Risoluzione dei problemi relativi ai telefoni VPN AnyConnect - IP Phone, ASA e CUCM

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi con i telefoni IP che usano il protocollo Secure Sockets Layer (SSL) (Cisco AnyConnect Secure Mobility Client) per connettersi a una appliance Cisco Adaptive Security (ASA) che viene usata come gateway VPN e per connettersi a un Cisco Unified Communications Manager (CUCM) che viene usato come server vocale.

Per esempi di configurazione di AnyConnect con telefoni VPN, fare riferimento a questi documenti:

- Esempio di configurazione di SSLVPN con telefoni IP
- Esempio di configurazione di AnyConnect VPN Phone con autenticazione certificato

Premesse

Prima di distribuire una VPN SSL con telefoni IP, verificare di aver soddisfatto i seguenti requisiti iniziali per le licenze AnyConnect per l'appliance ASA e per la versione americana CUCM con restrizioni all'esportazione.

Conferma licenza VPN Phone su ASA

La licenza VPN permette di usare la funzione nell'appliance ASA. Per verificare il numero di utenti che possono connettersi con AnyConnect (anche se non è un telefono IP), controllare la licenza AnyConnect Premium SSL. Per ulteriori informazioni, consultare il documento sulla licenza ASA richiesta per le connessioni IP Phone e VPN per dispositivi mobili? per ulteriori dettagli.

Sull'appliance ASA, usare il comando **show version** per verificare se la funzione è abilitata. Il nome della licenza è diverso nella versione ASA:

- ASA release 8.0.x: Il nome della licenza è AnyConnect per Linksys Phone.
- ASA release 8.2.x e successive: Il nome della licenza è AnyConnect per Cisco VPN Phone.

Di seguito è riportato un esempio di 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.
```

Di seguito è riportato un esempio di appliance ASA release 8.2.x e successive:

```
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.
```

Esporta CUCM con restrizioni ed Esporta CUCM senza restrizioni

Èconsigliabile distribuire una versione americana con restrizioni all'esportazione di CUCM per la funzionalità telefono VPN.

Se si utilizza una versione americana di CUCM non limitata, tenere presente che:

- Le configurazioni di sicurezza per i telefoni IP vengono modificate per disabilitare la segnalazione e la crittografia dei supporti; inclusa la crittografia fornita dalla funzionalità telefono VPN.
- Non è possibile esportare i dettagli della VPN tramite Importa/Esporta.
- Le caselle di controllo per la configurazione di profili VPN, gateway VPN, gruppi VPN e funzionalità VPN non vengono visualizzate.

Nota: Una volta eseguito l'aggiornamento alla versione americana di esportazione senza restrizioni di CUCM, non è possibile eseguire l'aggiornamento alla versione americana con restrizioni all'esportazione o eseguirne una nuova installazione.

Problemi comuni dell'appliance ASA

Nota: È possibile usare Cisco CLI Analyzer (solo clienti registrati) per visualizzare un'analisi degli output del comando **show**. Prima di usare i comandi di **debug,** consultare il documento Cisco sulle informazioni importanti sui comandi di **debug**.

Certificati da utilizzare sull'appliance ASA

Sull'appliance ASA, è possibile usare certificati SSL autofirmati, certificati SSL di terze parti e certificati jolly. ciascuna di esse permette la comunicazione tra il telefono IP e l'appliance ASA.

Èpossibile utilizzare un solo certificato di identità perché a ogni interfaccia è possibile assegnare un solo certificato.

Per i certificati SSL di terze parti, installare la catena completa nell'appliance ASA e includere tutti i certificati intermedi e radice.

Trustpoint/certificato per esportazione ASA e importazione CUCM

Il certificato che l'ASA presenta al telefono IP durante la negoziazione SSL deve essere esportato dall'ASA e importato nel CUCM. Per sapere quale certificato esportare dall'appliance ASA, controllare il trust point assegnato all'interfaccia a cui si connettono i telefoni IP.

Utilizzare il comando **show run ssl** per verificare il trust point (certificato) da esportare. Per ulteriori informazioni, fare riferimento all'esempio di configurazione dell'autenticazione del certificato per i

telefoni VPN AnyConnect.

> **Nota:** Se un certificato di terze parti è stato distribuito in una o più appliance ASA, non è necessario esportare ciascun certificato di identità da ciascuna appliance ASA e quindi importarlo nel CUCM come phone-vpn-trust.

L'appliance ASA presenta il certificato autofirmato ECDSA anziché il certificato RSA configurato

Quando si verifica questo problema, i telefoni di modello più recenti non sono in grado di connettersi, mentre i telefoni di modello più vecchi non presentano problemi. Di seguito sono riportati i registri del telefono quando si verifica questo problema:

```
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
```

Nelle versioni 9.4.1 e successive, la crittografia a curva ellittica è supportata per SSL/TLS. Quando un client VPN SSL con curva ellittica compatibile, ad esempio un nuovo modello di telefono, si connette all'ASA, la suite di cifratura a curva ellittica viene negoziata e l'ASA presenta al client VPN SSL un certificato a curva ellittica, anche quando l'interfaccia corrispondente è configurata con un trust point basato su RSA. Per impedire che l'ASA presenti un certificato SSL autofirmato, l'amministratore deve rimuovere le suite di cifratura corrispondenti con il comando **ssl**

cipher. Ad esempio, per un'interfaccia configurata con un trust point RSA, l'amministratore può eseguire questo comando in modo che vengano negoziate solo le cifrature basate su RSA:

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

Con l'implementazione dell'ID bug Cisco CSCuu02848, la configurazione è prioritaria. I certificati configurati in modo esplicito vengono sempre utilizzati. I certificati autofirmati vengono utilizzati solo in assenza di un certificato configurato.

Crittografi client proposti	Solo certificato RSA	Solo certificato CE	Entrambi i certificati	Nessuna
Solo crittografia RSA	Utilizzo del certificato RSA Utilizzo delle cifrature RSA	Utilizza il certificato autofirmato RSA Utilizzo delle cifrature RSA	Utilizzo del certificato RSA Utilizzo delle cifrature RSA	Utilizza il certificato autofirmato RSA Utilizzo delle cifrature RSA
Solo cifrari CE (rari)	**Connessione non riuscita**	Utilizza il certificato EC Utilizza cifratura EC	Utilizza il certificato EC Utilizza cifratura EC	Utilizza il certificato autofirmato CE Utilizza cifratura EC
Solo due cifrari	Utilizzo del certificato RSA Utilizzo delle cifrature RSA	Utilizza il certificato EC Utilizza cifratura EC	Utilizza il certificato EC Utilizza cifratura EC	Utilizza il certificato autofirmato CE Utilizza cifratura EC

Database esterno per l'autenticazione degli utenti di telefoni IP

Èpossibile utilizzare un database esterno per autenticare gli utenti del telefono IP. Protocolli quali il protocollo LDAP (Lightweight Directory Access Protocol) o RADIUS (Remote Authentication Dial In User Service) possono essere utilizzati per l'autenticazione degli utenti di telefoni VPN.

L'hash del certificato corrisponde tra il certificato ASA e l'elenco di scopi consentiti ai telefoni VPN

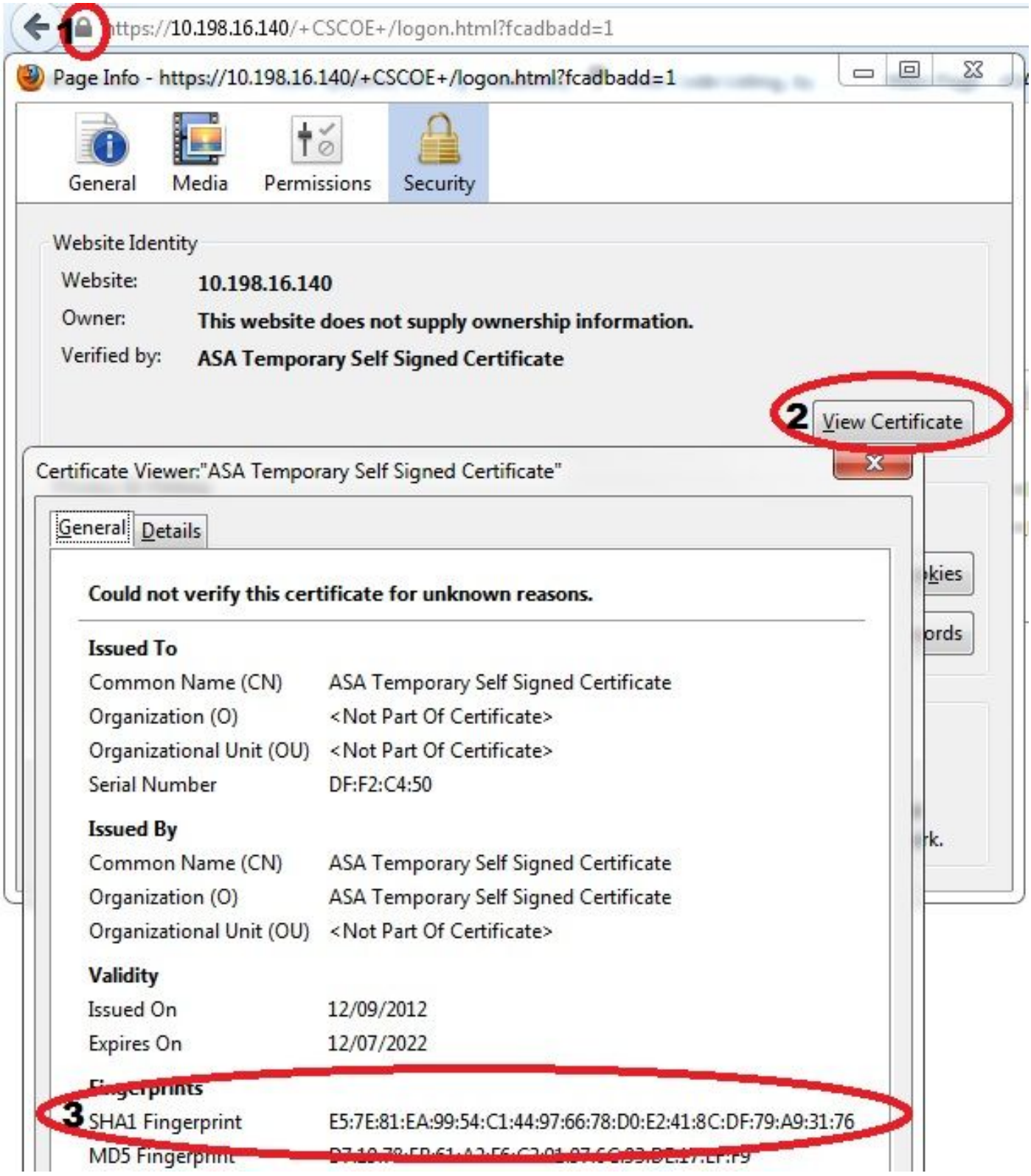
Tenere presente che è necessario scaricare il certificato assegnato all'interfaccia ASA SSL e caricarlo come certificato Phone-VPN-Trust nel CUCM. In circostanze diverse, l'hash per questo certificato presentato dall'ASA potrebbe non corrispondere all'hash generato dal server CUCM e inviato al telefono VPN tramite il file di configurazione.

Al termine della configurazione, verificare la connessione VPN tra il telefono IP e l'appliance ASA. Se la connessione continua a non riuscire, verificare che l'hash del certificato ASA corrisponda a quello previsto dal telefono IP:

1. Controllare l'hash SHA1 (Secure Hash Algorithm 1) presentato dall'ASA.
2. Usare il protocollo TFTP per scaricare il file di configurazione del telefono IP da CUCM.
3. Decodificare l'hash da esadecimale a base 64 o da base 64 a esadecimale.

Controlla hash SHA1

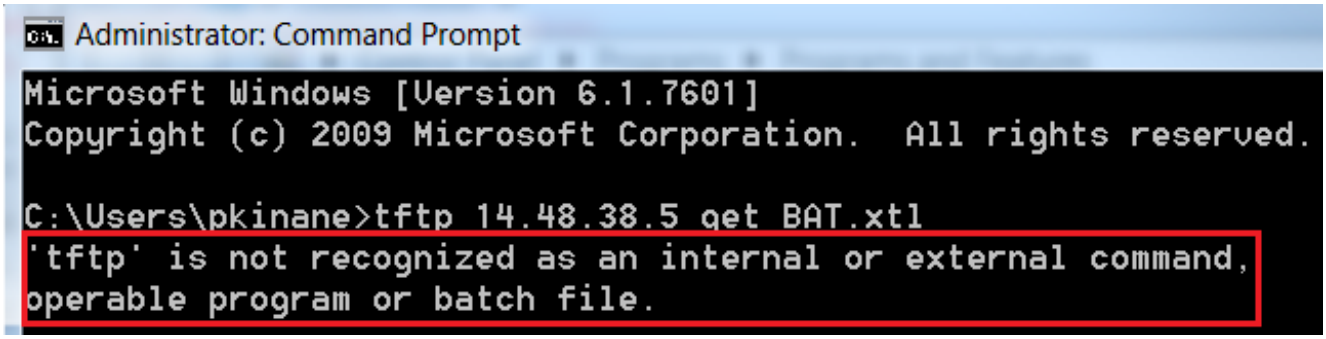
L'ASA presenta il certificato applicato con il comando **ssl trustpoint** sull'interfaccia a cui si connette il telefono IP. Per verificare questo certificato, aprire il browser (in questo esempio, Firefox), e immettere l'URL (group-url) a cui i telefoni devono connettersi:

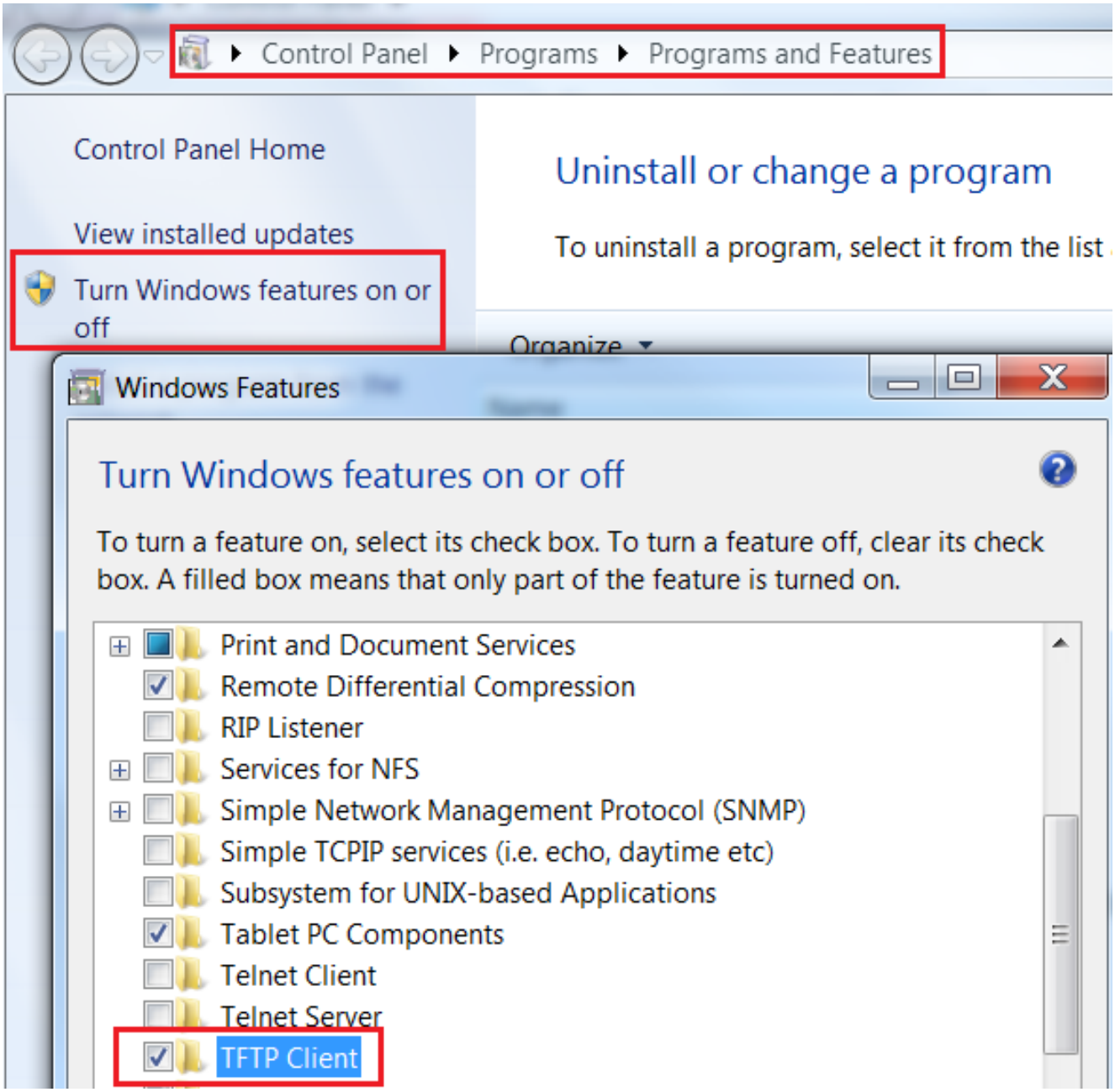


Scarica file di configurazione telefono IP

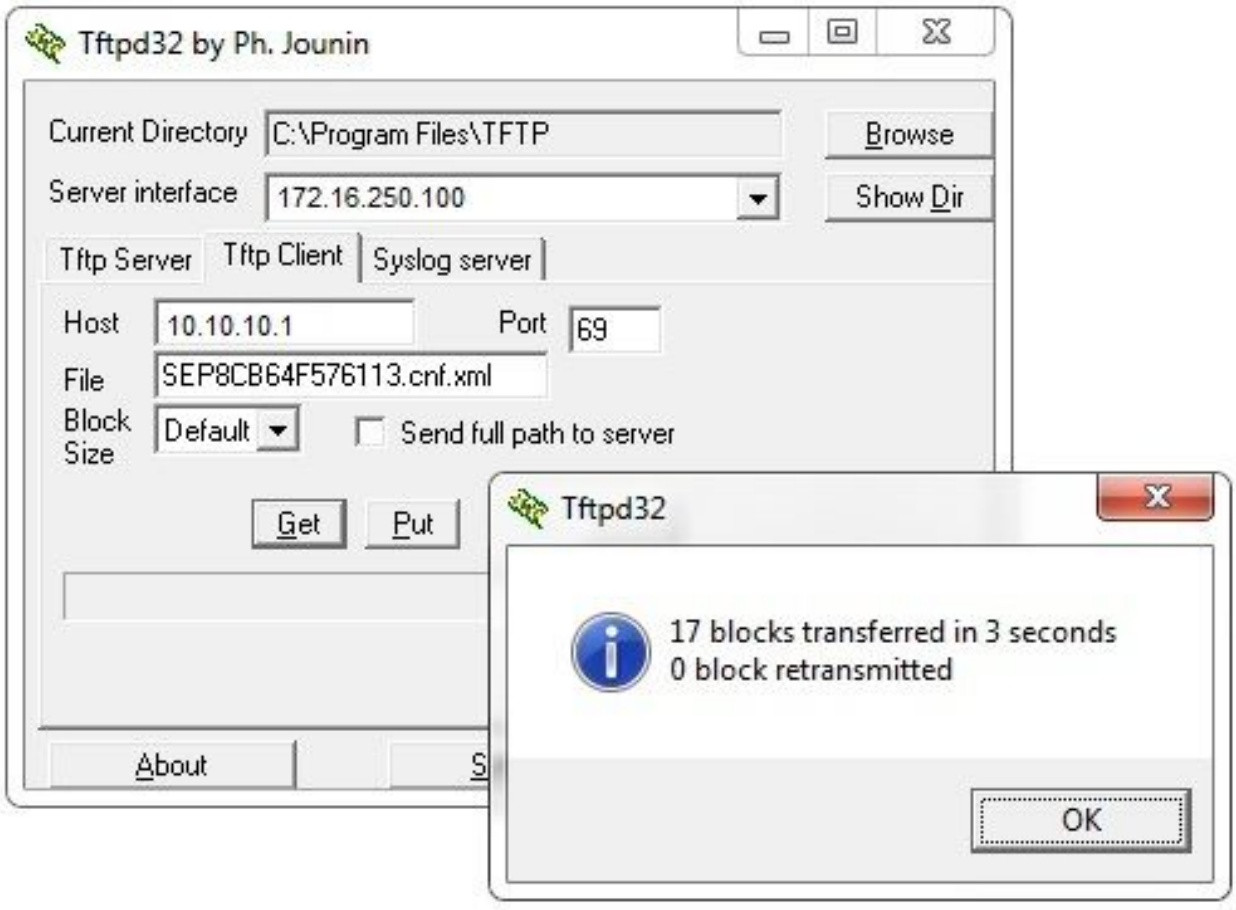
Da un PC con accesso diretto al CUCM, scaricare il file di configurazione TFTP per il telefono con problemi di connessione. Due metodi di download sono:

1. Aprire una sessione CLI in Windows e utilizzare il comando **tftp -i** *<Server TFTP>* **GET SEP***<Indirizzo Mac Telefono>***.cnf.xml**.
   Nota: Se viene visualizzato un errore simile a quello riportato di seguito, verificare che la funzione Client TFTP sia
   abilitata.





2. Utilizzare un'applicazione come Tftpd32 per scaricare il file:

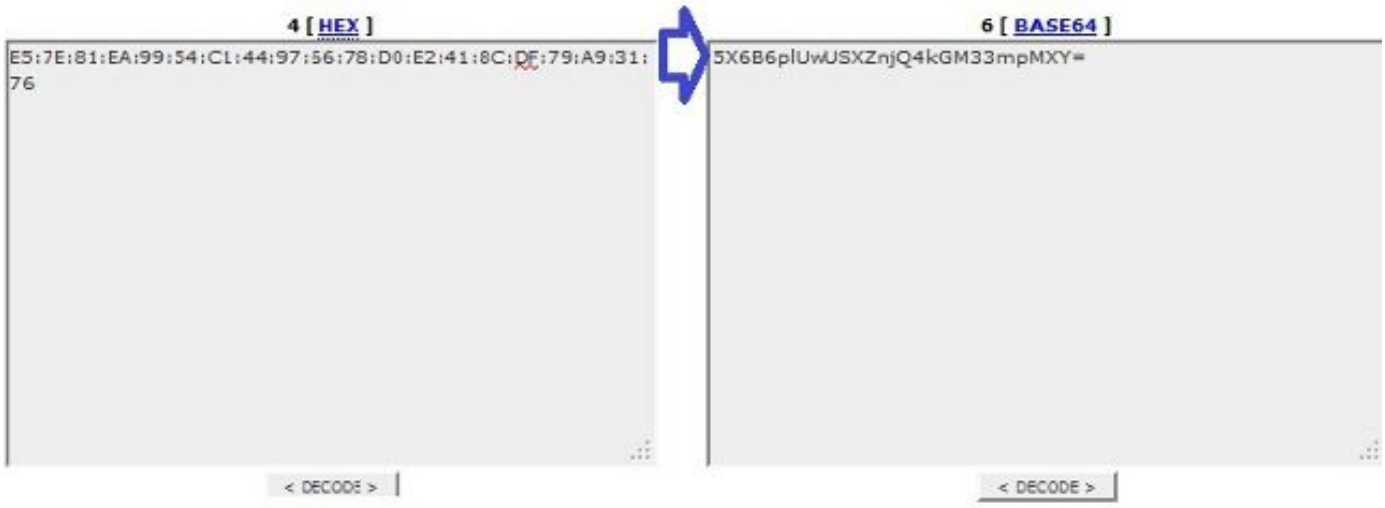


3. Una volta scaricato il file, aprire il file XML e trovare la configurazione *vpnGroup*. In questo esempio vengono illustrati la sezione e il *certHash* da verificare:

```
<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>
```

Decodifica l'hash

Confermare che entrambi i valori hash corrispondano. Il browser presenta l'hash in formato esadecimale, mentre il file XML utilizza base 64, quindi converte un formato nell'altro per confermare la corrispondenza. Ci sono molti traduttori disponibili; un esempio è TRANSLATOR, BINARY .



Nota: Se il valore hash precedente non corrisponde, il telefono VPN non considera attendibile la connessione negoziata con l'ASA e la connessione non riesce.

Bilanciamento del carico VPN e telefoni IP

La VPN SSL con carico bilanciato non è supportata per i telefoni VPN. I telefoni VPN non eseguono la convalida dei certificati reali, ma utilizzano gli hash trasmessi dal CUCM per convalidare i server. Poiché il bilanciamento del carico della VPN è fondamentalmente un reindirizzamento HTTP, è necessario che i telefoni convalidino più certificati, con conseguente errore. I sintomi di errore di bilanciamento del carico VPN includono:

- Il telefono si alterna tra i server e impiega un tempo di connessione eccezionalmente lungo, se non addirittura guasto.
- Le note telefonate contengono messaggi quali:

```
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 e telefoni IP

Al momento, i telefoni IP non supportano Cisco Secure Desktop (CSD) e non si connettono quando CSD è abilitato per il gruppo di tunnel o globalmente nell'appliance ASA.

In primo luogo, confermare se l'ASA ha un CSD abilitato. Immettere il comando **show run webvpn** nella CLI dell'ASA:

```
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#
```

Per controllare i problemi del CSD durante una connessione telefonica IP, controllare i log o i debug nell'appliance ASA.

Log ASA

```
%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.
```

Debug dell'ASA

```
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>
```

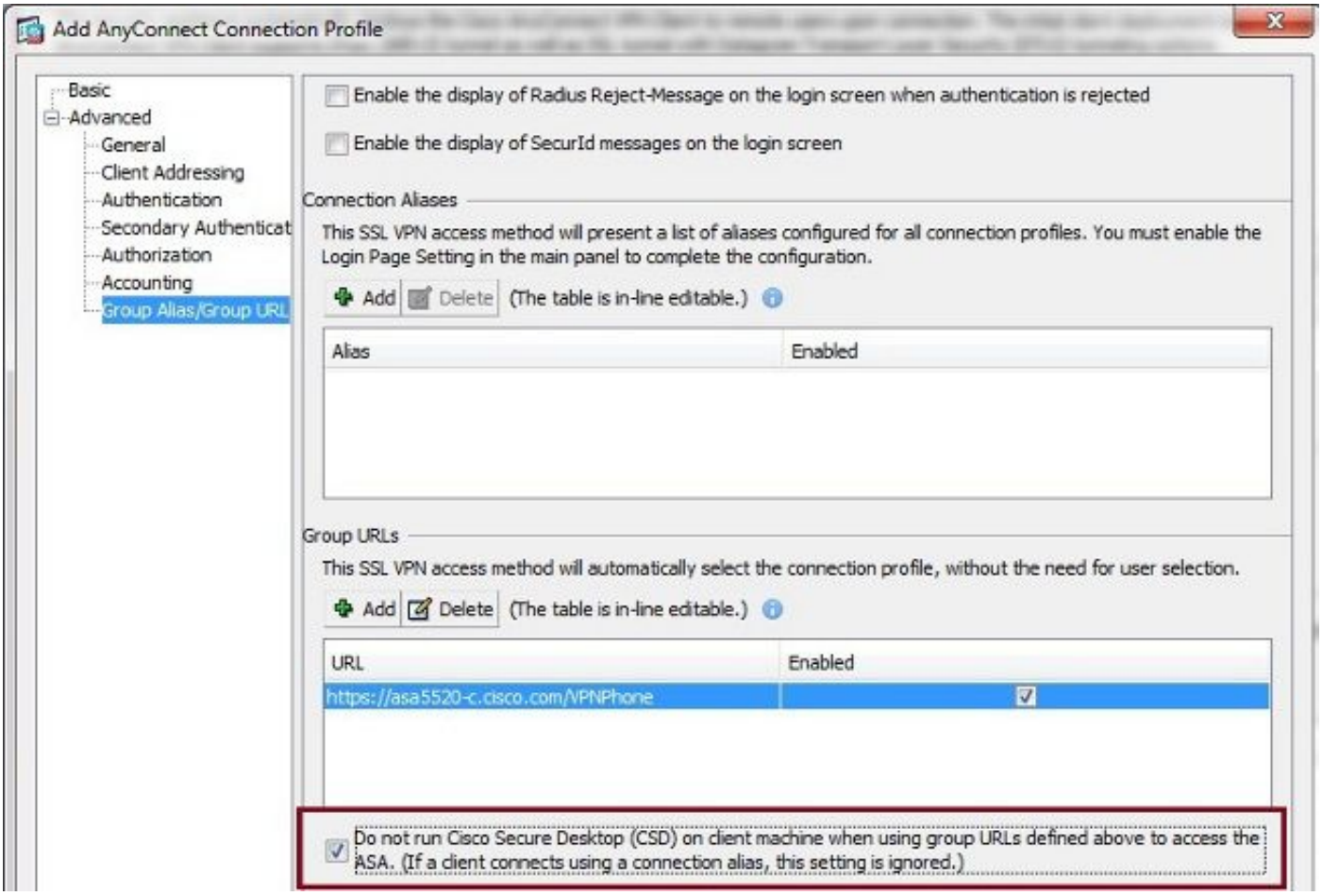
Nota: In un'implementazione di grandi dimensioni con un carico elevato di utenti AnyConnect, Cisco consiglia di non abilitare il **debug webvpn anyconnect**. Poiché l'output non può essere filtrato in base all'indirizzo IP, è possibile che venga creata una grande quantità di informazioni.

Nelle versioni ASA 8.2 e successive, è necessario applicare il comando **without-csd** agli attributi webvpn del gruppo di tunnel:

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

Nelle versioni precedenti dell'ASA, questa operazione non era possibile, quindi l'unica soluzione era disabilitare il CSD a livello globale.

In Cisco Adaptive Security Device Manager (ASDM), è possibile disabilitare CSD per un profilo di connessione specifico, come mostrato nell'esempio:

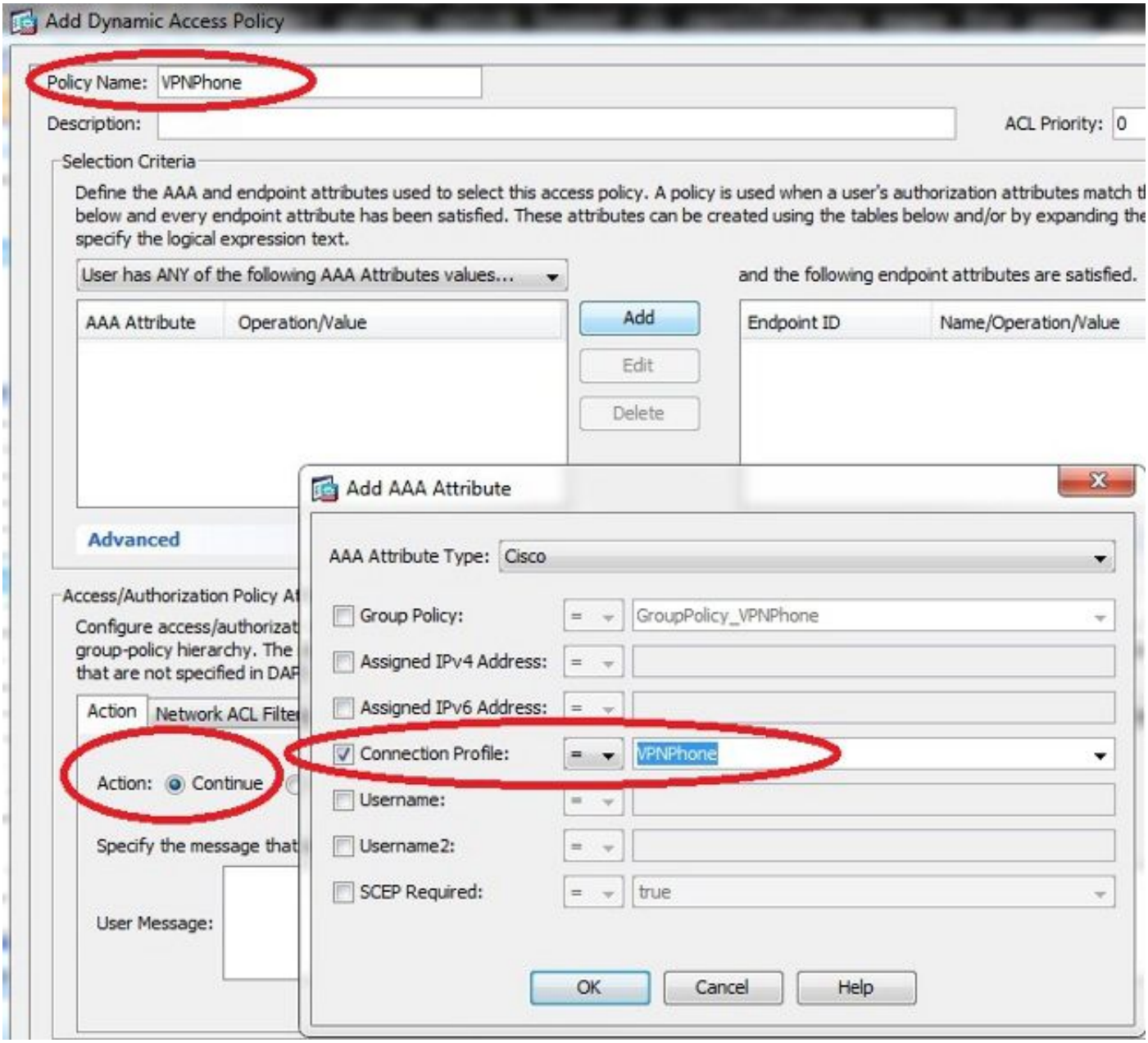


Nota: Per disattivare la funzionalità CSD, utilizzare un URL di gruppo.

Regole DAP

La maggior parte delle implementazioni non solo connette i telefoni IP all'appliance ASA, ma connette anche diversi tipi di macchine (Microsoft, Linux, Mac OS) e dispositivi mobili (Android, iOS). Per questo motivo, è normale trovare una configurazione esistente di regole DAP (Dynamic Access Policy), dove, nella maggior parte dei casi, l'azione predefinita in DfltAccessPolicy è la terminazione della connessione.

In questo caso, creare una regola DAP separata per i telefoni VPN. Utilizzate un parametro specifico, ad esempio il profilo di connessione, e impostate l'azione su **Continua (Continue)**:



Se non si crea un criterio DAP specifico per i telefoni IP, l'ASA visualizza una corrispondenza in DfltAccessPolicy e una connessione non riuscita:

```
%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
```

Dopo aver creato un criterio DAP specifico per i telefoni IP con l'azione impostata su **Continua**, è

possibile connettersi:

```
%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
```

Valori ereditati da DfltGrpPolicy o altri gruppi

In molti casi, DfltGrpPolicy è impostato con diverse opzioni. Per impostazione predefinita, queste impostazioni vengono ereditate per la sessione telefonica IP a meno che non vengano specificate manualmente nei Criteri di gruppo che il telefono IP deve utilizzare.

Di seguito sono riportati alcuni parametri che potrebbero influire sulla connessione se ereditati da DfltGrpPolicy:

- group-lock
- vpn-tunnel-protocol
- vpn-simultous-logins
- vpn-filter

Si supponga di disporre della configurazione di esempio seguente in DfltGrpPolicy e in 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
```

La connessione eredita i parametri da DfltGrpPolicy non specificati in modo esplicito in GroupPolicy_VPNPhone e durante la connessione esegue il push di tutte le informazioni al telefono IP.

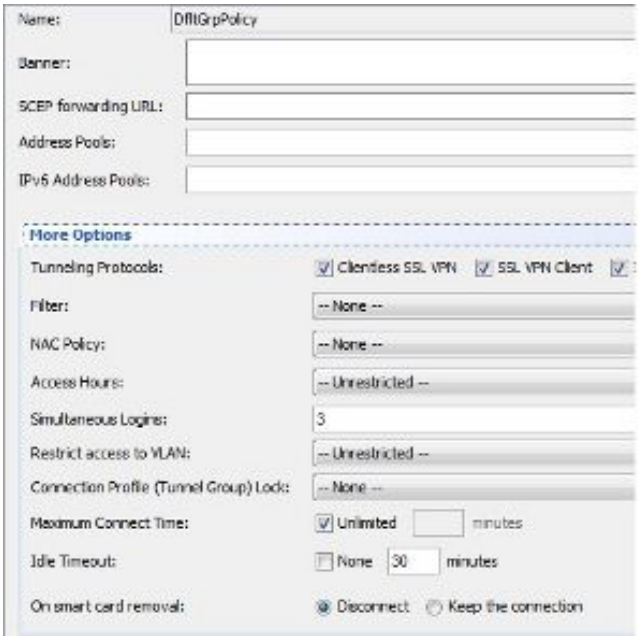
Per evitare ciò, specificare manualmente i valori necessari direttamente nel gruppo:

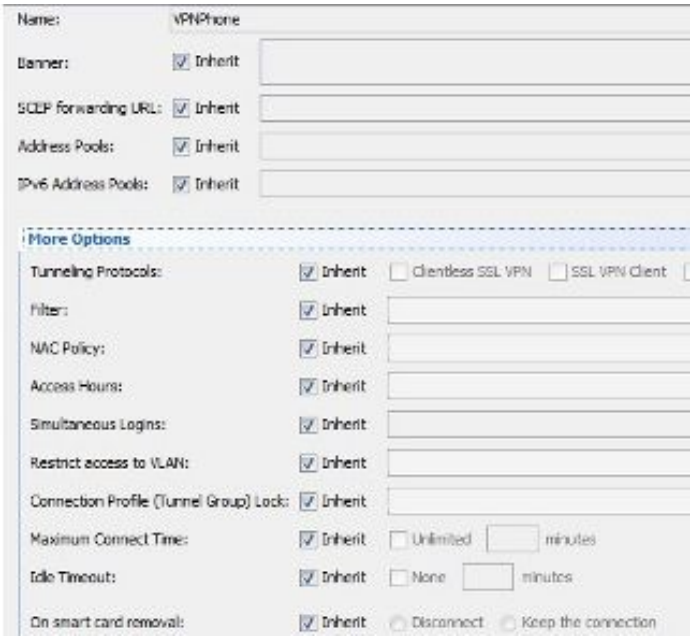
```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
 vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
 vpn-filter none
 default-domain value cisco.com
```

Per controllare i valori predefiniti di DfltGrpPolicy, utilizzare il comando **show run all group-policy**; questo esempio chiarisce la differenza tra i risultati:

```
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
```

Di seguito è riportato l'output degli attributi di ereditarietà dei criteri di gruppo tramite ASDM:





Crittografia supportata

Un telefono VPN AnyConnect testato con 7962G IP phone e firmware versione 9.1.1 supporta solo due cifrari, entrambi AES (Advanced Encryption Standard): AES256-SHA e AES128-SHA. Se non si specificano i cifrari corretti nell'appliance ASA, la connessione viene rifiutata, come mostrato nel log dell'appliance:

```
%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
```

Per confermare se l'appliance ASA ha i cifrari abilitati corretti, immettere i comandi **show run all ssl** e **show ssl**:

```
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
```

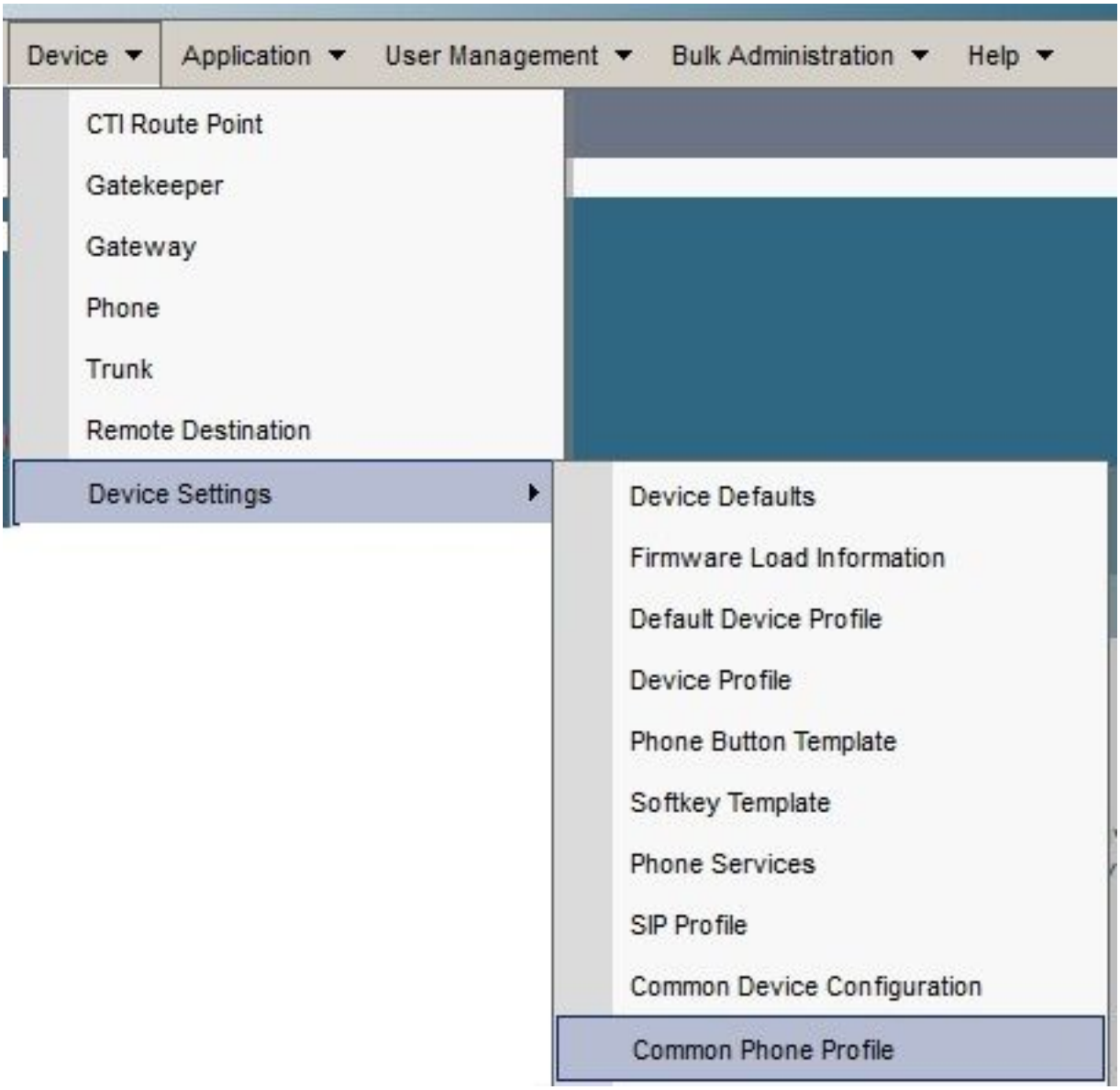
```
ASA5510-F#

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#
```

Problemi comuni relativi al CUCM

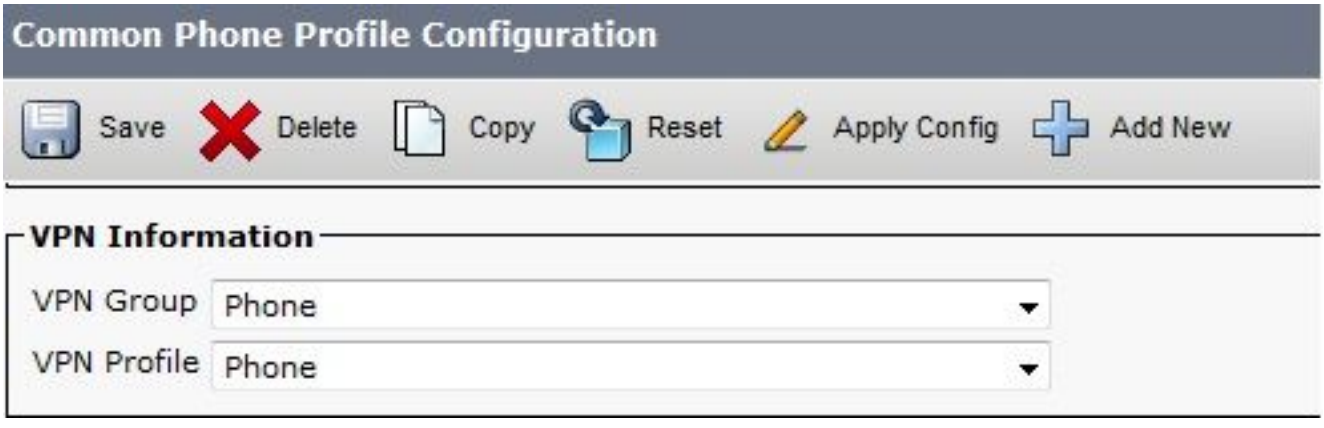
Impostazioni VPN non applicate al telefono IP

Una volta creata la configurazione sul CUCM (Gateway, Group, and Profile), applicare le impostazioni VPN in Common Phone Profile:

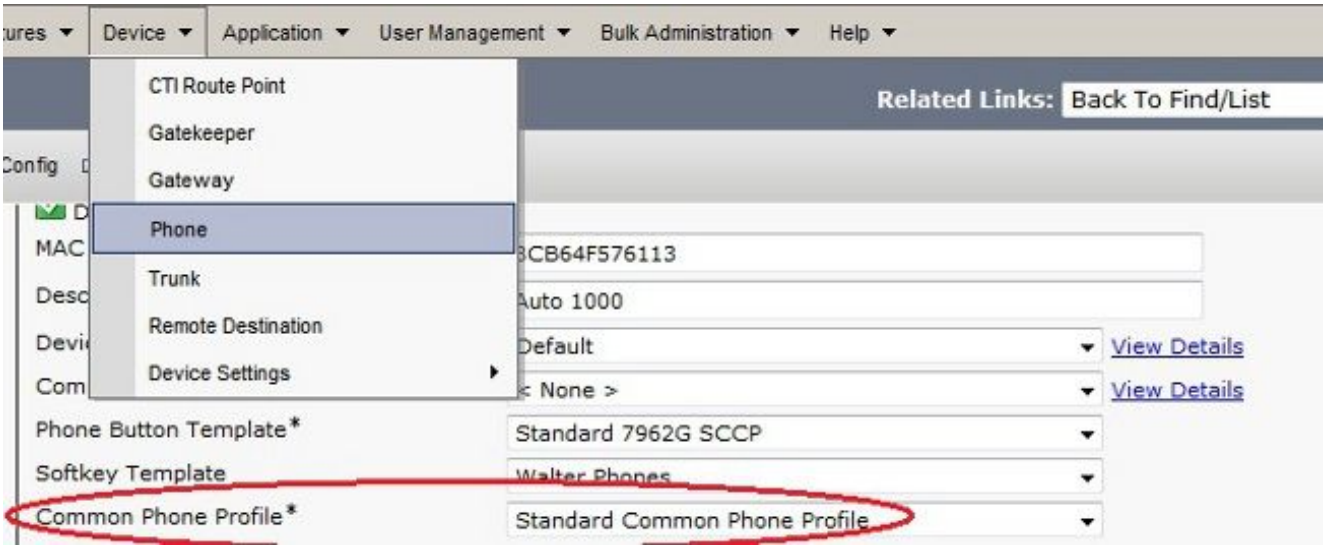
1. Selezionare **Dispositivo > Impostazioni dispositivo > Profilo telefonico comune**.



2. Immettere le informazioni sulla VPN:



3. Passare a **Dispositivo > Telefono** e verificare che il profilo sia assegnato alla configurazione del telefono:



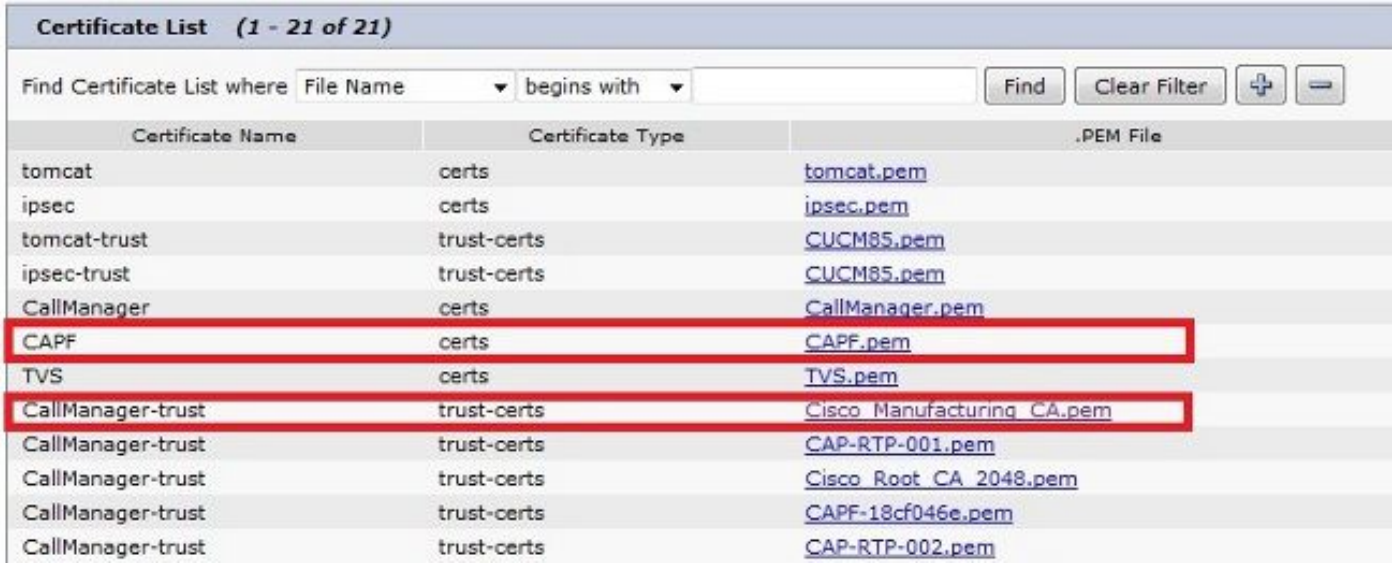
Metodo di autenticazione certificato

Esistono due modi per configurare l'autenticazione dei certificati per i telefoni IP: Certificato installato dal produttore (MIC) e Certificato significativo a livello locale (LSC). Per scegliere l'opzione migliore per la tua situazione, fai riferimento all'esempio di configurazione dell'autenticazione del certificato per i telefoni VPN AnyConnect.

Quando si configura l'autenticazione dei certificati, esportare i certificati (CA radice) dal server CUCM e importarli nell'appliance ASA:

1. Accedere a CUCM.
2. Passare a **Amministrazione del sistema operativo unificato > Protezione > Gestione certificati**.
3. individuare la funzione CAPF (Certificate Authority Proxy Function) o Cisco_Manufacturing_CA; il tipo di certificato dipende dall'utilizzo dell'autenticazione dei certificati MIC o LSC.
4. Scaricare il file nel computer locale.

Una volta scaricati i file, accedere all'ASA dalla CLI o da ASDM e importare il certificato come certificato CA.



Certificate List (1 - 21 of 21)

Find Certificate List where File Name begins with 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

Per impostazione predefinita, tutti i telefoni che supportano VPN sono precaricati con MIC. I telefoni dei modelli 7960 e 7940 non sono dotati di MIC e richiedono una procedura di installazione speciale in modo che la LSC si registri in modo sicuro.

I più recenti telefoni IP Cisco (8811, 8841, 8851 e 8861) includono certificati MIC firmati dalla nuova CA SHA2 di produzione:

- CUCM versione 10.5(1) include e considera attendibili i nuovi certificati SHA2.
- Se si esegue una versione precedente di CUCM, potrebbe essere necessario scaricare il nuovo certificato CA di produzione e:

  Caricarlo nel trust CAPF in modo che i telefoni possano autenticarsi con CAPF per ottenere un LSC.

  Caricarlo sul CallManager-trust se si desidera consentire ai telefoni di autenticarsi con un MIC per SIP 5061.

Suggerimento: Fare clic su questo collegamento per ottenere la CA SHA2 se CUCM attualmente esegue una versione precedente.

Attenzione: Cisco consiglia di utilizzare i MIC solo per l'installazione di LSC. Cisco supporta le LCS per l'autenticazione della connessione TLS con CUCM. Poiché i certificati radice MIC possono essere compromessi, i clienti che configurano i telefoni per l'utilizzo dei MIC per l'autenticazione TLS o per qualsiasi altro scopo lo fanno a proprio rischio. Cisco non si assume alcuna responsabilità in caso di compromissione dei MIC.

Per impostazione predefinita, se nel telefono è presente una scheda LSC, l'autenticazione utilizza la scheda LSC, indipendentemente dal fatto che nel telefono sia presente un MIC. Se nel telefono sono presenti un MIC e un LSC, l'autenticazione utilizza il LSC. Se nel telefono non esiste un lettore LCS, ma un microfono MIC esiste, l'autenticazione utilizza il microfono MIC.

> **Nota:** Notare che, per l'autenticazione del certificato, è necessario esportare il certificato SSL dall'appliance ASA e importarlo nel CUCM.

Verifica ID host

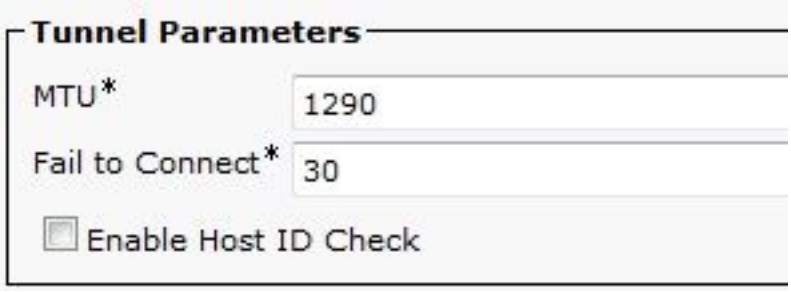
Se il nome comune (CN) nel soggetto del certificato non corrisponde all'URL (URL del gruppo) usato dai telefoni per connettersi all'ASA tramite la VPN, disabilitare il controllo dell'ID host sul dispositivo CUCM o usare un certificato nell'ASA che corrisponda all'URL sull'ASA.

Questa operazione è necessaria quando il certificato SSL dell'appliance ASA è un certificato con caratteri jolly, il certificato SSL contiene una rete SAN (Subject Alternative Name) diversa o l'URL è stato creato con l'indirizzo IP anziché con il nome di dominio completo (FQDN).

Questo è un esempio di nota telefonata IP in cui il CN del certificato non corrisponde all'URL che il telefono sta tentando di raggiungere.

```
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!!
```

Per disabilitare il controllo dell'ID host nel CUCM, selezionare **Advanced Features > VPN > VPN Profile** (Funzionalità avanzate **> VPN > Profilo VPN)**:



Ulteriori procedure di risoluzione dei problemi

Log e debug da usare nell'appliance ASA

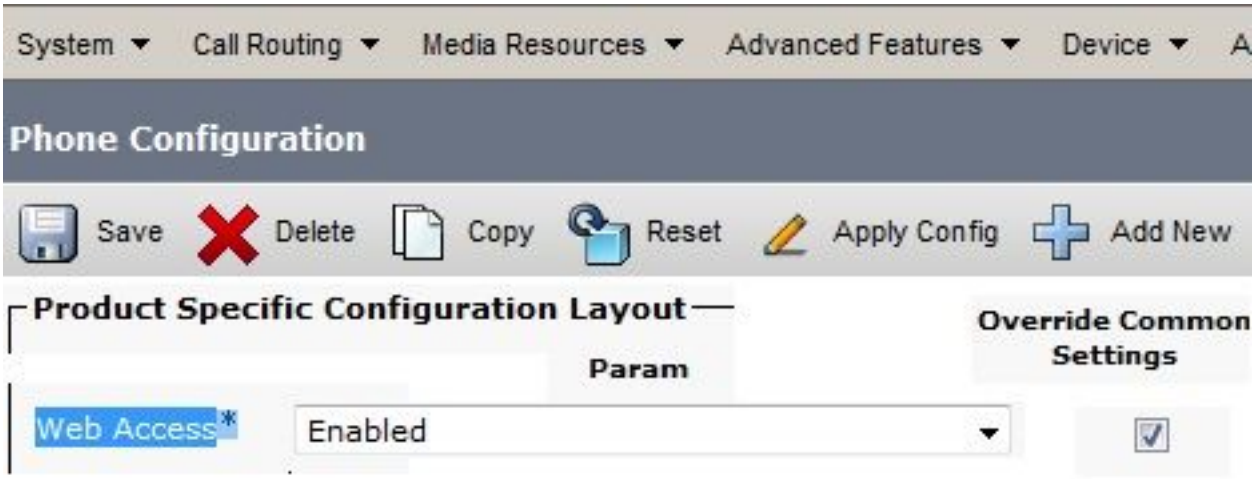
Sull'appliance ASA, è possibile abilitare i seguenti debug e log per la risoluzione dei problemi:

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

debug webvpn anyconnect 255
```

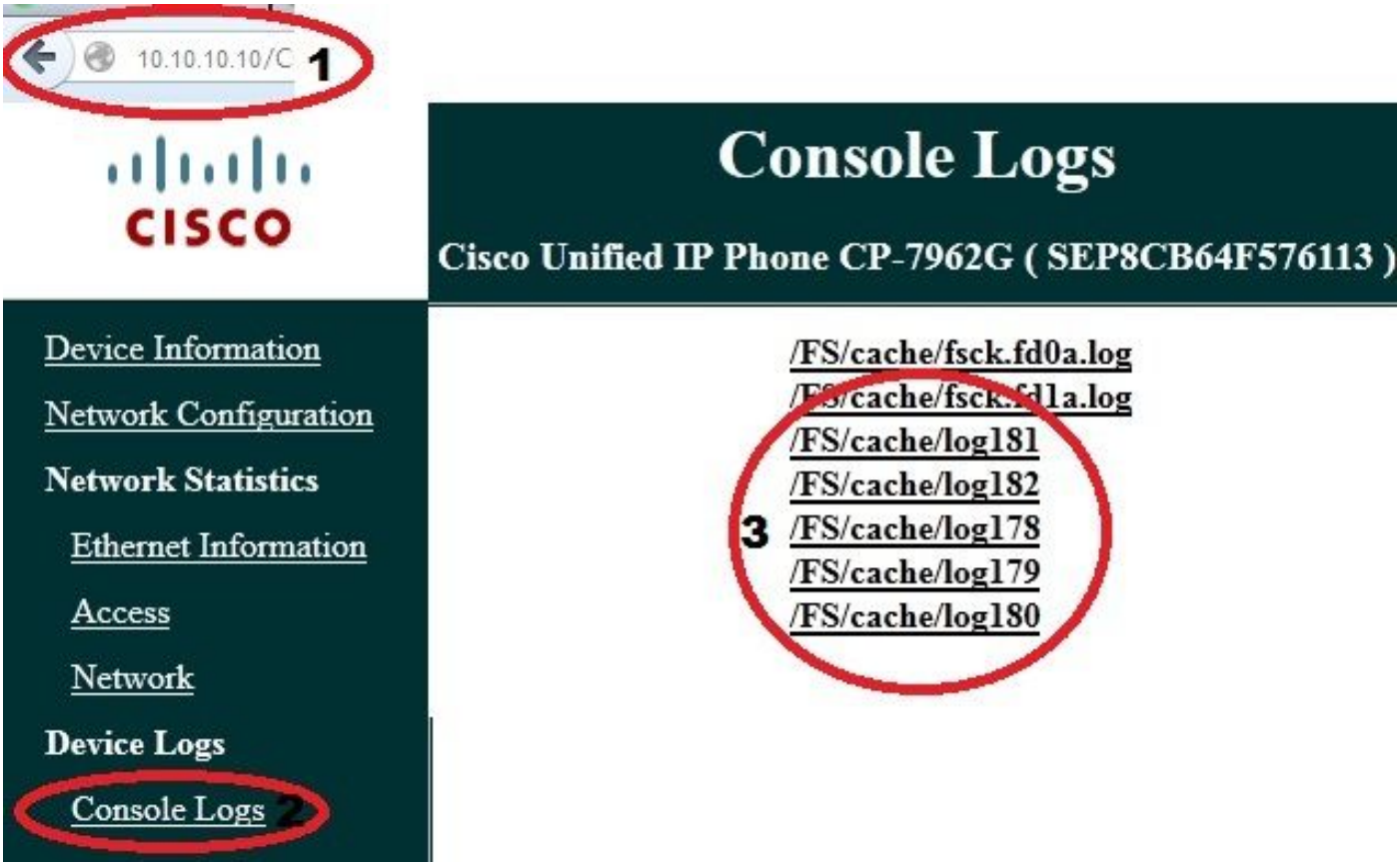
> **Nota:** In un'implementazione di grandi dimensioni con un carico elevato di utenti AnyConnect, Cisco consiglia di non abilitare il comando **debug webvpnh anyconnect**. Poiché l'output non può essere filtrato in base all'indirizzo IP, è possibile che venga creata una grande quantità di informazioni.

Registri telefonici IP

Per accedere alle note telefonate, attivare la funzionalità Accesso Web. Accedere a CUCM e selezionare **Device > Phone >** Phone Configuration (Dispositivo **> Telefono > Configurazione telefono)**. Individuare il telefono IP su cui si desidera attivare questa caratteristica e la sezione relativa ad Accesso Web. Applicare le modifiche alla configurazione al telefono IP:



Una volta attivato il servizio e reimpostato il telefono per inserire questa nuova funzione, è possibile accedere alle note telefonate IP nel browser; utilizzare l'indirizzo IP del telefono da un computer con accesso alla subnet. Andare ai log della console e controllare i cinque file di log. Poiché il telefono sovrascrive i cinque file, è necessario controllare tutti questi file per trovare le informazioni che si cercano.



Problemi correlati tra i log ASA e i log dei telefoni IP

Questo è un esempio di come correlare i registri dall'ASA al telefono IP. In questo esempio, l'hash del certificato sull'appliance ASA non corrisponde all'hash del certificato sul file di configurazione del telefono, in quanto il certificato sull'appliance ASA è stato sostituito con un certificato diverso.

Log ASA

```
%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
```

Note telefonate

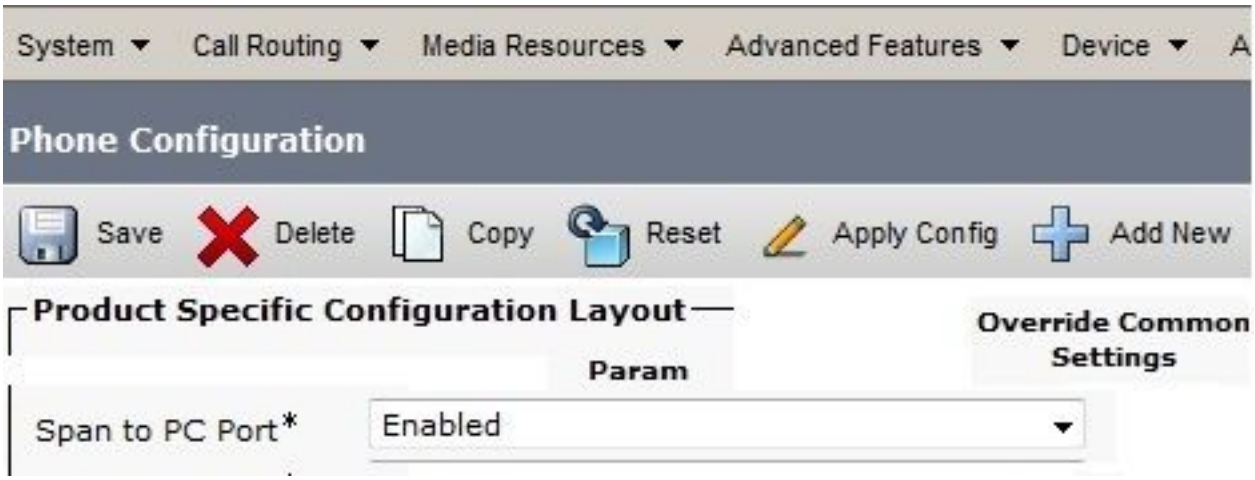
```
 902: NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect
initialization
903: NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state
904: NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A
905: NOT 10:19:27.364687 VPNC: 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
```

Funzione Span to PC Port

Èpossibile collegare un computer direttamente a un telefono. Il telefono ha una porta di commutazione nel piano posteriore.

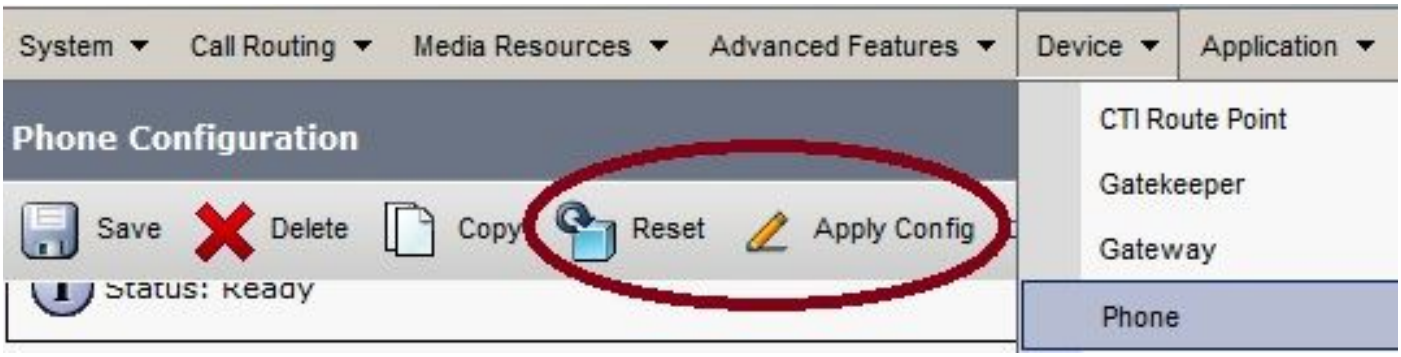
Configurare il telefono come in precedenza, abilitare Span to PC Port sul CUCM e applicare la configurazione. Il telefono inizia a inviare una copia di ogni fotogramma al PC. Usare Wireshark in modalità promiscua per catturare il traffico per l'analisi.



Modifiche alla configurazione del telefono IP durante la connessione tramite VPN

Una domanda comune è se è possibile modificare la configurazione della VPN quando il telefono IP è connesso alla rete da AnyConnect. La risposta è sì, ma è necessario confermare alcune impostazioni di configurazione.

Apportare le modifiche necessarie nel CUCM, quindi applicare le modifiche al telefono. Ci sono tre opzioni (Apply Config, Reset, Restart) per inviare la nuova configurazione al telefono. Sebbene tutte e tre le opzioni disconnettano la VPN dal telefono e dall'ASA, è possibile riconnettersi automaticamente se si utilizza l'autenticazione del certificato; se si utilizza Authentication, Authorization, and Accounting (AAA), verranno nuovamente richieste le credenziali.



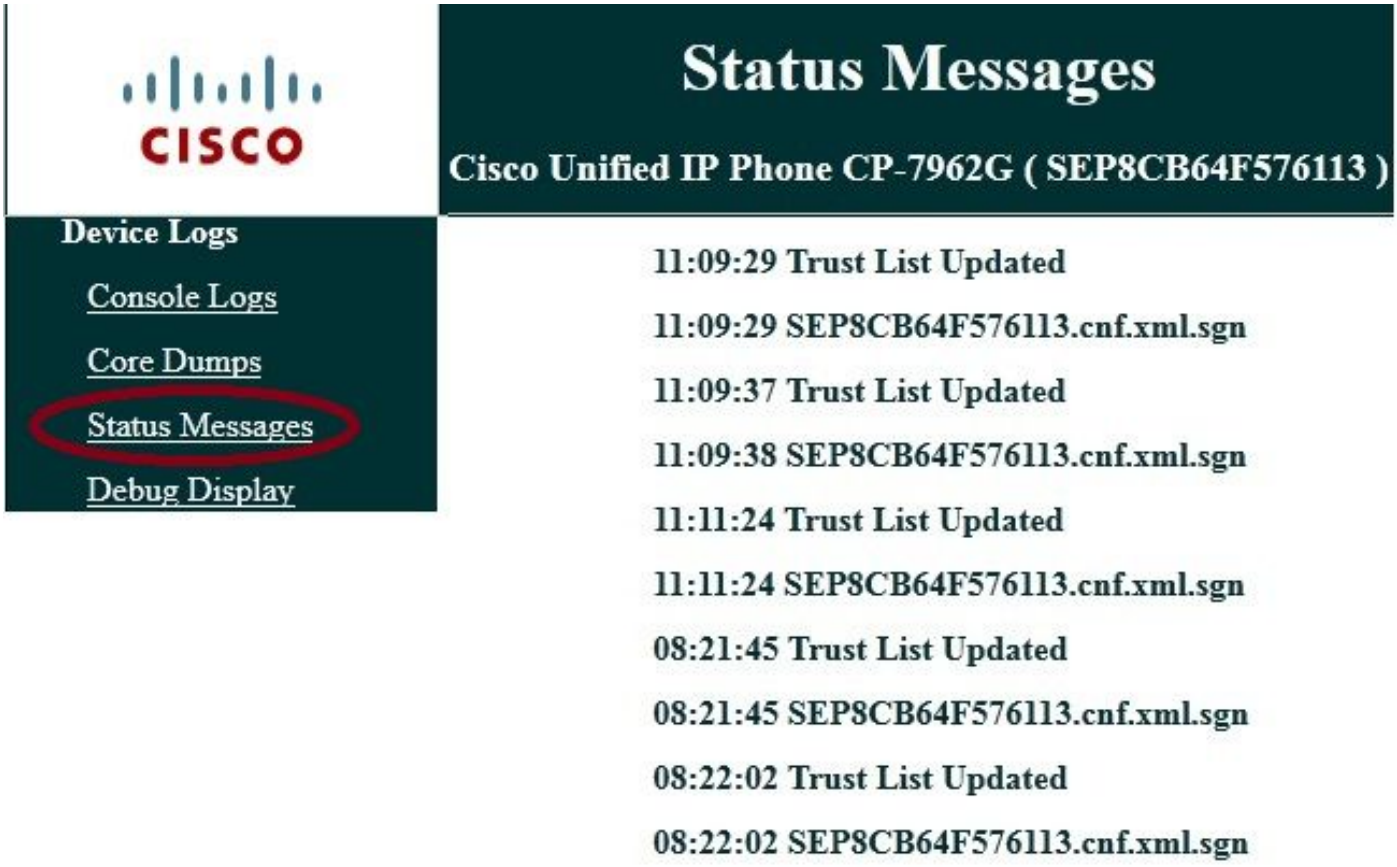
Nota: Quando il telefono IP si trova sul lato remoto, in genere riceve un indirizzo IP da un server DHCP esterno. Affinché il telefono IP riceva la nuova configurazione dal CUCM, deve contattare il server TFTP nell'ufficio principale. Normalmente CUCM è lo stesso server TFTP.

Per ricevere i file di configurazione con le modifiche, verificare che l'indirizzo IP del server TFTP sia impostato correttamente nelle impostazioni di rete del telefono; per conferma, usare l'opzione 150 del server DHCP o impostare manualmente il protocollo TFTP sul telefono. Questo server TFTP è accessibile tramite una sessione AnyConnect.

Se il telefono IP riceve il server TFTP da un server DHCP locale ma l'indirizzo non è corretto, è possibile utilizzare l'opzione del server TFTP alternativo per ignorare l'indirizzo IP del server TFTP fornito dal server DHCP. In questa procedura viene descritto come applicare il server TFTP alternativo:

1. Selezionare **Impostazioni > Configurazione di rete > Configurazione IPv4**.
2. Scorrere fino all'opzione TFTP alternativo.
3. Premere il tasto softkey Yes per il telefono per utilizzare un server TFTP alternativo; in caso contrario, premere il tasto softkey No. Se l'opzione è bloccata, premere * * # per sbloccarla.
4. Premere il tasto Salva.
5. Applicare il server TFTP alternativo all'opzione Server TFTP 1.

Esaminare i messaggi di stato nel browser Web o nei menu del telefono direttamente per verificare che il telefono riceva le informazioni corrette. Se la comunicazione è impostata correttamente, verranno visualizzati messaggi come i seguenti:



Se il telefono non è in grado di recuperare le informazioni dal server TFTP, si ricevono messaggi di errore TFTP:

Rinnovo del certificato SSL ASA

Se si ha una configurazione VPN AnyConnect funzionante, ma il certificato SSL ASA sta per scadere, non è necessario portare tutti i telefoni IP sul sito principale per inserire i nuovi certificati SSL nel telefono; è possibile aggiungere i nuovi certificati mentre la VPN è connessa.

Se il certificato CA radice dell'appliance ASA è stato esportato o importato anziché il certificato di identità e si desidera continuare a utilizzare lo stesso fornitore (CA) durante il rinnovo, non è necessario modificare il certificato nel CUCM in quanto rimane lo stesso. Tuttavia, se è stato utilizzato il certificato di identità, questa procedura è necessaria; in caso contrario, il valore hash tra l'ASA e il telefono IP non corrisponde e la connessione non è considerata attendibile dal telefono.

1. Rinnovare il certificato sull'appliance ASA.
   Nota: Per ulteriori informazioni, consultare il documento ASA 8.x: Rinnovare e installare il

certificato SSL con ASDM. Creare un trust point separato e non applicare il nuovo certificato con il comando **ssl trustpoint <nome> esterno** finché il certificato non sarà stato applicato a tutti i telefoni IP VPN.
2. Esporta il nuovo certificato.

3. Importa il nuovo certificato nel CUCM come certificato Phone-VPN-Trust.
   Nota: Tieni presente che **CSCuh19734 Caricando certificati con lo stesso CN, il vecchio certificato verrà sovrascritto in Phone-VPN-trust**
4. Passare alla configurazione del gateway VPN in CUCM e applicare il nuovo certificato. Sono ora disponibili entrambi i certificati: il certificato che sta per scadere e il nuovo certificato che non è stato ancora applicato all'appliance ASA.

5. Applica la nuova configurazione al telefono IP. Selezionare **Apply Config > Reset > Restart** (Applica configurazione **> Ripristina >** Riavvia) per inserire le nuove modifiche alla configurazione del telefono IP tramite il tunnel VPN. Verificare che tutti i telefoni IP siano connessi tramite la VPN e che possano raggiungere il server TFTP tramite il tunnel.

6. Usare il protocollo TFTP per controllare i messaggi di stato e il file di configurazione per verificare che il telefono IP abbia ricevuto il file di configurazione con le modifiche.

7. Applicare il nuovo trust point SSL nell'appliance ASA e sostituire il vecchio certificato.

Nota: Se il certificato ASA SSL è già scaduto e i telefoni IP non sono in grado di connettersi tramite AnyConnect; è possibile eseguire il push delle modifiche (ad esempio, l'hash del nuovo certificato ASA) sul telefono IP. Impostare manualmente il TFTP nel telefono IP su un indirizzo IP pubblico in modo che il telefono IP possa recuperare le informazioni da tale indirizzo. Utilizzare un server TFTP pubblico per ospitare il file di configurazione; Ad esempio, è possibile creare una porta di inoltro sull'appliance ASA e reindirizzare il traffico al server TFTP interno.