排除AnyConnect VPN电话故障- IP电话、ASA和CUCM

Contents

Introduction

使用安全套接字协议层(SSL)协议的本文描述如何用IP电话排除问题故障(Cisco AnyConnect安全移动客户端)为了连接到使用的Cisco可适应的安全工具(ASA)， VPN网关和为了联络到Cisco Unified通信使用作为语音服务器的管理器(CUCM)。

关于AnyConnect配置示例用VPN电话，请参见这些文件：

- 与IP电话配置示例的SSLVPN
- 有证书验证配置示例的AnyConnect VPN电话

背景信息

在您配置与IP电话前的SSL VPN，请确认您符合了AnyConnect许可证的这些最初的要求的ASA和的CUCM的美国导出被限制的版本。

确认VPN在ASA的电话许可证

VPN电话许可证enable (event)在ASA的功能。为了确认能连接AnyConnect用户的数量(它是否是IP电话)，请检查AnyConnect优质SSL许可证。参考什么ASA许可证为IP电话和便携VPN连接是需要的？以获取更多详细信息。

在ASA，请使用**show version命令**为了检查功能是否是启用的。许可证名字有所不同与ASA版本：

- ASA版本8.0.x ：许可证名字是Linksys电话的AnyConnect。
- ASA版本8.2.x和以后：许可证名字是Cisco VPN电话的AnyConnect。

这是ASA版本的8.0.x一个示例：

```
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.
```

这是ASA版本的8.2.x一个示例和以后：

```
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.
```

被限制的导出和导出无限制的CUCM

您应该配置CUCM的美国导出被限制的版本VPN电话功能的。

如果使用CUCM的美国导出无限制的版本，请注释那：

- 修改IP电话安全配置为了禁用信令和媒体加密;这包括VPN电话功能提供的加密。
- 您不能通过导入/导出导出VPN详细资料。
- VPN配置文件、VPN网关、VPN组和VPN功能的复选框配置没有显示。

> **Note**:一旦升级到CUCM的美国导出无限制的版本，您不能以后升级对，或者请执行一个新安装，此软件的美国导出被限制的版本。

在ASA的常见问题

Note:您能使用Cisco CLI分析器(仅限注册用户)为了查看show命令输出分析。在您使用调试指令前，您应该也是指关于调试Cisco命令文件的重要信息。

证书为在ASA的使用

在ASA，您能使用自己签署的SSL证书、第三方SSL证书和通配符证书;中的任一这些安全IP电话和ASA之间的通信。

仅一个身份认证，因为仅一个认证可以分配到每个接口，可以使用。

对于第三方SSL证书，在ASA上请安装完全一系列，并且包括所有中间和根证明。

信任点/ASA导出和CUCM导入的认证

ASA提交到IP电话在SSL协商时的认证必须从ASA导出和导入到CUCM。检查信任点分配到IP电话连接为了知道的接口导出的哪个认证从ASA。

请使用**show run ssl**命令为了验证(认证)将被导出的信任点。参考有证书验证配置示例的AnyConnect VPN电话欲知更多信息。

Note:如果配置了一个第三方认证对一个或更多ASA，您需要从每个ASA导出每个身份认证然后导入它CUCM作为电话VPN信任。

ASA而不是被配置的RSA认证的存在ECDSA自签证书

当此问题出现时，新模型电话无法接通，而更旧的式样电话不遇到任何问题。这，当此问题出现时，请是注册电话：

```
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.
```

在版本9.4.1和以上，椭圆曲线密码学为SSL/TLS支持。当一椭圆曲线能够SSL VPN客户端例如一个新的电话型号连接到ASA时，椭圆曲线密码套件协商，并且ASA提交与一个椭圆曲线认证的SSL VPN客户端，既使当对应的接口配置有一基于RSA的信任点。为了防止ASA提交一个自己签署的SSL认证，管理员必须去除通过**ssl密码**命令对应的密码套件。例如，为配置有RSA信任点的接口，管理员能执行此命令，以便仅基于RSA的密码协商：

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

使用Cisco Bug ID CSCuu02848的实施，优先级制定配置。总是使用明确配置的证书。自署名的认证在没有一个被配置的认证时只使用。

提出的客户端密码	RSA仅Cert	EC仅Cert	两Certs	无
RSA只加密	使用RSA cert 使用RSA密码	使用RSA自己签署的cert 使用RSA密码	使用RSA cert 使用RSA密码	使用RSA自己签署的cert 使用RSA密码
EC只加密(少见)	连接发生故障	使用EC cert 使用EC密码	使用EC cert 使用EC密码	使用EC自己签署的cert 使用EC密码
仅两个密码	使用RSA cert 使用RSA密码	使用EC cert 使用EC密码	使用EC cert 使用EC密码	使用EC自己签署的cert 使用EC密码

IP电话用户的认证的外部数据库

您能使用外部数据库为了验证IP电话用户。协议例如轻量级目录访问协议(LDAP)或远程认证拨入用户服务(RADIUS)可以用于VPN电话用户的认证。

认证在ASA认证和VPN电话信任列表之间的哈希匹配

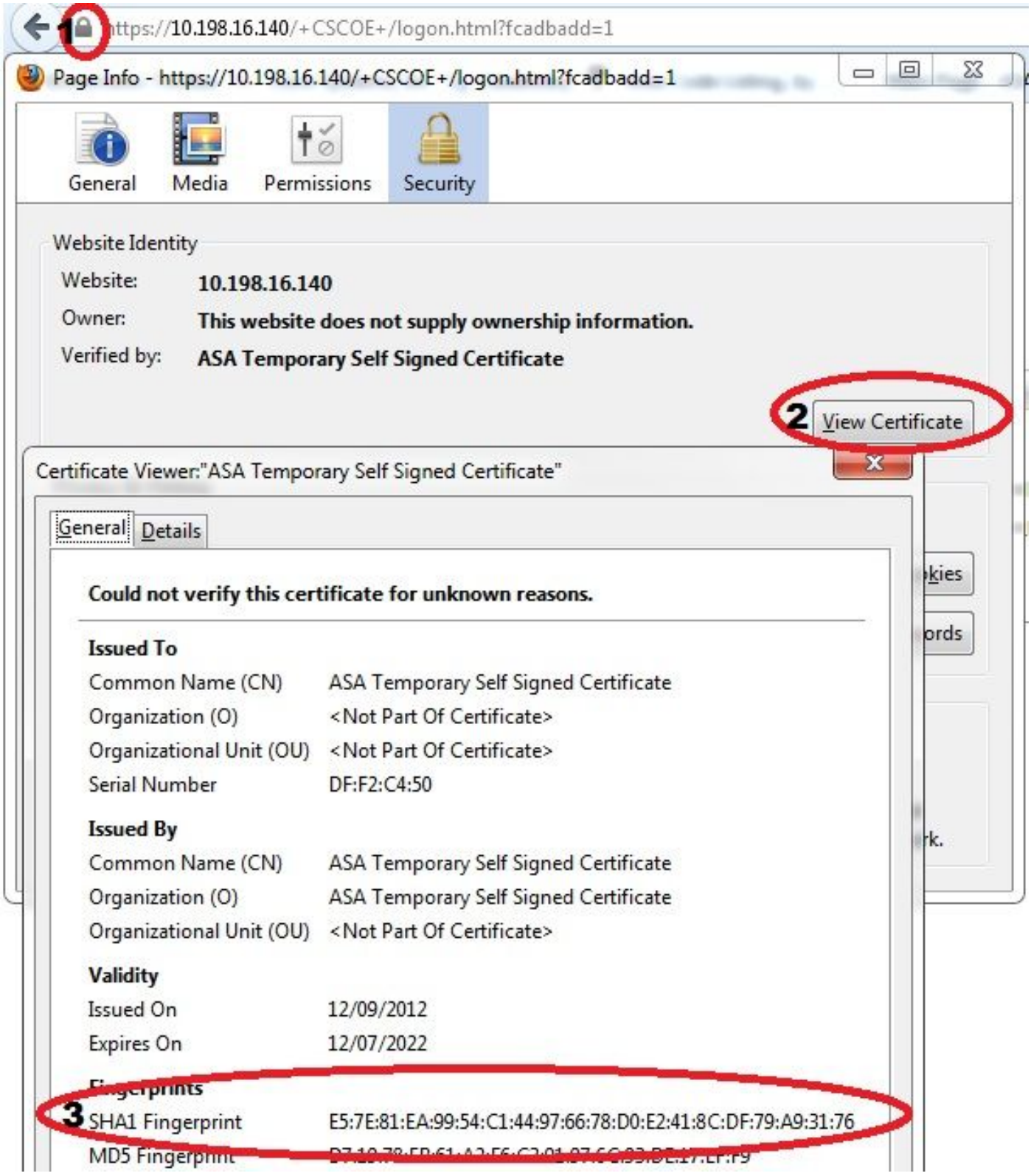
切记您必须下载分配到ASA SSL接口的认证和加载它作为在CUCM的电话VPN信任认证。不同的情况也许导致ASA提交的此认证的哈希不匹配CUCM服务器生成并且穿过对VPN电话配置文件的哈希。

一旦配置完成，请测试IP电话和ASA之间的VPN连接。如果连接继续发生故障，检查ASA认证的哈希是否匹配哈希IP电话预计：

1. 检查ASA提交的安全散列算法1 (SHA1)哈希。
2. 请使用TFTP为了从CUCM下载IP电话配置文件。
3. 解码哈希从十六进制到base64或从base64到十六进制。

检查SHA1哈希

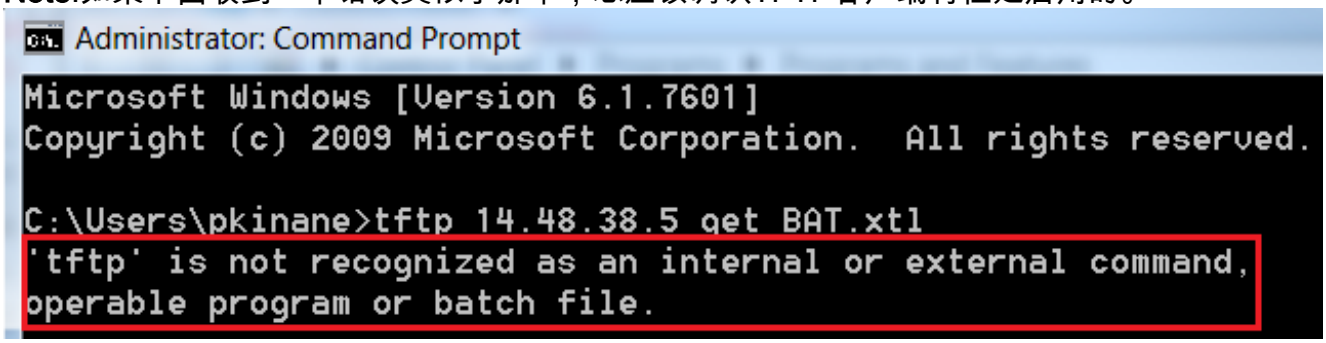
ASA提交认证应用与**ssl信任点**on命令IP电话接通的接口。要检查此认证，请打开浏览器(在本例中，Firefox)，并且输入(组URL)电话应该接通的URL ：

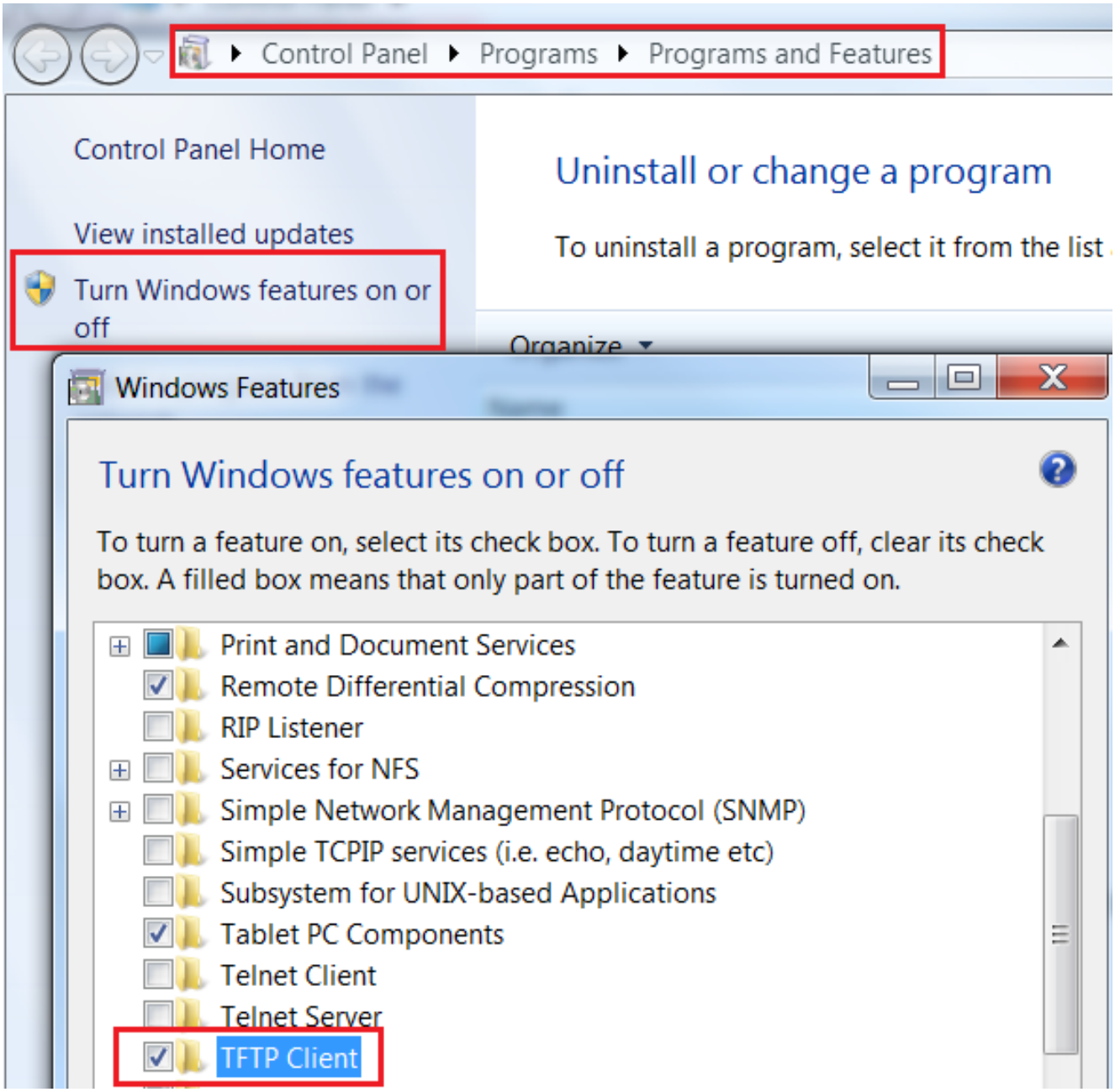


下载IP电话配置文件

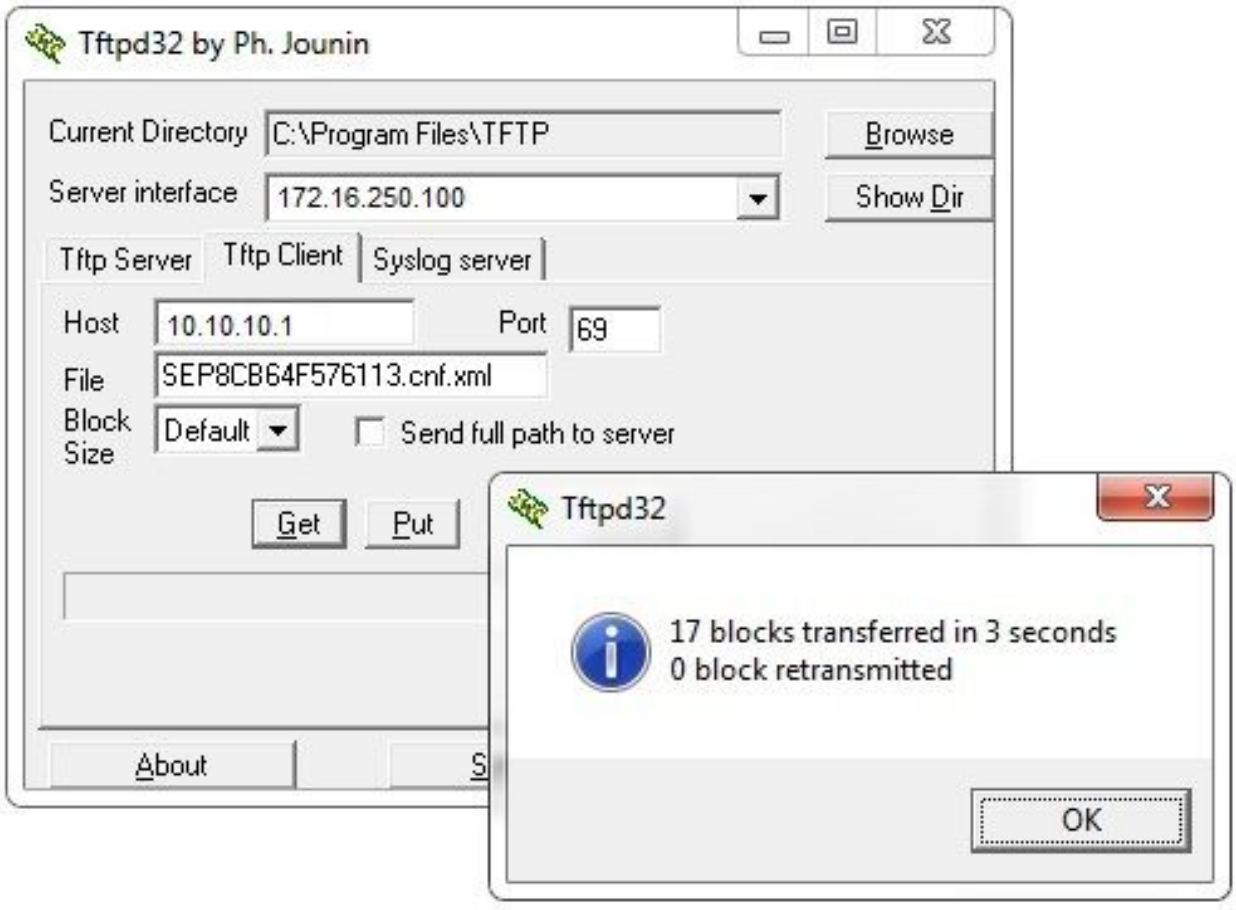
从有直接访问的PC对CUCM，请下载电话的TFTP配置文件有连接问题的。两个下载方法是：

1. 开始在Windows的一次CLI会话，并且请使用**tftp - i** *<TFTP Server>* **GET SEP** *<Phone MAC地址>.cnf.xml***命令**。
   Note:如果下面收到一个错误类似于那个，您应该确认TFTP客户端特性是启用的。





2. 请使用一个应用程序例如Tftpd32下载文件：

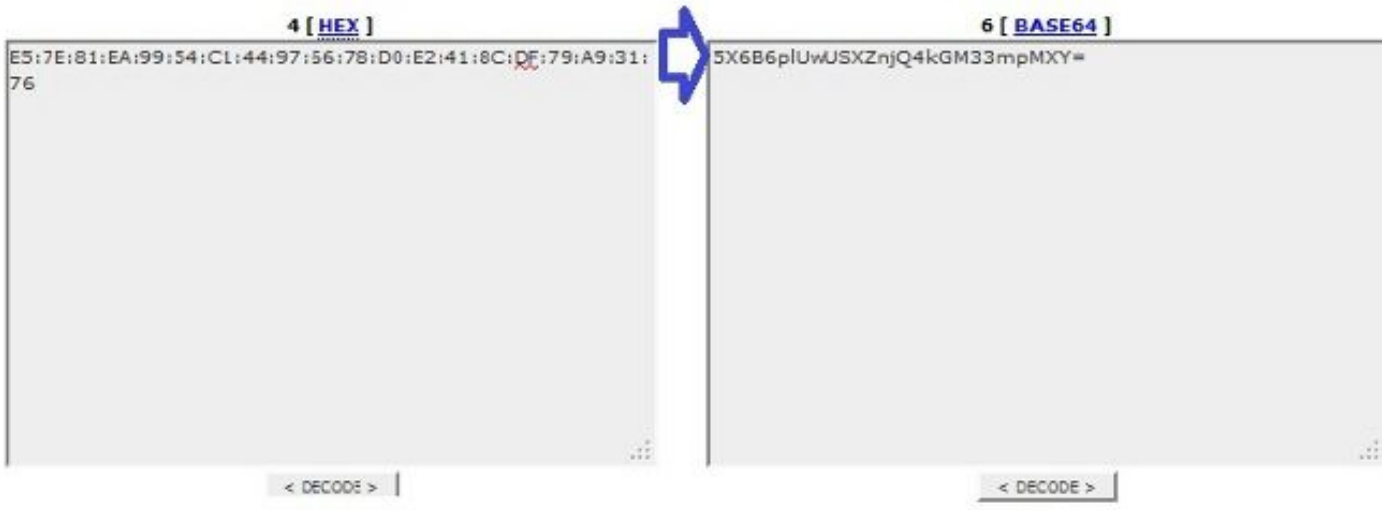


3. 一旦下载文件，请打开XML并且查找*vpngroup*配置。此示例显示将被验证的部分和*certHash*：

```
<vpnGroup>
<mtu>1290</mtu>
<failConnectTime>30</failConnectTime>
<authMethod>2</authMethod>
<pswdPersistent>0</pswdPersistent>
<autoNetDetect>0</autoNetDetect>
<enableHostIDCheck>0</enableHostIDCheck>
<addresses>
<url1>https://10.198.16.140/VPNPhone</url1>
</addresses>
<credentials>
<hashAlg>0</hashAlg>
<certHash1>5X6B6plUwUSXZnjQ4kGM33mpMXY=</certHash1>
</credentials>
</vpnGroup>
```

解码哈希

确认两个Hash值配比。浏览器提交哈希以十六进制格式，而XML文件使用base64，因此转换一种格式成其他为了确认匹配。有可用许多的译码器;一个示例是[译码器，二进制](#)。



Note:如果早先Hash值不配比， VPN电话不委托与ASA协商的连接，并且连接发生故障。

VPN负荷-平衡和IP电话

负载均衡的SSL VPN不为VPN电话支持。VPN电话不执行实际证书确认，反而使用切细增加由CUCM验证服务器。由于VPN负载平衡基本上是HTTP重定向，要求电话验证多重证明，导致故障。VPN负载平衡故障的症状包括：

- 电话交替在服务器之间并且需要格外很长时间接通或最终出故障。
- 电话日志包含消息例如这些：

```
<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和IP电话

目前， IP电话不支持Cisco Secure Desktop (CSD)和不连接，当CSD是启用的为隧道组或全局在ASA。

首先，确认ASA是否有被启用的CSD。输入**webvpn命令的show run**在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#
```

为了在IP电话连接时检查CSD问题，请检查日志或调试在ASA。

ASA日志

```
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#
```

ASA调试

```
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>
```

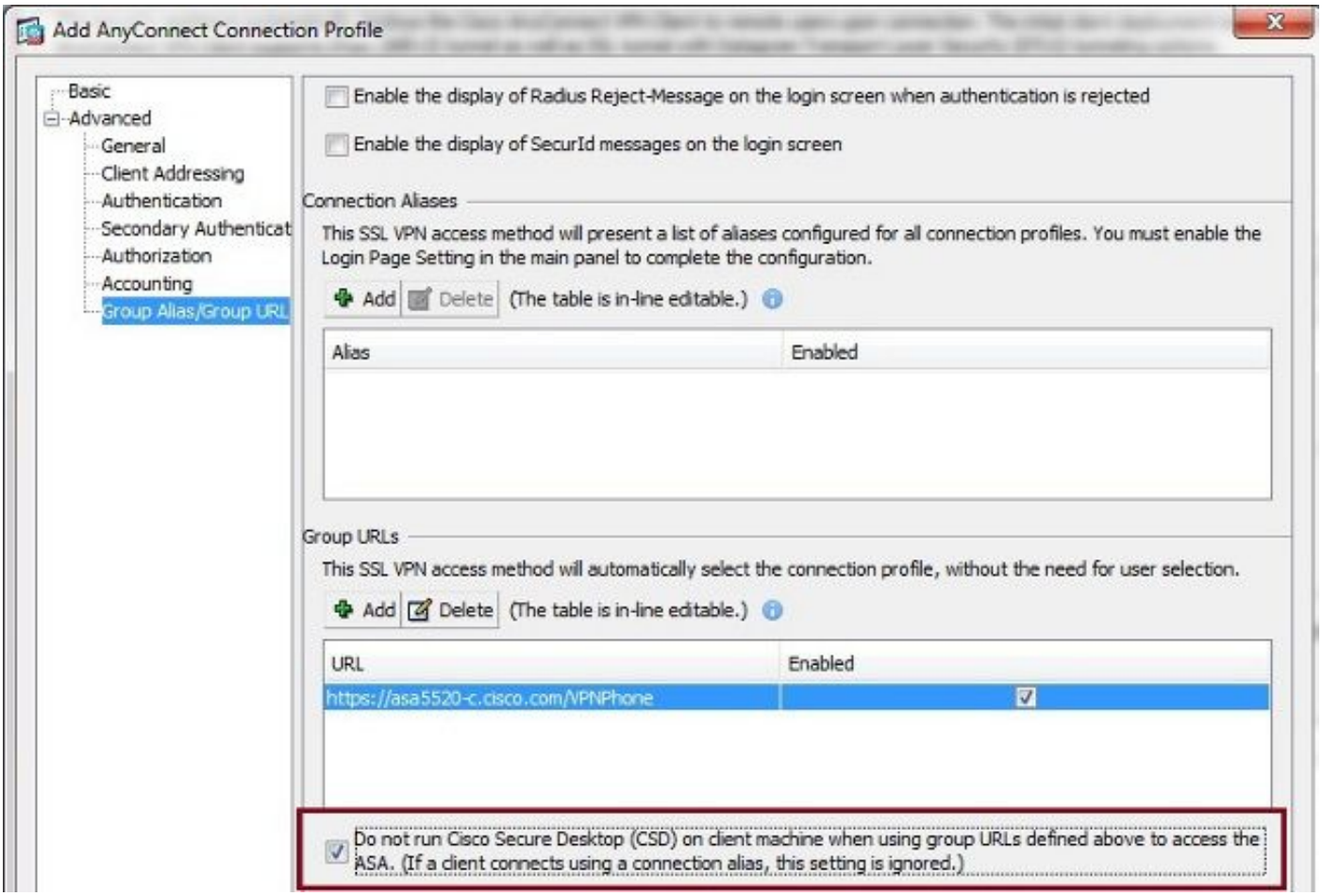
> **Note**:在与AnyConnect用户高负载的一大的部署， Cisco建议您不enable (event)**调试WebVPN anyconnect**。其输出不可能由IP地址过滤，因此很多信息也许被创建。

在ASA版本8.2和以上，您必须适用没有**csd**发出命令在隧道组的WebVPN属性下：

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

在ASA中的老版本，这不是可能的，因此唯一的解决方法是禁用CSD全局。

在Cisco Adaptive Security Device Manager (ASDM)如此示例所显示，您能禁用一个特定连接配置文件的CSD ：

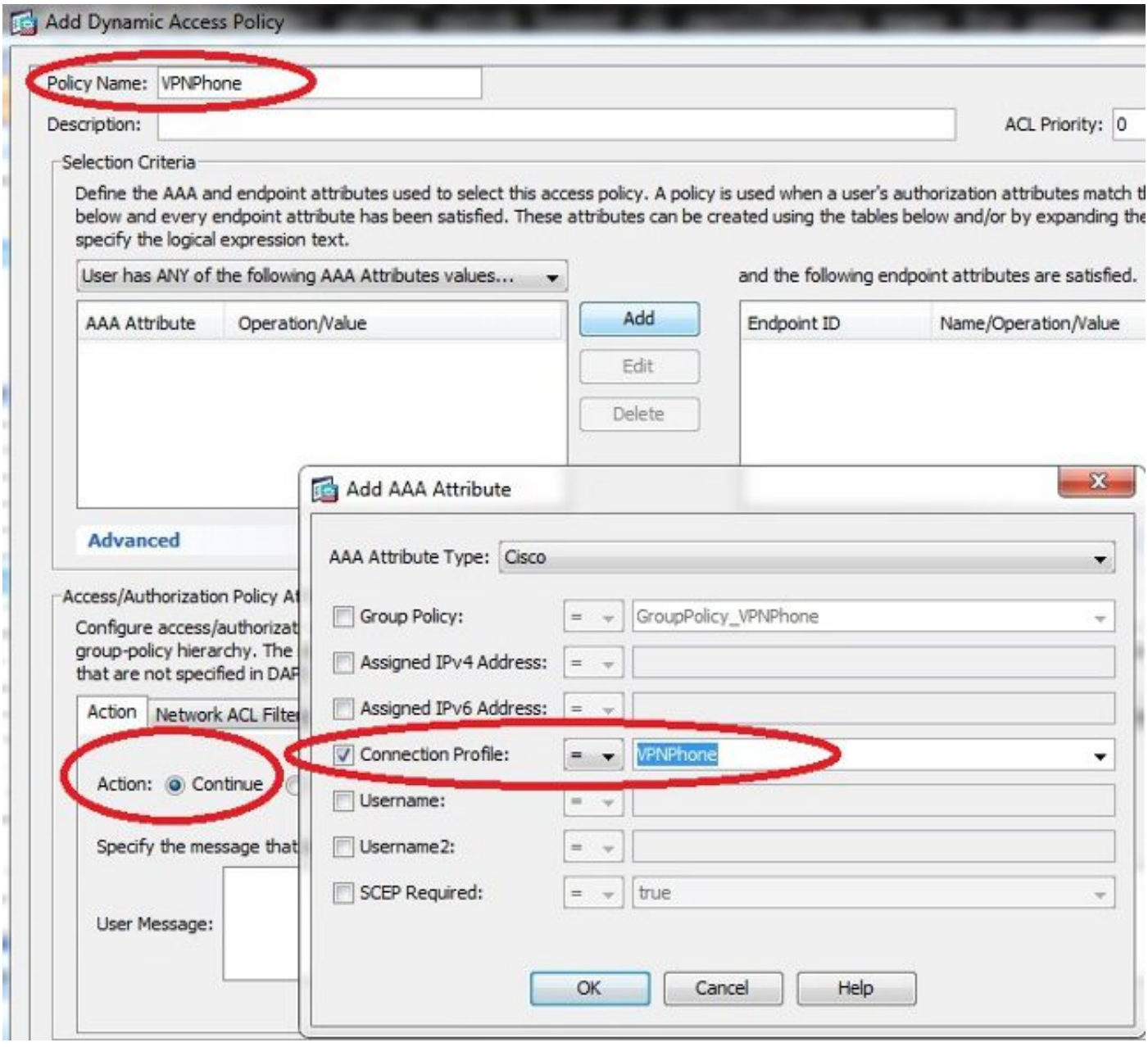


Note:请使用一个组URL为了关闭CSD以为特色。

DAP规则

多数配置不仅连接IP电话到ASA，而且连接不同种类的机器(Microsoft， Linux， Mac OS)和移动设备(机器人， iOS)。为此，查找动态访问策略(DAP)是正常的规则的一个现有配置，大多时间，在DfltAccessPolicy下的默认动作是连接的终端。

如果这是实际情形，请创建VPN电话的一个分开的DAP规则。请使用一个特定参数，例如连接配置文件，并且设置动作**继续**：



如果不创建IP电话的一个特定DAP策略， ASA显示命中在DfltAccessPolicy和一个失败的连接下：

```
%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
```

一旦创建IP电话的一个特定DAP策略以动作集**继续**，您能连接：

```
%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
```

从DfltGrpPolicy或其他组的被继承的值

在许多情况下， DfltGrpPolicy设置几个选项。默认情况下，这些设置为IP电话会话被继承，除非他们在IP电话应该使用的组策略手工指定。

也许影响连接的某些参数，如果他们从DfltGrpPolicy被继承是：

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

假设，您有此示例配置在DfltGrpPolicy和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
```

连接继承未明确地指定在GroupPolicy_VPNPhone下从DfltGrpPolicy的参数并且推进所有信息到IP电话在连接时。

为了避免此，请手工指定您直接地在组需要的值：

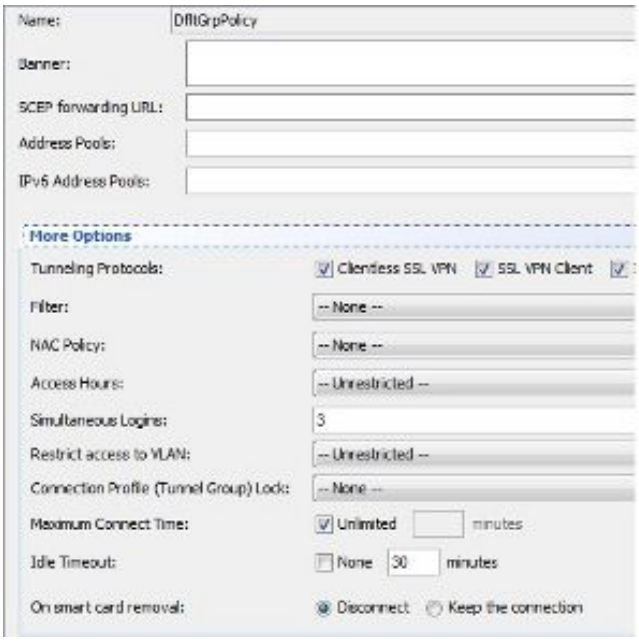
```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
 vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
 vpn-filter none
 default-domain value cisco.com
```

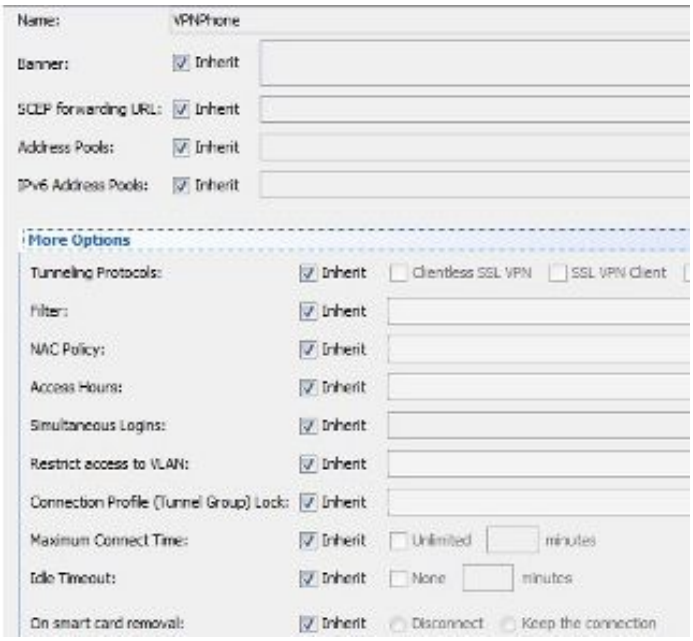
为了检查DfltGrpPolicy的默认值，请使用**show run所有组策略**命令;此示例澄清输出之间的区别：

```
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
```

这是组策略的输出通过ASDM继承属性：





支持的加密密码

用7962G IP电话和固件版本9.1.1技术支持测试的AnyConnect VPN电话仅两个密码，是两高级加密标准(AES) ：AES256-SHA和AES128-SHA。如果正确的密码在ASA没有指定，如ASA日志所显示，连接被拒绝， ：

```
%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
```

为了确认ASA是否有被启用的正确的密码，请输入**show run所有ssl**并且**显示ssl**命令：

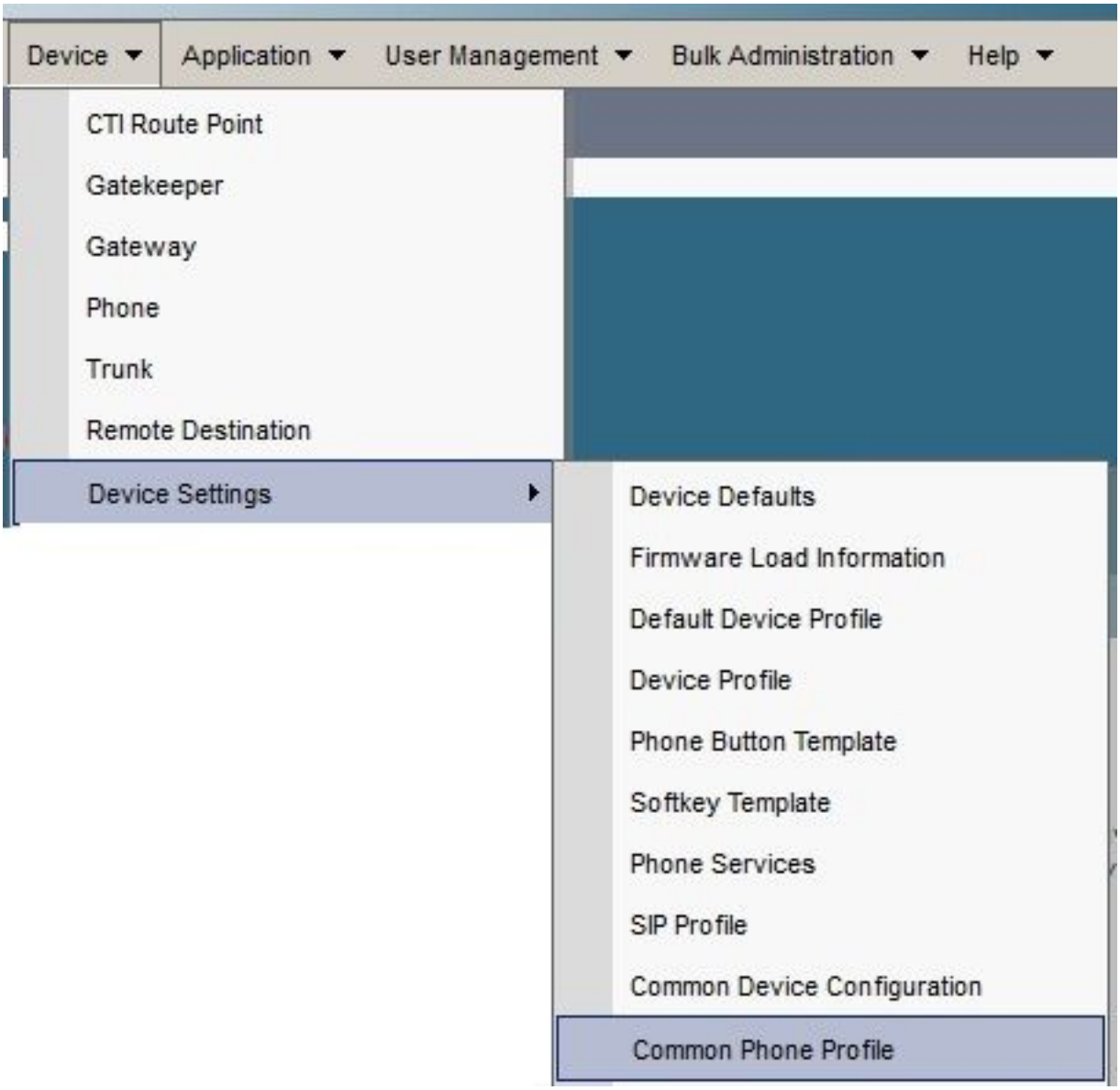
```
ASA5510-F# show run all ssl
ssl server-version any
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point SSL outside
ASA5510-F#

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#
```

在CUCM的常见问题

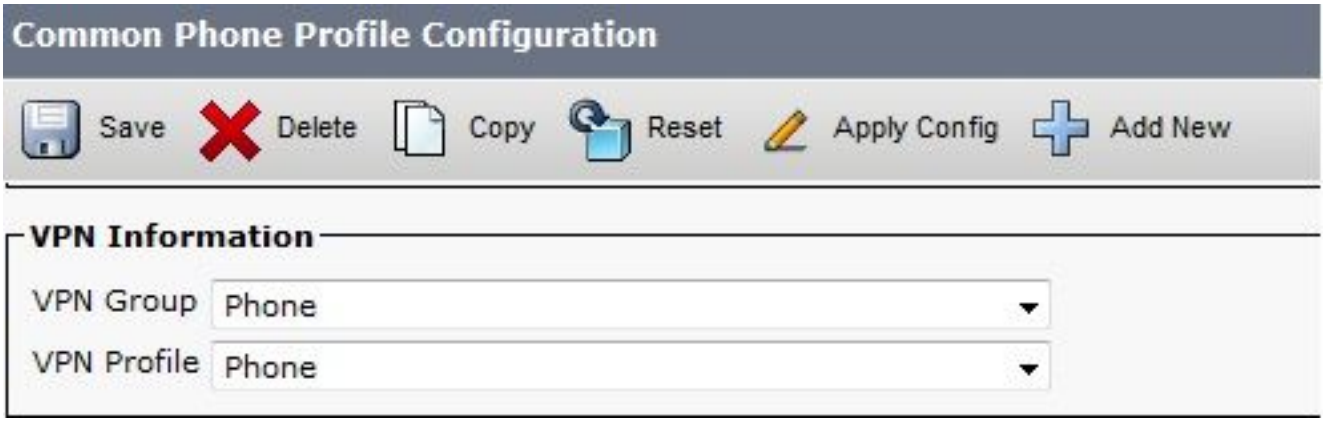
VPN设置没适用于IP电话

一旦在CUCM的配置被创建(网关，组队和配置文件)，请应用在普通的电话配置文件的VPN设置：

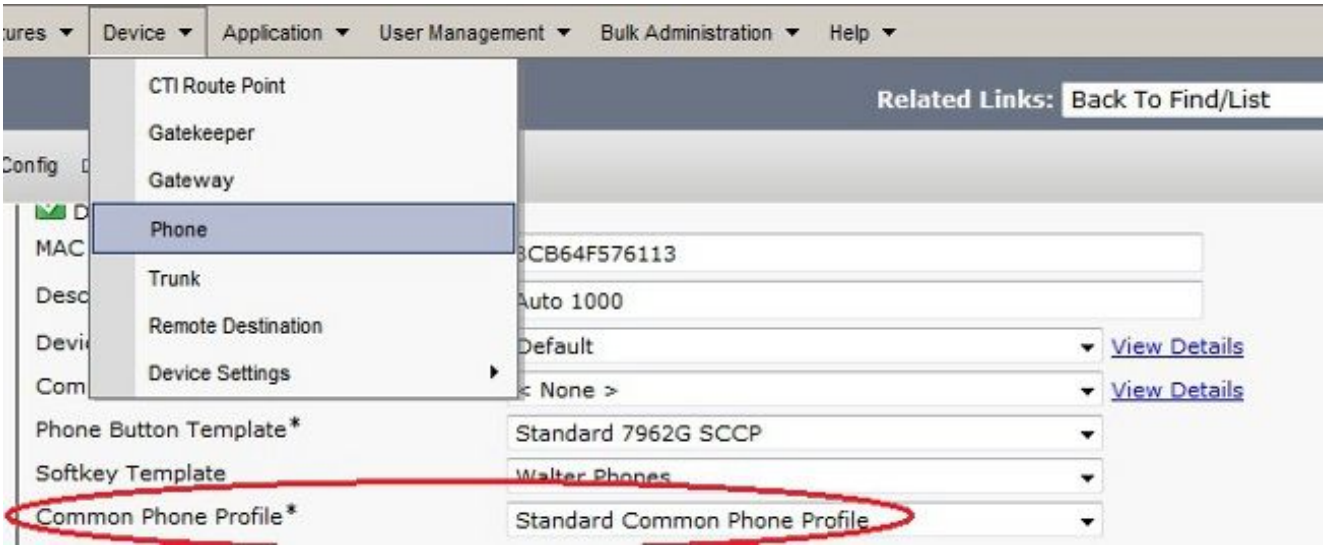
1. 连接对**设备>设备设置>普通的电话配置文件。**



2. 输入VPN信息：



3. 连接对**Device > Phone**并且确认此配置文件分配到电话配置：



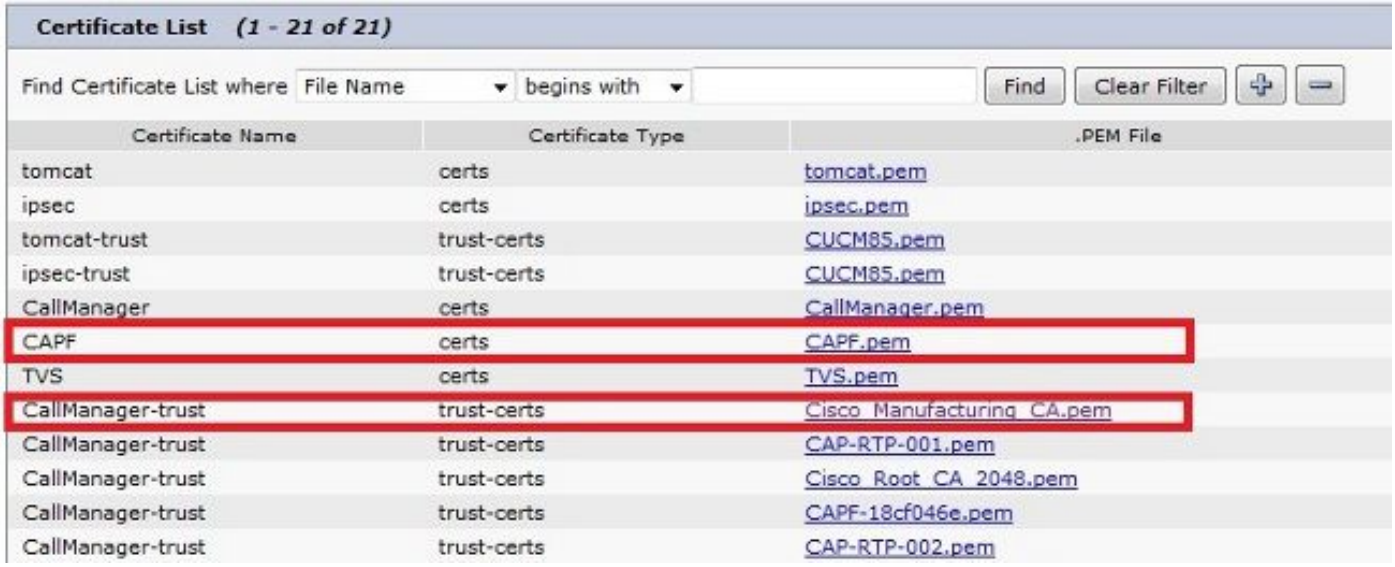
证书验证方法

有两种方式配置IP电话的证书验证：制造商预装证书(MIC)和局部重要的认证(LSC)。参考有证书验证配置示例的AnyConnect VPN电话为了选择您的情况的最佳的选项。

当您配置证书验证时，从CUCM服务器请导出认证(根CA)并且导入他们ASA ：

1. 登陆对CUCM。
2. 连接**统一的OS管理> Security > Certificate Management**。
3. 查找认证机关代理功能(CAPF)或Cisco_Manufacturing_CA;认证的种类取决于您是否使用了MIC或LSC证书验证。
4. 下载文件到本地计算机。

一旦下载文件，请登陆对ASA通过CLI或ASDM并且导入认证作为CA证书。



默认情况下，支持VPN的所有电话预先输入与MICs。7960个和7940个式样电话不附有MIC并且要求特殊安装安装过程，以便LSC安全地注册。

最新的Cisco IP电话(8811， 8841， 8851和8861)包括由新的制造的SHA2 CA签字的MIC证书：

- CUCM版本10.5(1)包括并且委托新的SHA2证书。
- 如果运行一个初期的CUCM版本，也许要求您下载新的制造CA证书和：

  加载它到CAPF信任，以便电话能验证与CAPF为了获得LSC。

  如果要允许电话验证与SIP的5061， MIC请加载它到呼叫管理器信任。

  提示：如果CUCM当前运行一个更早版本，请点击此链路为了获得SHA2 CA。

  警告：Cisco建议您使用MICs仅LSC安装。Cisco支持TLS连接的认证的LSCs与CUCM的。由于MIC根证明可以折衷，配置电话使用MICs TLS认证或其他目的用户那么责任自负。如果MICs折衷， Cisco不假设负债。

默认情况下，如果LSC存在于电话，认证使用LSC，不管MIC是否存在于电话。如果MIC和LSC存在于电话，认证使用LSC。如果LSC不存在于电话，但是MIC存在，认证使用MIC。

Note:切记，为证书验证，您应该从ASA导出SSL认证和导入它CUCM。

主机标识符检查

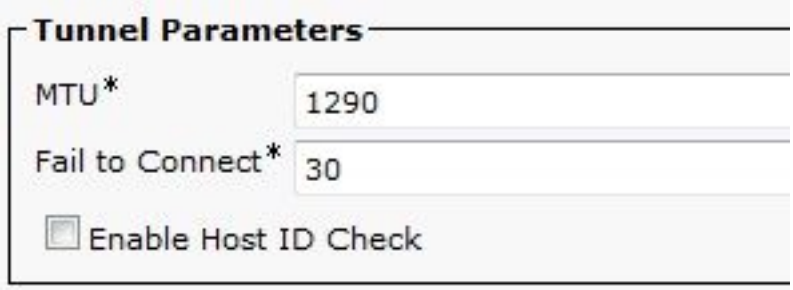
如果在认证的主题的共同名称(CN)不匹配URL (组URL)电话使用为了接通到ASA通过VPN，禁用在CUCM的主机标识符检查或请使用匹配在ASA的该URL的一个认证在ASA。

这是必要的，当ASA的SSL认证是通配符认证时， SSL认证包含不同的SAN (附属的代替名字)，或者URL用IP地址创建了而不是完全合格的域名(FQDN)。

这是IP电话日志的示例，当认证的CN不匹配电话设法到达的URL时。

```
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!!
```

为了禁用主机标识符请登记CUCM，连接对**高级特性> VPN > VPN配置文件**：



另外的故障排除

使用的日志和调试在ASA

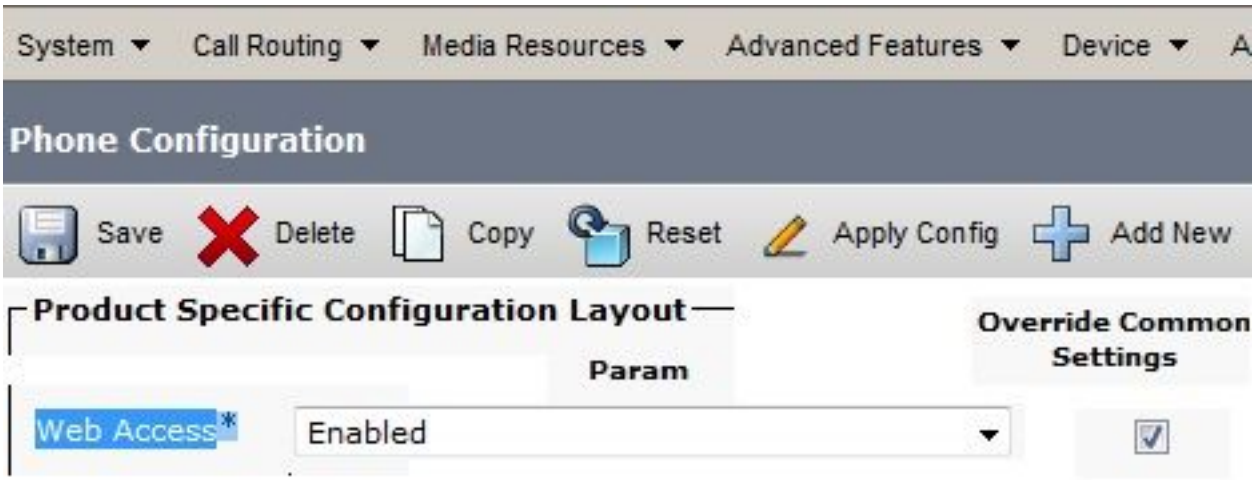
在ASA，您能enable (event)这些调试和日志排除故障的：

```
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!!
```

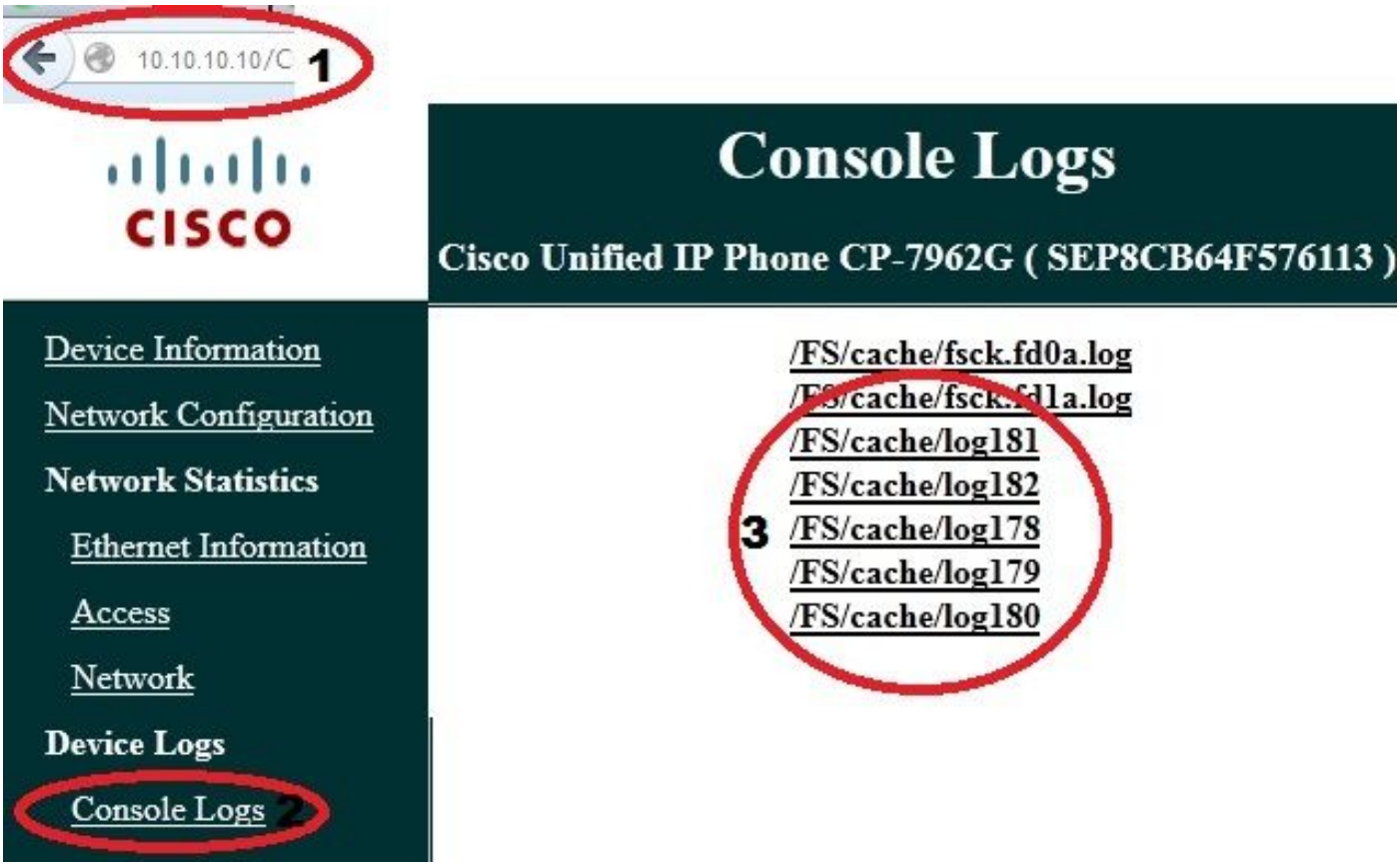
> **Note**:在与AnyConnect用户高负载的一大的部署， Cisco建议您不enable (event)**调试webvpnh anyconnect**。其输出不可能由IP地址过滤，因此很多信息也许被创建。

IP电话日志

为了访问电话日志， enable (event) Web访问功能。登陆对CUCM，并且连接对**Device > Phone >电话配置**。查找您想要对enable (event)此功能的IP电话，并且查找Web访问的部分。应用对IP电话的配置更改：



一旦enable (event)服务和重置电话为了注入此新功能，您能访问IP电话登陆浏览器;以对该子网的访问使用电话的IP地址从计算机。去控制台日志并且检查五日志文件。由于电话覆盖五个文件，您必须检查所有这些文件按顺序找到您寻找的信息。



在ASA日志和IP电话日志之间的关联的问题

这是示例如何关联从ASA和IP电话的日志。在本例中，因为在ASA的认证用不同的身份验证，替换认证的哈希在ASA的不匹配认证的哈希在电话的配置文件的。

ASA日志

```
%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
```

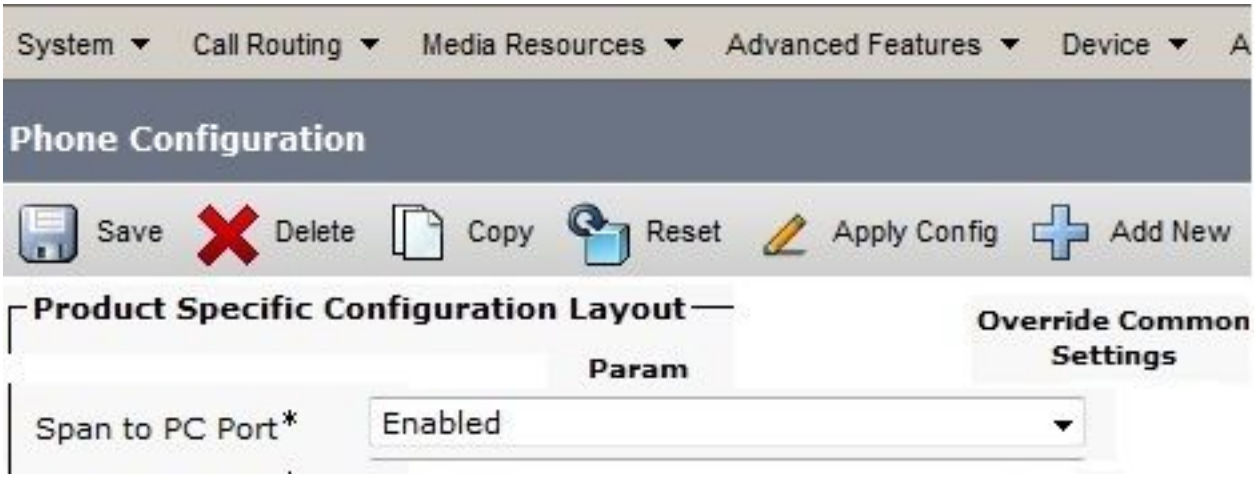
电话日志

```
 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
```

对PC端口功能的间距

您能连接计算机直接地到电话。电话有一个交换端口在底板。

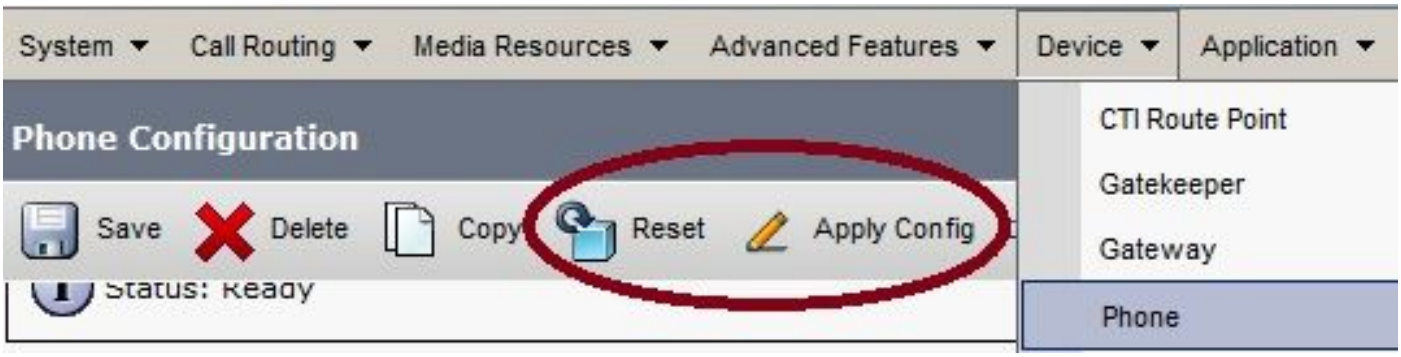
配置电话，您以前， enable (event)间距对在CUCM的PC端口和运用配置。电话开始发送每个帧的复制到PC。请使用Wireshark在混杂模式为了捕获分析的数据流。



IP电话配置更改，当连接由VPN时

常见问题是您是否能修改VPN配置，当IP电话被连接在网络外面由AnyConnect时。答案是，但是您应该确认一些配置设置。

做在CUCM的必要的更改，然后应用对电话的更改。有(请运用设置，重置，重新启动)推进新的配置的三个选项对电话。虽然全部三个选项从电话和ASA断开VPN，您能自动地重新连接，如果使用证书验证;如果使用验证、授权和统计(AAA)，再提示对于您的证件。



Note:当IP电话在远端时，从外部DHCP服务器通常收到一个IP地址。为了使IP电话接受新的配置从CUCM，应该与TFTP server联系在总部。通常CUCM是同样TFTP server。

为了接收与更改的配置文件，请确认TFTP server的IP地址在电话的网络设置正确地设置;对于确认，请使用从DHCP服务器的选项150或手工设置在电话的TFTP。此TFTP server通过AnyConnect会话是可取得。

如果IP电话从本地DHCP服务器接受TFTP server，但是该地址是不正确的，您能使用备选TFTP server选项为了改写DHCP服务器提供的TFTP服务器IP地址。此程序描述如何适用备选TFTP server ：

1. 连接对**设置> Network Configuration > IPv4配置**。
2. 移动到备选TFTP选项。
3. 按电话的是Softkey能使用一代替TFTP server;否则，请勿按Softkey。如果选项是锁着的，请按** #为了打开它。
4. 按保存Softkey。
5. 适用备选TFTP server在TFTP server下1个选项。

直接地检查状态消息在Web浏览器或在电话菜单为了确认电话获得正确的信息。如果通信正确地设置，您看到消息例如这些：

如果电话无法从TFTP server检索信息，您收到TFTP错误信息：

ASA SSL认证的续订

如果安排一个功能AnyConnect VPN电话设置，但是您的ASA SSL认证将到期，您不需要给主要站点带来所有IP电话为了注入新的SSL证书到电话;当VPN被连接时，您能添加新的证书。

如果导出了或导入了ASA的根CA证书而不是身份认证，并且，如果要继续使用同一个供应商(CA)在此续订期间，更改在CUCM的认证是不必要的，因为保持同样。但是，如果使用了身份认证，此程序是必要的;否则，在ASA和IP电话范围的Hash值不配比，并且连接没有由电话委托。

1. 更新在ASA的认证。
   Note:关于详细资料，请参见ASA 8.x ：更新并且安装与ASDM的SSL认证。请创建一分开的信任点，并且请勿适用与**ssl信任点<name>的**此新证书命令的外部，直到您应用了认证于所有VPN IP电话。

2. 导出新证书。

3. 导入新证书CUCM作为电话VPN信任认证。
   Note:注意CSCuh19734**与同样CN的加载的certs将重写在电话VPN信任的老cert**
4. 连接对在CUCM的VPN网关配置，并且适用新证书。您当前有两证书：将到期的认证和未适用于ASA的新证书。

5. 适用于此新的配置IP电话。连接**运用设置>重置>重新启动**为了注入对IP电话的新的配置更改到VPN隧道。保证所有IP电话通过VPN被连接，并且他们能通过隧道到达TFTP server。

6. 请使用TFTP检查状态消息和配置文件为了确认IP电话接收了与更改的配置文件。

7. 适用在ASA的新的SSL信任点，并且取代认证。

Note:如果ASA SSL认证已经过期，并且，如果IP电话无法通过AnyConnect连接;您能推进更改(例如新的ASA认证哈希)对IP电话。请手工设置在IP电话的TFTP为一个公共IP地址，因此IP电话能从那里检索信息。请使用一公共TFTP server主机配置文件;一个示例是创建转发在ASA的端口和重定向数据流对内部TFTP server。