# Pesquise defeitos o telefone de AnyConnect VPN - Telefones IP, ASA, e CUCM

## Índice



## Introdução

Este documento descreve como pesquisar defeitos edições com Telefones IP que usa o protocolo do secure sockets layer (SSL) (Cliente de mobilidade Cisco AnyConnect Secure) a fim conectar a Cisco uma ferramenta de segurança adaptável (ASA) que seja usada como um gateway de VPN e a fim conectar às comunicações unificadas de Cisco um gerente (CUCM) que está usado como um server da Voz.

Para exemplos de configuração de AnyConnect com telefones VPN, refira estes documentos:

- SSLVPN com exemplo de configuração dos Telefones IP
- Telefone de AnyConnect VPN com exemplo de configuração do certificado de autenticação

# Informações de Apoio

Antes que você distribua SSL VPN com os Telefones IP, confirme que você cumpriu estas exigências iniciais para licenças de AnyConnect para o ASA e para a versão restringida exportação E.U. do CUCM.

## Confirme a licença do telefone VPN no ASA

A licença do telefone VPN permite a característica no ASA. A fim confirmar o número de usuários que podem conectar com o AnyConnect (mesmo se é um telefone IP), verifique a licença superior de AnyConnect SSL. Refira que licença ASA é precisada para o telefone IP e conexões de VPN móveis? para detalhes mais adicionais.

No ASA, use o **comando show version** a fim verificar se a característica é permitida. O nome da licença difere com a liberação ASA:

- Liberação 8.0.x ASA: o nome da licença é AnyConnect para o telefone de Linksys.
- O ASA libera 8.2.x e mais tarde: o nome da licença é AnyConnect para o telefone de Cisco VPN.

Está aqui um exemplo para a liberação 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.
```

Está aqui um exemplo para as liberações 8.2.x ASA e mais tarde:

```
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.
```

## Exportação restringida e exportação CUCM ilimitado

Você deve distribuir uma versão restringida exportação E.U. de CUCM para os recursos de telefone VPN.

Se você usa uma versão ilimitada da exportação E.U. de CUCM, note isso:

- As configurações de segurança do telefone IP são alteradas a fim desabilitar a sinalização e a criptografia de mídias; isto inclui a criptografia fornecida pelos recursos de telefone VPN.
- Você não pode exportar detalhes VPN através da importação/exportação.
- As caixas de seleção para o perfil VPN, o gateway de VPN, o grupo de VPN, e da característica VPN configuração não são indicadas.

**Note**: Uma vez que você promove à versão ilimitada da exportação E.U. de CUCM, você não pode promover mais tarde a, ou execute um fresco instalam de, a versão restringida exportação E.U. deste software.

# Problemas comuns no ASA

**Note**: Você pode usar o analisador do CLI Cisco (clientes registrados somente) a fim ver análises do emissor de comando de execução. Você deve igualmente referir a informação importante no documento Cisco dos comandos Debug antes que você use **comandos debug**.

## Certificados para o uso no ASA

No ASA, você pode usar Certificados auto-assinados SSL, Certificados da terceira SSL, e Certificados do convite; qualquer um seguro a comunicação entre o telefone IP e o ASA.

Somente um certificado de identidade pode ser usado porque somente um certificado pode ser atribuído a cada relação.

Para Certificados da terceira SSL, instale a corrente completa no ASA, e inclua todo o intermediário e certificados de raiz.

## Ponto confiável/certificado para a exportação ASA e a importação CUCM

O certificado que o ASA apresenta ao telefone IP durante a negociação de SSL deve ser exportado do ASA e ser importado no CUCM. Verifique o ponto confiável atribuído à relação a que os Telefones IP conectam a fim saber que certificado a exportar do ASA.

Use o comando **SSL da corrida da mostra** a fim verificar o ponto confiável (certificado) a ser exportado. Refira o telefone de AnyConnect VPN com exemplo de configuração do certificado de autenticação para mais informação.

**Note**: Se você distribuiu um certificado da terceira a uns ou vários ASA, você precisa de exportar cada certificado de identidade de cada ASA e de importá-lo então ao CUCM como a telefone-VPN-confiança.

## O ASA apresenta o certificado auto-assinado ECDSA em vez do certificado configurado RSA

Quando esta edição ocorre, os telefones de um modelo mais novo são incapazes de conectar, quando os telefones modelo mais velhos não experimentarem nenhuma edições. Seja aqui entra o telefone quando esta edição ocorre:

```
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.
```

Nas versões 9.4.1 e mais recente, a criptografia elíptico da curva é apoiada para o SSL/TLS. Quando um cliente VPN curva-capaz elíptico SSL tal como um modelo novo do telefone conecta ao ASA, a série elíptico da cifra da curva está negociada, e o ASA apresenta o cliente VPN SSL com um certificado elíptico da curva, mesmo quando a relação que corresponde é configurada com um ponto confiável RSA-baseado. A fim impedir que o ASA apresente um certificado auto-assinado SSL, o administrador deve remover as séries da cifra que correspondem através do comando da **cifra SSL**. Por exemplo, para uma relação que seja configurada com um ponto confiável RSA, o administrador pode executar este comando de modo que somente as cifras RSA-baseadas sejam negociadas:

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

Com a aplicação da identificação de bug Cisco CSCuu02848, a prioridade é dada à configuração. os Certificados Explícito-configurados são usados sempre. Os certificados auto-assinados são usados somente na ausência de um certificado configurado.

| Cifras propostas do cliente | CERT RSA somente | CERT EC somente | Ambo Certs | Nenhum |
|---|---|---|---|---|
| O RSA calcula somente | CERT dos usos RSA<br>Cifras dos usos RSA | CERT auto-assinado RSA dos usos<br>Cifras dos usos RSA | CERT dos usos RSA<br>Cifras dos usos RSA | CERT auto-assinado dos usos<br>Cifras dos usos RSA |
| O EC calcula somente (raro) | A conexão falha | CERT dos usos EC<br>Cifras dos usos EC | CERT dos usos EC<br>Cifras dos usos EC | CERT auto-assinado dos usos<br>Cifras dos usos EC |
| Ambas as cifras somente | CERT dos usos RSA<br>Cifras dos usos RSA | CERT dos usos EC<br>Cifras dos usos EC | CERT dos usos EC<br>Cifras dos usos EC | CERT auto-assinado dos usos<br>Cifras dos usos EC |

## Base de dados externo para a autenticação dos usuários de telefone IP

Você pode usar um base de dados externo a fim autenticar usuários de telefone IP. Os protocolos tais como o Lightweight Directory Access Protocol (LDAP) ou o Remote Authentication Dial In User Service (RAIO) podem ser usados para a autenticação de usuários do telefone VPN.

## Harmonia da mistura do certificado entre a lista da confiança do certificado ASA e do telefone VPN

Recorde que você deve transferir o certificado que é atribuído à relação ASA SSL e o transferir arquivos pela rede como um certificado da Telefone-VPN-confiança no CUCM. As circunstâncias diferentes puderam causar a mistura para este certificado apresentado pelo ASA para não combinar a mistura que o server CUCM gerencie e empurra para o telefone VPN através do arquivo de configuração.

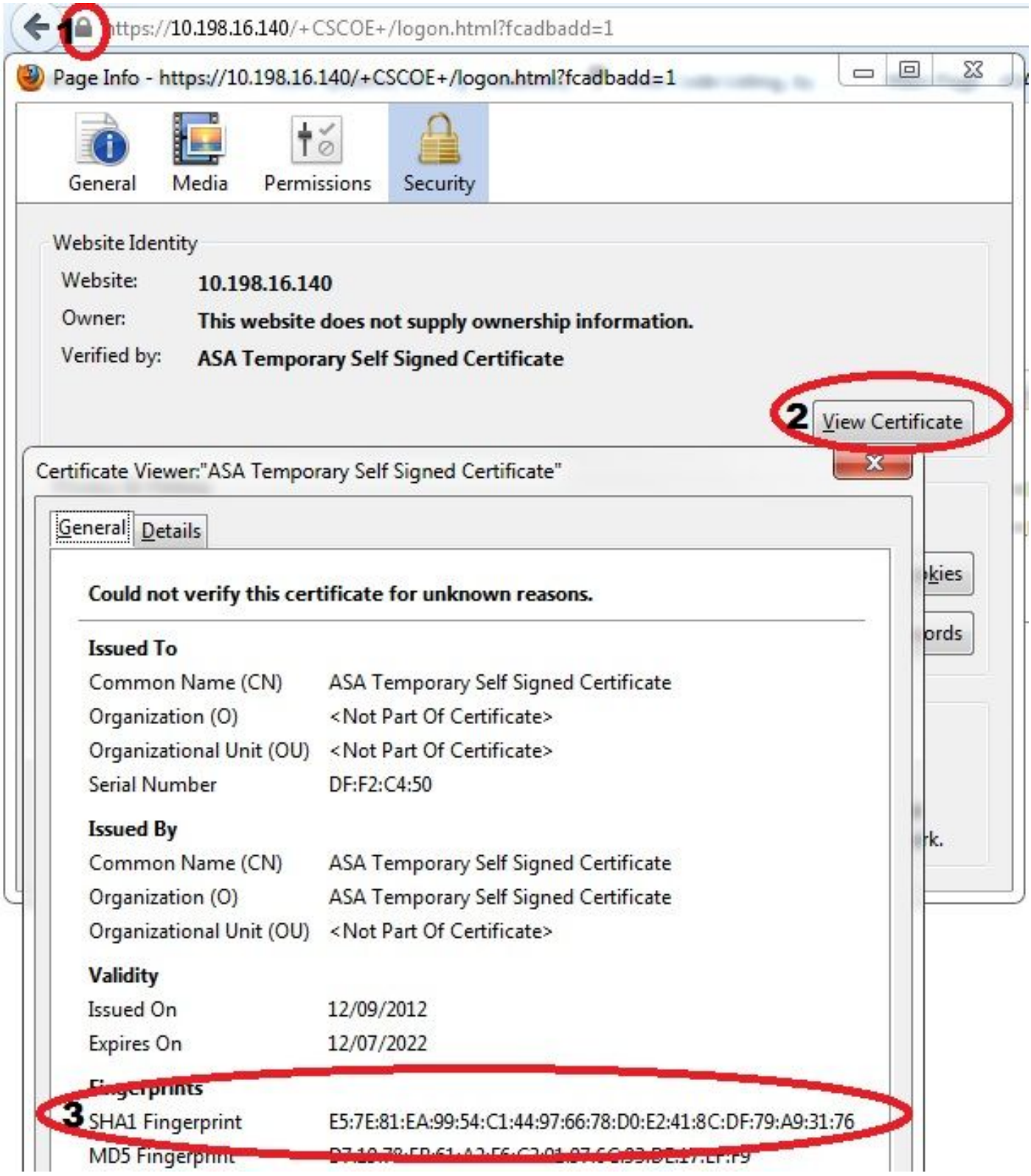
Uma vez que a configuração está completa, teste a conexão de VPN entre o telefone IP e o ASA. Se a conexão continua a falhar, para verificar se a mistura do certificado ASA combina a mistura o telefone IP está esperando:

1. Verifique a mistura do algoritmo de mistura segura 1 (SHA1) apresentada pelo ASA.
2. Use o TFTP a fim transferir o arquivo de configuração de telefone IP do CUCM.

3. Descodifique a mistura do hexadecimal para basear 64 ou da base 64 ao hexadecimal.

### Verifique a mistura SHA1

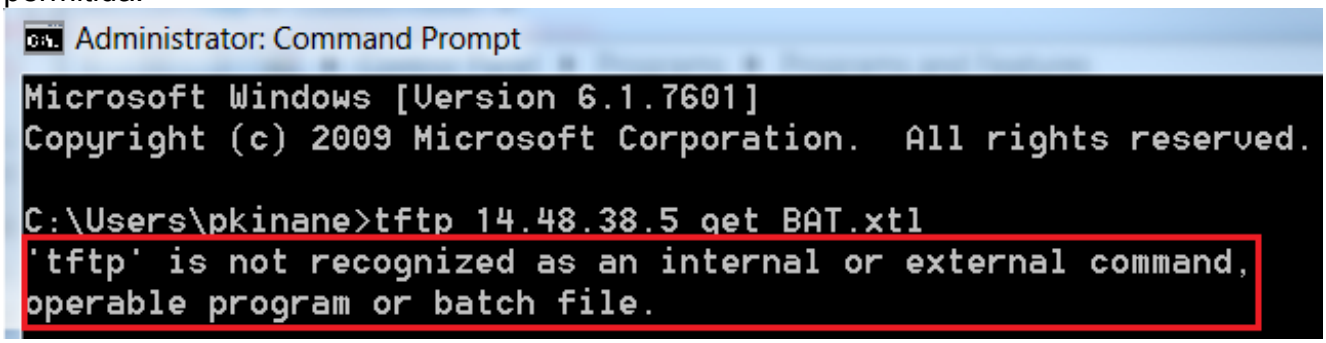
O ASA apresenta o certificado aplicado com o comando do **ponto confiável SSL na** relação a que o telefone IP conecta. Para verificar este certificado, abra o navegador (neste exemplo, Firefox), e incorpore a URL (a grupo-URL) a que os telefones devem conectar:

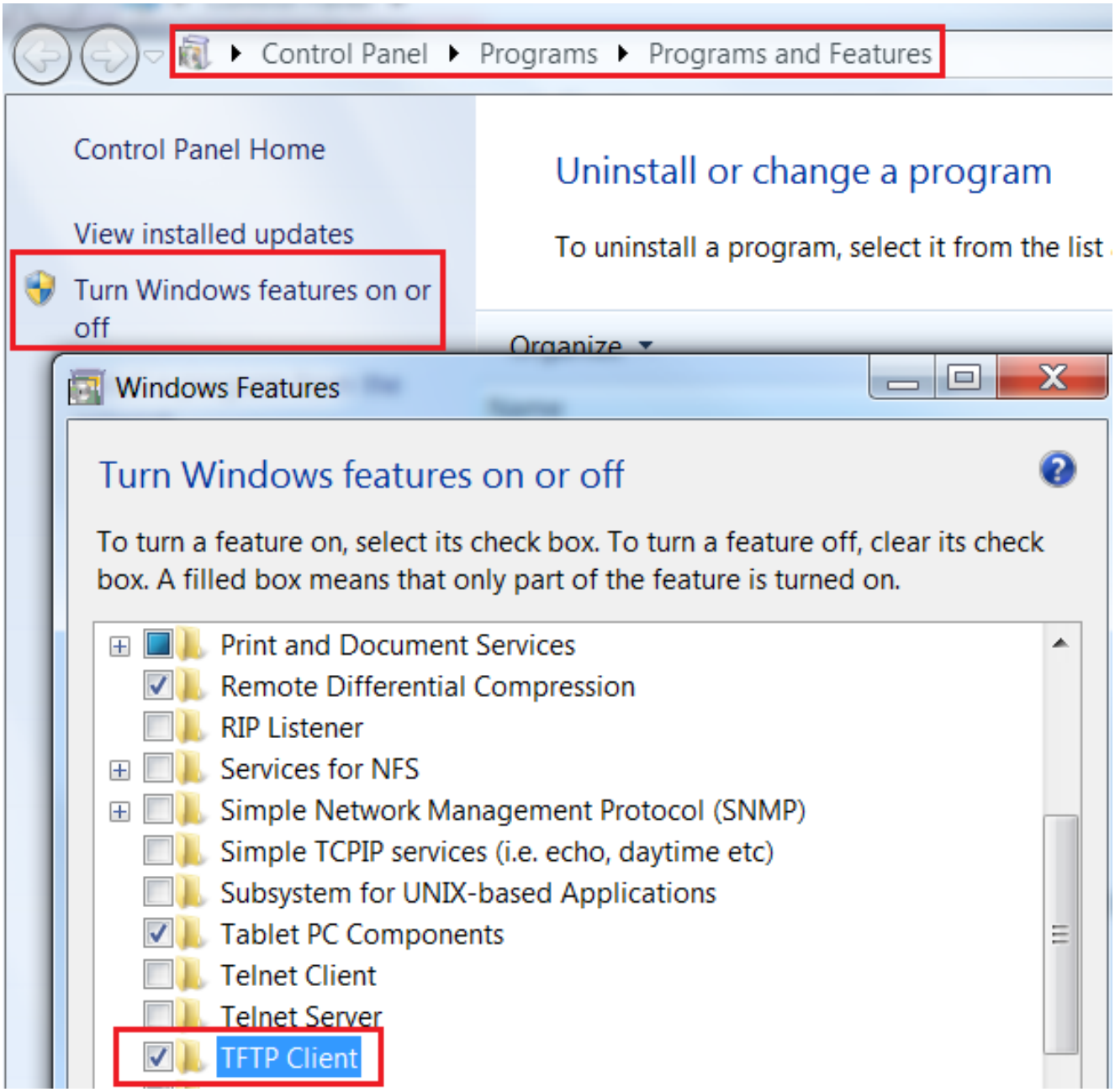



## Transfira o arquivo de configuração de telefone IP

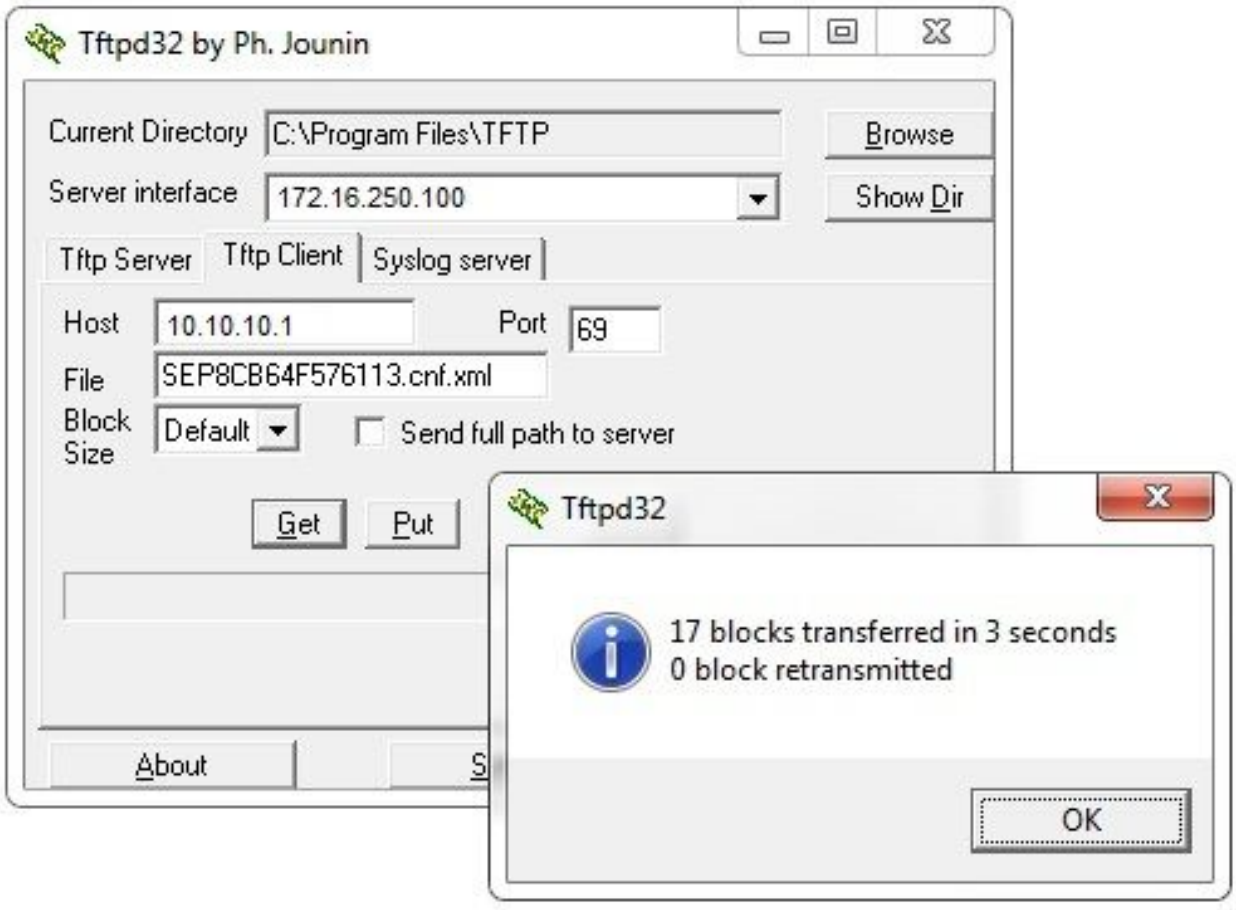
De um PC com o de acesso direto ao CUCM, transfira o arquivo de configuração TFTP para o telefone com questões de conexão. Dois métodos da transferência são:

1. Abra uma sessão CLI em Windows, e use **tftp - comando do** *MAC address >.cnf.xml do <Phone* **i** *<TFTP Server>* **GET SEP**.
   **Note**: Se você recebe um erro similar a esse abaixo, você deve confirmar que a característica do cliente de TFTP está
   permitida.




2. Use um aplicativo tal como Tftpd32 transferir o arquivo:

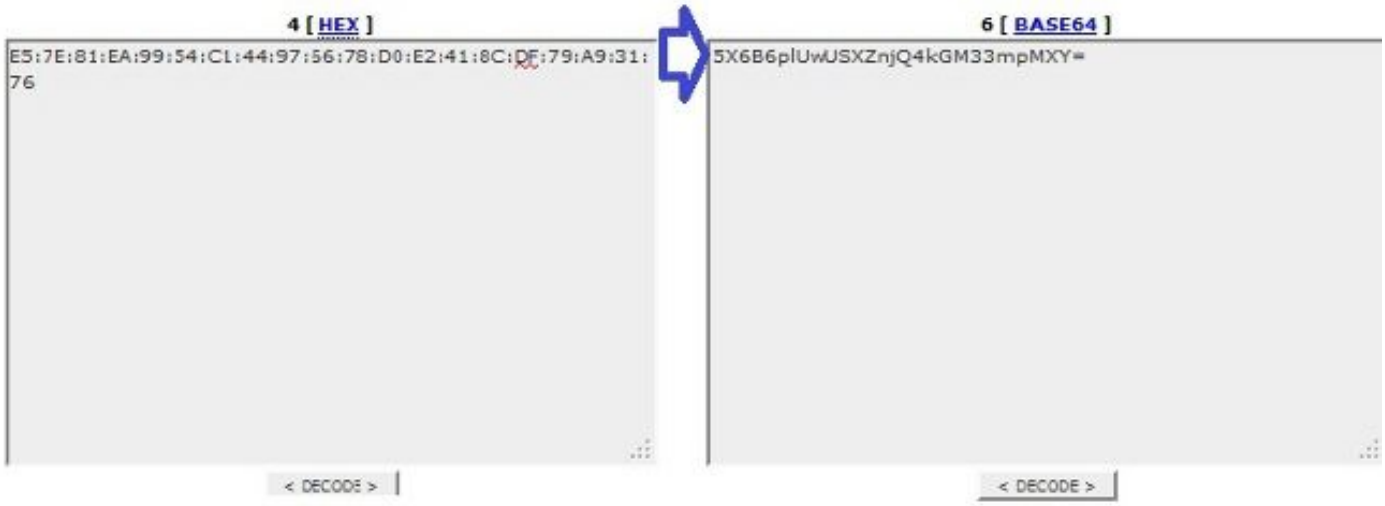



3. Uma vez o arquivo é transferido, abre o XML e encontra a configuração do *vpnGroup*. Este exemplo mostra a seção e o *certHash* a ser verificados:

```
<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>
```

### Descodifique a mistura

Confirme que ambos os valores de hash combinam. O navegador apresenta a mistura no formato hexadecimal, quando o arquivo XML usar a base 64, assim que converte um formato ao outro a fim confirmar o fósforo. Há muitos tradutores disponíveis; um exemplo é o TRADUTOR, BINÁRIO.




**Note**: Se o valor de hash precedente não combina, o telefone VPN não confia a conexão que é negociada com o ASA, e a conexão falha.

## Função de balanceamento de carga e Telefones IP VPN

A função de balanceamento de carga SSL VPN não é apoiada para telefones VPN. Os telefones VPN não executam a validação certificada real mas usar-se pelo contrário pica abaixado pelo CUCM para validar os server. Porque a função de balanceamento de carga VPN é basicamente um Redireção do HTTP, exige os telefones validar certificados múltiplos, que conduz à falha. Os sintomas da falha da função de balanceamento de carga VPN incluem:

- O telefone alterna entre server e toma excepcionalmente um muito tempo conectar ou falha eventualmente.
- Os logs do telefone contêm mensagens tais como estes:

```
<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 e Telefones IP

Atualmente, os Telefones IP não apoiam o Cisco Secure Desktop (CSD) e não o conectam quando o CSD é permitido para o grupo de túneis ou globalmente no ASA.

Primeiramente, confirme se o ASA tem o CSD permitido. Inscreva o **comando webvpn da corrida da mostra no** 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#
```

A fim verificar edições CSD durante uma conexão do telefone IP, verifique os logs ou debugar-los no ASA.

### Logs 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#
```

### O ASA debuga

```
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>
```

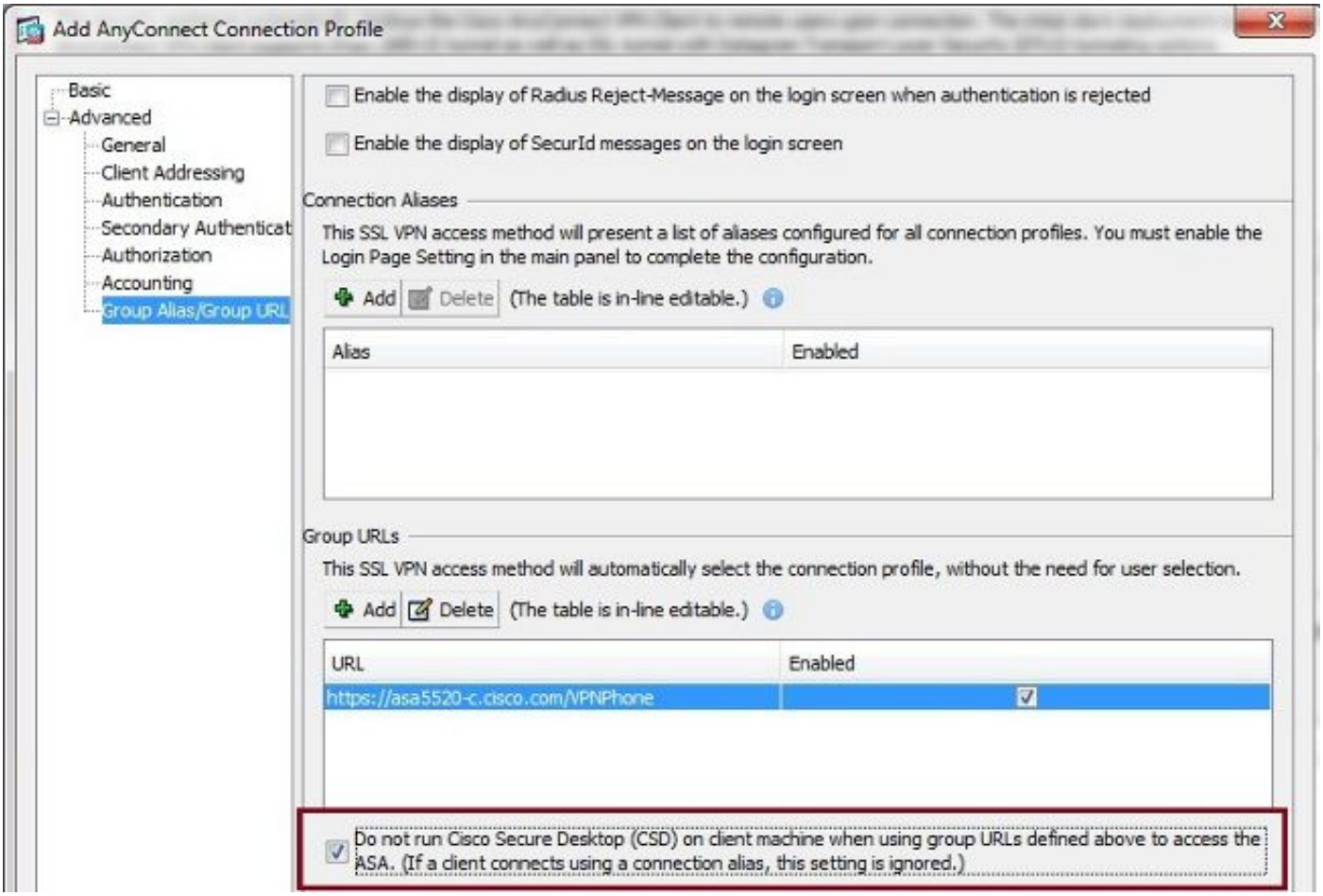
> **Note**: Em um grande desenvolvimento com uma carga elevada de usuários de AnyConnect, Cisco recomenda que você não permite **debuga o anyconnect do webvpn**. Sua saída não pode ser filtrada pelo endereço IP de Um ou Mais Servidores Cisco ICM NT, assim que uma grande quantidade de informação pôde ser criada.

Nas versões ASA 8.2 e mais atrasado, você deve aplicar o comando sem-**CSD** sob os WebVPN-atributos do grupo de túneis:

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

Nas versões anterior do ASA, isto não era possível, assim que a única ação alternativa era desabilitar globalmente o CSD.

No Cisco Adaptive Security Device Manager (ASDM), você pode desabilitar o CSD para um perfil de conexão específico segundo as indicações deste exemplo:

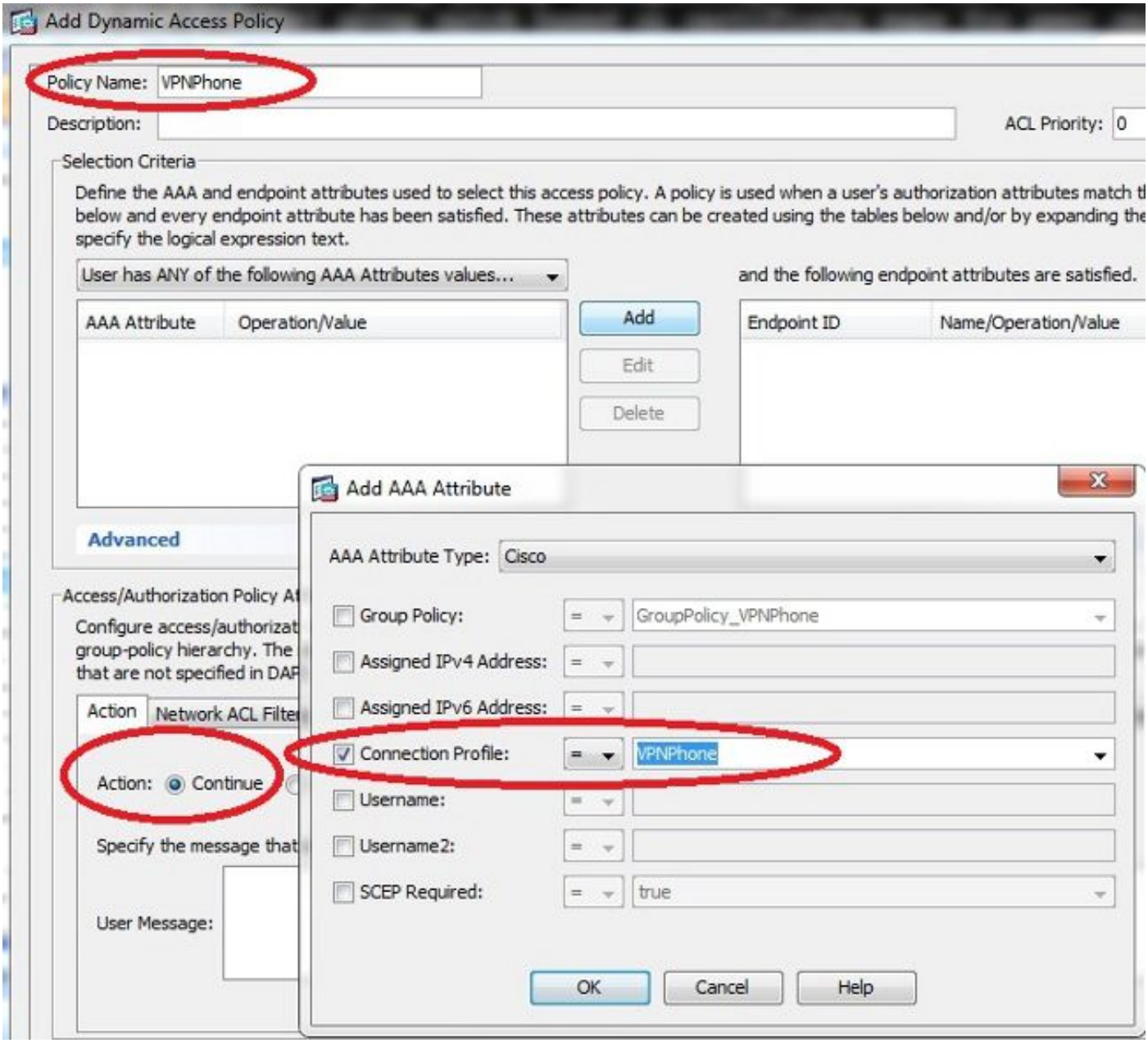



**Note**: Use uma grupo-URL a fim desligar a característica CSD.

## Regras DAP

A maioria de disposições não somente para conectar Telefones IP ao ASA mas para conectar igualmente tipos diferentes de máquinas (Microsoft, Linux, Mac OS) e de dispositivos móveis (Android, iOS). Por este motivo, é normal encontrar uma configuração existente das regras da política do acesso dinâmico (DAP), onde, na maioria das vezes, a ação padrão sob o DfltAccessPolicy é terminação da conexão.

Se este é o caso, crie uma regra separada DAP para os telefones VPN. Use um parâmetro específico, tal como o perfil de conexão, e ajuste a ação **para continuar**:




Se você não cria uma política específica DAP para Telefones IP, o ASA mostra uma batida sob o DfltAccessPolicy e uma falha na conexão:

```
%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
```

Uma vez que você cria uma política específica DAP para os Telefones IP com o grupo da ação

para continuar, você pode 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 herdados de DfltGrpPolicy ou de outros grupos

Em muitos casos, o DfltGrpPolicy estabelece-se com diversas opções. À revelia, estes ajustes estão herdados para a sessão do telefone IP a menos que forem especificados manualmente na grupo-política que o telefone IP deve usar.

Alguns parâmetros que puderam afetar a conexão se são herdados do DfltGrpPolicy são:

- grupo-fechamento
- VPN-túnel-protocolo
- VPN-simultâneo-inícios de uma sessão
- VPN-filtro

Supõe que você tem este exemplo de configuração no DfltGrpPolicy e no 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
```

A conexão herda os parâmetros do DfltGrpPolicy que não foram especificados explicitamente sob o GroupPolicy_VPNPhone e empurra toda a informação para o telefone IP durante a conexão.

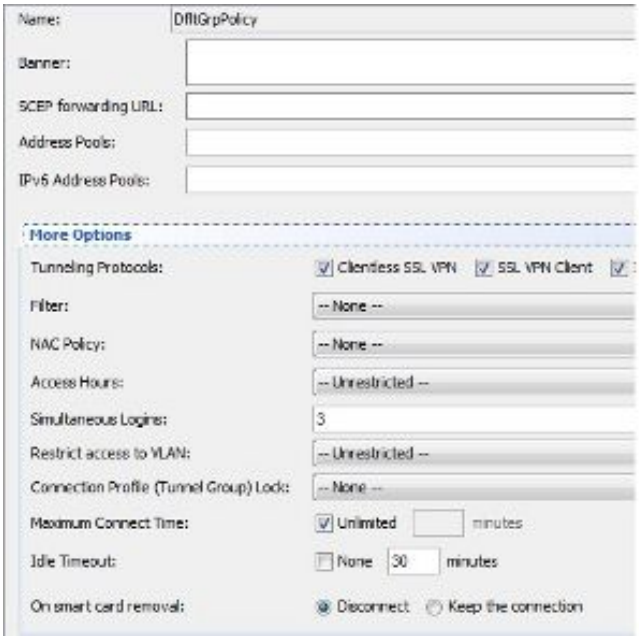
A fim evitar isto, especifique manualmente os valores que você precisa diretamente no grupo:

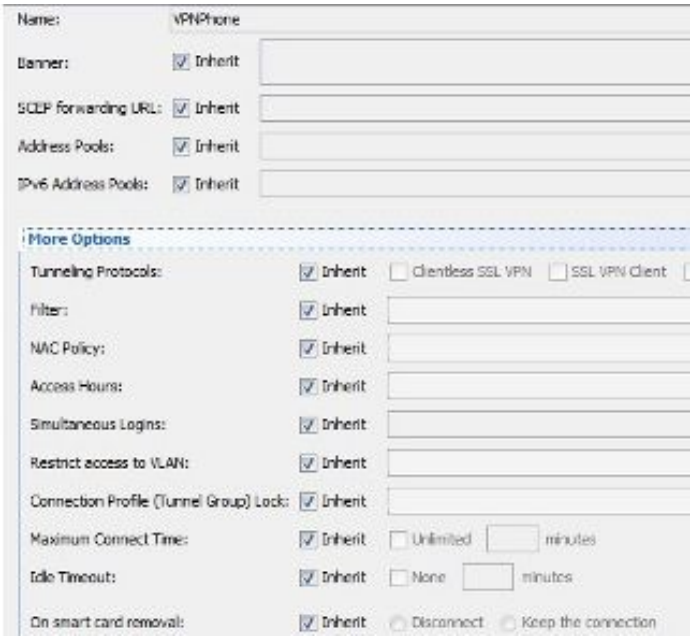
```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
 vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
 vpn-filter none
 default-domain value cisco.com
```

A fim verificar os valores padrão do DfltGrpPolicy, use a **mostra executam todo o** comando da grupo-**política**; este exemplo esclarece a diferença entre as saídas:

```
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
```

Está aqui a saída da grupo-política herda atributos com o ASDM:




## Cifras apoiadas da criptografia

Um telefone de AnyConnect VPN testado com apoios do telefone IP 7962G e da versão de firmware 9.1.1 somente duas cifras, que são ambo o Advanced Encryption Standard (AES): AES256-SHA e AES128-SHA. Se as cifras corretas não são especificadas no ASA, a conexão está rejeitada, segundo as indicações do log 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
```

A fim confirmar se o ASA tem as cifras corretas permitidas, incorpore a **mostra executam todo o SSL** e **mostram** 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
```

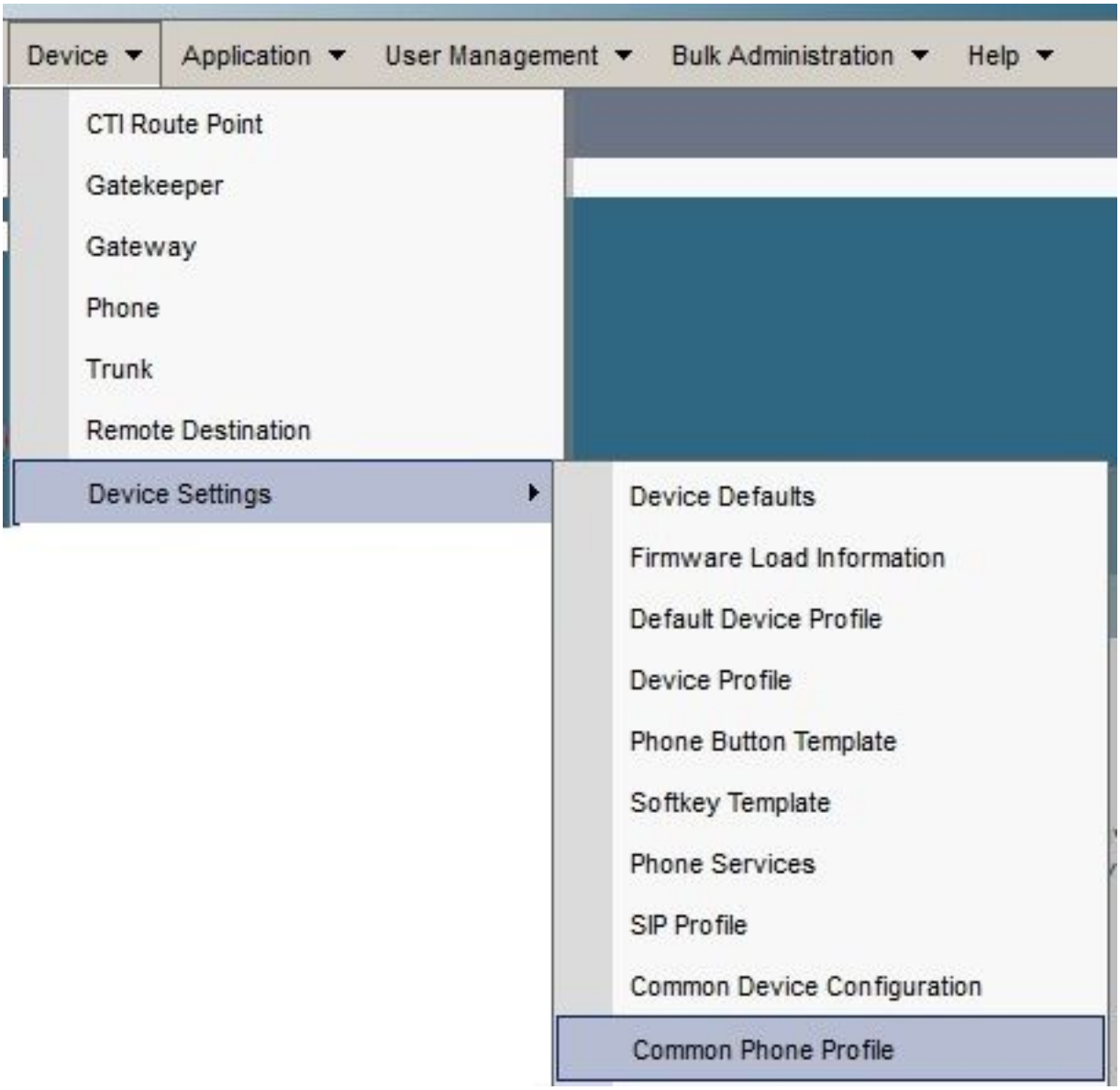
```
ASA5510-F#

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 comuns no CUCM

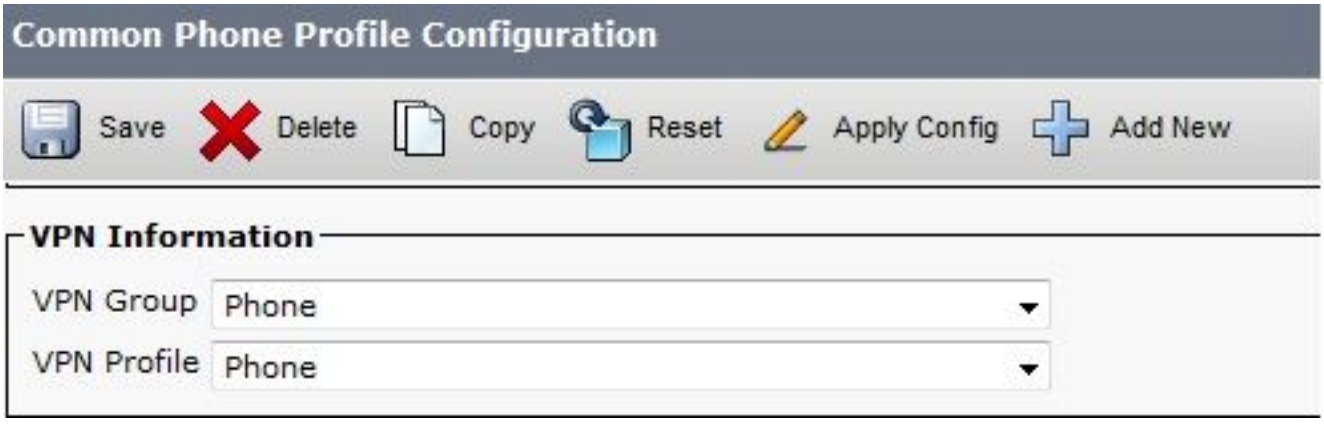
## Ajustes VPN não aplicados ao telefone IP

A configuração no CUCM é criada uma vez (gateway, grupo, e perfil), aplica os ajustes VPN no perfil comum do telefone:

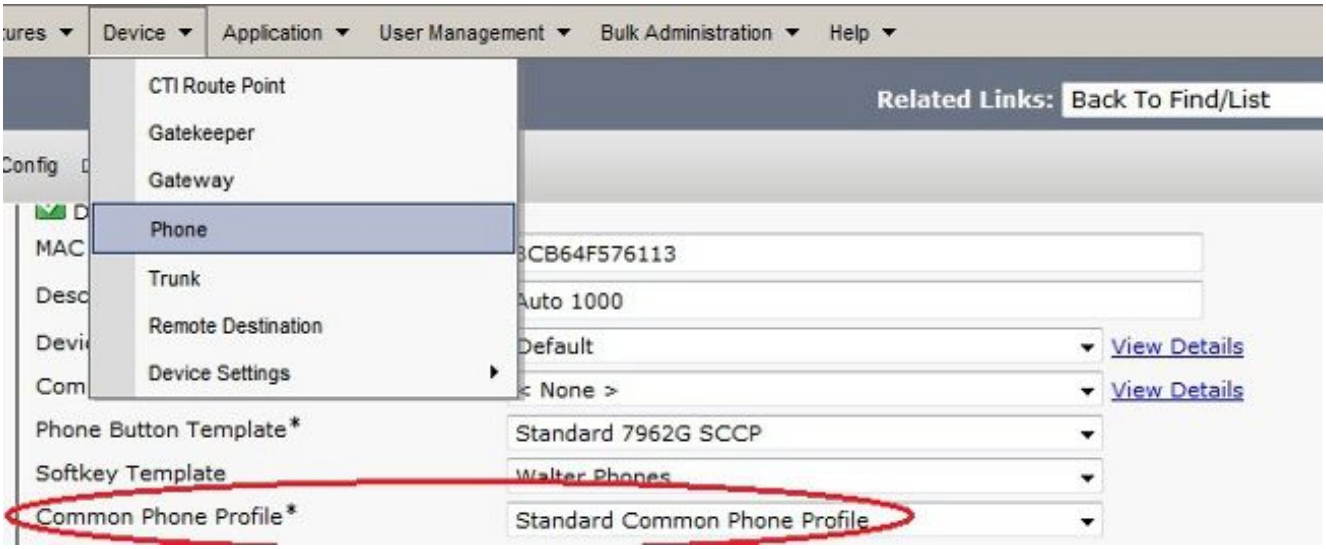
1. Navegue ao **dispositivo** > aos **ajustes do dispositivo** > **perfil comum do telefone**.




2. Incorpore a informação de VPN:




3. Navegue ao **dispositivo** > ao **telefone** e confirme este perfil é atribuído à configuração telefônica:



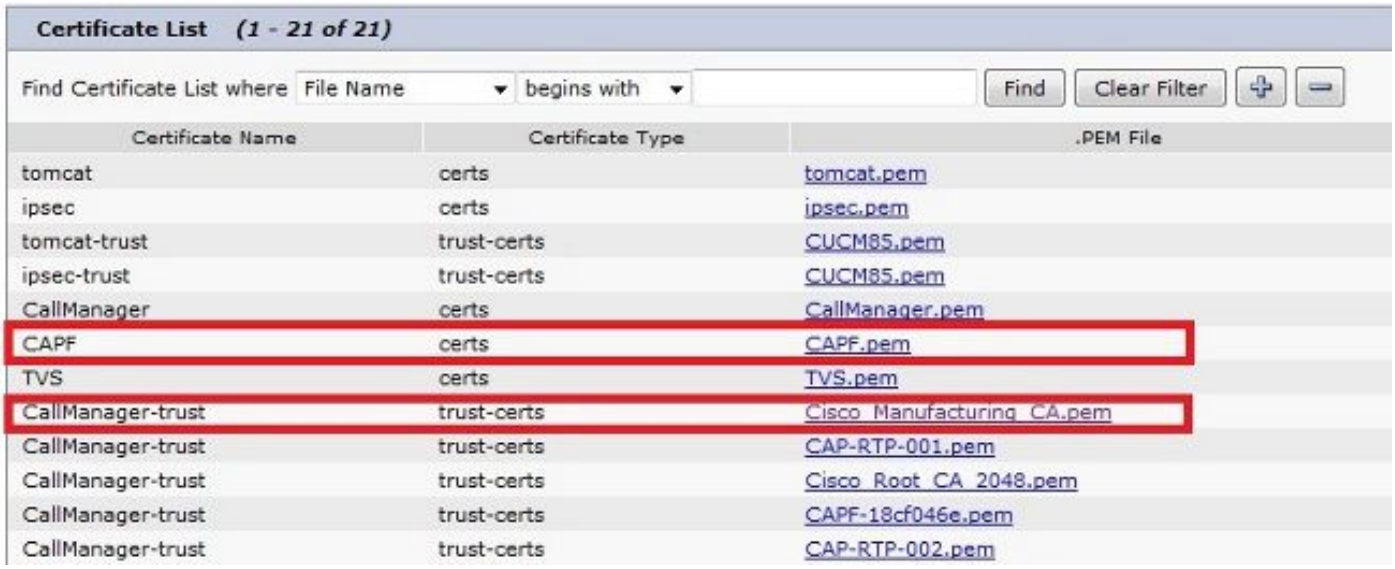

## Método de certificado de autenticação

Há duas maneiras de configurar o certificado de autenticação para Telefones IP: O fabricante instalou o certificado (MIC) e localmente - o certificado significativo (LSC). Refira o telefone de AnyConnect VPN com exemplo de configuração do certificado de autenticação a fim escolher a melhor opção para sua situação.

Quando você configura o certificado de autenticação, exporte os certificados (CA raiz) do server CUCM e importe-os ao ASA:

1. Entre ao CUCM.
2. Navegue ao **> gerenciamento de certificado unificado do > segurança da administração do OS**.
3. Encontre a função do proxy do Certificate Authority (CAPF) ou Cisco_Manufacturing_CA; o tipo de certificado depende em cima se você usou o certificado de autenticação MIC ou LSC.
4. Transfira o arquivo ao computador local.

Uma vez que os arquivos são transferidos, entre ao ASA com o CLI ou o ASDM e importe o certificado como um 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 |

Àrevelia, todos os telefones que apoiam o VPN PRE-são carregados com os MIC. Os 7960 e 7940 telefones modelo não vêm com um MIC e exigem um procedimento de instalação especial de modo que o LSC se registre firmemente.

Os Telefones IP os mais novos de Cisco (8811, 8841, 8851, e 8861) incluem os Certificados MIC que são assinados pelo SHA2 de fabricação novo CA:

- A versão 10.5(1) CUCM inclui e confia os Certificados SHA2 novos.
- Se você executa uma versão mais adiantada CUCM, você pôde ser exigido transferir o certificado de CA novo da fabricação e:

  Transfira-o arquivos pela rede à CAPF-confiança de modo que os telefones possam autenticar com CAPF a fim obter um LSC.

  Transfira-o arquivos pela rede à CallManager-confiança se você quer permitir que os telefones autentiquem com um MIC para o SORVO 5061.

**Tip**: Clique este link a fim obter o SHA2 CA se o CUCM executa atualmente uma versão anterior.

**Caution**: Cisco recomenda que você usa MIC para a instalação LSC somente. Cisco apoia LSC para a autenticação da conexão TLS com o CUCM. Porque os certificados de raiz MIC podem ser comprometidos, os clientes que configuram telefones para usar MIC para a autenticação TLS ou para toda a outra finalidade fazem tão por sua conta e risco. Cisco não supõe nenhuma responsabilidade se os MIC são comprometidos.

Àrevelia, se um LSC existe no telefone, a autenticação usa o LSC, apesar de se um MIC existe no telefone. Se um MIC e um LSC existem no telefone, a autenticação usa o LSC. Se um LSC não existe no telefone, mas um MIC existe, a autenticação usa o MIC.

> **Note**: Recorde que, para o certificado de autenticação, você deve exportar o certificado SSL do ASA e o importar ao CUCM.

## Verificação do ID do host

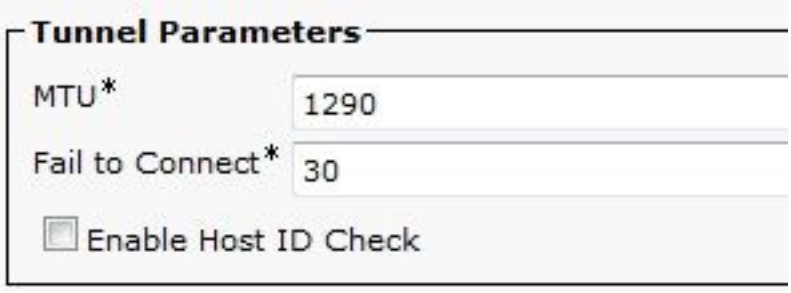
Se o Common Name (CN) no assunto do certificado não combina a URL (grupo-URL) que os telefones se usam a fim conectar ao ASA com o VPN, se desabilitam a verificação do ID do host nos CUCM ou use um certificado no ASA que fósforo essa URL no ASA.

Isto é necessário quando o certificado SSL do ASA é um certificado do convite, o certificado SSL contém um SAN diferente (nome alternativo sujeito), ou a URL foi criada com o endereço IP de Um ou Mais Servidores Cisco ICM NT em vez do nome de domínio totalmente qualificado (FQDN).

Este é um exemplo de um log do telefone IP quando o CN do certificado não combina a URL que o telefone está tentando alcançar.

```
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!!
```

A fim desabilitar o ID do host verifique dentro o CUCM, navegam aos **recursos avançados** > ao **perfil VPN** > **VPN**:




# Troubleshooting Adicional

## Os logs e debugam para usar-se no ASA

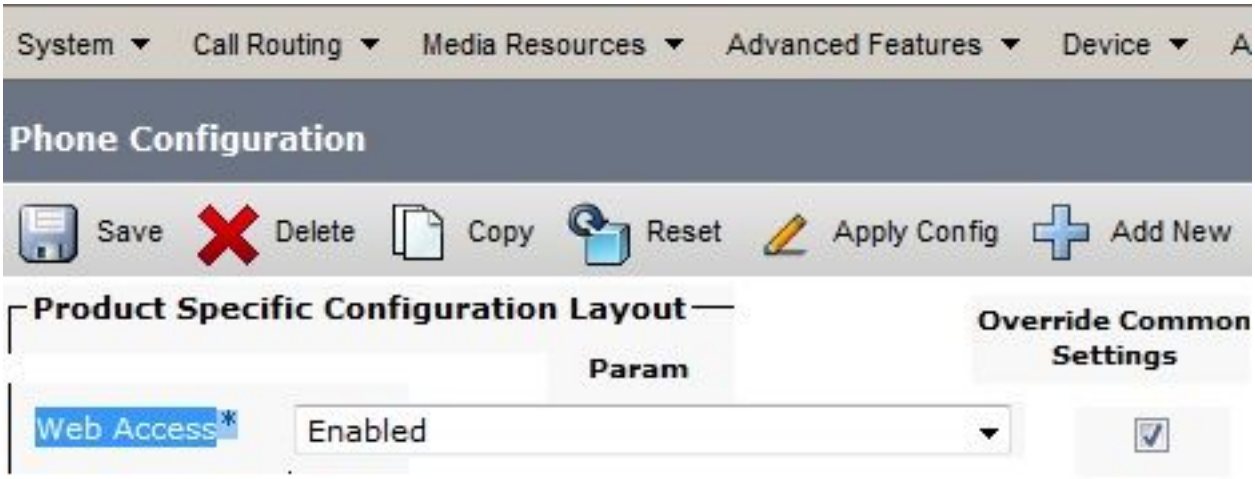
No ASA, você pode permitir estes debuga e logs para pesquisar defeitos:

```
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!!
```

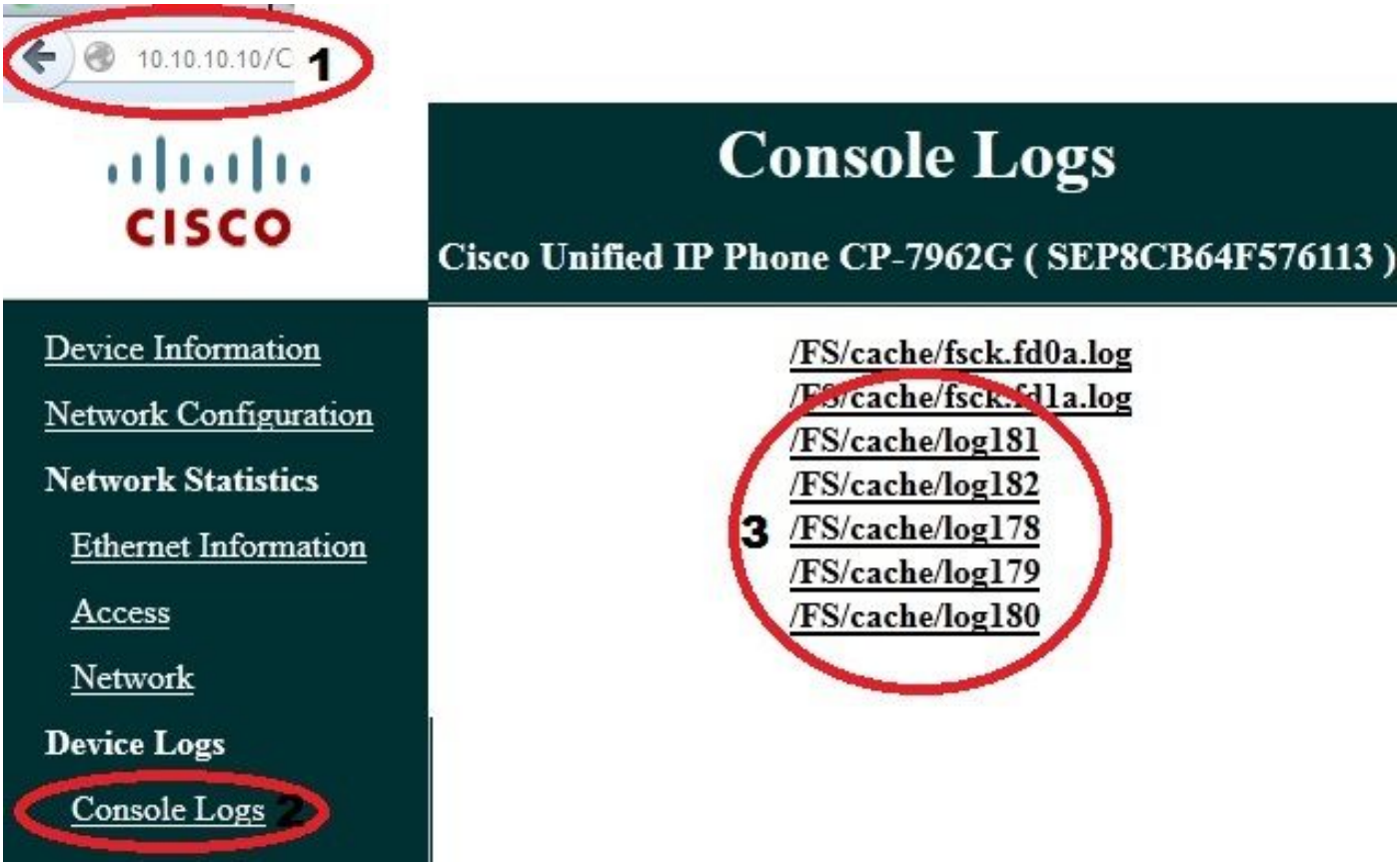
> **Note**: Em um grande desenvolvimento com uma carga elevada de usuários de AnyConnect, Cisco recomenda que você não permite o **anyconnect do webvpnh debugar**. Sua saída não pode ser filtrada pelo endereço IP de Um ou Mais Servidores Cisco ICM NT, assim que uma grande quantidade de informação pôde ser criada.

## Logs do telefone IP

A fim alcançar os logs do telefone, permita a característica do acesso à Web. Entre ao CUCM, e navegue ao **dispositivo** > ao **telefone** > à **configuração telefônica**. Encontre o telefone IP em que você quer permitir esta característica, e encontre a seção para o acesso à Web. Aplique as alterações de configuração ao telefone IP:




Uma vez que você permite o serviço e restaura o telefone a fim injetar estes novos recursos, você pode alcançar o telefone IP entra o navegador; use o endereço IP de Um ou Mais Servidores Cisco ICM NT do telefone de um computador com acesso a essa sub-rede. Vá aos logs do console e verifique os cinco arquivos de registro. Porque o telefone overwrites os cinco arquivos, você deve verificar todos estes arquivos em ordem encontra a informação que você procura.




## Edições correlacionadas entre logs ASA e logs do telefone IP

Este é um exemplo de como correlacionar os logs do ASA e do telefone IP. Neste exemplo, a mistura do certificado no ASA não combina a mistura do certificado no arquivo de configuração do telefone porque o certificado no ASA foi substituído com um certificado diferente.

## Logs 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
```

## Logs do telefone

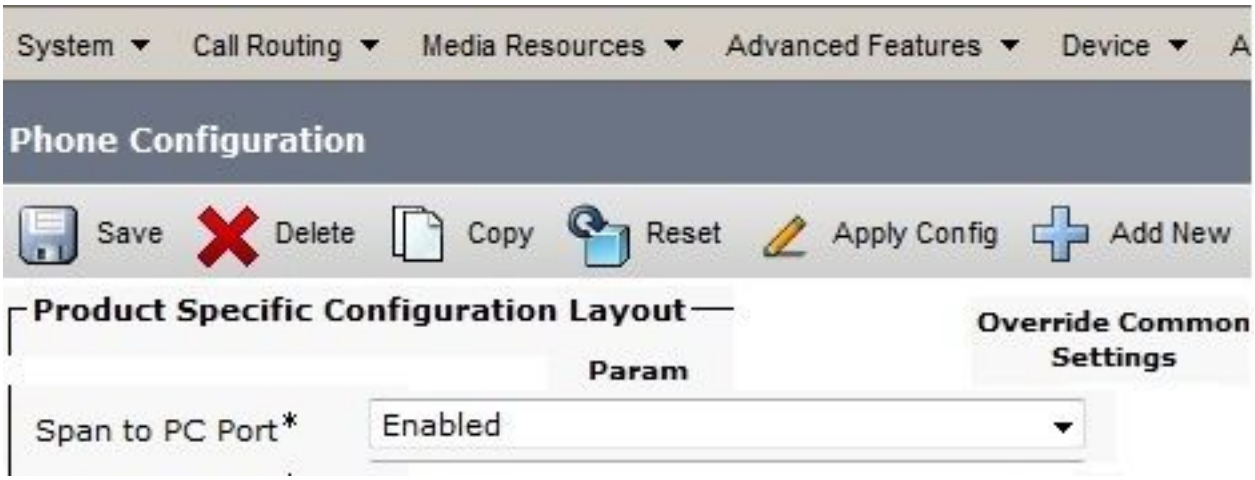
```
 902: NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect
initialization
903: NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state
904: NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A
905: NOT 10:19:27.364687 VPNC: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

## Período à característica da porta de PC

Você pode conectar um computador diretamente a um telefone. O telefone tem uma porta de switch no back plane.

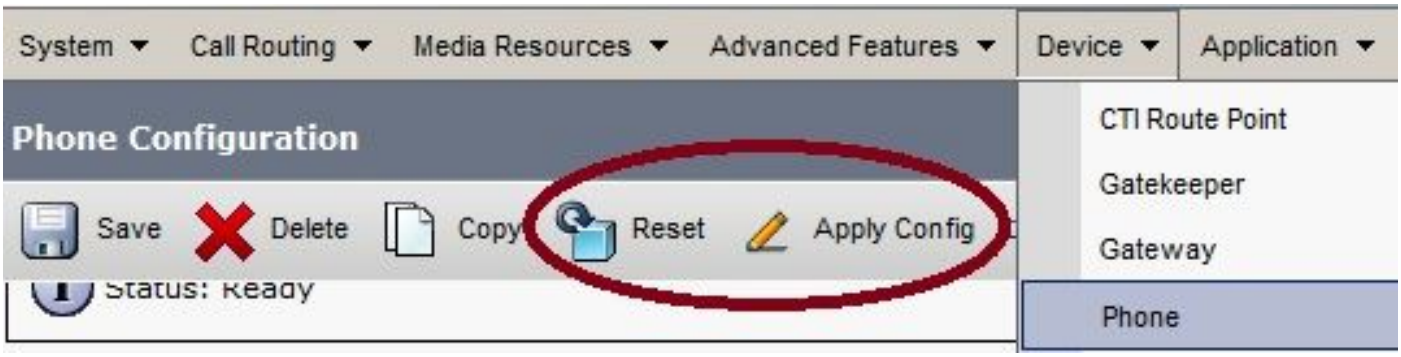
Configurar o telefone como você fez previamente, para permitir o período à porta de PC no CUCM, e para aplicar a configuração. O telefone começa a enviar uma cópia de cada quadro ao PC. Use Wireshark no modo misturado a fim capturar o tráfego para a análise.




## Mudanças de configuração de telefone IP quando conectado pelo VPN

Uma pergunta comum é se você pode alterar a configuração de VPN quando o telefone IP for conectado fora da rede por AnyConnect. A resposta é sim, mas você deve confirmar alguns ajustes de configuração.

Faça as alterações necessárias no CUCM, a seguir aplique as mudanças ao telefone. Há três opções (aplique a configuração, restauram, reinício) para empurrar a configuração nova para o telefone. Embora todas as três opções desliguem o VPN do telefone e do ASA, você pode reconectar automaticamente se você está usando o certificado de autenticação; se você está usando o Authentication, Authorization, and Accounting (AAA), você é alertado para suas credenciais outra vez.




**Note**: Quando o telefone IP está no lado remoto, recebe normalmente um endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor de DHCP externo. Para que o telefone IP receba a configuração nova do CUCM, deve contactar o servidor TFTP no escritório principal. Normalmente o CUCM é o mesmo servidor TFTP.

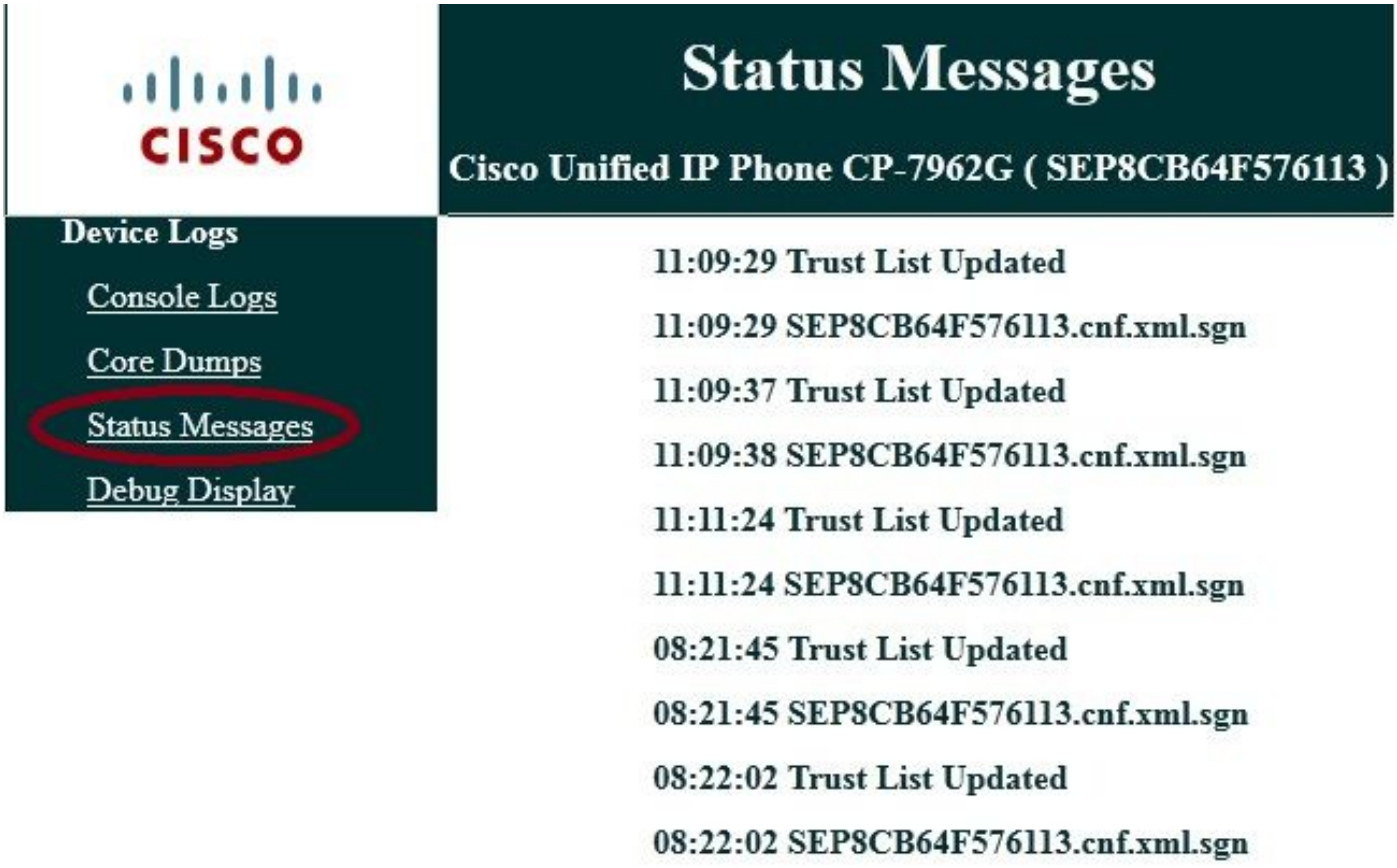
A fim receber os arquivos de configuração com as mudanças, confirme que o endereço IP de Um ou Mais Servidores Cisco ICM NT para o servidor TFTP se estabelece corretamente nas configurações de rede no telefone; para a confirmação, use a opção 150 do servidor DHCP ou ajuste manualmente o TFTP no telefone. Este servidor TFTP é acessível com uma sessão de AnyConnect.

Se o telefone IP está recebendo o servidor TFTP de um servidor DHCP local mas esse endereço está incorreto, você pode usar a opção alternativa do servidor TFTP a fim cancelar o endereço IP do servidor de TFTP fornecido pelo servidor DHCP. Este procedimento descreve como aplicar o servidor TFTP alternativo:

1. Navegue aos **ajustes** > à **configuração de rede** > à **configuração do IPv4**.
2. Rolo à opção TFTP alternativa.
3. Pressione a chave macia do Yes para que o telefone use um servidor TFTP alternativo; se não, não pressione nenhuma chave macia. Se a opção é travada, pressione * * # a fim destravá-la.
4. Pressione a tecla de software **Save**.
5. Aplique o servidor TFTP alternativo sob a opção do servidor TFTP 1.

Reveja os mensagens de status no navegador da Web ou nos menus do telefone diretamente a fim confirmar que o telefone está recebendo a informação correta. Se a comunicação se

estabelece corretamente, você vê mensagens tais como estes:




Se o telefone é incapaz de recuperar a informação do servidor TFTP, você recebe mensagens de erro de TFTP:


## Renovação do certificado ASA SSL

Se você tem um telefone funcional de AnyConnect VPN setup mas seu certificado ASA SSL está a ponto de expirar, você não precisa de trazer todos os Telefones IP ao local principal a fim injetar os Certificados novos SSL ao telefone; você pode adicionar os Certificados novos quando o VPN for conectado.

Se você exportou ou importou o certificado CA raiz do ASA em vez do certificado de identidade e se você quer continuar a usar o mesmo vendedor (CA) durante esta renovação, não é necessário mudar o certificado no CUCM porque permanece o mesmo. Mas, se você usou o certificado de identidade, este procedimento é necessário; se não, o valor de hash entre o ASA e o telefone IP não combina, e a conexão não é confiada pelo telefone.

1. Renove o certificado no ASA.
   **Note**: Para detalhes, refira ASA 8.x: Renove e instale o certificado SSL com ASDM. Crie um

ponto confiável separado e não aplique este certificado novo com o **<name> do ponto confiável SSL fora do** comando até que você aplique o certificado a todos os Telefones IP VPN.

2. Exporte o certificado novo.

3. Importe o certificado novo ao CUCM como o certificado da Telefone-VPN-confiança.
   **Note**: Esteja ciente dos **certs** CSCuh19734 **transferindo arquivos pela rede com o mesmo CN overwrite o CERT velho na Telefone-VPN-confiança**
4. Navegue à configuração de gateway de VPN no CUCM, e aplique o certificado novo. Você tem agora ambos os Certificados: o certificado que está a ponto de expirar e o certificado novo que não foi aplicado ao ASA ainda.

5. Aplique esta configuração nova ao telefone IP. Navegue **para aplicar a configuração > restaurado > reinício** a fim injetar as alterações de configuração novas ao telefone IP através do túnel VPN. Assegure-se de que todos os Telefones IP estejam conectados com o VPN e que podem alcançar o servidor TFTP através do túnel.

6. Use o TFTP para verificar os mensagens de status e o arquivo de configuração a fim confirmar que o telefone IP recebeu o arquivo de configuração com as mudanças.

7. Aplique o ponto confiável novo SSL no ASA, e substitua o certificado velho.

**Note**: Se o certificado ASA SSL é expirado já e se os Telefones IP são incapazes de conectar com AnyConnect; você pode empurrar as mudanças (tais como a mistura nova do certificado ASA) ao telefone IP. Ajuste manualmente o TFTP no telefone IP a um endereço IP público assim que o telefone IP pode recuperar a informação de lá. Use um servidor TFTP público para hospedar o arquivo de configuração; um exemplo é criar uma transmissão da porta no ASA e reorientar o tráfego ao servidor TFTP interno.