Teléfono de AnyConnect VPN del Troubleshooting - Teléfonos IP, ASA, y CUCM

Contenido

Introducción

Este documento describe cómo resolver problemas los problemas con los Teléfonos IP que utiliza el protocolo de Secure Sockets Layer (SSL) (Cliente de movilidad Cisco AnyConnect Secure) para conectar con Cisco un dispositivo de seguridad adaptante (ASA) se utilice que como un gateway de VPN y para conectar con las Comunicaciones unificadas de Cisco a un administrador (CUCM) que está utilizado como servidor de la Voz.

Para los ejemplos de configuración de AnyConnect con los teléfonos VPN, refiera a estos documentos:

- SSLVPN con el ejemplo de configuración de los Teléfonos IP
- Teléfono de AnyConnect VPN con el ejemplo de configuración de la autenticación certificada

Antecedentes

Antes de que usted despliegue SSL VPN con los Teléfonos IP, confirme que usted ha cumplido estos requisitos iniciales para las licencias de AnyConnect para el ASA y para la versión restringida exportación E.E.U.U. del CUCM.

Confirme la licencia del teléfono VPN en el ASA

La licencia del teléfono VPN habilita la característica en el ASA. Para confirmar el número de usuarios que puedan conectar con el AnyConnect (independientemente de si es un teléfono del IP), marque la licencia superior de AnyConnect SSL. ¿Refiérase a qué licencia ASA es necesaria para el teléfono del IP y las conexiones VPN móviles? para conocer más detalles.

En el ASA, utilice el **comando show version** para marcar si se habilita la característica. El nombre de la licencia diferencia con la versión ASA:

- Versión 8.0.x ASA: el nombre de la licencia es AnyConnect para el teléfono de Linksys.
- Versión 8.2.x ASA y posterior: el nombre de la licencia es AnyConnect para el teléfono del Cisco VPN.

Aquí está un ejemplo para la versión 8.0.x ASA:

```
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.
```

Aquí está un ejemplo para las versiones 8.2.x ASA y posterior:

```
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.
```

Exportación restringida y exportación CUCM sin restricción

Usted debe desplegar una versión restringida exportación E.E.U.U. de CUCM para la función del teléfono VPN.

Si usted utiliza una versión sin restricción de la exportación E.E.U.U. de CUCM, observe eso:

- Las Configuraciones de seguridad del teléfono del IP se modifican para inhabilitar el cifrado de la señalización y de los media; esto incluye el cifrado proporcionado por la función del teléfono VPN.
- Usted no puede exportar los detalles VPN a través de la importación/de la exportación.

- Las casillas de verificación para el perfil VPN, el gateway de VPN, el grupo VPN, y configuración de la característica VPN no se visualizan.

Note: Una vez que usted actualiza a la versión sin restricción de la exportación E.E.U.U. de CUCM, usted no puede actualizar más adelante a, o realice un fresco instalan de, la versión restringida exportación E.E.U.U. de este software.

Problemas frecuentes en el ASA

Note: Usted puede utilizar el analizador del CLI de Cisco (clientes registrados solamente) para ver una análisis de la salida del comando show. Usted debe también referir a la información importante en el documento de Cisco de los comandos Debug antes de que usted utilice los **comandos debug**.

Certificados para el uso en el ASA

En el ASA, usted puede utilizar los Certificados uno mismo-firmados SSL, los Certificados de tercera persona SSL, y los Certificados del comodín; ninguno de estos seguro la comunicación entre el teléfono del IP y el ASA.

Solamente un certificado de identidad puede ser utilizado porque solamente un certificado se puede asignar a cada interfaz.

Para los Certificados de tercera persona SSL, instale el encadenamiento completo en el ASA, e incluya cualquier intermedio y certificado raíz.

Trustpoint/certificado para la exportación ASA y la importación CUCM

El certificado que el ASA presenta al teléfono del IP durante la negociación SSL se debe exportar del ASA e importar en el CUCM. Marque el trustpoint asignado a la interfaz a la cual los Teléfonos IP conectan para saber qué certificado a exportar del ASA.

Utilice el comando **SSL del funcionamiento de la demostración** para verificar el trustpoint (certificado) que se exportará. Refiera al teléfono de AnyConnect VPN con el ejemplo de configuración de la autenticación certificada para más información.

> **Note**: Si usted ha desplegado un certificado de tercera persona a uno o más ASA, usted necesita exportar cada certificado de identidad de cada ASA y después importarlo al CUCM como teléfono-VPN-confianza.

El ASA presenta el certificado autofirmado ECDSA en vez del certificado configurado RSA

Cuando ocurre este problema, los teléfonos de un más nuevo modelo no pueden conectar, mientras que los teléfonos modelo más viejos no experimentan ninguna problemas. Aquí sea abre una sesión el teléfono cuando ocurre este problema:

```
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.
```

En las versiones 9.4.1 y posterior, la criptografía elíptica de la curva se soporta para el SSL/TLS. Cuando un cliente VPN curva-capaz elíptico SSL tal como un nuevo modelo del teléfono conecta con el ASA, se negocia la habitación elíptica de la cifra de la curva, y el ASA presenta al cliente VPN SSL con un certificado elíptico de la curva, incluso cuando la interfaz que corresponde se configura con un trustpoint RSA-basado. Para evitar que el ASA presente un certificado uno mismo-firmado SSL, el administrador debe quitar las habitaciones de la cifra que corresponden vía el comando de la **cifra SSL**. Por ejemplo, para una interfaz que se configure con un trustpoint RSA, el administrador puede ejecutar este comando para solamente negociar las cifras RSA-basadas:

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

Con la implementación del Id. de bug Cisco CSCuu02848, la prioridad se da a la configuración. los Certificados Explícito-configurados se utilizan siempre. Los certificados autofirmados se utilizan solamente en ausencia de un certificado configurado.

Cifras propuestas del cliente	CERT RSA solamente	CERT EC solamente	Ambo Certs	Ninguno
El RSA cifra solamente	CERT de las aplicaciones RSA Cifras de las aplicaciones RSA	CERT uno mismo-firmado RSA de las aplicaciones Cifras de las aplicaciones RSA	CERT de las aplicaciones RSA Cifras de las aplicaciones RSA	CERT uno mismo-firma RSA de las aplicacione Cifras de las aplicacior RSA
El EC cifra solamente (raro)	La conexión falla	CERT de las aplicaciones EC Cifras de las aplicaciones EC	CERT de las aplicaciones EC Cifras de las aplicaciones EC	CERT uno mismo-firma EC de las aplicaciones Cifras de las aplicacior EC
Ambas cifras solamente	CERT de las aplicaciones RSA Cifras de las aplicaciones RSA	CERT de las aplicaciones EC Cifras de las aplicaciones EC	CERT de las aplicaciones EC Cifras de las aplicaciones EC	CERT uno mismo-firma EC de las aplicaciones Cifras de las aplicacior EC

Base de datos externa para la autenticación de los usuarios del teléfono del IP

Usted puede utilizar una base de datos externa para autenticar a los usuarios del teléfono del IP. Los protocolos tales como el Lightweight Directory Access Protocol (LDAP) o Remote Authentication Dial In User Service (RADIUS) se pueden utilizar para la autenticación de los usuarios del teléfono VPN.

Coincidencias del hash del certificado entre la lista de la confianza del certificado ASA y del teléfono VPN

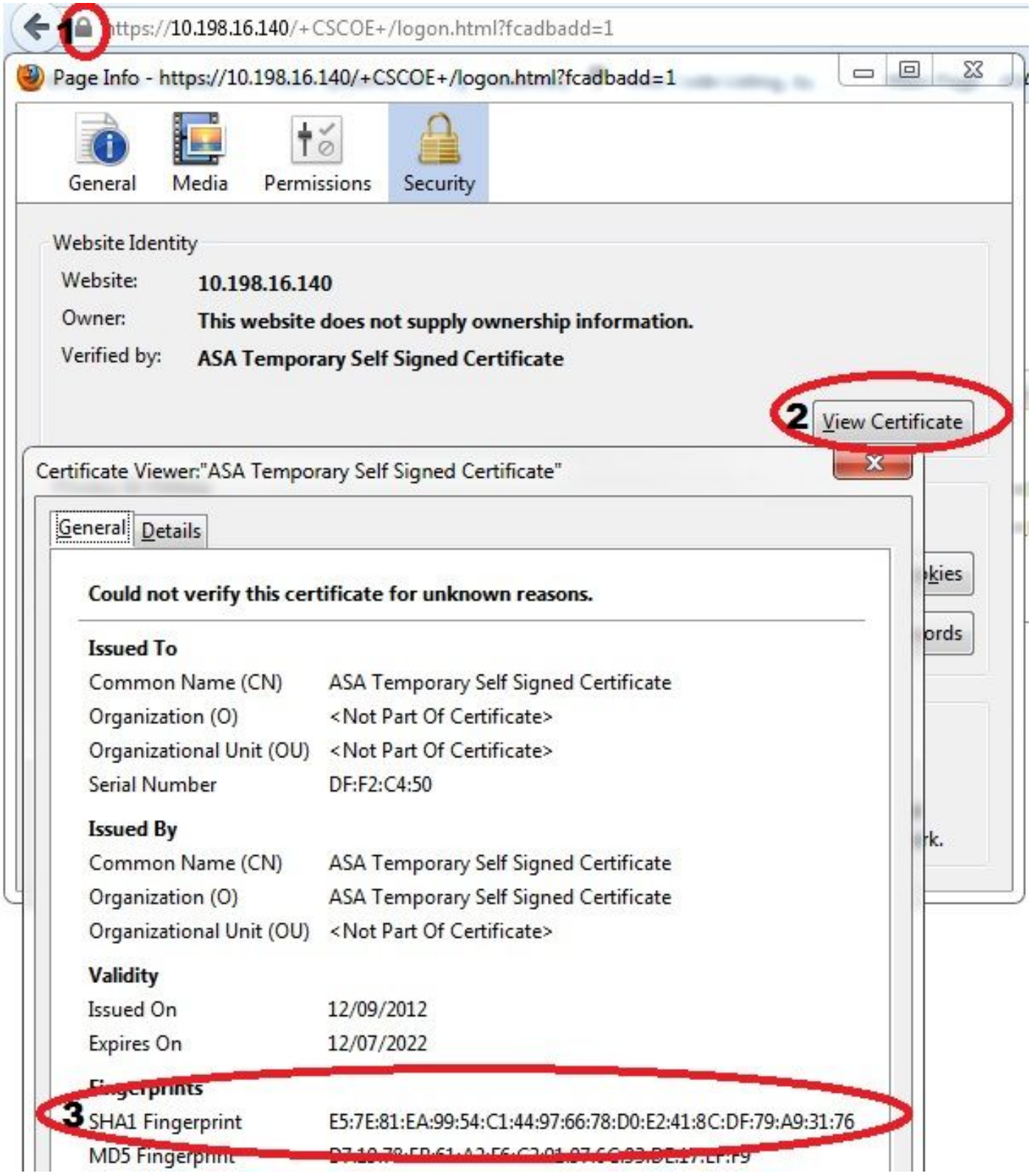
Recuerde que usted debe descargar el certificado que se asigna a la interfaz ASA SSL y cargarlo como certificado de la Teléfono-VPN-confianza en el CUCM. Diversas circunstancias pudieron causar el hash para este certificado presentado por el ASA para no hacer juego el hash que el servidor CUCM genera y avanza al teléfono VPN a través del archivo de configuración.

Una vez que la configuración es completa, pruebe la conexión VPN entre el teléfono del IP y el ASA. Si la conexión continúa fallando, marcar si el hash del certificado ASA hace juego el hash el teléfono del IP está esperando:

1. Marque el hash del algoritmo de troceo seguro 1 (SHA1) presentado por el ASA.
2. Utilice el TFTP para descargar Configuración del teléfono IP el archivo del CUCM.
3. Decodifique el hash del hexadecimal al base 64 o del base 64 al hexadecimal.

Marque el hash SHA1

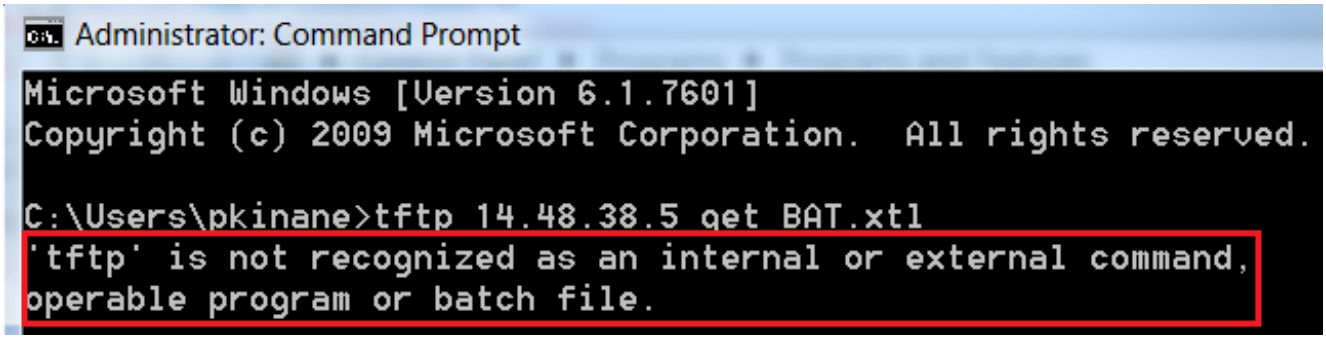
El ASA presenta el certificado aplicado con el comando del **trustpoint SSL** en la interfaz con la cual el teléfono del IP conecta. Para marcar este certificado, abra el hojeador (en este ejemplo, Firefox), y ingrese el URL (el grupo-URL) con el cual los teléfonos deben conectar:

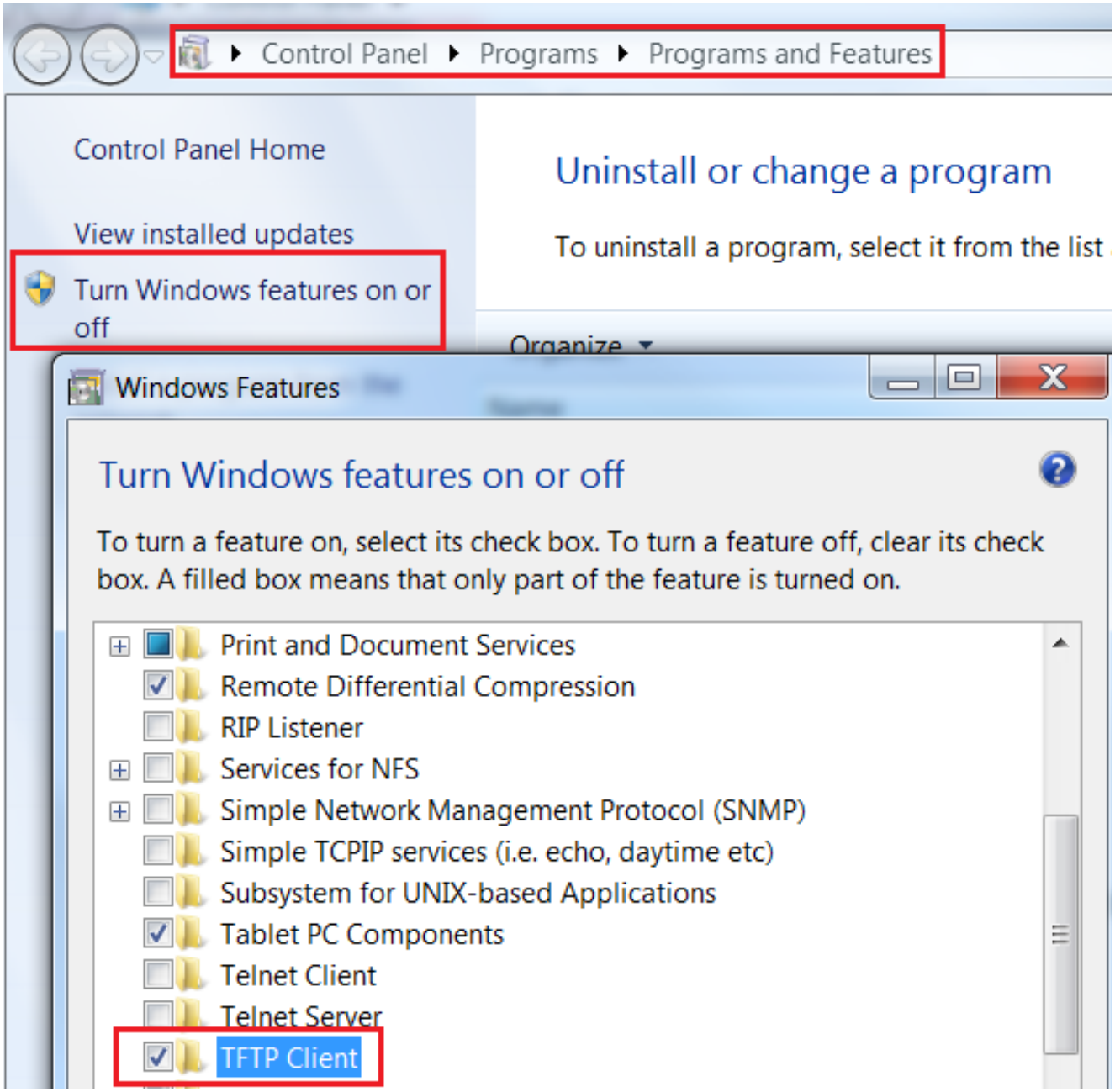


Descargue Configuración del teléfono IP el archivo

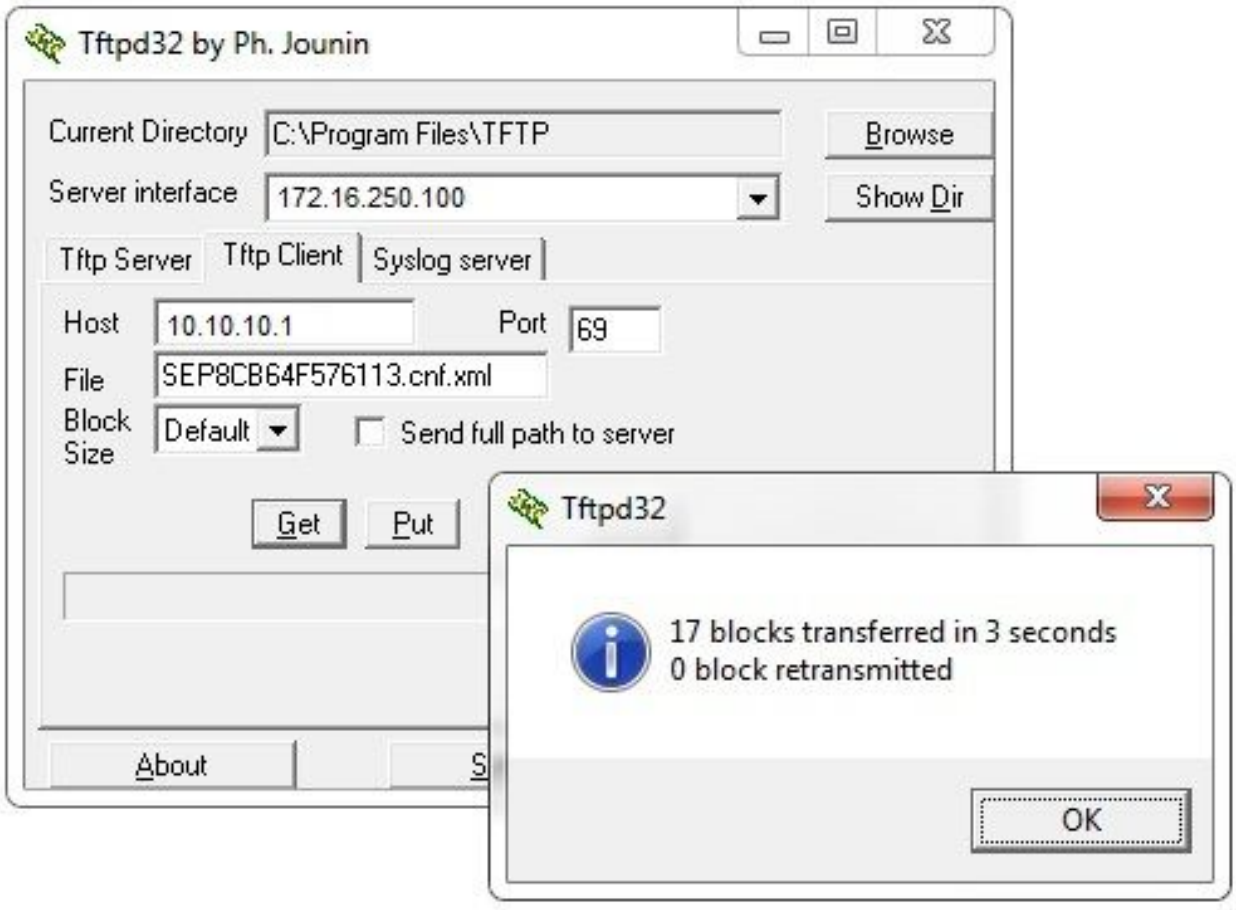
De un PC con el acceso directo al CUCM, descargue el archivo de configuración TFTP para el teléfono con los problemas de conexión. Dos métodos de la descarga son:

1. Abra a una sesión CLI en Windows, y utilice **tftp - comando del** *MAC address >.cnf.xml del <Phone del server>* **GET SEP i** *<TFTP*.
   Note: Si usted recibe un error similar al abajo, usted debe confirmar que la característica del cliente TFTP está
   habilitada.





2. Utilice una aplicación tal como Tftpd32 para descargar el archivo:

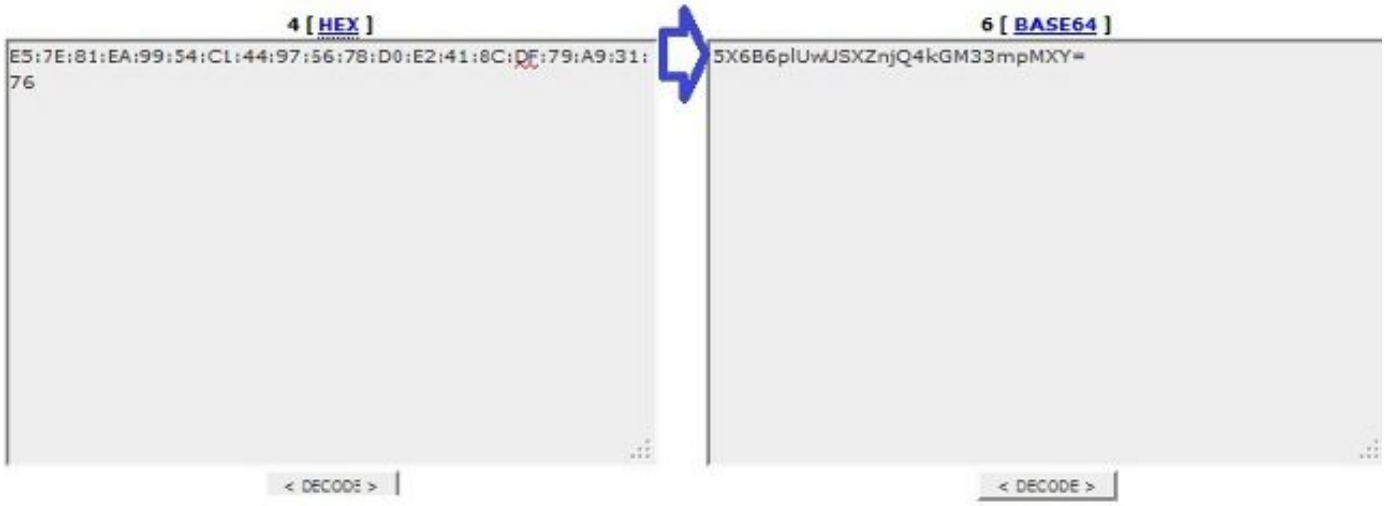


3. El archivo se descarga, abre el XML y encuentra una vez la configuración del *vpnGroup*. Este ejemplo muestra la sección y el *certHash* que se verificarán:

```
<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>
<certHash1>5X6B6plUwUSXZnjQ4kGM33mpMXY=</certHash1>
</credentials>
</vpnGroup>
```

Decodifique el hash

Confirme que ambos valores de troceo hacen juego. El navegador presenta el hash en el formato hexadecimal, mientras que el archivo XML utiliza el base 64, así que convierte un formato al otro para confirmar la coincidencia. Hay muchos traductores disponibles; un ejemplo es el TRADUCTOR, BINARIO.



Note: Si el valor de troceo anterior no hace juego, el teléfono VPN no confía en la conexión que se negocia con el ASA, y la conexión falla.

Balanceo de carga y Teléfonos IP VPN

La carga balanceada SSL VPN no se soporta para los teléfonos VPN. Los teléfonos VPN no realizan la validación de certificado real sino que por el contrario utilizar desmenuza empujado hacia abajo por el CUCM para validar los servidores. Porque el balanceo de carga VPN es básicamente una redirección de HTTP, requiere los teléfonos validar los certificados múltiples, que lleva al error. Los síntomas del error del balanceo de carga VPN incluyen:

- El teléfono alterna entre los servidores y tarda excepcionalmente un tiempo prolongado para conectar o falla eventual.
- Los registros del teléfono contienen los mensajes tales como éstos:

```
<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>
<certHash1>5X6B6plUwUSXZnjQ4kGM33mpMXY=</certHash1>
</credentials>
</vpnGroup>
```

CSD y Teléfonos IP

Actualmente, los Teléfonos IP no soportan el (CSD) del Cisco Secure Desktop y no conectan cuando el CSD se habilita para el grupo de túnel o global en el ASA.

Primero, confirme si el ASA tiene CSD habilitado. Ingrese el **comando webvpn del funcionamiento de la demostración** en el 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#
```

Para marcar los problemas CSD durante una conexión del teléfono del IP, marque los registros o los debugs en el ASA.

Registros 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#
```

Debugs 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>
```

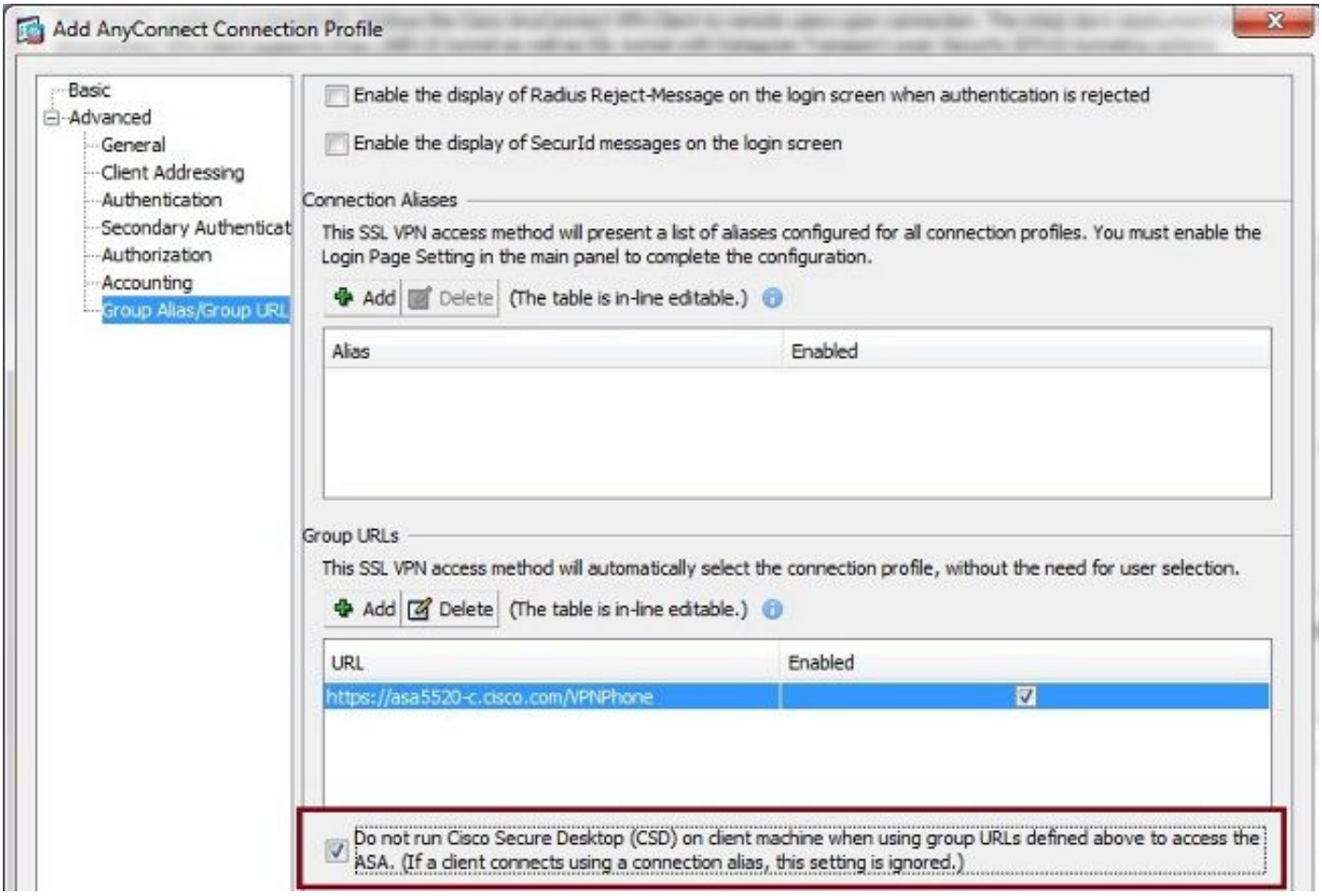
> **Note**: En un despliegue grande con una mucha carga de los usuarios de AnyConnect, Cisco recomienda que usted no habilita el **anyconnect del webvpn del debug**. Su salida no se puede filtrar por la dirección IP, así que una gran cantidad de información pudo ser creada.

En las Versiones de ASA 8.2 y posterior, usted debe aplicar el comando sin-**CSD** bajo WebVPN-atributos del grupo de túnel:

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

En las versiones anteriores del ASA, esto no era posible, así que la única solución alternativa era inhabilitar el CSD global.

En el Cisco Adaptive Security Device Manager (ASDM), usted puede inhabilitar el CSD para un perfil de la conexión específico tal y como se muestra en de este ejemplo:

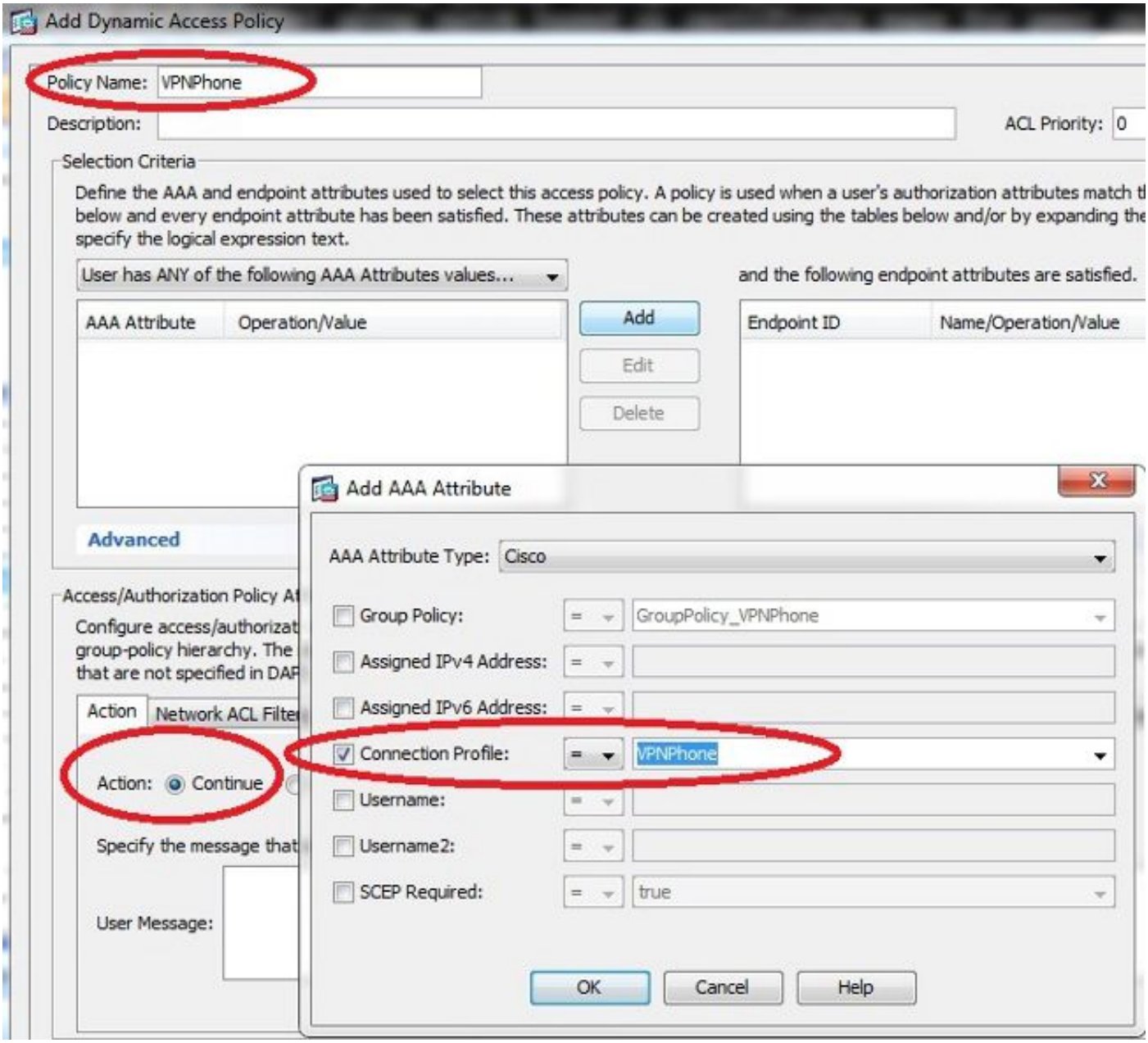


Note: Utilice un grupo-URL para apagar la característica CSD.

Reglas DAP

La mayoría de las implementaciones no sólo conectan los Teléfonos IP con el ASA pero también conectan diversos tipos de máquinas (Microsoft, Linux, Mac OS) y de dispositivos móviles (Android, IOS). Por este motivo, es normal encontrar una configuración existente de las reglas de la directiva del acceso dinámico (DAP), donde, la mayor parte del tiempo, está terminación la acción predeterminada bajo el DfltAccessPolicy de la conexión.

Si éste es el caso, cree una regla separada DAP para los teléfonos VPN. Utilice un parámetro específico, tal como el perfil de la conexión, y fije la acción **para continuar**:



Si usted no crea una directiva específica DAP para los Teléfonos IP, el ASA muestra un golpe bajo el DfltAccessPolicy y falla de conexión:

```
%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
```

Una vez que usted crea una directiva específica DAP para los Teléfonos IP con el conjunto de la

acción **para continuar**, usted puede conectar:

```
%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
```

Valores heredados de DfltGrpPolicy o de otros grupos

En muchos casos, el DfltGrpPolicy se configura con varias opciones. Por abandono, estas configuraciones se heredan para la sesión del teléfono del IP a menos que se especifiquen manualmente en la grupo-directiva que el teléfono del IP debe utilizar.

Algunos parámetros que pudieron afectar a la conexión si se heredan del DfltGrpPolicy son:

- grupo-bloqueo
- VPN-túnel-protocolo
- VPN-simultáneo-logines
- VPN-filtro

Asuma que usted tiene este ejemplo de configuración en el DfltGrpPolicy y el 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 conexión hereda los parámetros del DfltGrpPolicy que no fueron especificados explícitamente bajo el GroupPolicy_VPNPhone y avanza toda la información al teléfono del IP durante la conexión.

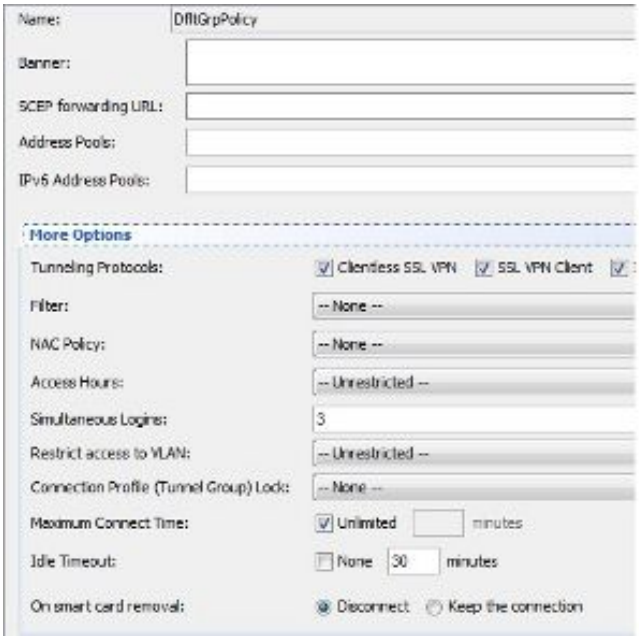
Para evitar esto, especifique manualmente los valores que usted necesita directamente en el grupo:

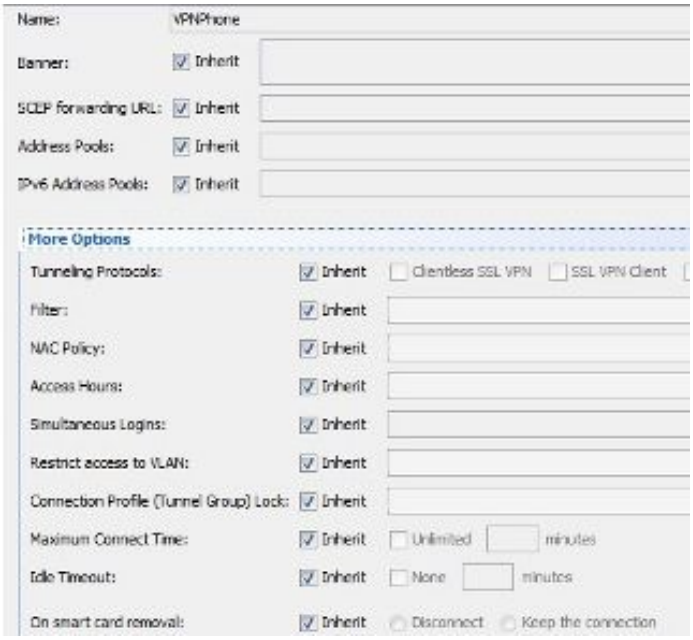
```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
 vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
 vpn-filter none
 default-domain value cisco.com
```

Para marcar los valores predeterminados del DfltGrpPolicy, utilice la **demostración funcionan con todo el** comando de la grupo-**directiva**; este ejemplo aclara la diferencia entre las salidas:

```
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
```

Aquí está la salida de la grupo-directiva hereda los atributos con el ASDM:





Cifras soportadas del cifrado

Un teléfono de AnyConnect VPN probado con los soportes del teléfono del IP 7962G y de la versión de firmware 9.1.1 solamente dos cifras, que son ambo Advanced Encryption Standard (AES): AES256-SHA y AES128-SHA. Si las cifras correctas no se especifican en el ASA, la conexión se rechaza, tal y como se muestra en del registro ASA:

```
%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
```

Para confirmar si el ASA tiene las cifras correctas habilitadas, ingrese la **demostración ejecutan todo el SSL** y **muestran los** comandos **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
```

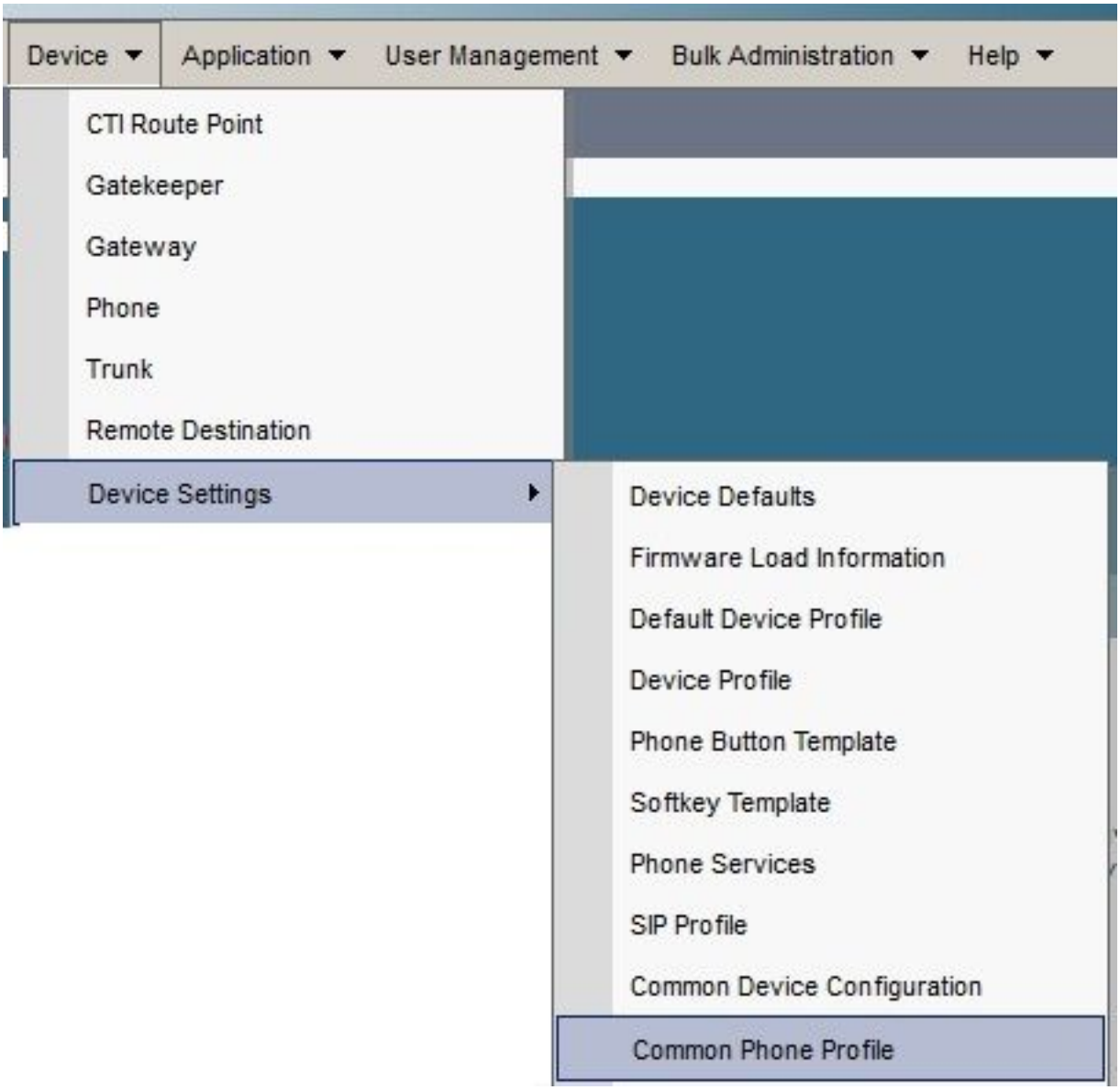
```
ASA5510-F#

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#
```

Problemas frecuentes en el CUCM

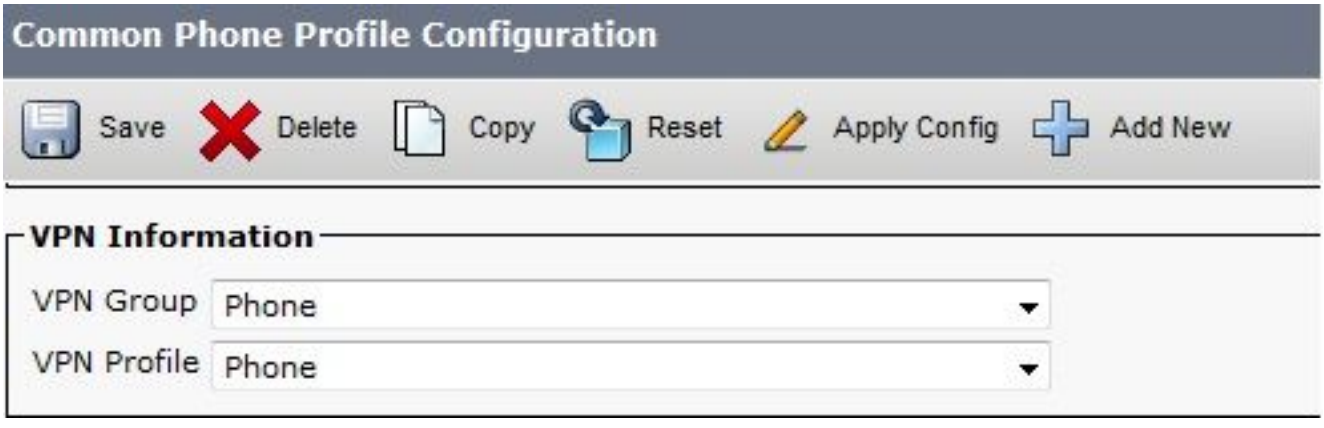
Configuraciones VPN no aplicadas al teléfono del IP

La configuración en el CUCM se crea una vez (gateway, grupo, y perfil), aplica las configuraciones VPN en el perfil común del teléfono:

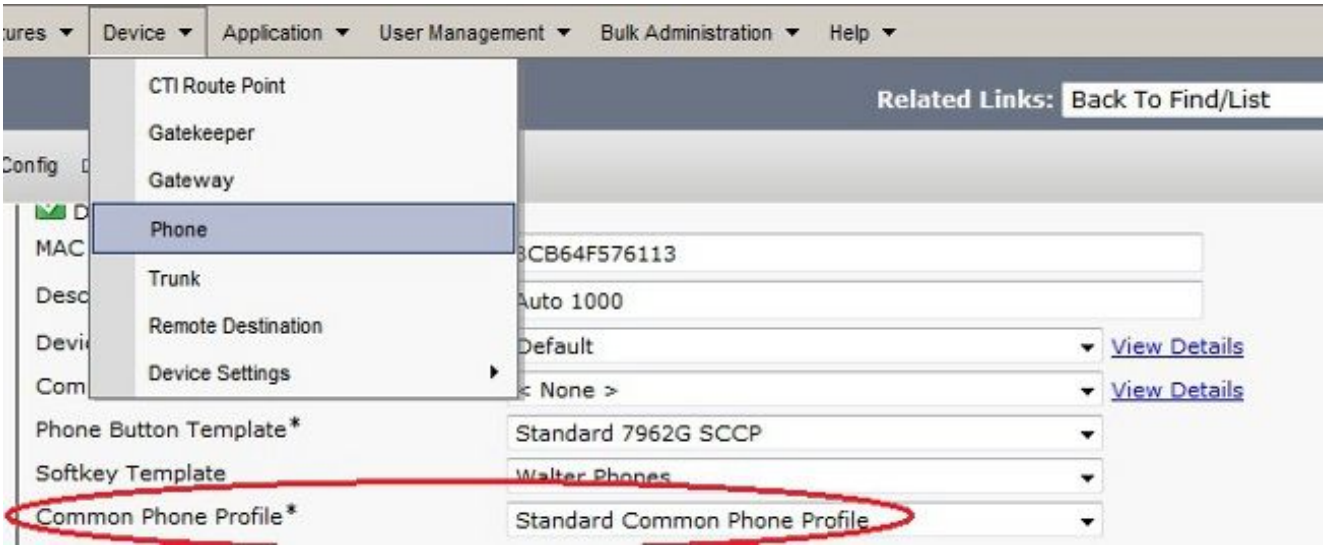
1. Navegue al **dispositivo >** a las **configuraciones del dispositivo > perfil común del teléfono**.



2. Ingrese la información de VPN:



3. Navegue al **Device (Dispositivo) > Phone (Teléfono)** y confirme este perfil se asigna a la Configuración del teléfono:



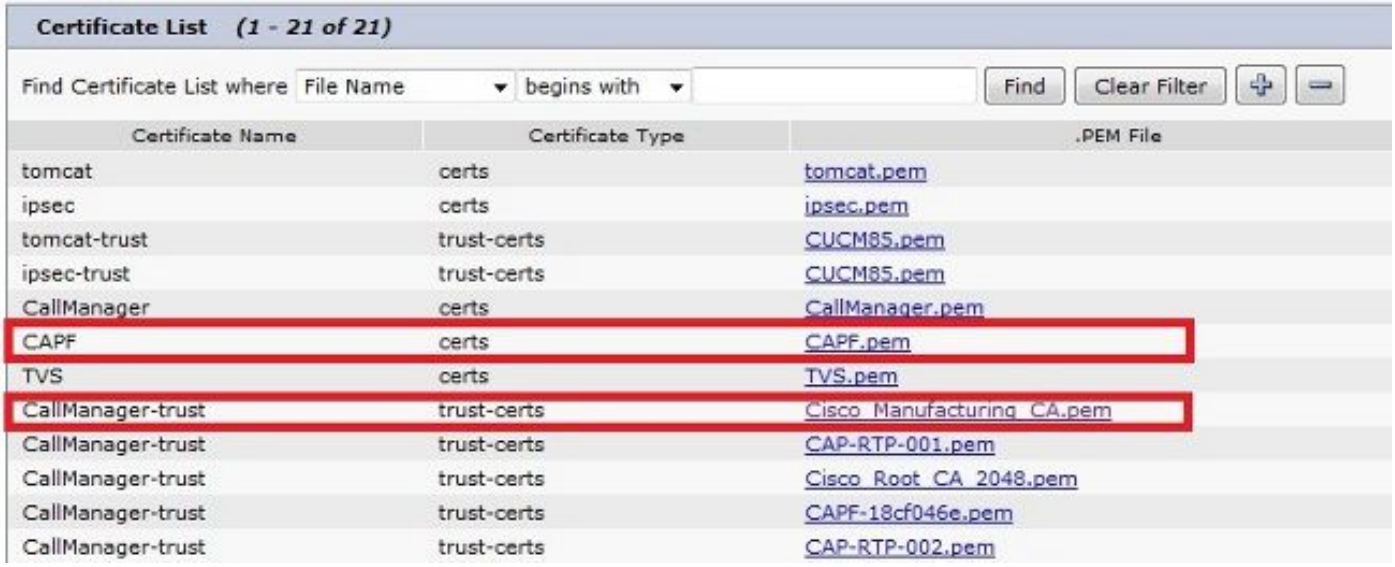
Método de autenticación certificada

Hay dos maneras de configurar la autenticación certificada para los Teléfonos IP: El fabricante instaló el certificado (MIC) y localmente - el certificado significativo (LSC). Refiera al teléfono de AnyConnect VPN con el ejemplo de configuración de la autenticación certificada para elegir la mejor opción para su situación.

Cuando usted configura la autenticación certificada, exporte los certificados (raíz CA) del servidor CUCM e impórtelos al ASA:

1. Inicie sesión al CUCM.
2. Navegue el **Certificate Management (Administración de certificados) unificado del > Security (Seguridad) de la administración OS**.
3. Encuentre la función de proxy del Certificate Authority (CAPF) o Cisco_Manufacturing_CA; el tipo de certificado depende sobre si usted utilizó la autenticación certificada MIC o LSC.
4. Descargue el archivo a la computadora local.

Una vez que se descargan los archivos, inicie sesión al ASA con el CLI o el ASDM e importe el certificado como certificado de 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

Por abandono, todos los teléfonos que soportan el VPN se cargan con los MIC. Los 7960 y 7940 teléfonos modelo no vienen con un MIC y requieren un procedimiento de la instalación especial de modo que el LSC se registre con seguridad.

Los Teléfonos IP más nuevos de Cisco (8811, 8841, 8851, y 8861) incluyen los Certificados MIC que son firmados por el nuevo SHA2 de fabricación CA:

- La versión 10.5(1) CUCM incluye y confía en los nuevos Certificados SHA2.
- Si usted funciona con una versión anterior CUCM, usted puede ser que sea requerido descargar el nuevo certificado de CA de la fabricación y:

  Carguela a la CAPF-confianza de modo que los teléfonos puedan autenticar con el CAPF para obtener un LSC.

  Carguelo a la CallManager-confianza si usted quiere permitir que los teléfonos autentiquen con un MIC para el SORBO 5061.

Tip: Haga clic este link para obtener el SHA2 CA si el CUCM funciona con actualmente una versión anterior.

Caution: Cisco recomienda que usted utiliza los MIC para la instalación LSC solamente. Cisco soporta los LSC para la autenticación de la conexión TLS con el CUCM. Porque los certificados raíz MIC pueden ser comprometidos, los clientes que configuran los teléfonos para utilizar los MIC para la autenticación de TLS o para cualquier otro propósito hacen tan por su cuenta y riesgo. Cisco no asume ningún defecto si se comprometen los MIC.

Por abandono, si un LSC existe en el teléfono, la autenticación utiliza el LSC, sin importar si un MIC existe en el teléfono. Si un MIC y un LSC existen en el teléfono, la autenticación utiliza el LSC. Si un LSC no existe en el teléfono, pero existe un MIC, la autenticación utiliza el MIC.

> **Note**: Recuerde que, para la autenticación certificada, usted debe exportar el certificado SSL del ASA e importarlo al CUCM.

Control del ID del host

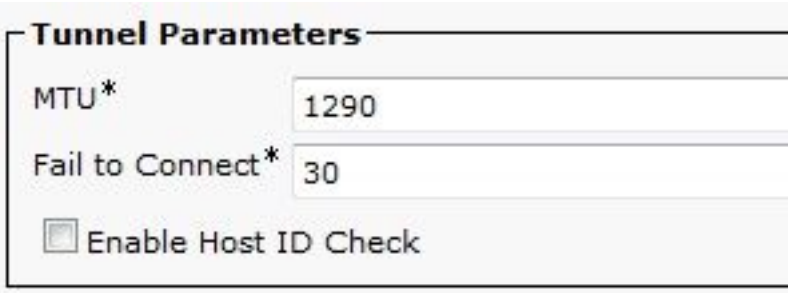
Si el Common Name (CN) en el tema del certificado no hace juego el URL (grupo-URL) que los teléfonos utilizan para conectar con el ASA con el VPN, que inhabilitan el control del ID del host en el CUCM o utilice un certificado en el ASA que hace juego ese URL en el ASA.

Esto es necesario cuando el certificado SSL del ASA es un certificado del comodín, el certificado SSL contiene un diverso SAN (nombre alternativo sujeto), o el URL fue creado con la dirección IP en vez del nombre de dominio completo (FQDN).

Éste es un ejemplo de un registro del teléfono del IP cuando el CN del certificado no hace juego el URL que el teléfono está intentando alcanzar.

```
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!!
```

Para inhabilitar el incorporar del ID del host los CUCM, navegan a las **funciones avanzadas** > al **perfil VPN** > **VPN**:



Resolución de otros problemas

Registros y debugs a utilizar en el ASA

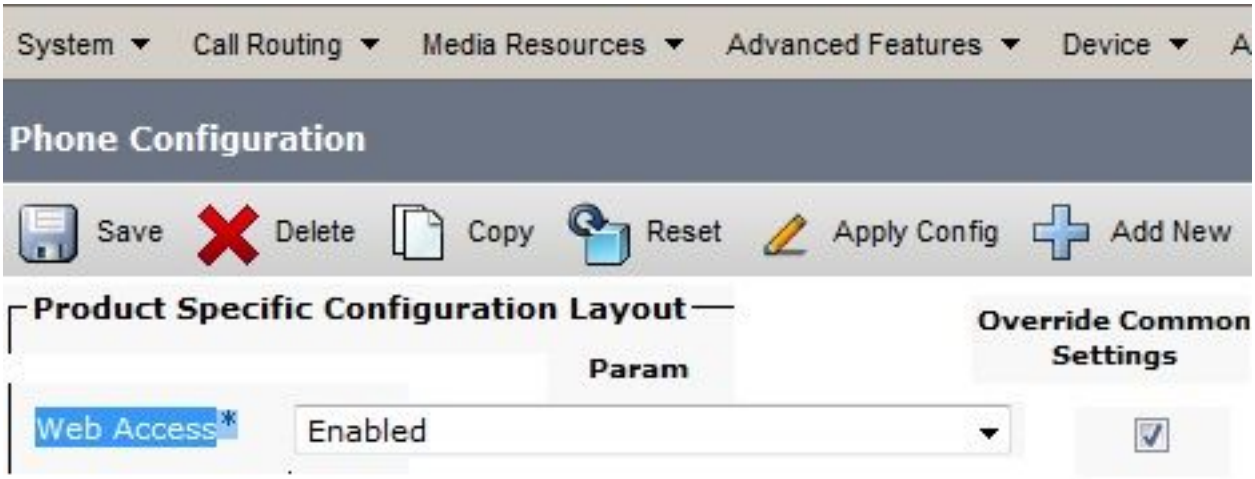
En el ASA, usted puede habilitar estos debugs y registros para resolver problemas:

```
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!!
```

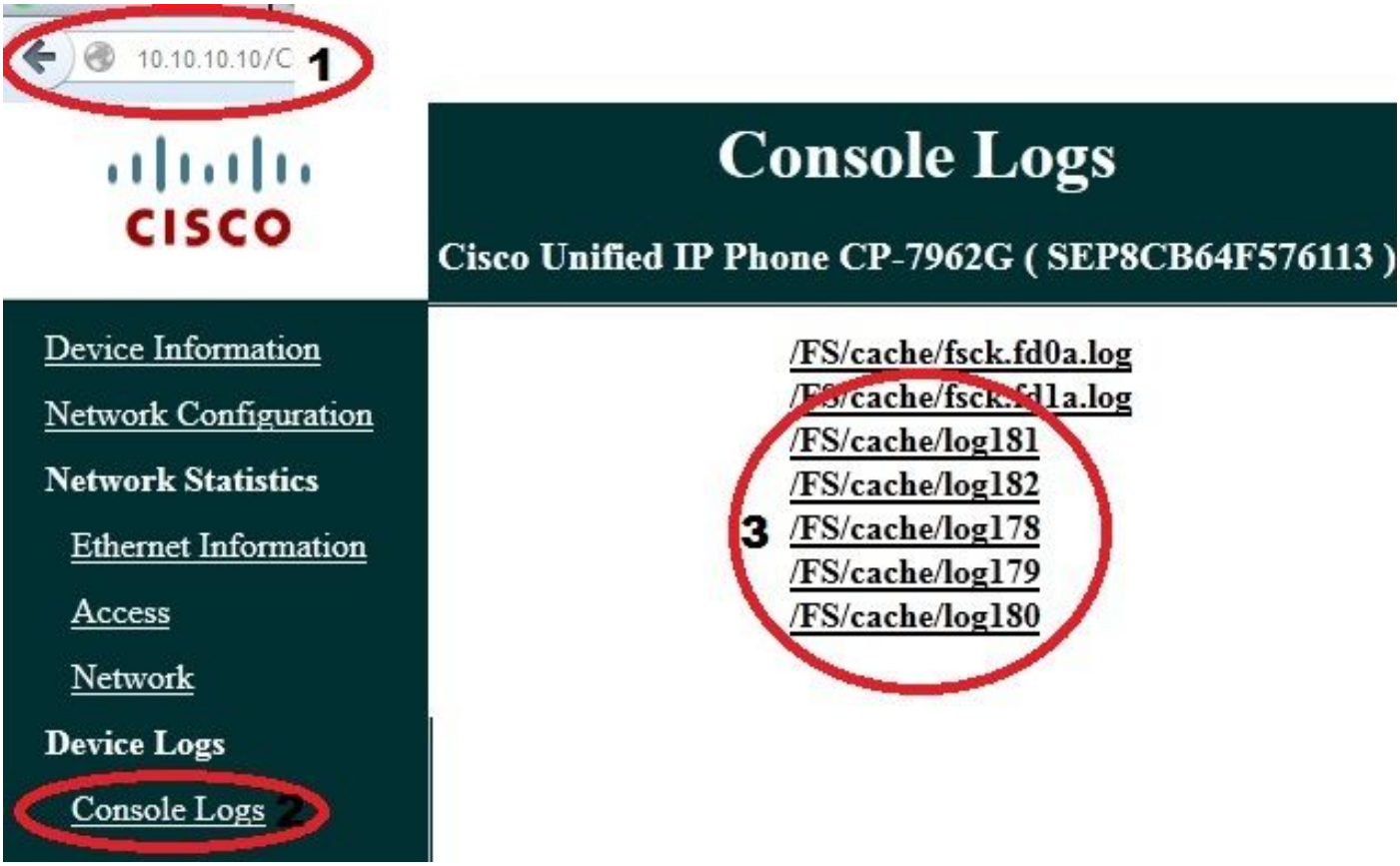
> **Note**: En un despliegue grande con una mucha carga de los usuarios de AnyConnect, Cisco recomienda que usted no habilita el **anyconnect del webvpnh del debug**. Su salida no se puede filtrar por la dirección IP, así que una gran cantidad de información pudo ser creada.

Registros del teléfono del IP

Para acceder los registros del teléfono, habilite la característica del Acceso Web. Inicie sesión al CUCM, y navegue al **Device (Dispositivo) > Phone (Teléfono) >** a la **Configuración del teléfono**. Encuentre el teléfono del IP en el cual usted quiere habilitar esta característica, y encuentre la sección para el Acceso Web. Aplique los cambios de configuración al teléfono del IP:



Una vez que usted habilita el servicio y reajusta el teléfono para inyectar esta nueva función, usted puede acceder el teléfono del IP abre una sesión al navegador; utilice la dirección IP del teléfono de un ordenador con el acceso a esa subred. Vaya a los registros de la consola y marque los cinco archivos del registro. Porque el teléfono sobregraba los cinco archivos, usted debe marcar todos estos archivos en la orden encuentra la información que usted busca.



Problemas correlacionados entre los registros ASA y los registros del teléfono del IP

Éste es un ejemplo de cómo correlacionar los registros del ASA y del teléfono del IP. En este ejemplo, el hash del certificado en el ASA no hace juego el hash del certificado en el archivo de configuración del teléfono porque el certificado en el ASA fue substituido por un diverso certificado.

Registros 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
```

Registros del teléfono

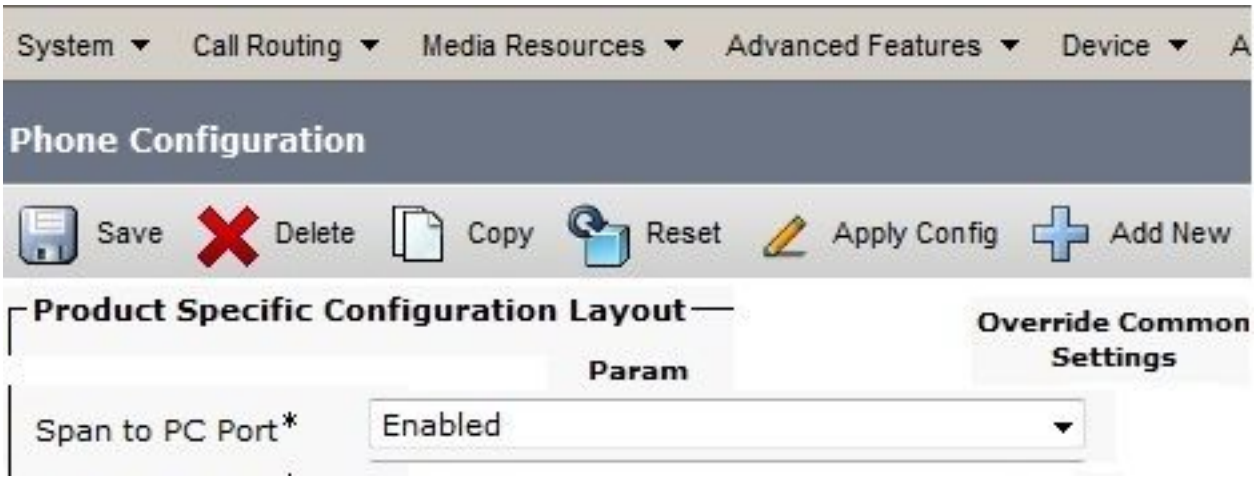
```
 902: NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect
initialization
903: NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state
904: NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A
905: NOT 10:19:27.364687 VPNC: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

Palmo a la característica del puerto de PC

Usted puede conectarse un ordenador directamente a un teléfono. El teléfono tiene un puerto del switch en la Placa posterior.

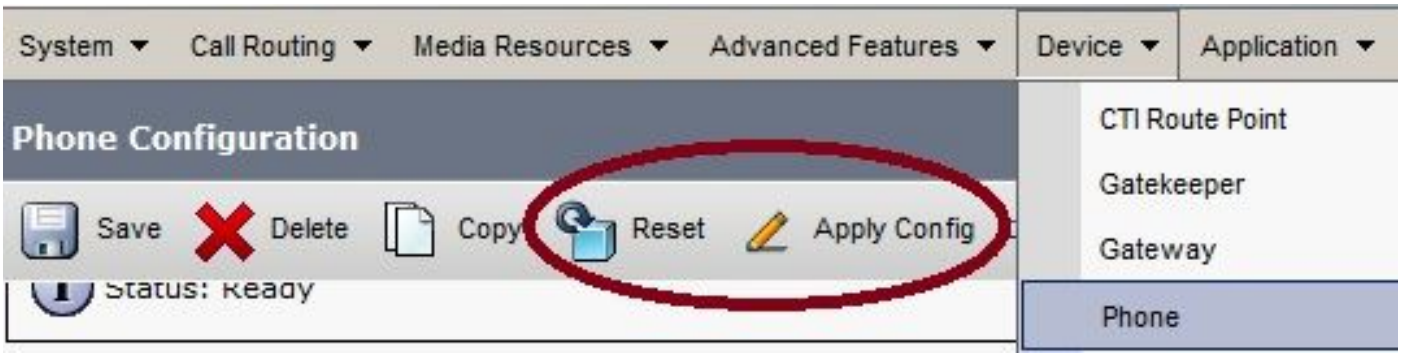
Configure el teléfono como usted lo hizo previamente, para habilitar el palmo al puerto de PC en el CUCM, y para aplicar la configuración. El teléfono comienza a enviar una copia de cada bastidor al PC. Utilice Wireshark en el modo promiscuo para capturar el tráfico para el análisis.



Configuración del teléfono IP cambios mientras que es conectado por el VPN

Una pregunta común es si usted puede modificar la configuración VPN mientras que el teléfono del IP es red conectada de los por AnyConnect. La respuesta está sí, pero usted debe confirmar algunos ajustes de la configuración.

Realice los cambios necesarios en el CUCM, después aplique los cambios al teléfono. Hay tres opciones (aplique los Config, reajustan, reinicio) para avanzar la nueva configuración al teléfono. Aunque las tres opciones desconecten el VPN del teléfono y del ASA, usted puede volver a conectar automáticamente si usted está utilizando la autenticación certificada; si usted está utilizando el Authentication, Authorization, and Accounting (AAA), le indican para sus credenciales otra vez.



> **Note**: Cuando el teléfono del IP está en el lado remoto, recibe normalmente una dirección IP de un servidor DHCP externo. Para que el teléfono del IP reciba la nueva configuración del CUCM, debe entrar en contacto al servidor TFTP en la oficina principal. El CUCM es normalmente el mismo servidor TFTP.

Para recibir los archivos de configuración con los cambios, confirme que la dirección IP para el servidor TFTP está configurada correctamente en las configuraciones de red en el teléfono; para la confirmación, utilice la opción 150 del servidor DHCP o fije manualmente el TFTP en el teléfono. Este servidor TFTP es accesible con una sesión de AnyConnect.

Si el teléfono del IP está recibiendo al servidor TFTP de un servidor DHCP local pero ese direccionamiento es incorrecto, usted puede utilizar la opción alterna del servidor TFTP para reemplazar el TFTP Server IP Address proporcionado por el servidor DHCP. Este procedimiento describe cómo aplicar al servidor TFTP alterno:

1. Navegue a las **configuraciones** > a la **configuración del IPv4 de la Configuración de la red**.
2. Navegue a la opción TFTP alterna.
3. Pulse la tecla suave del sí para que el teléfono utilice a un servidor TFTP alternativo; si no, no pulse la ninguna tecla suave. Si la opción es bloqueada, prensa * * # para desbloquearla.
4. Presione la tecla programable **Save**.
5. Aplique al servidor TFTP alterno bajo opción del servidor TFTP 1.

Revise los mensajes de estado en el buscador Web o en los menús del teléfono directamente para confirmar que el teléfono está recibiendo la información correcta. Si la comunicación se configura correctamente, usted ve los mensajes tales como éstos:

Si el teléfono no puede extraer la información del servidor TFTP, usted recibe los mensajes de error TFTP:

Renovación del certificado ASA SSL

Si usted hace un teléfono funcional de AnyConnect VPN poner pero su certificado ASA SSL está a punto de expirar, usted no necesita traer todos los Teléfonos IP al sitio principal para inyectar los nuevos Certificados SSL al teléfono; usted puede agregar los nuevos Certificados mientras que el VPN está conectado.

Si usted ha exportado o importado certificado raíz CA del ASA en vez del certificado de identidad y si usted quiere continuar utilizando al mismo vendedor (CA) durante esta renovación, no es necesario cambiar el certificado en el CUCM porque sigue siendo lo mismo. Pero, si usted utilizó el certificado de identidad, este procedimiento es necesario; si no, el valor de troceo entre el ASA y el teléfono del IP no hace juego, y la conexión no es confiada en por el teléfono.

1. Renueve el certificado en el ASA.
   Note: Para los detalles, refiera a ASA 8.x: Renueve y instale el certificado SSL con el ASDM.

Cree un trustpoint separado y no aplique este nuevo certificado con el **<name> del trustpoint SSL fuera del** comando hasta que usted haya aplicado el certificado a todos los Teléfonos IP VPN.

2. Exporte el nuevo certificado.

3. Importe el nuevo certificado al CUCM como certificado de la Teléfono-VPN-confianza.
   Note: Sea consciente de **CSCuh19734 que carga los certs con el mismo CN sobregrabará el CERT viejo en la Teléfono-VPN-confianza**
4. Navegue a la configuración de gateway de VPN en el CUCM, y aplique el nuevo certificado. Usted ahora tiene ambos Certificados: el certificado que está a punto de expirar y el nuevo certificado que no se ha aplicado al ASA todavía.

5. Aplique esta nueva configuración al teléfono del IP. Navegue **para aplicar los Config > reajustado > reinicio** para inyectar los nuevos cambios de configuración al teléfono del IP a través del túnel VPN. Asegúrese de que todos los Teléfonos IP estén conectados con el VPN y de que pueden alcanzar al servidor TFTP a través del túnel.

6. Utilice el TFTP para marcar los mensajes de estado y el archivo de configuración para confirmar que el teléfono del IP recibió el archivo de configuración con los cambios.

7. Aplique el nuevo trustpoint SSL en el ASA, y substituya el certificado viejo.

Note: Si se expira el certificado ASA SSL ya y si los Teléfonos IP no pueden conectar con AnyConnect; usted puede avanzar los cambios (tales como el nuevo hash del certificado ASA) al teléfono del IP. Fije manualmente el TFTP en el teléfono del IP a un IP Address público así que el teléfono del IP puede extraer la información de allí. Utilice a un servidor TFTP público para recibir el archivo de configuración; un ejemplo es crear una expedición del puerto en el ASA y reorientar el tráfico al servidor TFTP interno.