Contents

[Introduction](#)
[Requirements](#)
[Confirm VPN Phone License on ASA](#)
[Export Restricted and Export Unrestricted CUCM](#)
[Common Issues on the ASA](#)
[Certificates for Use on the ASA](#)
[Trustpoint/Certificate for ASA Export and CUCM Import](#)
[ASA Presents ECDSA Self-Signed Certificate Instead of Configured RSA Certificate](#)
[External Database for Authentication of IP Phone Users](#)
[Certificate Hash Matches Between ASA Certificate and VPN Phone Trust List](#)
[Check SHA1 Hash](#)
[Download IP Phone Configuration File](#)
[Decode the Hash](#)
[VPN Load-Balancing and IP Phones](#)
[CSD and IP Phones](#)
[ASA Logs](#)
[ASA Debugs](#)
[DAP Rules](#)
[Inherited Values from DfltGrpPolicy or Other Groups](#)
[Supported Encryption Ciphers](#)
[Common Issues on the CUCM](#)
[VPN Settings Not Applied to IP Phone](#)
[Certificate Authentication Method](#)
[Host ID Check](#)
[Additional Troubleshooting](#)
[Logs and Debugs to Use in the ASA](#)
[IP Phone Logs](#)
[Correlated Issues Between ASA Logs and IP Phone Logs](#)
[ASA Logs](#)
[Phone Logs](#)
[Span to PC Port Feature](#)
[IP Phone Configuration Changes While Connected by VPN](#)
[Renewal of the ASA SSL Certificate](#)

Introduction

This document describes how to troubleshoot issues with IP phones that use the Secure Sockets Layer (SSL) protocol (Cisco AnyConnect Secure Mobility Client) in order to connect to a Cisco Adaptive Security Appliance (ASA) that is used as a VPN Gateway and in order to connect to a

Cisco Unified Communications Manager (CUCM) that is used as a voice server.

For configuration examples of AnyConnect with VPN phones, refer to these documents:

- SSLVPN with IP Phones Configuration Example
- AnyConnect VPN Phone with Certificate Authentication Configuration Example

Requirements

Before you deploy SSL VPN with IP phones, confirm that you have met these initial requirements for AnyConnect licenses for the ASA and for the U.S. export restricted version of the CUCM.

Confirm VPN Phone License on ASA

The VPN phone license enables the feature in the ASA. In order to confirm the number of users that can connect with the AnyConnect (whether or not it is an IP phone), check the AnyConnect Premium SSL License. Refer to What ASA License Is Needed for IP Phone and Mobile VPN Connections? for further details.

On the ASA, use the **show version** command in order to check if the feature is enabled. The license name differs with the ASA release:

- ASA Release 8.0.x: license name is AnyConnect for Linksys Phone.
- ASA Release 8.2.x and later: license name is AnyConnect for Cisco VPN Phone.

Here is an example for ASA Release 8.0.x:

```
ASA5505(config)# show ver

Cisco Adaptive Security Appliance Software Version 8.0(5)
Device Manager Version 7.0(2)
```

```
<snip>
Licensed features for this platform:
VPN Peers : 10
WebVPN Peers : 2
AnyConnect for Linksys phone : Disabled
<snip>
This platform has a Base license.
```

Here is an example for ASA Releases 8.2.x and later:

```
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.
```

Export Restricted and Export Unrestricted CUCM

You should deploy a U.S. export restricted version of CUCM for the VPN phone feature.

If you use an U.S. export unrestricted version of CUCM, note that:

- IP phone security configurations are modified in order to disable signaling and media encryption; this includes encryption provided by the VPN phone feature.
- You cannot export VPN details through Import/Export.
- The check boxes for VPN Profile, VPN Gateway, VPN Group, and VPN Feature Configuration are not displayed.

> **Note**: Once you upgrade to the U.S. export unrestricted version of CUCM, you cannot upgrade later to, or perform a fresh install of, the U.S. export restricted version of this software.

Common Issues on the ASA

> **Note**: You can use the Cisco CLI Analyzer (registered customers only) in order to view an analysis of **show** command outputs. You should also refer to the Important Information on Debug Commands Cisco document before you use **debug** commands.

Certificates for Use on the ASA

On the ASA, you can use self-signed SSL certificates, third-party SSL certificates, and wildcard certificates; any of these secure the communication between the IP phone and the ASA.

Only one identity certificate can be used because only one certificate can be assigned to each interface.

For third-party SSL certificates, install the complete chain in the ASA, and include any intermediate and root certificates.

Trustpoint/Certificate for ASA Export and CUCM Import

The certificate the ASA presents to the IP phone during the SSL negotiation must be exported from the ASA and imported into the CUCM. Check the trustpoint assigned to the interface to which the IP phones connect in order to know which certificate to export from the ASA.

Use the **show run ssl** command in order to verify the trustpoint (certificate) to be exported. Refer to AnyConnect VPN Phone with Certificate Authentication Configuration Example for more information.

> **Note**: If you have deployed a third-party certificate to one or more ASAs, you can also export the Root CA Certificate that is shared between all the firewalls; once you do this, you do not need to export each Identity Certificate for each ASA and then import it to the CUCM.

ASA Presents ECDSA Self-Signed Certificate Instead of Configured RSA Certificate

When this issue occurs, newer model phones are unable to connect, while the older model phones do not experience any issues. Here are the logs on the phone when this issue occurs:

```
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.
```

In Versions 9.4.1 and later, the elliptic curve cryptography is supported for SSL/TLS. When an elliptic curve-capable SSL VPN client such as a new phone model connects to the ASA, the elliptic curve cipher suite is negotiated, and the ASA presents the SSL VPN client with an elliptic curve certificate, even when the interface that corresponds is configured with an RSA-based trustpoint. In order to prevent the ASA from presenting a self-signed SSL certificate, the administrator must remove the cipher suites that correspond via the **ssl cipher** command. For example, for an interface that is configured with an RSA trustpoint, the administrator can execute this command so that only RSA-based ciphers are negotiated:

```
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:DHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA:
DES-CBC3-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5"
```

With the implementation of Cisco bug ID CSCuu02848, priority is given to the configuration. Explicitly-configured certificates are always used. Self-signed certificates are only used in the absence of a configured certificate.

Proposed Client Ciphers	RSA Cert Only	EC Cert Only	Both Certs	None
RSA Ciphers only	Uses RSA cert Uses RSA ciphers	Uses RSA self-signed cert Uses RSA ciphers	Uses RSA cert Uses RSA ciphers	Uses RSA self-sign cert Uses RSA ciphers
EC Ciphers only (rare)	**Connection Fails**	Uses EC cert Uses EC ciphers	Uses EC cert Uses EC ciphers	Uses EC self-signe cert Uses EC ciphers

Both Ciphers only	Uses RSA cert Uses RSA ciphers	Uses EC cert Uses EC ciphers	Uses EC cert Uses EC ciphers	Uses EC self-signe cert Uses EC ciphers

External Database for Authentication of IP Phone Users

You can use an external database in order to authenticate IP phone users. Protocols such as the Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial In User Service (RADIUS) can be used for authentication of VPN phone users.

Certificate Hash Matches Between ASA Certificate and VPN Phone Trust List

Remember that you must download the certificate that is assigned to the ASA SSL interface and upload it as a Phone-VPN-Trust Certificate in the CUCM. Different circumstances might cause the hash for this certificate presented by the ASA to not match the hash that the CUCM server generates and pushes to the VPN phone through the configuration file.

Once the configuration is complete, test the VPN connection between the IP phone and the ASA. If the connection continues to fail, check if the hash of the ASA certificate matches the hash the IP phone is expecting:

1. Check the Secure Hash Algorithm 1 (SHA1) hash presented by the ASA.
2. Use TFTP in order to download the IP phone configuration file from the CUCM.
3. Decode the hash from hexadecimal to base 64 or from base 64 to hexadecimal.

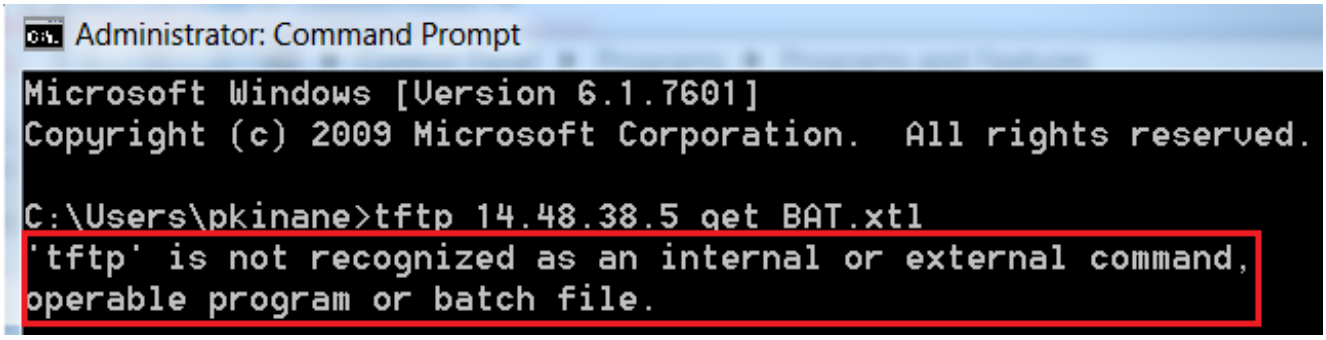
Check SHA1 Hash

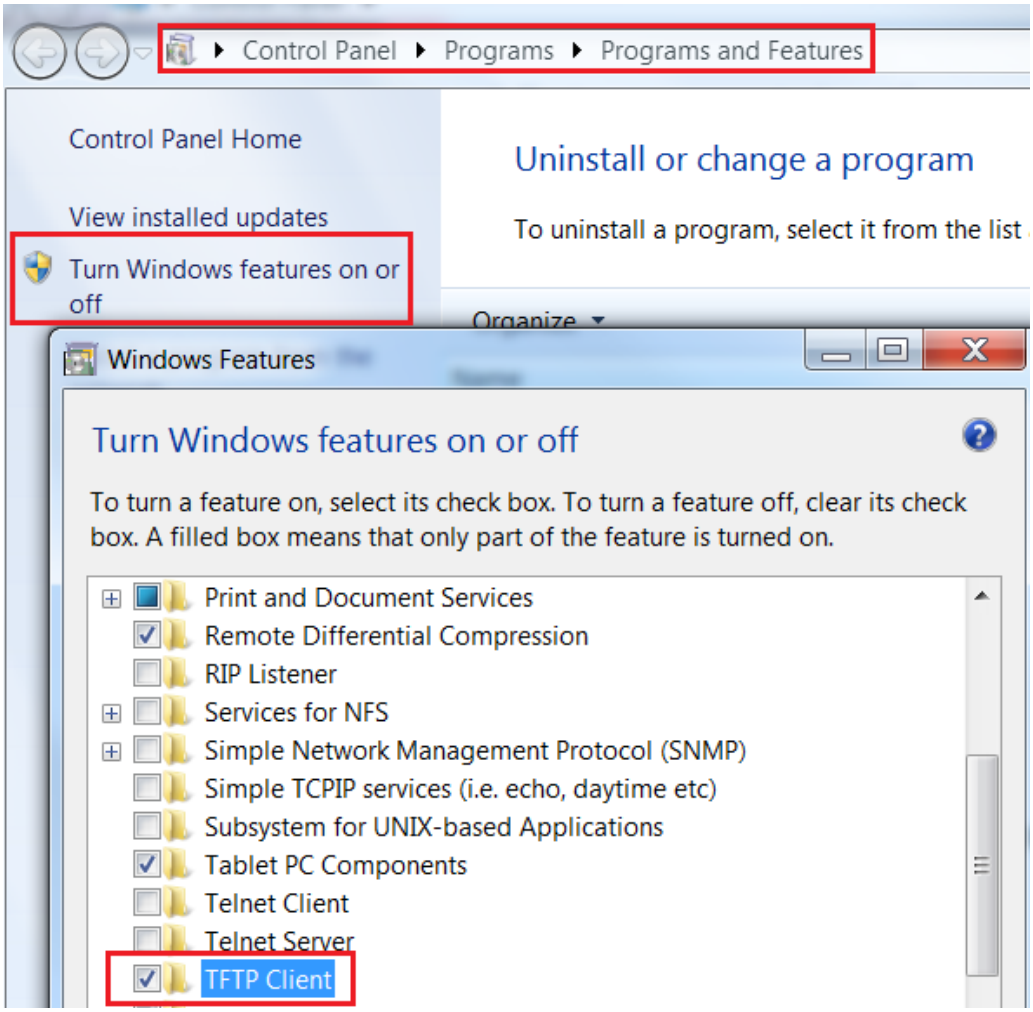
The ASA presents the certificate applied with the **ssl trustpoint** command on the interface to which the IP phone connects. To check this certificate, open the browser (in this example, Firefox), and enter the URL (group-url) to which the phones should be connecting:

Download IP Phone Configuration File

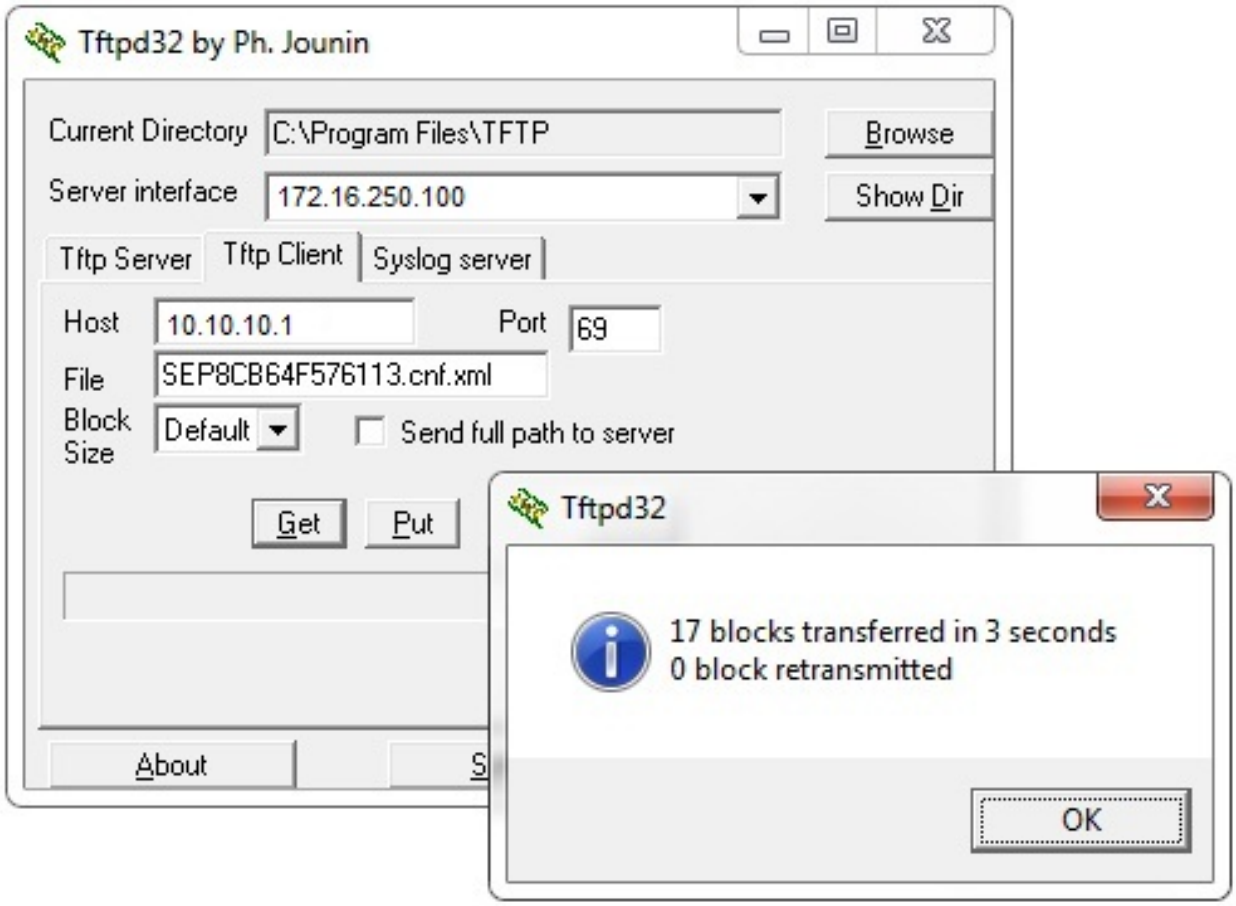
From a PC with direct access to the CUCM, download the TFTP config file for the phone with connection issues. Two download methods are:

1. Open a CLI session in Windows, and use the **tftp -i** <*TFTP Server*> **GET SEP**<*Phone Mac Address*>**.cnf.xml** command.
   Note: If you receive an error similar to the one below, you should confirm that the TFTP Client feature is
   enabled.





2. Use an application such as Tftpd32 to download the file:



3. Once the file is downloaded, open the XML and find the *vpnGroup* configuration. This example shows the section and the *certHash* to be verified:

```
<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>
```

Decode the Hash

Confirm that both hash values match. The browser presents the hash in hexadecimal format, while

the XML file uses base 64, so convert one format to the other in order to confirm the match. There are many translators available; one example is the TRANSLATOR, BINARY .

Note: If the previous hash value does not match, the VPN phone does not trust the connection that is negotiated with the ASA, and the connection fails.

VPN Load-Balancing and IP Phones

Load-balanced SSL VPN is not supported for VPN phones. VPN phones do not perform real certificate validation but instead use hashes pushed down by the CUCM to validate the servers. Because VPN load-balancing is basically an HTTP redirection, it requires the phones to validate multiple certificates, which leads to failure. Symptoms of VPN load-balancing failure include:

- The phone alternates between servers and takes an exceptionally long time to connect or eventually fails.
- The phone logs contain messages such as these:

```
<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 and IP Phones

Currently, IP phones do not support the Cisco Secure Desktop (CSD) and do not connect when CSD is enabled for tunnel-group or globally in the ASA.

First, confirm whether the ASA has CSD enabled. Enter the **show run webvpn** command in the 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#
```

In order to check CSD issues during an IP phone connection, check the logs or debugs in the ASA.

ASA Logs

```
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 Debugs

```
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>
```

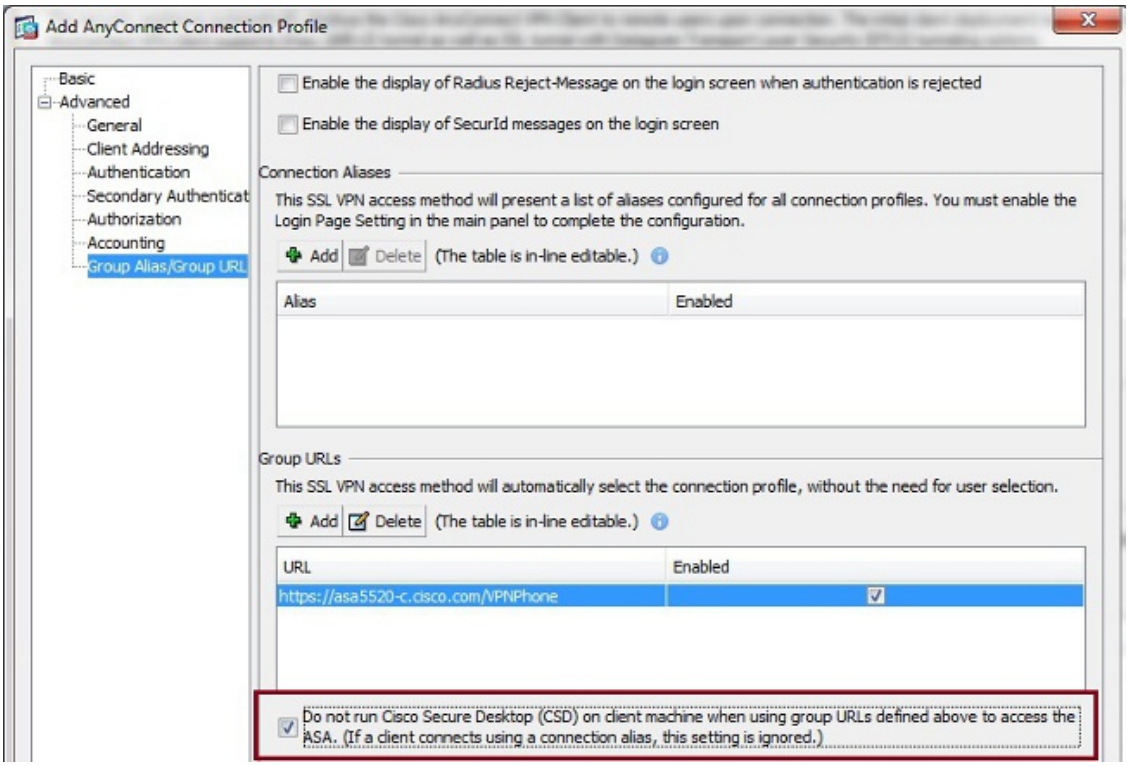
> **Note**: In a large deployment with a high load of AnyConnect users, Cisco recommends that you do not enable **debug webvpn anyconnect**. Its output cannot be filtered by IP address, so a large amount of information might be created.

In ASA Versions 8.2 and later, you must apply the **without-csd** command under the webvpn-attributes of the tunnel-group:

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

In previous versions of the ASA, this was not possible, so the only workaround was to disable the CSD globally.

In the Cisco Adaptive Security Device Manager (ASDM), you can disable CSD for a specific connection profile as shown in this example:

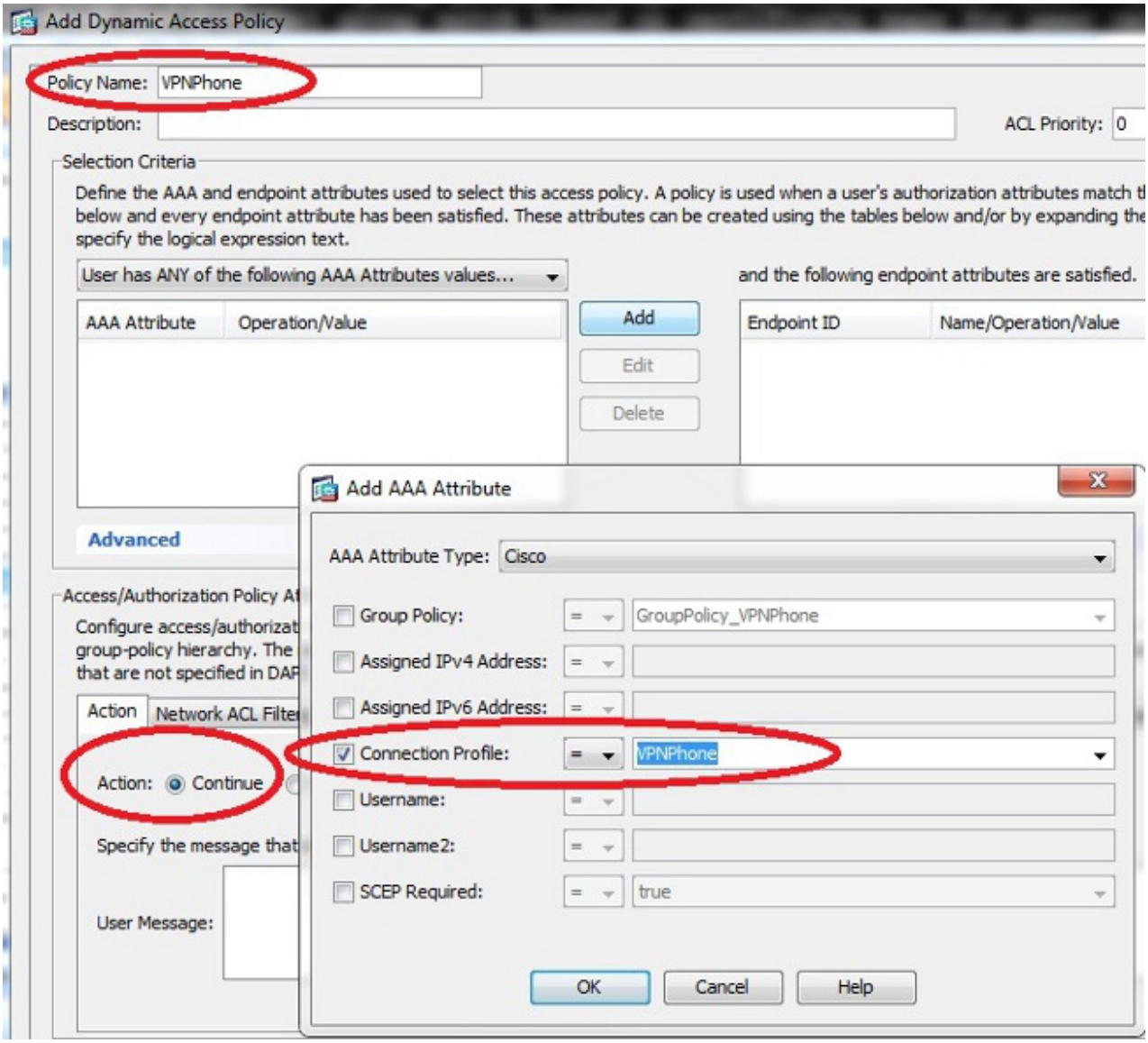


Note: Use a group-url in order to turn off the CSD feature.

DAP Rules

Most deployments not only connect IP phones to the ASA but also connect different types of machines (Microsoft, Linux, Mac OS) and mobile devices (Android, iOS). For this reason, it is normal to find an existing configuration of Dynamic Access Policy (DAP) rules, where, most of the time, the Default Action under the DfltAccessPolicy is termination of the connection.

If this is the case, create a separate DAP rule for the VPN phones. Use a specific parameter, such as the Connection Profile, and set the action to **Continue**:



If you do not create a specific DAP policy for IP phones, the ASA shows a hit under the DfltAccessPolicy and a failed connection:

```
%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
```

Once you create a specific DAP policy for the IP phones with the action set to **Continue**, you are able to connect:

```
%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
```

Inherited Values from DfltGrpPolicy or Other Groups

In many cases, the DfltGrpPolicy is set up with several options. By default, these settings are inherited for the IP phone session unless they are manually specified in the group-policy which the IP phone should use.

Some parameters that might affect the connection if they are inherited from the DfltGrpPolicy are:

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

Assume that you have this example configuration in the DfltGrpPolicy and the 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
```

The connection inherits the parameters from the DfltGrpPolicy that were not explicitly specified under the GroupPolicy_VPNPhone and pushes all of the information to the IP phone during the connection.

In order to avoid this, manually specify the value(s) you need directly in the group:

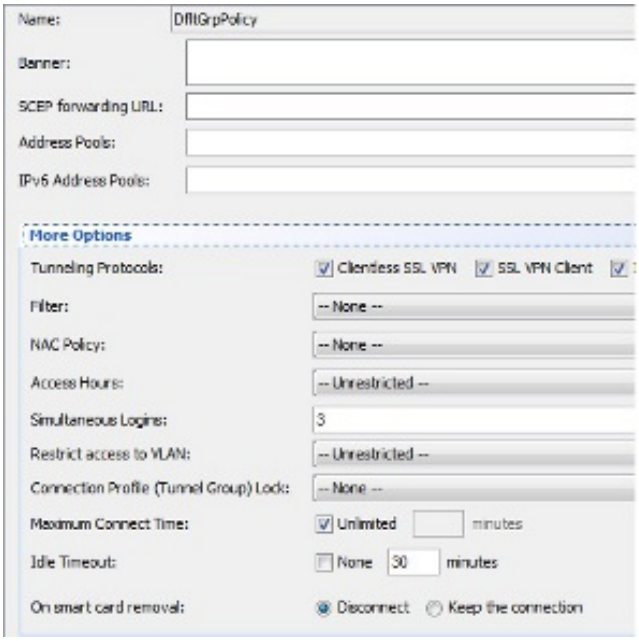
```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
 vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
 vpn-filter none
 default-domain value cisco.com
```

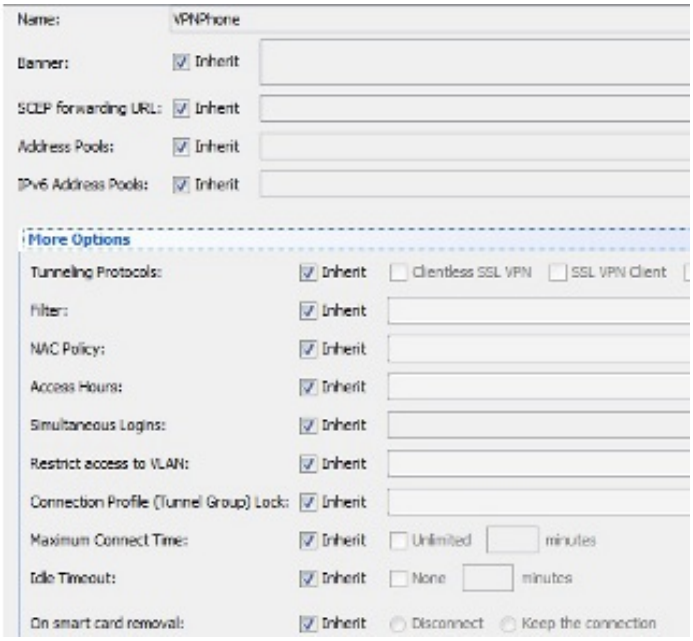
In order to check the default values of the DfltGrpPolicy, use the **show run all group-policy** command; this example clarifies the difference between the outputs:

```
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
```

Here is the output of the group-policy inherit attributes through the ASDM:





Supported Encryption Ciphers

An AnyConnect VPN phone tested with 7962G IP phone and firmware Version 9.1.1 supports only two ciphers, which are both Advanced Encryption Standard (AES): AES256-SHA and AES128-SHA. If the correct ciphers are not specified in the ASA, the connection is rejected, as shown in the ASA log:

```
%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
```

In order to confirm whether the ASA has the correct ciphers enabled, enter the **show run all ssl**

and **show ssl** commands:

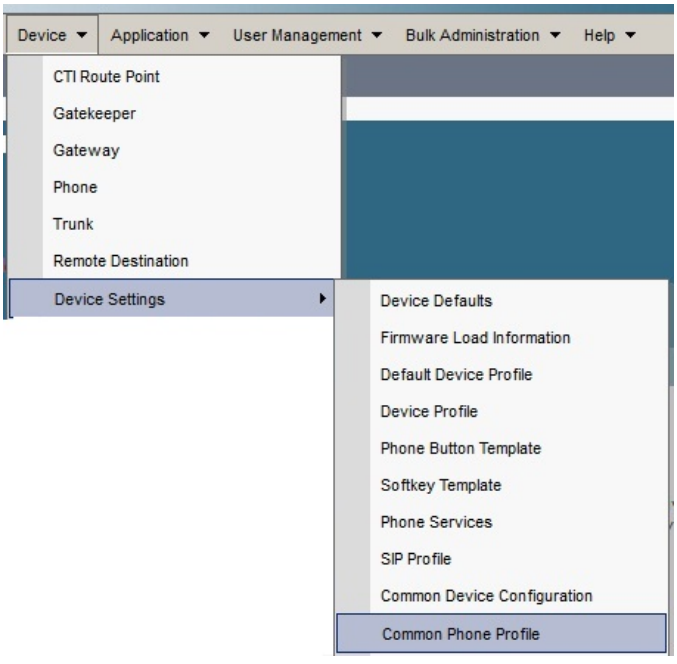
```
ASA5510-F# show run all ssl
ssl server-version any
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point SSL outside
ASA5510-F#

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#
```

Common Issues on the CUCM

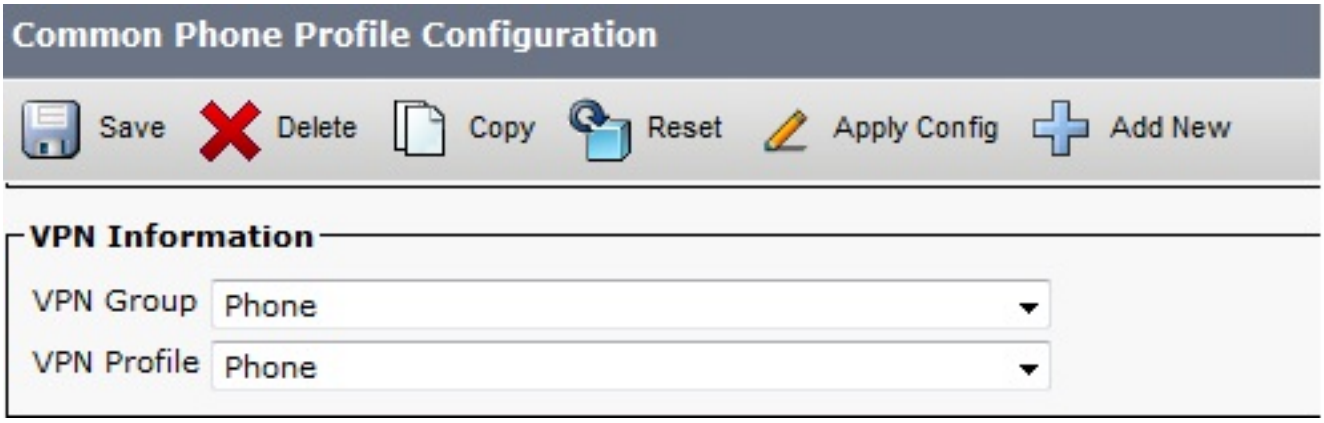
VPN Settings Not Applied to IP Phone

Once the configuration on the CUCM is created (Gateway, Group, and Profile), apply the VPN settings in the Common Phone Profile:

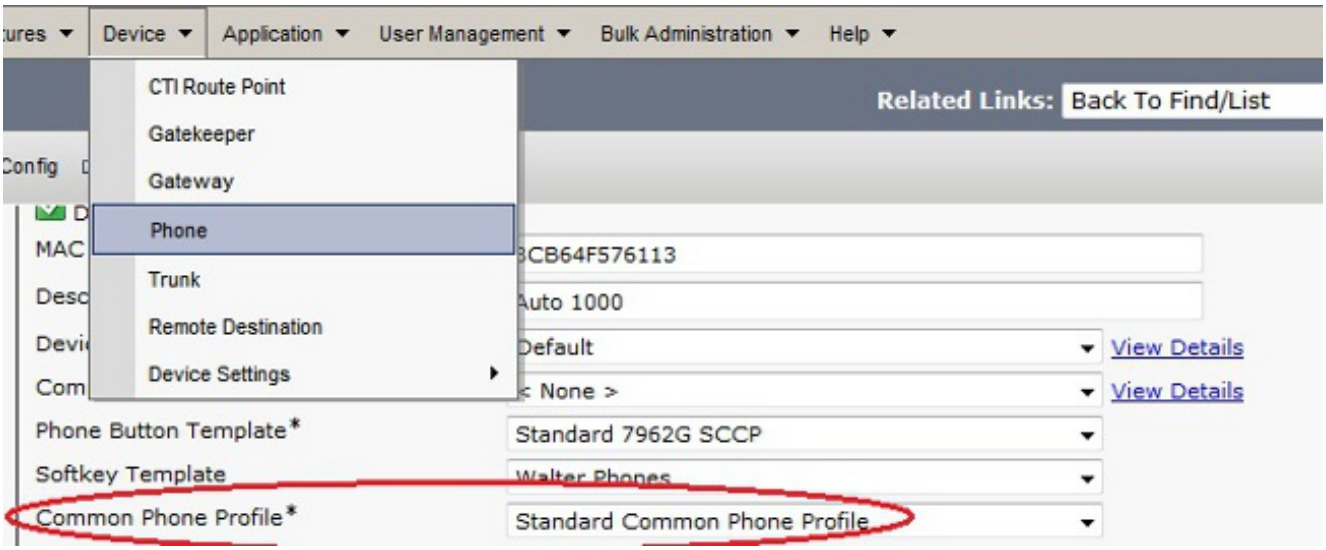
1. Navigate to **Device** > **Device Settings** > **Common Phone Profile**.



2. Enter the VPN information:



3. Navigate to **Device** > **Phone** and confirm this profile is assigned to the phone configuration:



Certificate Authentication Method

There are two ways to configure certificate authentication for IP phones: Manufacturer Installed Certificate (MIC) and Locally Significant Certificate (LSC). Refer to AnyConnect VPN Phone with Certificate Authentication Configuration Example in order to choose the best option for your situation.

When you configure certificate authentication, export the certificate(s) (Root CA) from the CUCM server and import them to the ASA:

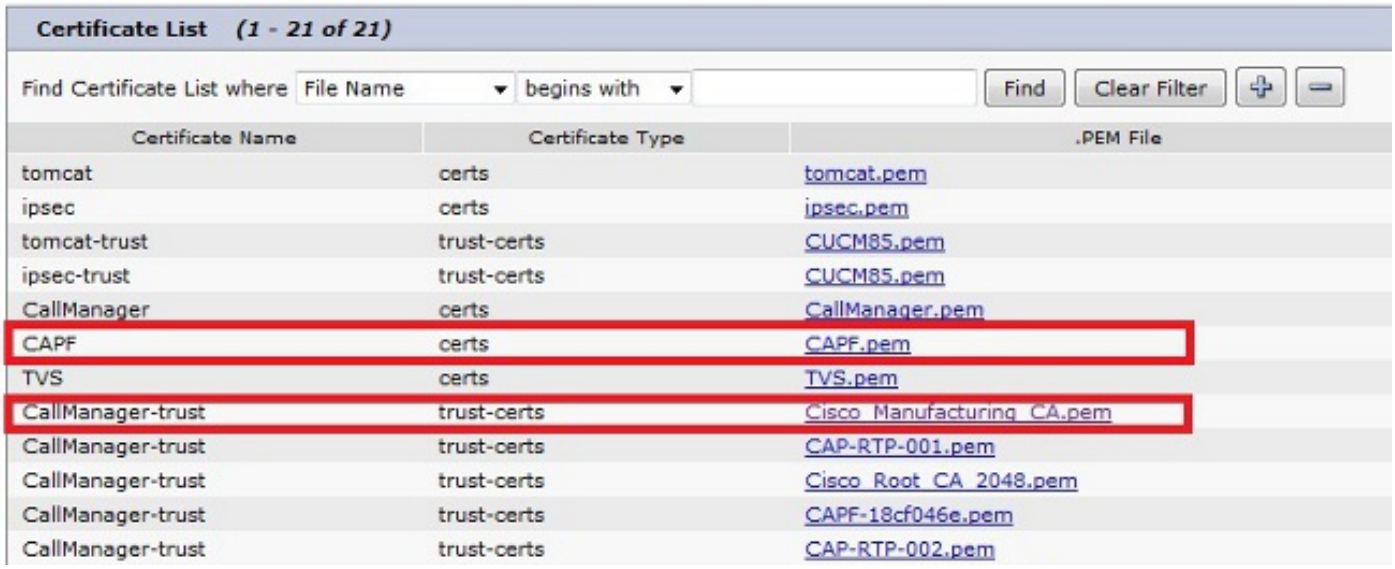
1. Log in to the CUCM.

2. Navigate to **Unified OS Administration > Security > Certificate Management**.

3. Find the Certificate Authority Proxy Function (CAPF) or Cisco_Manufacturing_CA; the type of certificate depends upon whether you used MIC or LSC certificate authentication.

4. Download the file to the local computer.

Once the files are downloaded, log in to the ASA through the CLI or ASDM and import the certificate as a CA Certificate.



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

By default, all of the phones that support VPN are pre-loaded with MICs. The 7960 and 7940 model phones do not come with an MIC and require a special installation procedure so that the LSC registers securely.

The newest Cisco IP phones (8811, 8841, 8851, and 8861) include MIC certificates that are signed by the new Manufacturing SHA2 CA:

- The CUCM Version 10.5(1) includes and trusts the new SHA2 certificates.
- If you run an earlier CUCM version, you might be required to download the new Manufacturing CA certificate and:

  Upload it to the CAPF-trust so that the phones can authenticate with CAPF in order to obtain an LSC.

  Upload it to the CallManager-trust if you want to allow the phones to authenticate with an MIC for SIP 5061.

Tip: Click this link in order to obtain the SHA2 CA if the CUCM currently runs an earlier version.

Caution: Cisco recommends that you use MICs for LSC installation only. Cisco supports LSCs for authentication of the TLS connection with the CUCM. Because the MIC root certificates can be compromised, customers who configure phones to use MICs for TLS authentication or for any other purpose do so at their own risk. Cisco assumes no liability if the MICs are compromised.

By default, if a LSC exists in the phone, authentication uses the LSC, regardless of whether a MIC exists in the phone. If a MIC and LSC exist in the phone, authentication uses the LSC. If a LSC does not exist in the phone, but a MIC does exist, authentication uses the MIC.

Note: Remember that, for certificate authentication, you should export the SSL certificate from the ASA and import it to the CUCM.

Host ID Check

If the common name (CN) in the subject of the certificate does not match the URL (group-url) the phones use in order to connect to the ASA through the VPN, disable the Host ID Check on the CUCM or use a certificate in the ASA that matches that URL on the ASA.

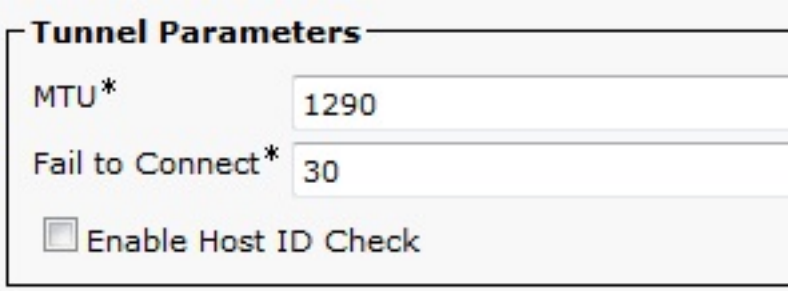
This is necessary when the SSL certificate of the ASA is a wildcard certificate, the SSL certificate contains a different SAN (Subject Alternative Name), or the URL was created with the IP address instead of the fully qualified domain name (FQDN).

This is an example of an IP phone log when the CN of the certificate does not match the URL the phone is trying to reach.

```
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!!
```

In order to disable the Host ID Check in the CUCM, navigate to **Advanced Features** > **VPN** > **VPN Profile**:



Additional Troubleshooting

Logs and Debugs to Use in the ASA

On the ASA, you can enable these debugs and logs for troubleshooting:

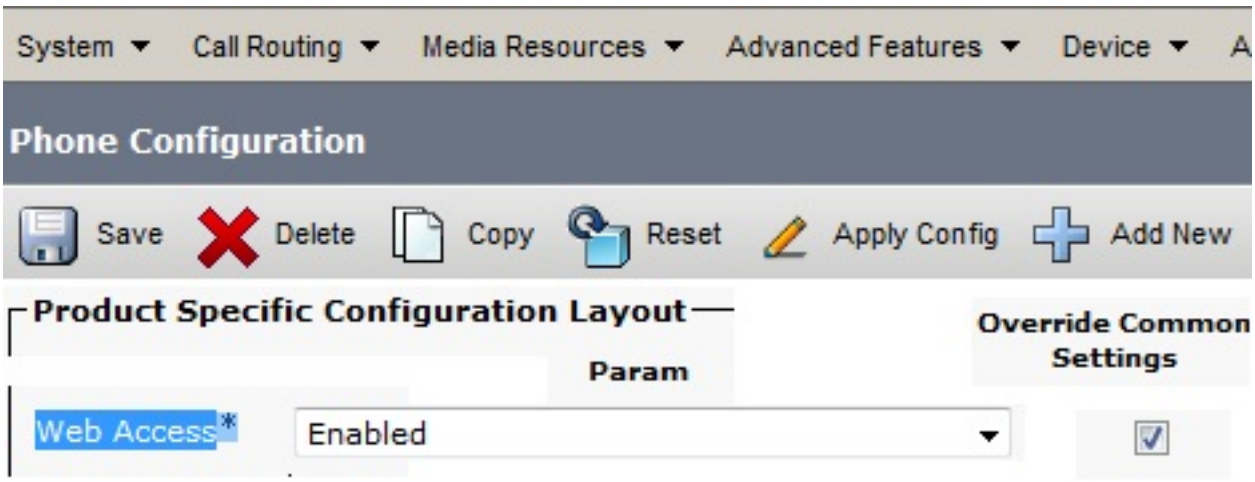
```
1231: NOT 07:07:32.445560 VPNC: DNS has wildcard, starting checks...
1232: ERR 07:07:32.446239 VPNC: Generic third level wildcards are not allowed,
stopping checks on host=(test.vpn.com) and dns=(*.vpn.com)
1233: NOT 07:07:32.446993 VPNC: hostID not found in subjectAltNames
1234: NOT 07:07:32.447703 VPNC: hostID not found in subject name
1235: ERR 07:07:32.448306 VPNC: hostIDCheck failed!!
```

> **Note**: In a large deployment with a high load of AnyConnect users, Cisco recommends that you do not enable the **debug webvpnh anyconnect**. Its output cannot be filtered by IP address, so a large amount of information might be created.

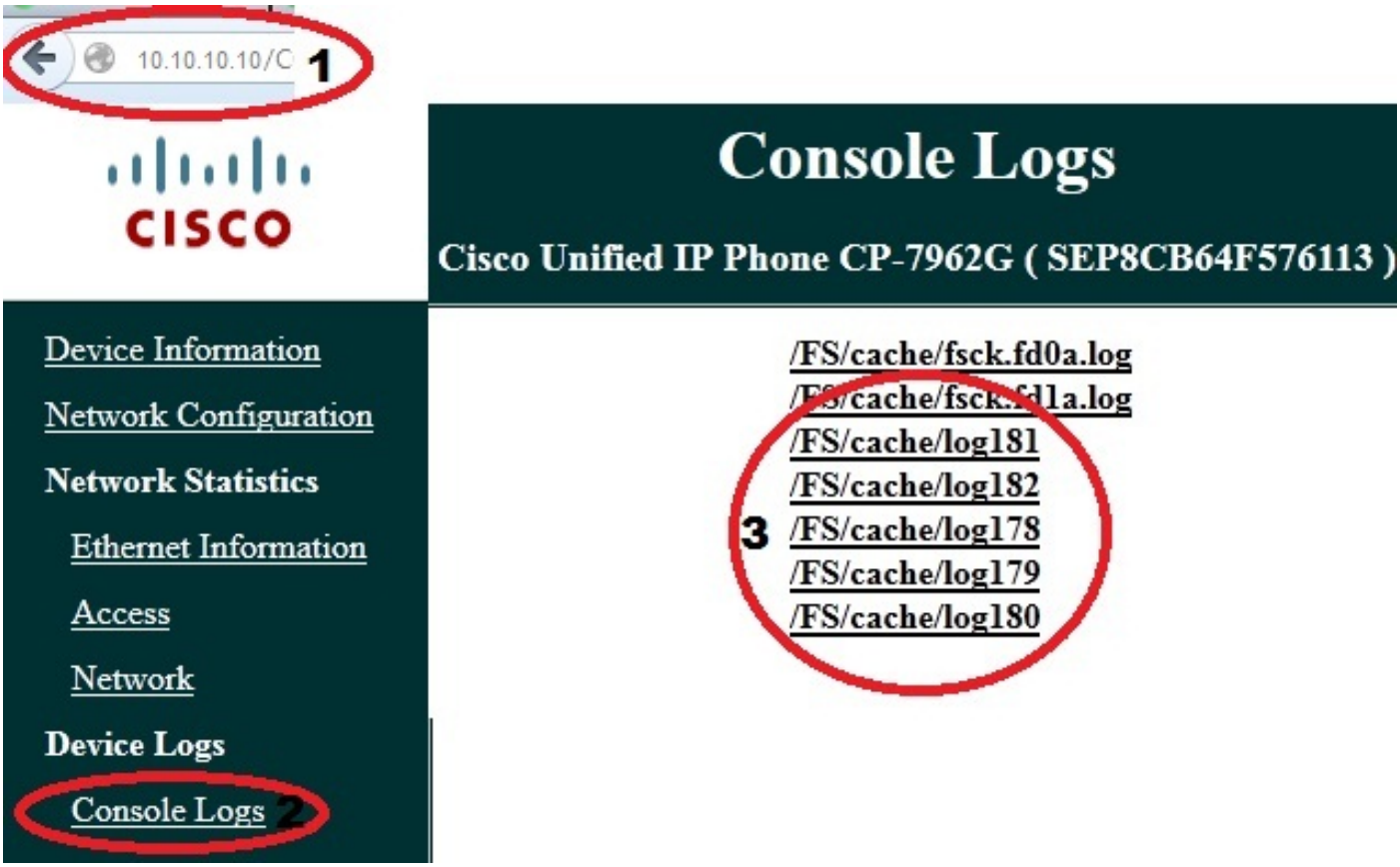
IP Phone Logs

In order to access the phone logs, enable the Web Access Feature. Log in to the CUCM, and navigate to **Device** > **Phone** > **Phone Configuration**. Find the IP phone on which you want to

enable this feature, and find the section for Web Access. Apply the configuration changes to the IP phone:



Once you enable the service and reset the phone in order to inject this new feature, you can access IP phone logs in the browser; use the IP address of the phone from a computer with access to that subnet. Go to the console logs and check the five log files. Because the phone overwrites the five files, you must check all of these files in order find the information you seek.



Correlated Issues Between ASA Logs and IP Phone Logs

This is an example of how to correlate the logs from the ASA and the IP phone. In this example, the hash of the certificate on the ASA does not match the hash of the certificate on the configuration file of the phone because the certificate on the ASA was replaced with a different certificate.

ASA Logs

```
%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
```

Phone Logs

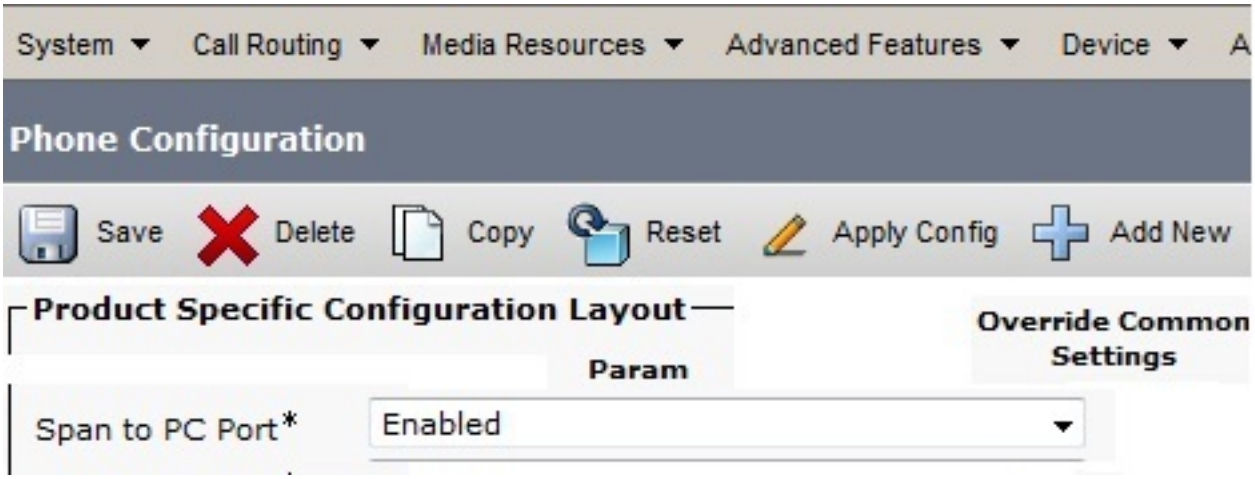
```
 902: NOT 10:19:27.155936 VPNC: ssl_state_cb: TLSv1: SSL_connect: before/connect
initialization
903: NOT 10:19:27.162212 VPNC: ssl_state_cb: TLSv1: SSL_connect: unknown state
904: NOT 10:19:27.361610 VPNC: ssl_state_cb: TLSv1: SSL_connect: SSLv3 read server hello A
905: NOT 10:19:27.364687 VPNC: cert_vfy_cb: depth:1 of 1, subject:
</CN=10.198.16.140/unstructuredName=10.198.16.140>
906: NOT 10:19:27.365344 VPNC: cert_vfy_cb: depth:1 of 1, pre_err: 18 (self signed certificate)
907: NOT 10:19:27.368304 VPNC: cert_vfy_cb: peer cert saved: /tmp/leaf.crt
908: NOT 10:19:27.375718 SECD: Leaf cert hash = 1289B8A7AA9FFD84865E38939F3466A61B5608FC
909: ERR 10:19:27.376752 SECD: EROR:secLoadFile: file not found </tmp/issuer.crt>
910: ERR 10:19:27.377361 SECD: Unable to open file /tmp/issuer.crt
911: ERR 10:19:27.420205 VPNC: VPN cert chain verification failed, issuer certificate not found
and leaf not trusted
912: ERR 10:19:27.421467 VPNC: ssl_state_cb: TLSv1: write: alert: fatal:
unknown CA
913: ERR 10:19:27.422295 VPNC: alert_err: SSL write alert: code 48, unknown CA
914: ERR 10:19:27.423201 VPNC: create_ssl_connection: SSL_connect ret -1 error 1
915: ERR 10:19:27.423820 VPNC: SSL: SSL_connect: SSL_ERROR_SSL (error 1)
916: ERR 10:19:27.424541 VPNC: SSL: SSL_connect: error:14090086:SSL
routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
 917: ERR 10:19:27.425156 VPNC: create_ssl_connection: SSL setup failure
918: ERR 10:19:27.426473 VPNC: do_login: create_ssl_connection failed
919: NOT 10:19:27.427334 VPNC: vpn_stop: de-activating vpn
920: NOT 10:19:27.428156 VPNC: vpn_set_auto: auto -> auto
921: NOT 10:19:27.428653 VPNC: vpn_set_active: activated -> de-activated
922: NOT 10:19:27.429187 VPNC: set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
923: NOT 10:19:27.429716 VPNC: set_login_state: VPNC : 1 (LoggingIn) --> 3
(LoginFailed)
924: NOT 10:19:27.430297 VPNC: vpnc_send_notify: notify type: 1 [LoginFailed]
```

```
925: NOT 10:19:27.430812 VPNC: vpnc_send_notify: notify code: 37
[SslAlertSrvrCert]
926: NOT 10:19:27.431331 VPNC: vpnc_send_notify: notify desc: [alert: Unknown
CA (server cert)]
927: NOT 10:19:27.431841 VPNC: vpnc_send_notify: sending signal 28 w/ value 13 to
pid 14
928: ERR 10:19:27.432467 VPNC: protocol_handler: login failed
```

Span to PC Port Feature

You can connect a computer directly to a phone. The phone has a switch port in the back plane.

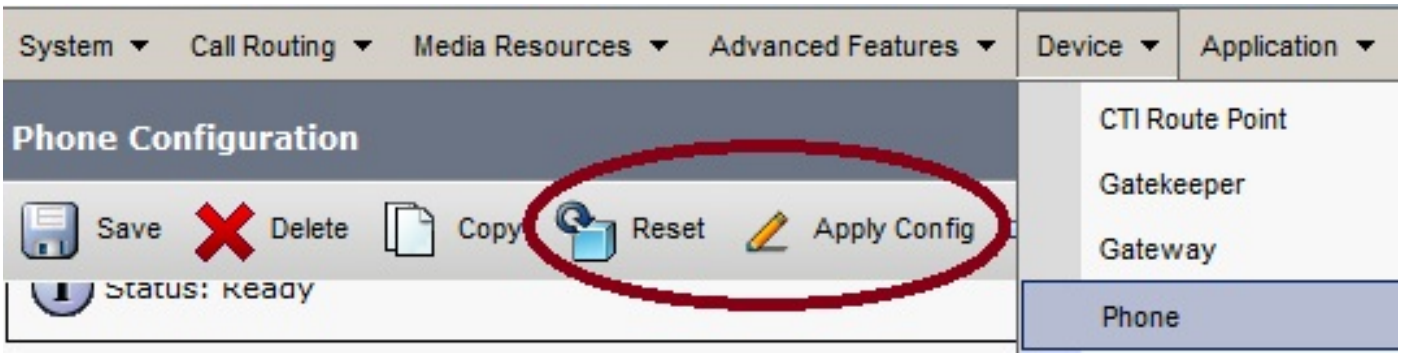
Configure the phone as you did previously, enable the Span to PC Port on the CUCM, and apply the configuration. The phone begins to send a copy of each frame to the PC. Use Wireshark in promiscuous mode in order to capture traffic for analysis.



IP Phone Configuration Changes While Connected by VPN

A common question is whether you can modify the VPN configuration while the IP phone is connected out of the network by AnyConnect. The answer is yes, but you should confirm some configuration settings.

Make the necessary changes in the CUCM, then apply the changes to the phone. There are three options (Apply Config, Reset, Restart) to push the new configuration to the phone. Although all three options disconnect the VPN from the phone and the ASA, you can reconnect automatically if you are using certificate authentication; if you are using Authentication, Authorization, and Accounting (AAA), you are prompted for your credentials again.



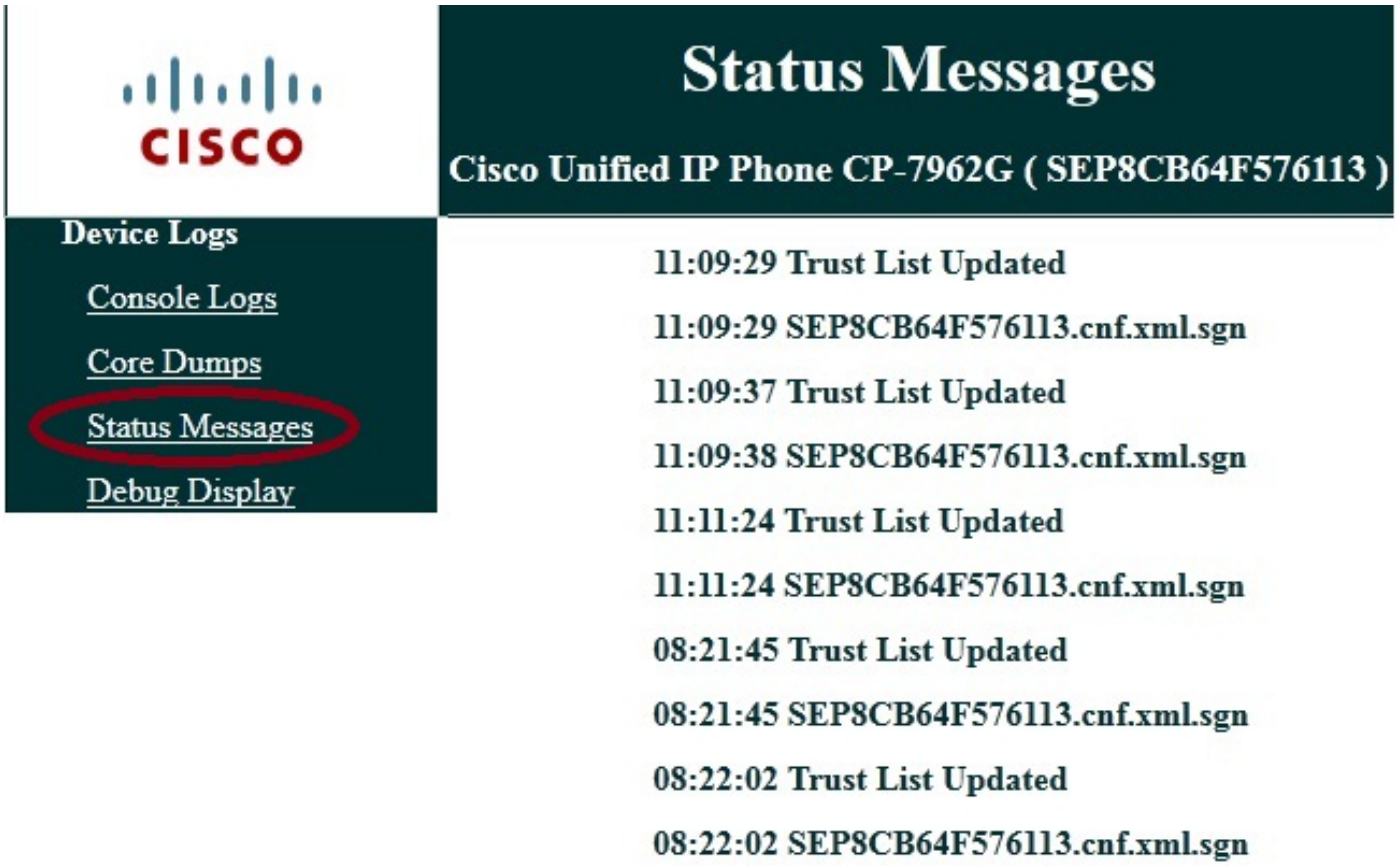
> **Note**: When the IP phone is in the remote side, it normally receives an IP address from an external DHCP server. For the IP phone to receive the new configuration from the CUCM, it should contact the TFTP server in the Main Office. Normally the CUCM is the same TFTP server.

In order to receive the configuration files with the changes, confirm that the IP address for the TFTP server is set up correctly in the network settings in the phone; for confirmation, use option 150 from the DHCP server or manually set the TFTP on the phone. This TFTP server is accessible through an AnyConnect session.

If the IP phone is receiving the TFTP server from a local DHCP server but that address is incorrect, you can use the alternate TFTP server option in order to override the TFTP server IP address provided by the DHCP server. This procedure describes how to apply the alternate TFTP server:

1. Navigate to **Settings** > **Network Configuration** > **IPv4 Configuration**.
2. Scroll to the Alternate TFTP option.
3. Press the Yes softkey for the phone to use an alternative TFTP server; otherwise, press the No softkey. If the option is locked, press * * # in order to unlock it.
4. Press the Save softkey.
5. Apply the Alternate TFTP Server under TFTP Server 1 option.

Review the status messages in the web browser or in the phone menus directly in order to confirm that the phone is receiving the correct information. If the communication is set up correctly, you see messages such as these:



If the phone is unable to retrieve the information from the TFTP server, you receive TFTP error messages:

Renewal of the ASA SSL Certificate

If you have a functional AnyConnect VPN phone setup but your ASA SSL certificate is about to expire, you do not need to bring all IP phones to the Main Site in order to inject the new SSL certificates to the phone; you can add the new certificates while the VPN is connected.

If you have exported or imported the Root CA certificate of the ASA instead of the Identity Certificate and if you want to continue to use the same Vendor (CA) during this renewal, it is not necessary to change the certificate in the CUCM because it remains the same. But, if you used the Identity Certificate, this procedure is necessary; otherwise, the hash value between the ASA and IP phone do not match, and the connection is not trusted by the phone.

1. Renew the certificate on the ASA.
   Note: For details, refer to ASA 8.x: Renew and Install the SSL Certificate with ASDM. Create a separate trustpoint and do not apply this new certificate with the **ssl trustpoint <name> outside** command until you have applied the certificate to all VPN IP phones.
2. Export the new certificate.
3. Import the new certificate to the CUCM as Phone-VPN-Trust certificate.
4. Navigate to the VPN Gateway Configuration in the CUCM, and apply the new certificate. You now have both certificates: the certificate that is about to expire and the new certificate that has not been applied to the ASA yet.
5. Apply this new configuration to the IP phone. Navigate to **Apply Config** > **Reset** > **Restart** in order to inject the new configuration changes to the IP phone through the VPN tunnel. Ensure that all the IP phones are connected through the VPN and that they can reach the TFTP server through the tunnel.
6. Use TFTP to check the status messages and the configuration file in order to confirm that the IP phone received the configuration file with the changes.
7. Apply the new SSL Trustpoint in the ASA, and replace the old certificate.

Note: If the ASA SSL certificate is already expired and if the IP phones are unable to connect through AnyConnect; you can push the changes (such as the new ASA certificate hash) to the IP phone. Manually set the TFTP in the IP phone to a public IP address so the IP phone can retrieve the information from there. Use a public TFTP server to host the configuration file; one example is to create a Port Forwarding on the ASA and redirect the traffic to the internal TFTP server.