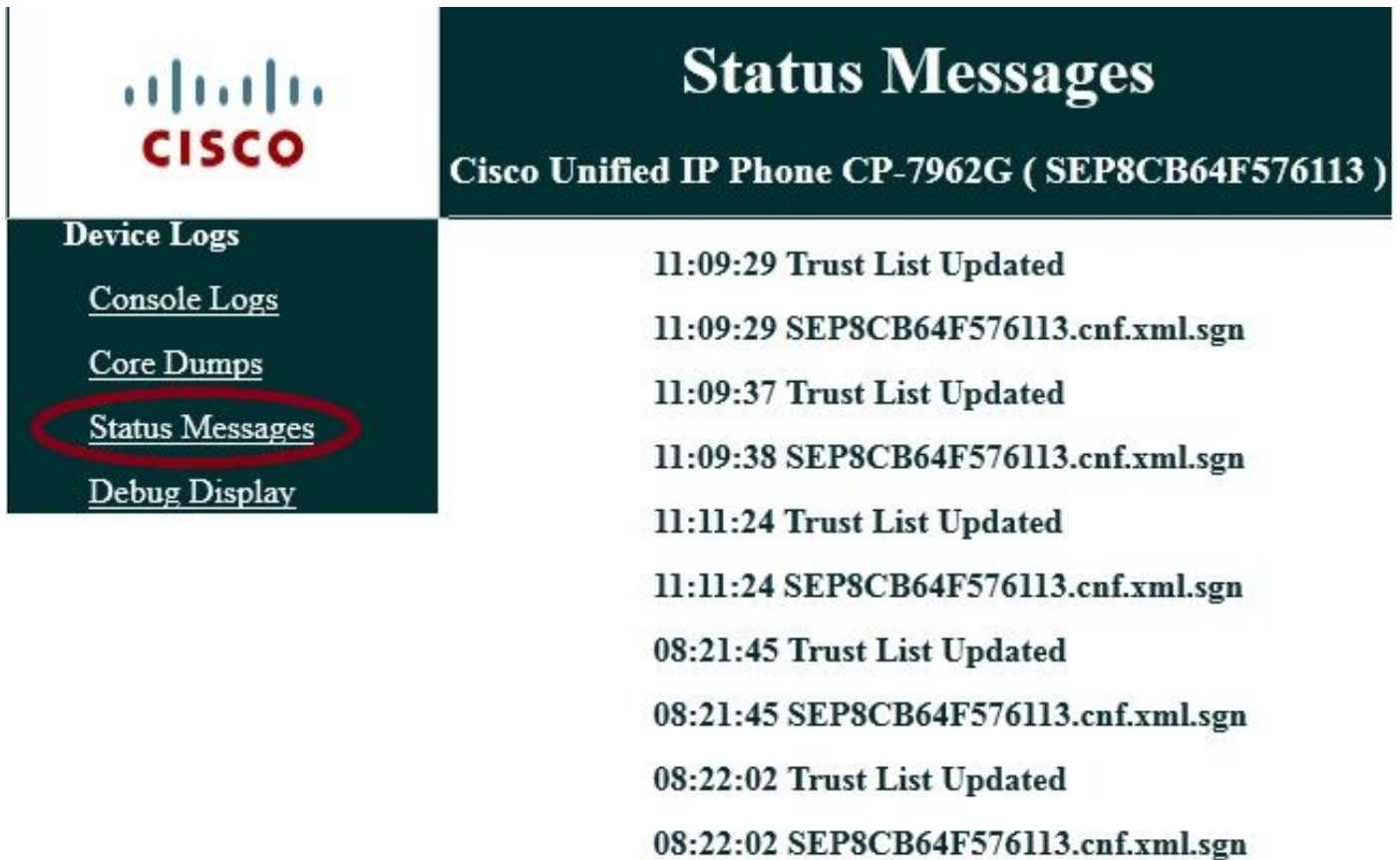
Hinweis: Wenn sich das IP-Telefon auf der Remote-Seite befindet, erhält es normalerweise eine IP-Adresse von einem externen DHCP-Server. Damit das IP-Telefon die neue Konfiguration vom CUCM erhält, sollte es sich an den TFTP-Server in der Hauptniederlassung wenden. Normalerweise ist der CUCM derselbe TFTP-Server.

Um die Konfigurationsdateien mit den Änderungen zu erhalten, überprüfen Sie, ob die IP-Adresse des TFTP-Servers in den Netzwerkeinstellungen des Telefons korrekt eingerichtet ist. Um eine Bestätigung zu erhalten, verwenden Sie Option 150 vom DHCP-Server oder legen Sie das TFTP manuell auf dem Telefon fest. Der Zugriff auf diesen TFTP-Server erfolgt über eine AnyConnect-Sitzung.

Wenn das IP-Telefon den TFTP-Server von einem lokalen DHCP-Server empfängt, diese Adresse jedoch falsch ist, können Sie die alternative TFTP-Serveroption verwenden, um die vom DHCP-Server angegebene IP-Adresse des TFTP-Servers zu überschreiben. In diesem Verfahren wird beschrieben, wie der alternative TFTP-Server angewendet wird:

1. Navigieren Sie zu **Einstellungen > Netzwerkkonfiguration > IPv4-Konfiguration**.
2. Navigieren Sie zur Option Alternate TFTP (Alternatives TFTP).
3. Drücken Sie die programmierbare Taste Ja, um einen anderen TFTP-Server zu verwenden. Drücken Sie andernfalls die programmierbare Taste Nein. Wenn die Option gesperrt ist, drücken Sie * * #, um sie zu entsperren.
4. Drücken Sie die programmierbare Taste Speich.
5. Wenden Sie unter TFTP Server 1 die Option Alternate TFTP Server (Alternativer TFTP-Server) an.

Überprüfen Sie die Statusmeldungen im Webbrowser oder in den Telefonmenüs direkt, um sicherzustellen, dass das Telefon die richtigen Informationen erhält. Wenn die Kommunikation korrekt eingerichtet ist, werden Meldungen wie folgende angezeigt:



The screenshot shows the Cisco Unified IP Phone web interface. On the left, a dark green sidebar contains navigation links: [Device Logs](#), [Console Logs](#), [Core Dumps](#), [Status Messages](#) (highlighted with a red oval), and [Debug Display](#). The main content area has a dark green header with the Cisco logo and the text "Status Messages" and "Cisco Unified IP Phone CP-7962G (SEP8CB64F576113)". Below the header, a list of status messages is displayed, alternating between "Trust List Updated" and configuration file download logs for "SEP8CB64F576113.cnf.xml.sgn".

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

Wenn das Telefon die Informationen nicht vom TFTP-Server abrufen kann, erhalten Sie TFTP-Fehlermeldungen:

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

Verlängerung des ASA SSL-Zertifikats

Wenn Sie über eine funktionale AnyConnect VPN-Telefoneinrichtung verfügen, Ihr ASA-SSL-Zertifikat jedoch bald abläuft, müssen Sie nicht alle IP-Telefone an den Hauptstandort bringen, um dem Telefon die neuen SSL-Zertifikate zuzuweisen. Sie können die neuen Zertifikate hinzufügen, während das VPN verbunden ist.

Wenn Sie das Zertifikat der Stammzertifizierungsstelle (Root CA) der ASA anstelle des Identitätszertifikats exportiert oder importiert haben und weiterhin dieselbe Zertifizierungsstelle (CA) während dieser Verlängerung verwenden möchten, ist es nicht erforderlich, das Zertifikat im CUCM zu ändern, da es unverändert bleibt. Wenn Sie jedoch das Identitätszertifikat verwenden, ist dieses Verfahren erforderlich. Andernfalls stimmt der Hash-Wert zwischen ASA und IP-Telefon nicht überein, und die Verbindung wird vom Telefon nicht als vertrauenswürdig eingestuft.

1. Verlängern Sie das Zertifikat auf der ASA.

Hinweis: Weitere Informationen finden Sie unter [ASA 8.x: Verlängern und Installieren des](#)

[SSL-Zertifikats mit ASDM](#). Erstellen Sie einen separaten Trustpoint, und wenden Sie dieses neue Zertifikat nicht mit dem Befehl `ssl trustpoint <name> outside`, bevor Sie das Zertifikat auf alle VPN IP-Telefone angewendet haben.

2. Exportieren Sie das neue Zertifikat.
3. Importieren Sie das neue Zertifikat als Telefon-VPN-Trust-Zertifikat in den CUCM.
Hinweis: Achten Sie darauf, dass [CSCuh19734 Upload-Zertifikate mit derselben CN alte Zertifikate in Phone-VPN-trust überschreiben](#).
4. Navigieren Sie zur VPN Gateway-Konfiguration im CUCM, und wenden Sie das neue Zertifikat an. Sie haben jetzt beide Zertifikate: das Zertifikat, das bald abläuft, und das neue Zertifikat, das noch nicht auf die ASA angewendet wurde.
5. Wenden Sie diese neue Konfiguration auf das IP-Telefon an. Navigieren Sie zu **Apply Config > Reset > Restart (Konfiguration anwenden > Zurücksetzen > Neustart)**, um die neuen Konfigurationsänderungen über den VPN-Tunnel an das IP-Telefon zu injizieren. Stellen Sie sicher, dass alle IP-Telefone über das VPN verbunden sind und über den Tunnel den TFTP-Server erreichen können.
6. Verwenden Sie TFTP, um die Statusmeldungen und die Konfigurationsdatei zu überprüfen, um zu bestätigen, dass das IP-Telefon die Konfigurationsdatei mit den Änderungen erhalten hat.
7. Wenden Sie den neuen SSL Trustpoint in der ASA an, und ersetzen Sie das alte Zertifikat.

Hinweis: Wenn das ASA SSL-Zertifikat bereits abgelaufen ist und die IP-Telefone keine Verbindung über AnyConnect herstellen können, Sie können die Änderungen (z. B. den neuen ASA-Zertifikat-Hash) an das IP-Telefon übertragen. Legen Sie das TFTP auf dem IP-Telefon manuell auf eine öffentliche IP-Adresse fest, damit das IP-Telefon die Informationen von dort abrufen kann. Verwenden Sie einen öffentlichen TFTP-Server, um die Konfigurationsdatei zu hosten. Ein Beispiel hierfür ist die Erstellung einer Port Forwarding auf der ASA und die Umleitung des Datenverkehrs an den internen TFTP-Server.