# AnyConnect VPN Phone 문제 해결 - IP Phone, ASA 및 CUCM

## 목차



## 소개

이 문서에서는 VPN 게이트웨이로 사용되는 Cisco ASA(Adaptive Security Appliance)에 연결하고 음성 서버로 사용되는 Cisco CUCM(Unified Communications Manager)에 연결하기 위해 SSL(Secure Sockets Layer) 프로토콜(Cisco AnyConnect Secure Mobility Client)을 사용하는 IP 전화기의 문제를 해결하는 방법에 대해 설명합니다.

VPN 전화를 사용하는 AnyConnect의 컨피그레이션 예는 다음 문서를 참조하십시오.

- SSLVPN with IP Phones 컨피그레이션 예
- 인증서 인증 컨피그레이션이 있는 AnyConnect VPN Phone 예

# 배경 정보

IP 전화와 함께 SSL VPN을 구축하기 전에 ASA의 AnyConnect 라이센스 및 CUCM의 미국 수출 제한 버전에 대한 이러한 초기 요구 사항을 충족했는지 확인합니다.

## ASA에서 VPN Phone 라이센스 확인

VPN 전화 라이센스는 ASA에서 기능을 활성화합니다.AnyConnect에 연결할 수 있는 사용자 수(IP 전화인지 여부)를 확인하려면 AnyConnect Premium SSL 라이센스를 선택합니다.IP Phone 및 모바일 VPN 연결에 필요한 ASA 라이센스는 무엇입니까? 를 참조하십시오.자세한 내용을 확인하십시오.

ASA에서 **show version** 명령을 사용하여 기능이 활성화되었는지 확인합니다.라이센스 이름은 ASA 릴리스와 다릅니다.

- ASA 릴리스 8.0.x:라이센스 이름은 Linksys Phone용 AnyConnect입니다.
- ASA 릴리스 8.2.x 이상:라이센스 이름은 Cisco VPN Phone용 AnyConnect입니다.

다음은 ASA 릴리스 8.0.x의 예입니다.

```
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.
```

다음은 ASA 릴리스 8.2.x 이상의 예입니다.

```
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.
```

## 제한 및 무제한 CUCM 내보내기

VPN 전화기 기능을 위해 US 내보내기 제한 버전의 CUCM을 구축해야 합니다.

US 내보내기 무제한 버전의 CUCM을 사용하는 경우 다음 사항에 유의하십시오.

- 신호 및 미디어 암호화를 비활성화하기 위해 IP 전화 보안 컨피그레이션이 수정됩니다.여기에는 VPN 전화 기능에서 제공하는 암호화가 포함됩니다.
- Import/Export(가져오기/내보내기)를 통해 VPN 세부사항을 내보낼 수 없습니다.
- VPN 프로파일, VPN 게이트웨이, VPN 그룹 및 VPN 기능 컨피그레이션의 확인란이 표시되지 않습니다.

**참고:**미국 수출 제한 버전의 CUCM으로 업그레이드한 후에는 나중에 이 소프트웨어의 미국

수출 제한 버전으로 업그레이드하거나 새로 설치할 수 없습니다.

# ASA의 일반적인 문제

**참고:**Cisco CLI Analyzer(등록된 고객만)를 사용하여 **show** 명령 출력의 분석을 볼 수 있습니다.**debug** 명령을 사용하기 전에 Debug Commands Cisco 문서에 대한 중요 정보를 참조해야 합니다.

## ASA에서 사용할 인증서

ASA에서는 자체 서명 SSL 인증서, 서드파티 SSL 인증서 및 와일드카드 인증서를 사용할 수 있습니다.이 중 하나라도 IP 폰과 ASA 간의 통신을 보호합니다.

각 인터페이스에 하나의 인증서만 할당할 수 있으므로 ID 인증서는 하나만 사용할 수 있습니다.

서드파티 SSL 인증서의 경우 ASA에 전체 체인을 설치하고 중간 및 루트 인증서를 포함합니다.

## ASA 내보내기 및 CUCM 가져오기를 위한 신뢰 지점/인증서

SSL 협상 중에 ASA가 IP 전화에 제공하는 인증서는 ASA에서 내보낸 다음 CUCM으로 가져와야 합니다.ASA에서 어떤 인증서를 내보낼 것인지 알아보려면 IP 전화가 연결되는 인터페이스에 할당된 신뢰 지점을 확인하십시오.

내보낼 신뢰 지점(인증서)을 확인하려면 **show run ssl** 명령을 사용합니다.자세한 내용은 AnyConnect VPN Phone with Certificate Authentication Configuration Example을 참조하십시오.

**참고:**하나 이상의 ASA에 서드파티 인증서를 구축한 경우 각 ASA에서 각 ID 인증서를 내보낸 다음 CUCM에 phone-vpn-trust로 가져와야 합니다.

## ASA는 구성된 RSA 인증서 대신 ECDSA 자체 서명 인증서를 나타냅니다.

이 문제가 발생하면 최신 모델 폰에서 연결할 수 없지만 이전 모델 폰에서는 문제가 발생하지 않습니다.이 문제가 발생할 때 전화기의 로그는 다음과 같습니다.

```
VPNC: -protocol_handler: SSL dpd 30 sec from SG (enabled)
VPNC: -protocol_handler: connect: do_dtls_connect
VPNC: -do_dtls_connect: udp_connect
VPNC: -udp_connect: getsockname failed
VPNC: -udp_connect: binding sock to eth0 IP 63.85.30.39
VPNC: -udp_connect: getsockname failed
VPNC: -udp_connect: connecting to 63.85.30.34:443
VPNC: -udp_connect: connected to 63.85.30.34:443
VPNC: -do_dtls_connect: create_dtls_connection
VPNC: -create_dtls_connection: cipher list: AES256-SHA
VPNC: -create_dtls_connection: calling SSL_connect in non-block mode
VPNC: -dtls_state_cb: DTLS: SSL_connect: before/connect initialization
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 write client hello A
VPNC: -dtls_state_cb: DTLS: SSL_connect: DTLS1 read hello verify request A
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 write client hello A
VPNC: -dtls_state_cb: DTLS: SSL_connect: SSLv3 flush data
VPNC: -dtls_state_cb: DTLS: write: alert: fatal:illegal parameter
VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status: 0x0 error: 0x0
VPNC: -alert_err: DTLS write alert: code 47, illegal parameter
VPNC: -create_dtls_connection: SSL_connect ret -1, error 1
VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
VPNC: -DTLS: SSL_connect: error:140920C5:SSL routines:SSL3_GET_SERVER_HELLO:
old session cipher not returned VPNC: -create_dtls_connection: DTLS setup failure, cleanup VPNC:
-do_dtls_connect: create_dtls_connection failed VPNC: -protocol_handler: connect:
do_dtls_connect failed VPNC: -protocol_handler: connect : err: SSL success DTLS fail
```

버전 9.4.1 이상에서는 SSL/TLS에 대해 ELLIPTIC 커브 암호화가 지원됩니다.새 전화기 모델과 같은 타원 곡선 가능 SSL VPN 클라이언트가 ASA에 연결되면 ELLIPTIC 커브 암호 그룹이 협상되고, ASA는 RSA 기반 신뢰 지점으로 구성된 인터페이스에서도 SSL VPN 클라이언트에 ELLIPTIC 커브 인증서를 제공합니다.ASA가 자체 서명된 SSL 인증서를 제공하지 못하도록 하려면 관리자는 **ssl cipher** 명령을 통해 일치하는 암호 그룹을 제거해야 합니다.예를 들어, RSA 신뢰 지점으로 구성된 인터페이스의 경우 관리자는 RSA 기반 암호만 협상하도록 이 명령을 실행할 수 있습니다.

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

Cisco 버그 ID CSCuu02848을 구현하면 컨피그레이션에 우선 순위가 지정됩니다.명시적으로 구성된 인증서는 항상 사용됩니다.자체 서명 인증서는 구성된 인증서가 없는 경우에만 사용됩니다.

| 제안된 클라이언트 암호 | RSA 인증서 전용 | EC 인증서만 | 두 인증서 모두 | 없음 |
| --- | --- | --- | --- | --- |
| RSA 암호만 | RSA 인증서 사용<br>RSA 암호 사용 | RSA 자체 서명 인증서 사용<br>RSA 암호 사용 | RSA 인증서 사용<br>RSA 암호 사용 | RSA 자체 서명 인증<br>용<br>RSA 암호 사용 |
| EC 암호만 해당(드물게) | 연결 실패 | EC 인증서 사용<br>EC 암호 사용 | EC 인증서 사용<br>EC 암호 사용 | EC 자체 서명 인증서<br>EC 암호 사용 |
| 두 암호만 | RSA 인증서 사용<br>RSA 암호 사용 | EC 인증서 사용<br>EC 암호 사용 | EC 인증서 사용<br>EC 암호 사용 | EC 자체 서명 인증서<br>EC 암호 사용 |

## IP Phone 사용자 인증을 위한 외부 데이터베이스

외부 데이터베이스를 사용하여 IP 전화 사용자를 인증할 수 있습니다.LDAP(Lightweight Directory Access Protocol) 또는 RADIUS(Remote Authentication Dial In User Service)와 같은 프로토콜을 VPN 전화 사용자 인증에 사용할 수 있습니다.

## ASA 인증서와 VPN 전화 신뢰 목록 간의 인증서 해시 일치

ASA SSL 인터페이스에 할당된 인증서를 다운로드하고 CUCM에서 Phone-VPN-Trust 인증서로 업로드해야 합니다.다른 상황에서는 ASA에서 제공하는 이 인증서의 해시가 CUCM 서버가 생성하고 컨피그레이션 파일을 통해 VPN 전화기에 푸시되는 해시와 일치하지 않을 수 있습니다.

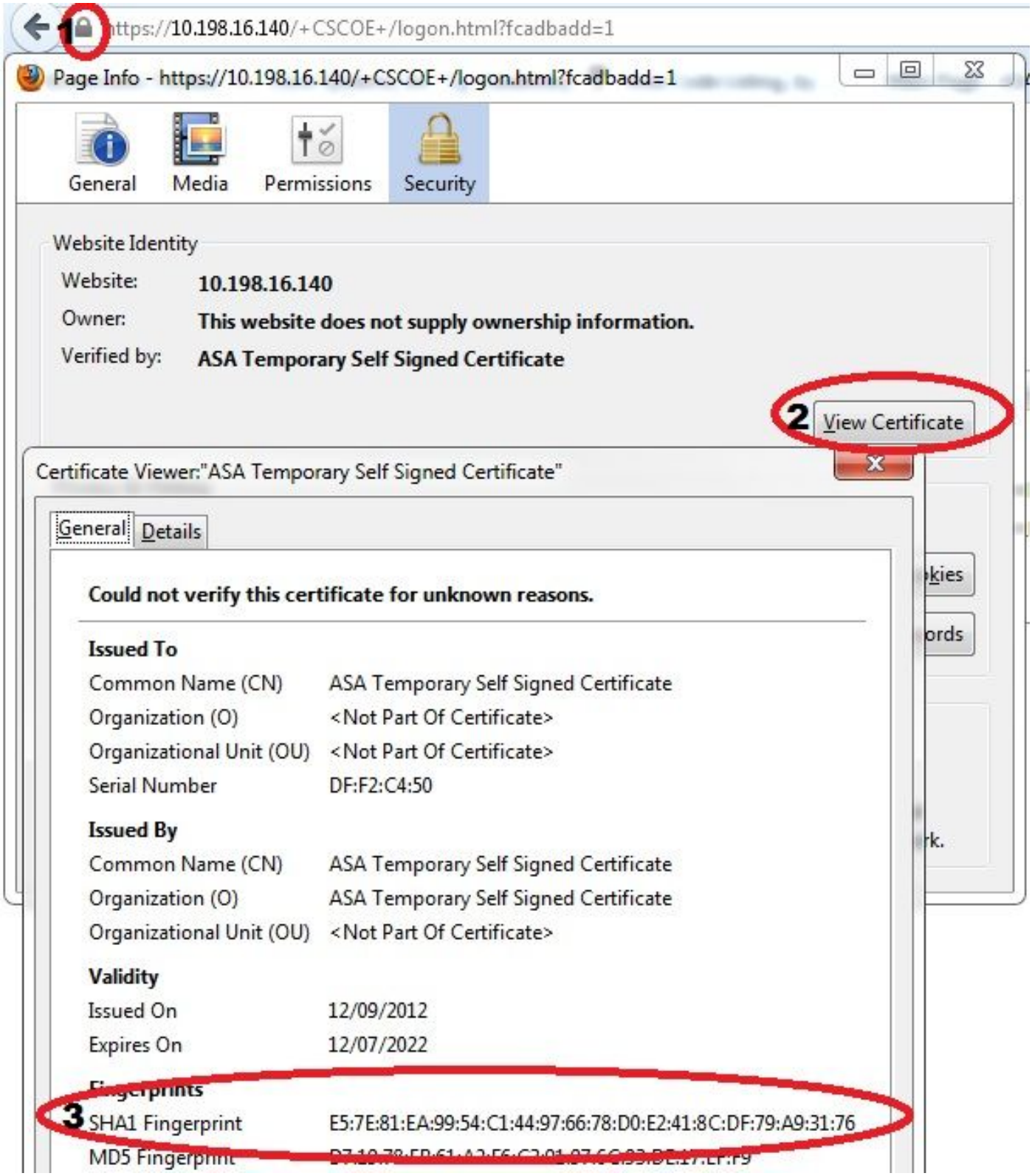
컨피그레이션이 완료되면 IP 전화기와 ASA 간의 VPN 연결을 테스트합니다.연결이 계속 실패할 경우 ASA 인증서의 해시가 IP 전화에서 기대하는 해시와 일치하는지 확인합니다.

1. ASA에서 제공하는 SHA1(Secure Hash Algorithm 1) 해시를 확인합니다.
2. CUCM에서 IP 전화 구성 파일을 다운로드하려면 TFTP를 사용합니다.
3. 16진수에서 16진수로 또는 기본 64에서 16진수로 해시를 디코딩합니다.

### SHA1 해시 확인

ASA는 IP Phone이 연결되는 인터페이스에서 **ssl trustpoint** 명령으로 적용된 인증서를 제공합니다.이 인증서를 확인하려면 브라우저(이 예에서는 Firefox)를 열고 전화기가 연결할 URL(group-url)을

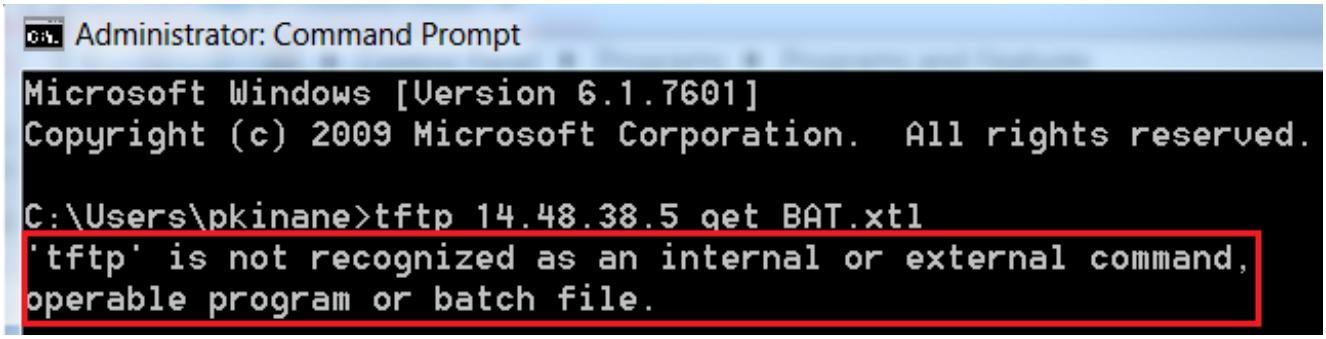
입력합니다.

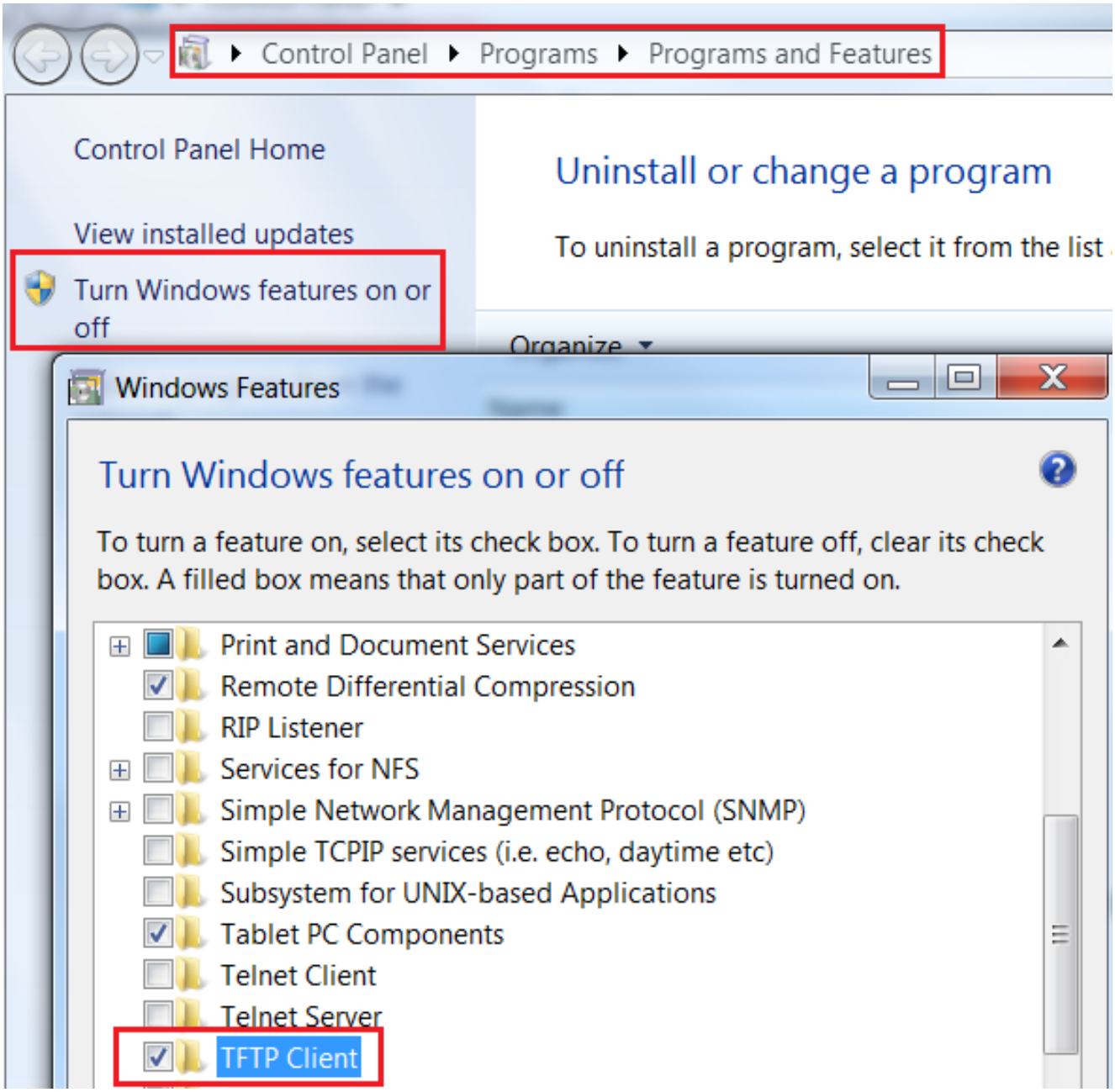



**IP Phone 구성 파일 다운로드**

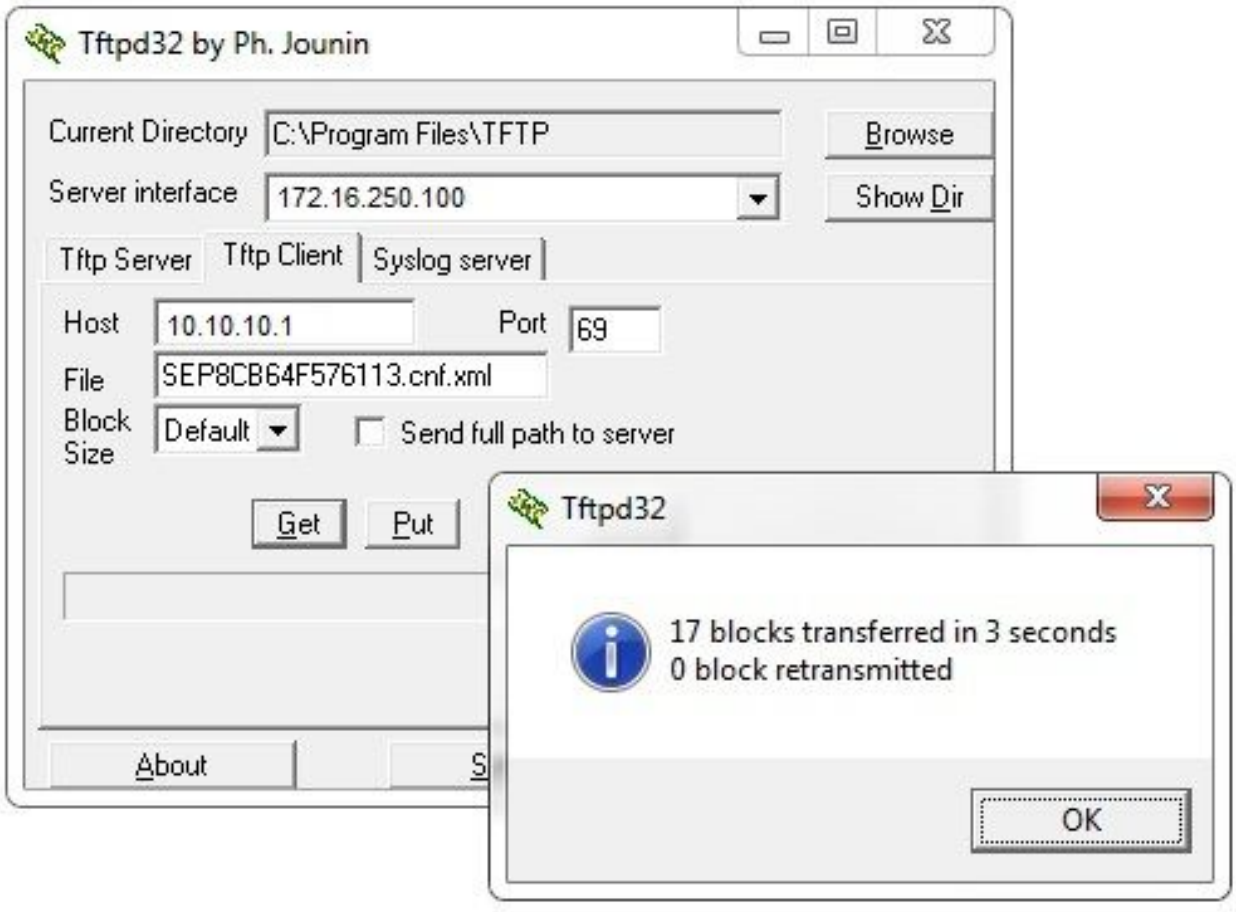
CUCM에 직접 액세스할 수 있는 PC에서 연결 문제가 있는 전화기의 TFTP 구성 파일을 다운로드합니다.두 가지 다운로드 방법은 다음과 같습니다.

1. Windows에서 CLI 세션을 열고 tftp **-i** <*TFTP Server*> **GET SEP**<*Phone Mac Address*>**.cnf.xml** 명령을 사용합니다.
   **참고:**아래 오류와 유사한 오류가 발생하면 TFTP 클라이언트 기능이 활성화되었는지 확인해야 합니다
   .






2. Tftpd32와 같은 응용 프로그램을 사용하여 파일을 다운로드합니다.

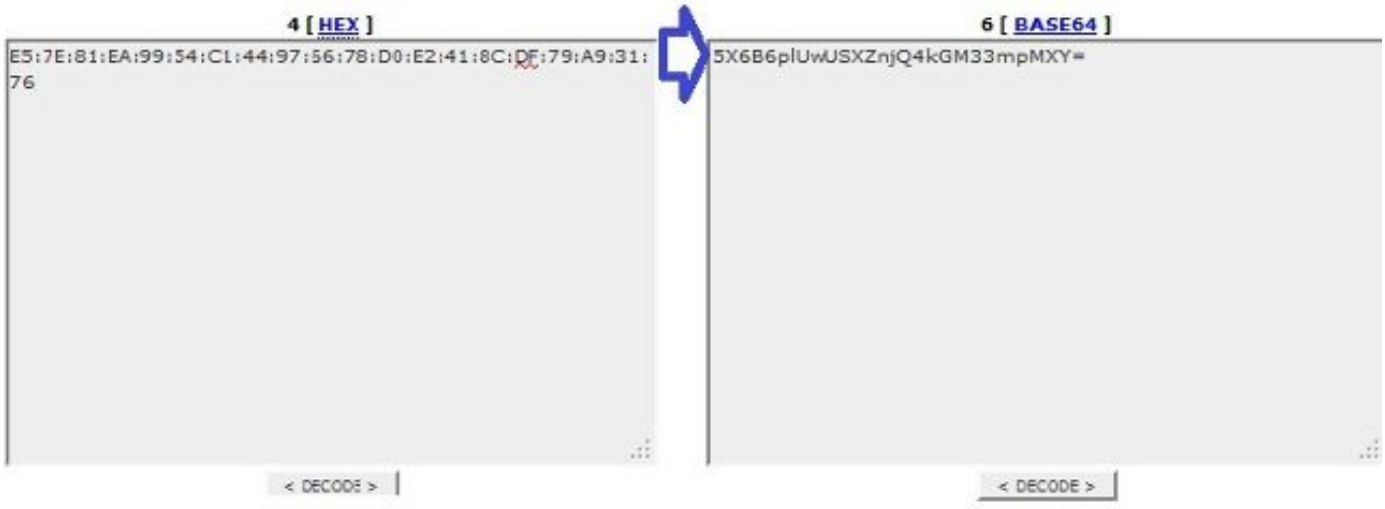



3. 파일이 다운로드되면 XML을 열고 vpnGroup 컨피그레이션을 *찾습니다*.다음 예에서는 확인할 섹션 및 *certHash*를 보여줍니다.

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




</credentials>
</vpnGroup>
```

## 해시 디코딩

두 해시 값이 모두 일치하는지 확인합니다.브라우저에서는 해시를 16진수 형식으로 표시하고 XML 파일은 base 64를 사용하므로 일치를 확인하기 위해 한 형식을 다른 형식으로 변환합니다.많은 번역가들이 있습니다.한 가지 예는 TRANSLATOR, BINARY입니다.




**참고:**이전 해시 값이 일치하지 않으면 VPN 전화기에서 ASA와 협상된 연결을 신뢰하지 않으며 연결이 실패합니다.

## VPN 로드 밸런싱 및 IP 전화

부하 분산 SSL VPN은 VPN 전화에 대해 지원되지 않습니다.VPN 전화기는 실제 인증서 검증을 수행하지 않고 CUCM에서 푸시된 해시를 사용하여 서버를 검증합니다.VPN 로드 밸런싱은 기본적으로 HTTP 리디렉션이므로 전화기가 여러 인증서의 유효성을 검사해야 하므로 오류가 발생합니다 .VPN 로드 밸런싱 실패의 증상은 다음과 같습니다.

- 이 전화는 서버 간에 번갈아 가며 연결되며 연결 시간이 매우 오래 걸리거나 결국 실패합니다.
- 전화 로그에는 다음과 같은 메시지가 포함됩니다.

```
909: NOT 20:59:50.051721 VPNC: do_login: got login response
910: NOT 20:59:50.052581 VPNC: process_login: HTTP/1.0 302 Temporary moved
911: NOT 20:59:50.053221 VPNC: process_login: login code: 302 (redirected)
912: NOT 20:59:50.053823 VPNC: process_login: redirection indicated
913: NOT 20:59:50.054441 VPNC: process_login: new 'Location':
/+webvpn+/index.html
914: NOT 20:59:50.055141 VPNC: set_redirect_url: new URL
<https://xyz1.abc.com:443/+webvpn+/index.html>
```

## CSD 및 IP 전화

현재 IP 전화는 Cisco CSD(Secure Desktop)를 지원하지 않으며 CSD가 터널 그룹에 대해 활성화되거나 ASA에서 전역적으로 활성화될 때 연결되지 않습니다.

먼저 ASA에서 CSD가 활성화되었는지 확인합니다.ASA CLI에서 **show run webvpn** 명령을 입력합니다.

```
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#
```

IP 전화 연결 중에 CSD 문제를 확인하려면 ASA에서 로그 또는 디버그를 확인합니다.

### ASA 로그

```
%ASA-4-724002: Group <VPNPhone> User <Phone> IP <172.6.250.9> WebVPN session not
terminated. Cisco Secure Desktop was not running on the client's workstation.
```

### ASA 디버그

```
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>
```

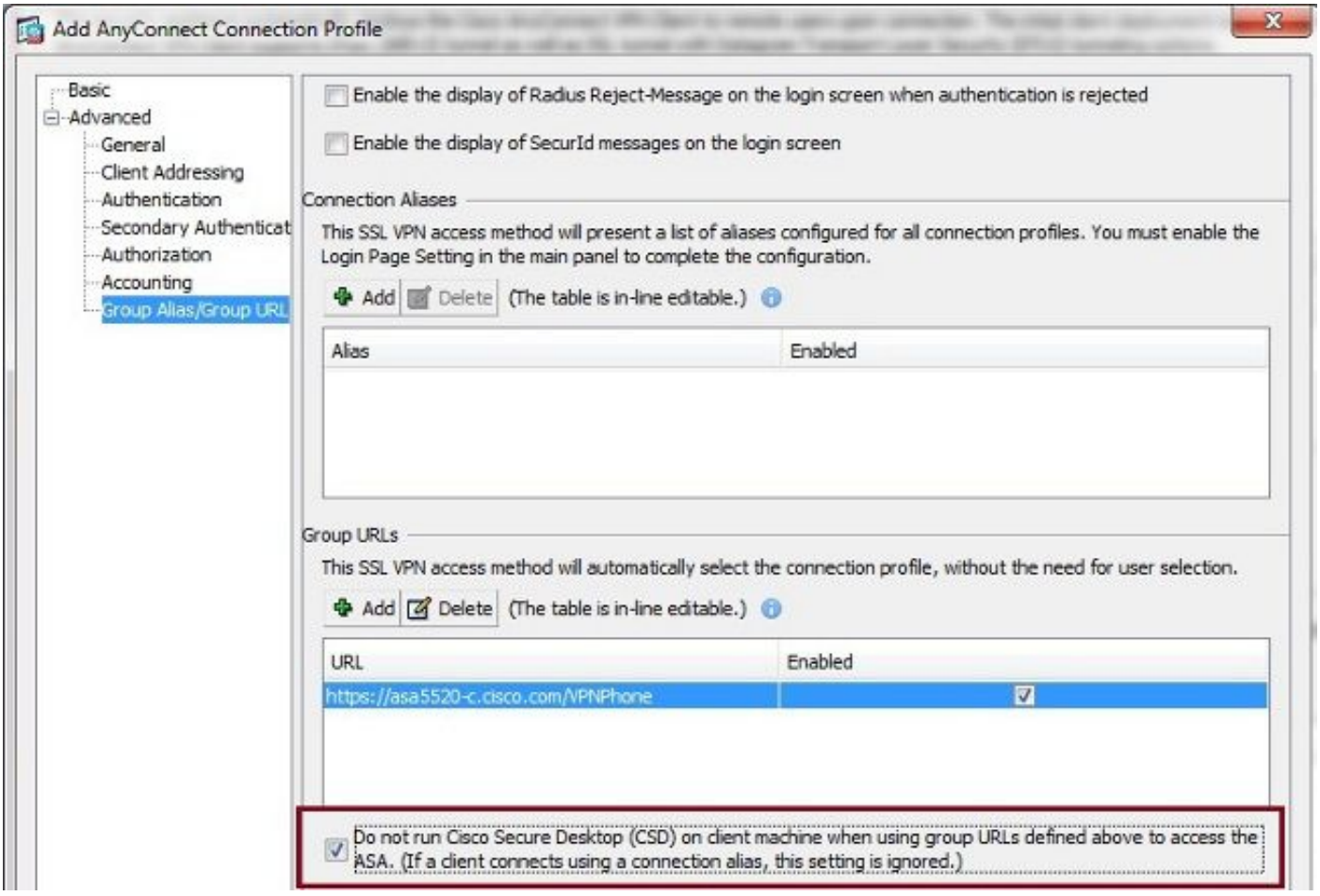
> **참고:**AnyConnect 사용자가 많은 대규모 구축에서는 debug webvpn anyconnect를 활성화하지 않는 것이 좋습니다.IP 주소로 출력을 필터링할 수 없으므로 많은 양의 정보가 생성될 수 있습니다.

ASA 버전 8.2 이상에서는 tunnel-group의 webvpn-attributes 아래에서 **without-csd** 명령을 적용해야 합니다.

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

이전 버전의 ASA에서는 이 방법이 불가능했기 때문에 유일한 해결 방법은 CSD를 전역적으로 비활성화하는 것이었습니다.

Cisco ASDM(Adaptive Security Device Manager)에서 다음 예와 같이 특정 연결 프로파일에 대해 CSD를 비활성화할 수 있습니다.

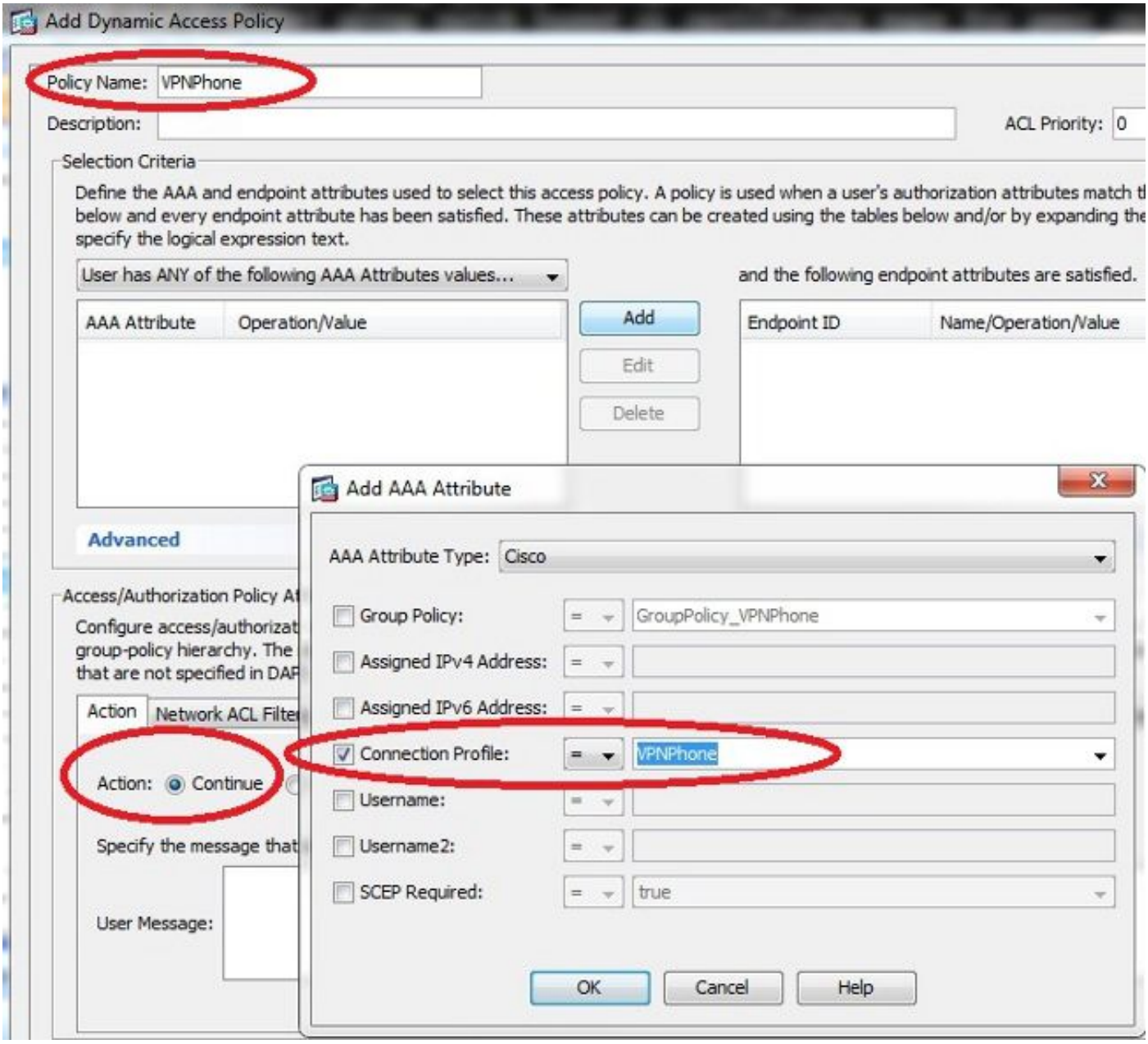



**참고:**CSD 기능을 끄려면 group-url을 사용합니다.

## DAP 규칙

대부분의 구축에서는 IP 전화기를 ASA에 연결할 뿐만 아니라 다양한 유형의 시스템(Microsoft, Linux, Mac OS) 및 모바일 디바이스(Android, iOS)를 연결합니다. 따라서 DAP(Dynamic Access Policy) 규칙의 기존 컨피그레이션을 찾는 것이 일반적입니다. 대부분의 경우 DfltAccessPolicy의 Default Action은 연결을 종료하는 것입니다.

이 경우 VPN 전화에 대해 별도의 DAP 규칙을 생성합니다.연결 프로파일과 같은 특정 매개변수를 사용하고 작업을 **계속**으로 설정합니다.



IP 전화에 대한 특정 DAP 정책을 생성하지 않을 경우 ASA는 DfltAccessPolicy 아래에 히트 및 실패한 연결을 표시합니다.

```
%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
```

작업이 Continue(계속)로 설정된 IP 전화에 대한 특정 DAP 정책을 만들면 다음을 연결할 수 있습니다.

```
%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
```

## DfltGrpPolicy 또는 기타 그룹에서 상속된 값

대부분의 경우 DfltGrpPolicy는 여러 옵션으로 설정됩니다.기본적으로 이러한 설정은 IP Phone에서 사용해야 하는 그룹 정책에 수동으로 지정되지 않는 한 IP Phone 세션에 대해 상속됩니다.

DfltGrpPolicy에서 상속된 경우 연결에 영향을 줄 수 있는 일부 매개 변수는 다음과 같습니다.

- 그룹 잠금
- vpn-tunnel-protocol
- vpn-simultaneous-logins
- vpn-filter

DfltGrpPolicy 및 GroupPolicy_VPNPhone에 이 컨피그레이션이 있다고 가정합니다.

```
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
```

연결은 GroupPolicy_VPNPhone에 명시적으로 지정되지 않은 DfltGrpPolicy에서 매개 변수를 상속하고 연결 중에 모든 정보를 IP 전화기에 푸시합니다.

이를 방지하려면 그룹에서 직접 필요한 값을 수동으로 지정합니다.

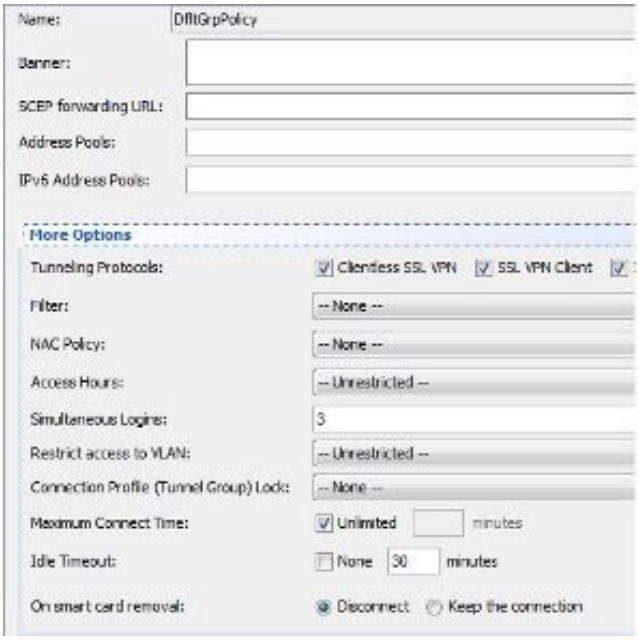
```
group-policy GroupPolicy_VPNPhone internal
group-policy GroupPolicy_VPNPhone attributes
wins-server none
dns-server value 10.198.29.20
 vpn-simultaneous-logins 3
vpn-tunnel-protocol ssl-client
group-lock value VPNPhone
 vpn-filter none
 default-domain value cisco.com
```

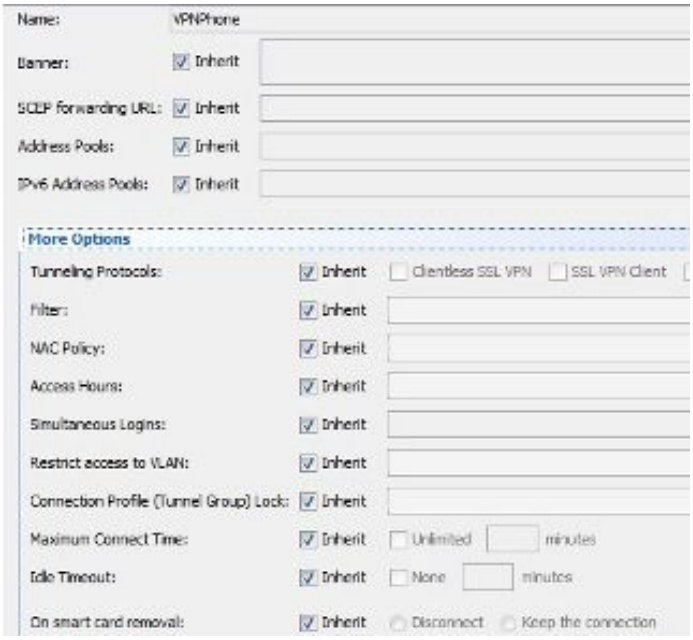
DfltGrpPolicy의 기본값을 확인하려면 **show run all group-policy** 명령을 사용합니다.이 예에서는 출력 간의 차이를 설명합니다.

```
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
```

다음은 ASDM을 통해 특성을 상속 받는 그룹 정책의 출력입니다.




## 지원되는 암호화 암호

7962G IP 전화 및 펌웨어 버전 9.1.1에서 테스트한 AnyConnect VPN 전화기는 두 개의 암호만 지원하며, 이는 모두 AES(Advanced Encryption Standard)입니다.AES256-SHA 및 AES128-SHA.ASA에 올바른 암호를 지정하지 않으면 ASA 로그에 표시된 대로 연결이 거부됩니다.

```
%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
```

ASA에 올바른 암호가 활성화되었는지 확인하려면 show run all ssl **및 show ssl** 명령을 **입력합니다**.

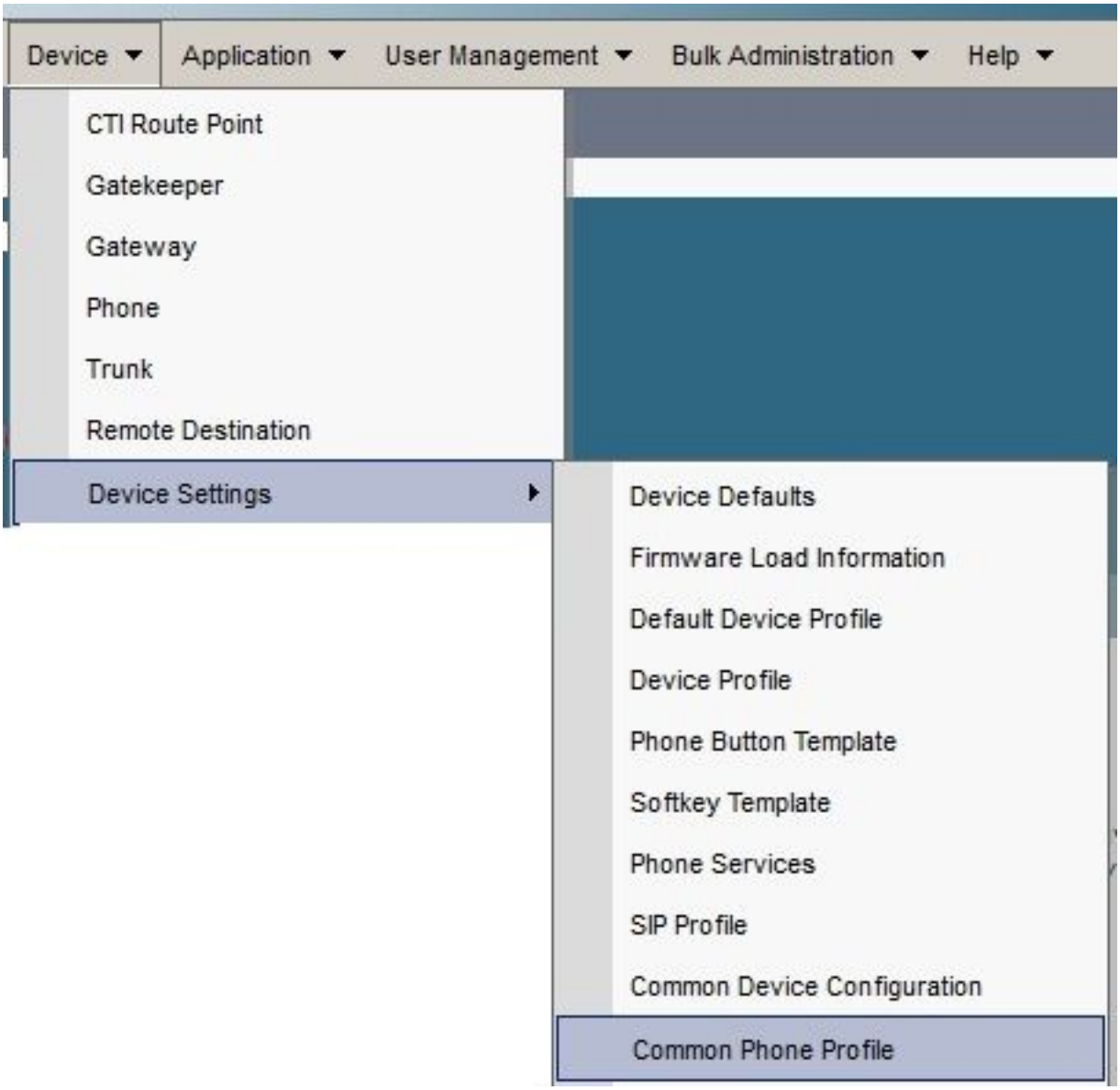
```
ASA5510-F# show run all ssl
ssl server-version any
ssl client-version any
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point SSL outside
ASA5510-F#

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#
```

# CUCM의 공통 문제

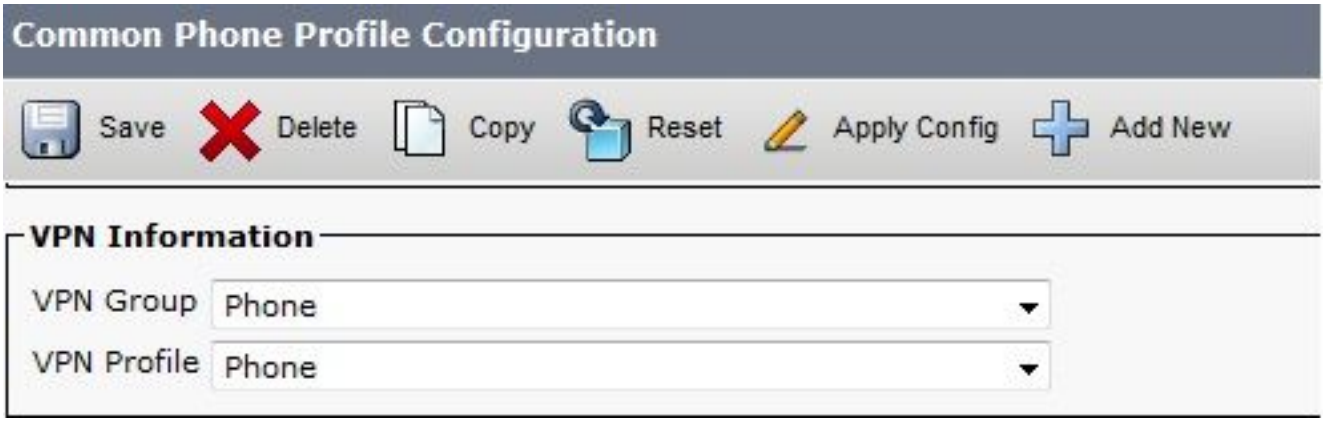
## IP 전화기에 적용되지 않는 VPN 설정

CUCM의 컨피그레이션(게이트웨이, 그룹 및 프로파일)이 생성되면 Common Phone Profile(일반 전화기 프로파일)에서 VPN 설정을 적용합니다.

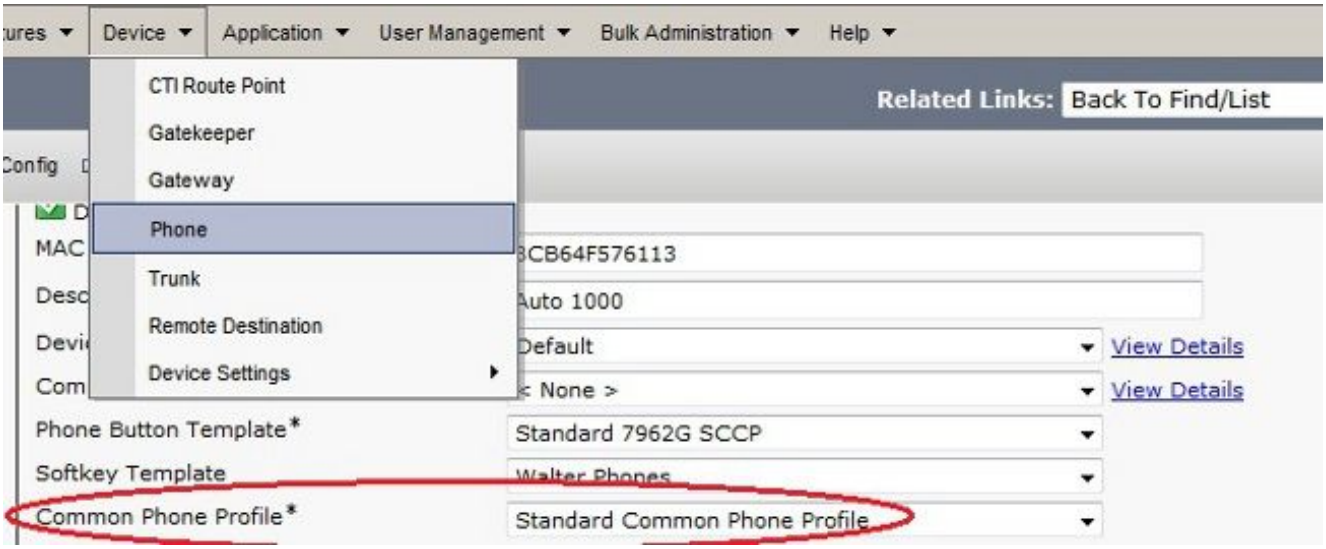
1. Device(**디바이스**) > Device Settings(디바이스 **설정**) > Common Phone **Profile(공통 전화기 프로파일)으로 이동합니다**.




2. VPN 정보를 입력합니다.




3. Device(**디바이스**) > **Phone(전화기)**으로 이동하여 이 프로파일이 전화기 컨피그레이션에 할당되었는지 확인합니다.



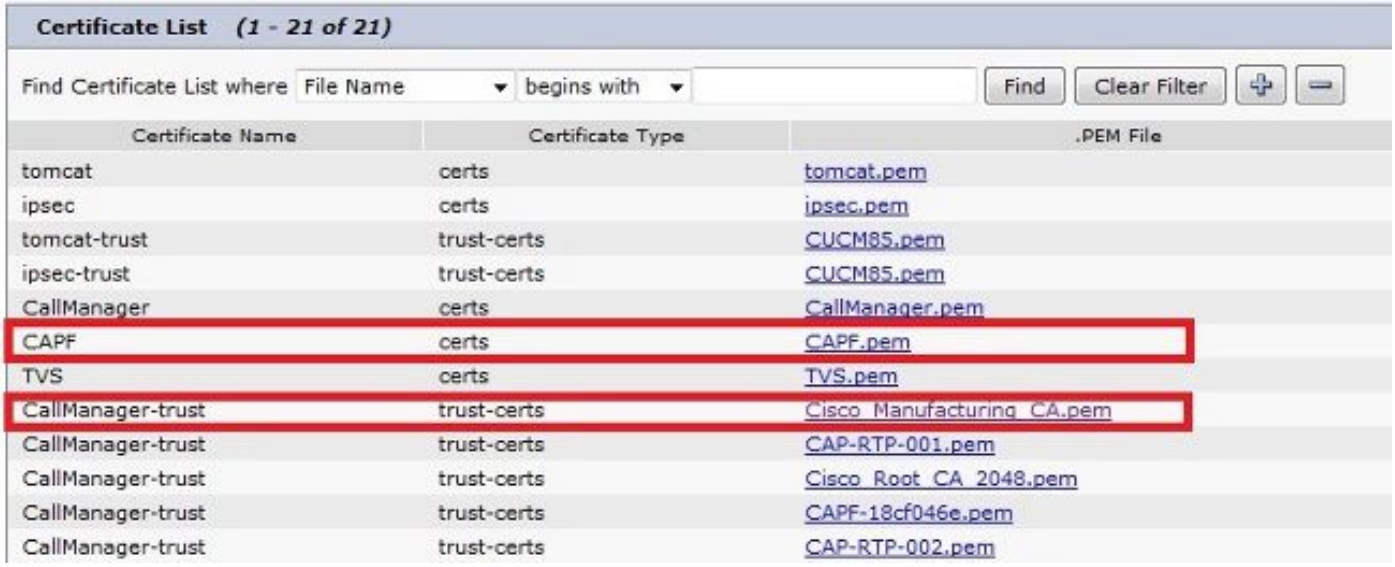

## 인증서 인증 방법

IP 전화에 대한 인증서 인증을 구성하는 방법에는 두 가지가 있습니다.MIC(Manufacturer Installed Certificate) 및 LSC(Locally Significant Certificate). 상황에 가장 적합한 옵션을 선택하려면 AnyConnect VPN Phone with Certificate Authentication Configuration Example(인증서 인증 컨피그레이션이 있는 AnyConnect VPN Phone)을 참조하십시오.

인증서 인증을 구성할 때 CUCM 서버에서 인증서(루트 CA)를 내보내고 ASA로 가져옵니다.

1. CUCM에 로그인합니다.
2. Unified **OS Administration > Security > Certificate Management로 이동합니다**.
3. CAPF(Certificate Authority Proxy Function) 또는 Cisco_Manufacturing_CA;인증서 유형은 MIC 또는 LSC 인증서 인증을 사용했는지에 따라 달라집니다.
4. 파일을 로컬 컴퓨터에 다운로드합니다.

파일이 다운로드되면 CLI 또는 ASDM을 통해 ASA에 로그인하고 인증서를 CA 인증서로 가져옵니다.



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 |

기본적으로 VPN을 지원하는 모든 전화기에 MIC가 사전 로드됩니다.7960 및 7940 모델 전화에는 MIC가 제공되지 않으며 LSC가 안전하게 등록되도록 특수 설치 절차가 필요합니다.

최신 Cisco IP Phone(8811, 8841, 8851 및 8861)에는 새로운 Manufacturing SHA2 CA에서 서명한 MIC 인증서가 포함됩니다.

- CUCM 버전 10.5(1)는 새 SHA2 인증서를 포함하고 신뢰합니다.
- 이전 CUCM 버전을 실행하는 경우 새 제조 CA 인증서를 다운로드하고 다음을 수행해야 할 수 있습니다.

  CAPF-trust에 업로드하여 전화기가 CAPF로 인증하여 LSC를 얻을 수 있도록 합니다.

  전화기가 SIP 5061용 MIC로 인증하도록 허용하려면 CallManager-trust에 업로드합니다.

  **팁**:CUCM이 현재 이전 버전을 실행하는 경우 SHA2 CA를 얻으려면 이 링크를 클릭합니다.

  **주의:**LSC 설치에만 MIC를 사용하는 것이 좋습니다.Cisco는 CUCM과의 TLS 연결 인증을 위해 LSC를 지원합니다.MIC 루트 인증서가 손상될 수 있으므로 TLS 인증 또는 다른 용도로 MIC를 사용하도록 전화기를 구성하는 고객은 위험을 감수해야 합니다.Cisco는 MIC가 손상된 경우 어떠한 책임도 지지 않습니다.

기본적으로 전화기에 LSC가 있는 경우 전화기에 MIC가 있는지 여부와 상관없이 인증에서는 LSC를 사용합니다.전화기에 MIC 및 LSC가 있는 경우 인증에서는 LSC를 사용합니다.전화기에

LSC가 없지만 MIC가 있는 경우 인증에서는 MIC를 사용합니다.

**참고:**인증서 인증의 경우 ASA에서 SSL 인증서를 내보내고 CUCM으로 가져와야 합니다.

## 호스트 ID 확인

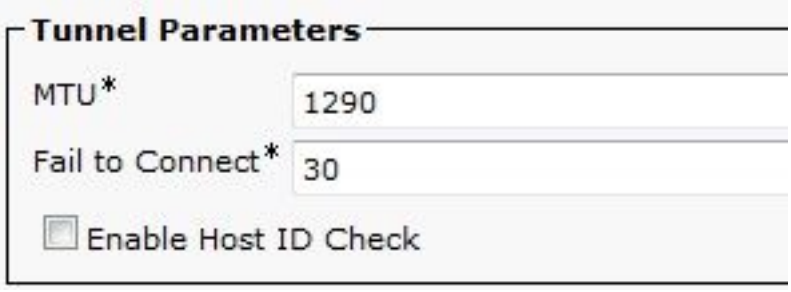
인증서의 제목에 있는 CN(common name)이 VPN을 통해 ASA에 연결하기 위해 전화기에서 사용하는 URL(group-url)과 일치하지 않을 경우, CUCM에서 Host ID Check(호스트 ID 확인)을 비활성화하거나 ASA의 해당 URL과 일치하는 ASA의 인증서를 사용합니다.

ASA의 SSL 인증서가 와일드카드 인증서이거나, SSL 인증서에 다른 SAN(Subject Alternative Name)이 포함되어 있거나, FQDN(Fully Qualified Domain Name) 대신 IP 주소로 URL이 생성된 경우 이 작업이 필요합니다.

이것은 인증서의 CN이 전화기가 연결하려는 URL과 일치하지 않을 때 IP 전화 로그의 예입니다.

```
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!!
```

CUCM에서 Host ID Check(호스트 ID 확인)를 비활성화하려면 Advanced Features(**고급 기능**) > **VPN > VPN Profile(VPN 프로파일)으로** 이동합니다.



# 추가 문제 해결

## ASA에서 사용할 로그 및 디버그

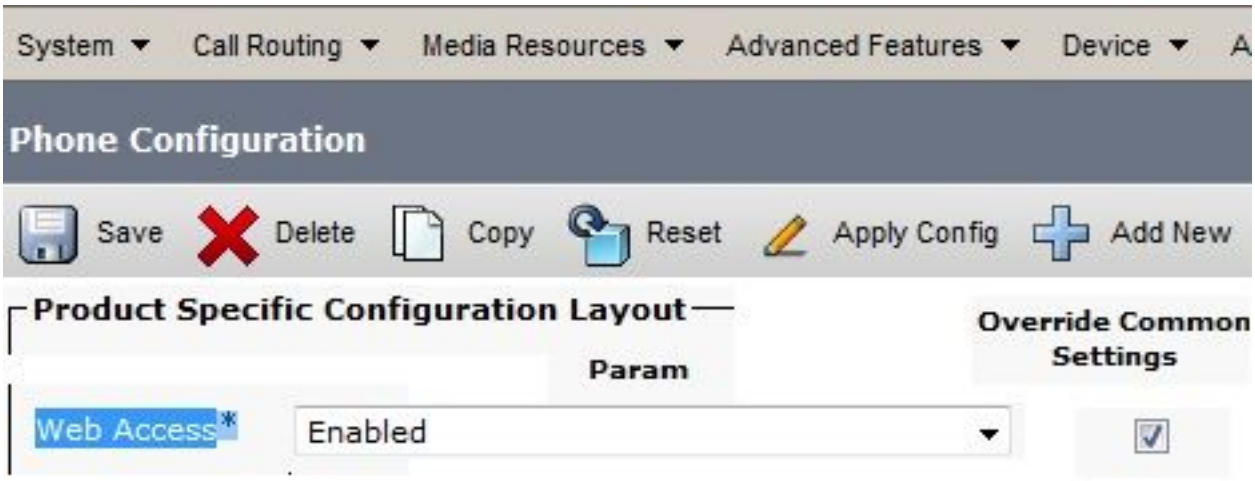
ASA에서 문제 해결을 위해 이러한 디버깅 및 로그를 활성화할 수 있습니다.

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

debug webvpn anyconnect 255
```

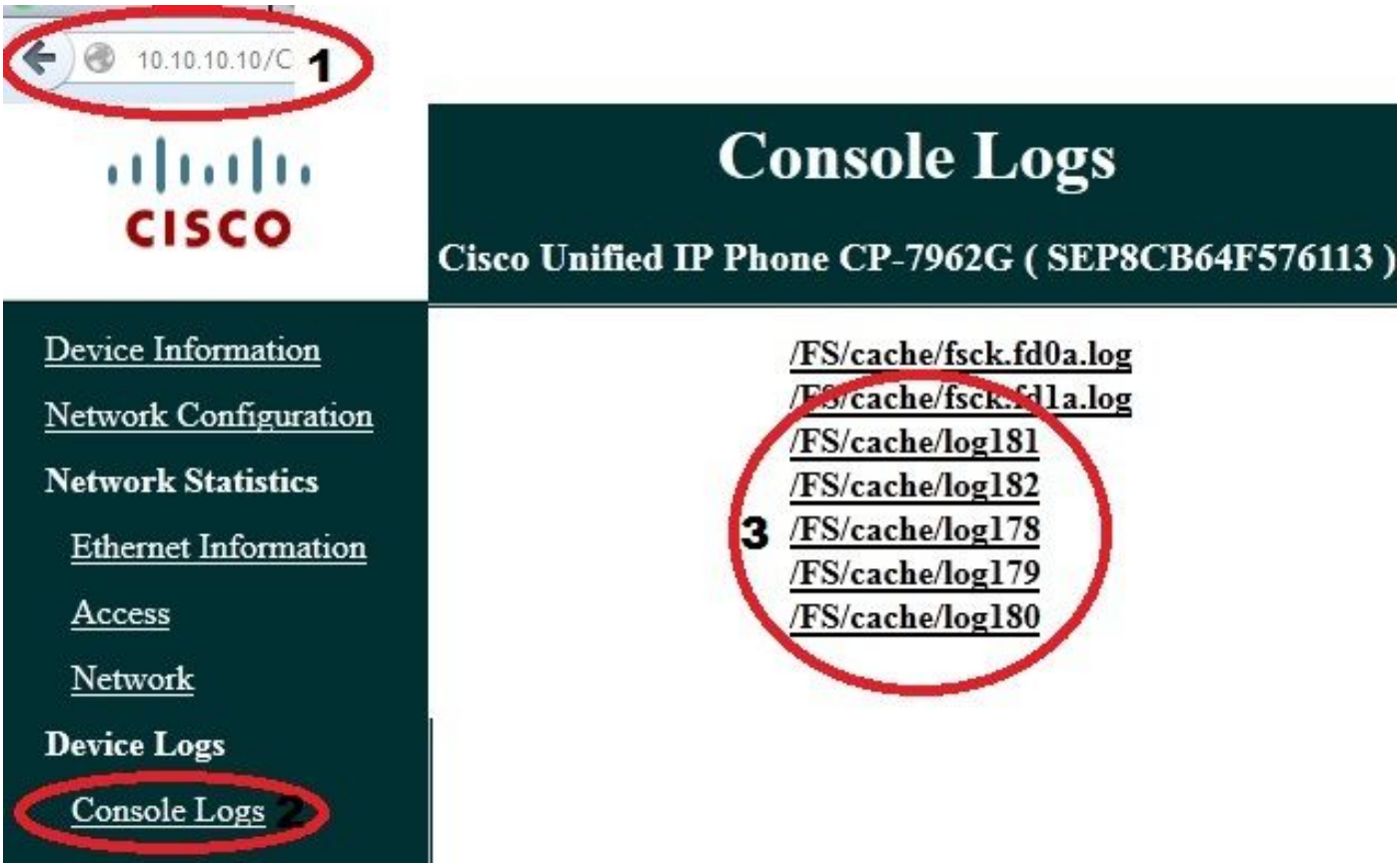
> **참고:**AnyConnect 사용자가 많은 대규모 구축에서는 디버그 webvpn anyconnect를 활성화하지 않는 것이 **좋습니다**.IP 주소로 출력을 필터링할 수 없으므로 많은 양의 정보가 생성될 수 있습니다.

## IP 전화 로그

전화 로그에 액세스하려면 웹 액세스 기능을 활성화합니다.CUCM에 로그인하고 Device(디바이스) > **Phone(전화기) > Phone(전화기 컨피그레이션)으로 이동합니다**.이 기능을 활성화할 IP 전화기를 찾아 웹 액세스 섹션을 찾습니다.IP 전화에 컨피그레이션 변경 사항을 적용합니다.



서비스를 활성화하고 이 새 기능을 삽입하기 위해 전화기를 재설정하면 브라우저에서 IP 전화 로그에 액세스할 수 있습니다.해당 서브넷에 액세스할 수 있는 컴퓨터에서 전화기의 IP 주소를 사용합니다.콘솔 로그로 이동하여 5개의 로그 파일을 확인합니다.전화기에서 5개의 파일을 덮어쓰므로 원하는 정보를 찾으려면 이러한 모든 파일을 확인해야 합니다.




## ASA 로그와 IP Phone 로그 간의 상관관계 문제

다음은 ASA와 IP 전화에서 로그를 상호 연결하는 방법의 예입니다.이 예에서는 ASA의 인증서가 다른 인증서로 대체되었기 때문에 ASA의 인증서 해시가 전화기의 컨피그레이션 파일에 있는 인증서의 해시와 일치하지 않습니다.

### ASA 로그

```
%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

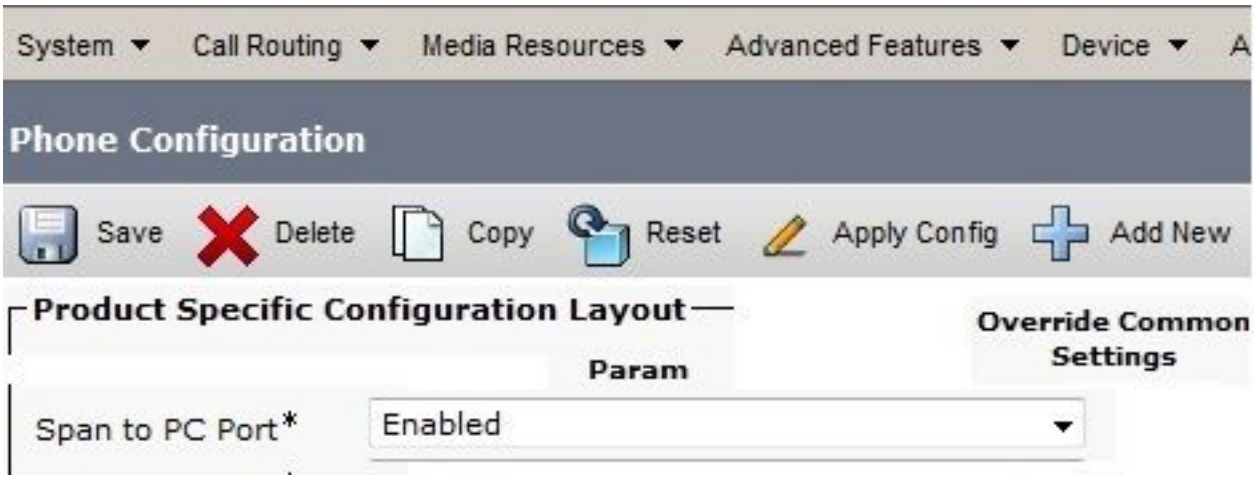
### 전화 로그

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

## PC 포트 범위 기능

컴퓨터를 전화기에 직접 연결할 수 있습니다.전화기의 후면 평면에 스위치 포트가 있습니다.

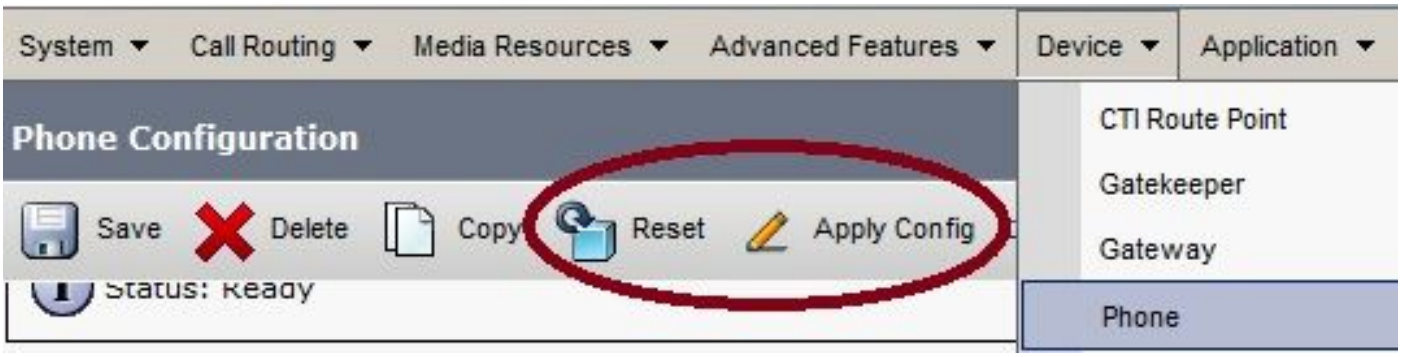
이전에 구성한 대로 전화기를 구성하고, CUCM에서 PC Port에 Span to PC Port를 활성화하고 컨피그레이션을 적용합니다.전화기가 각 프레임의 복사본을 PC에 보내기 시작합니다.분석을 위해 트래픽을 캡처하려면 프로미스큐어스 모드에서 Wireshark를 사용합니다.




## VPN에 의해 연결된 동안 IP Phone 컨피그레이션 변경

일반적인 질문은 AnyConnect를 통해 IP 전화가 네트워크에서 연결되어 있는 동안 VPN 컨피그레이션을 수정할 수 있는지 여부입니다.대답은 yes이지만 일부 컨피그레이션 설정을 확인해야 합니다.

CUCM에서 필요한 사항을 변경한 다음 변경 사항을 전화기에 적용합니다.새 컨피그레이션을 전화기에 푸시하기 위한 세 가지 옵션(Apply Config, Reset, Restart)이 있습니다.3가지 옵션 모두 전화와 ASA에서 VPN의 연결을 끊지만 인증서 인증을 사용하는 경우 자동으로 다시 연결할 수 있습니다.AAA(Authentication, Authorization, and Accounting)를 사용하는 경우 자격 증명을 다시 입력하라는 메시지가 표시됩니다.



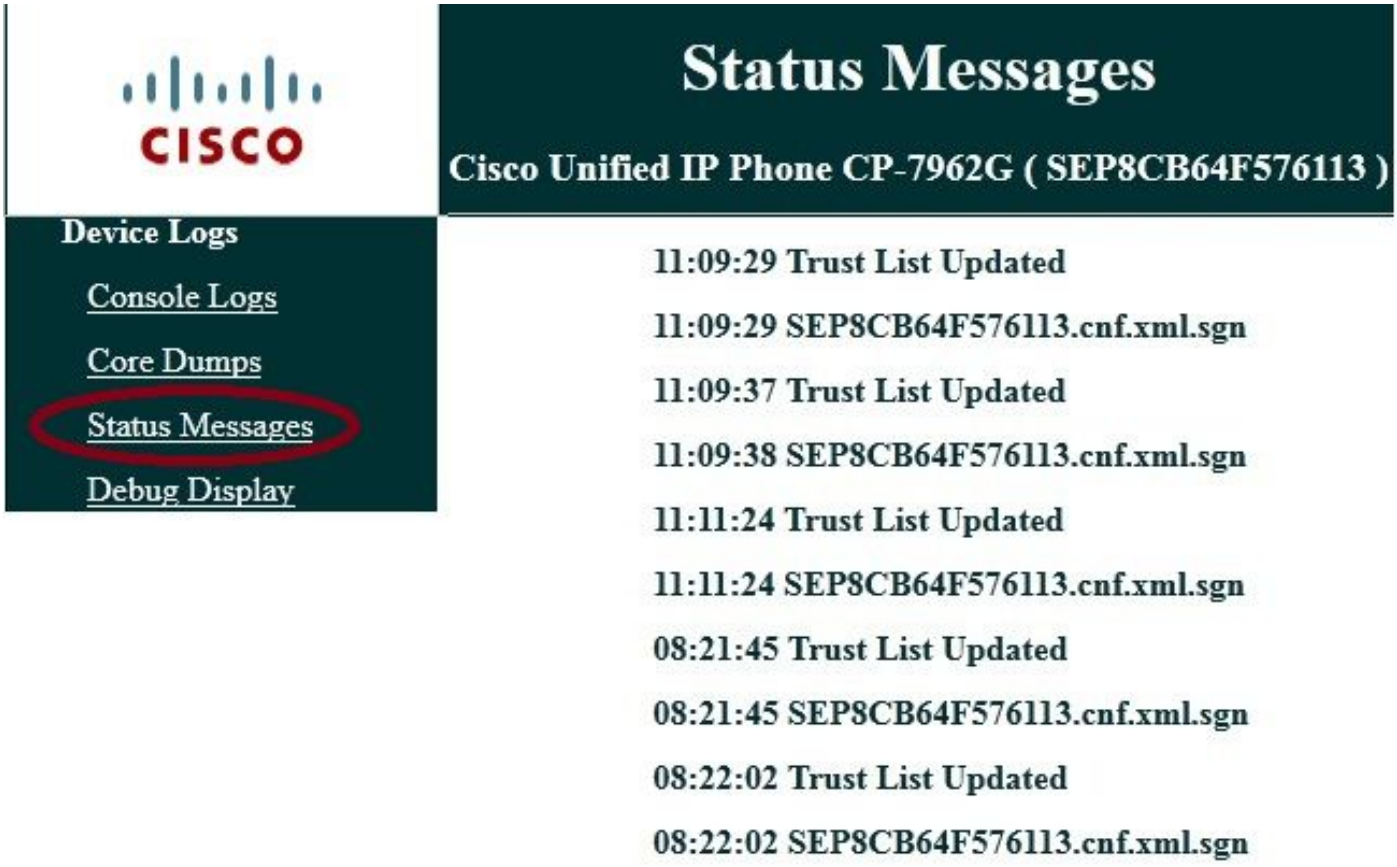

**참고:**IP 전화기가 원격 쪽에 있으면 일반적으로 외부 DHCP 서버로부터 IP 주소를 받습니다.IP 전화기에서 CUCM에서 새 컨피그레이션을 받으려면 Main Office의 TFTP 서버에 연결해야 합니다.일반적으로 CUCM은 동일한 TFTP 서버입니다.

변경 사항과 함께 컨피그레이션 파일을 수신하려면 전화기의 네트워크 설정에서 TFTP 서버의 IP 주소가 올바르게 설정되었는지 확인합니다.확인을 위해 DHCP 서버에서 옵션 150을 사용하거나 전화기에서 TFTP를 수동으로 설정합니다.이 TFTP 서버는 AnyConnect 세션을 통해 액세스할 수 있습니다.

IP 전화기에서 로컬 DHCP 서버로부터 TFTP 서버를 수신하지만 해당 주소가 잘못된 경우, DHCP 서버에서 제공하는 TFTP 서버 IP 주소를 재정의하려면 대체 TFTP 서버 옵션을 사용할 수 있습니다.다음 절차에서는 대체 TFTP 서버를 적용하는 방법에 대해 설명합니다.

1. Settings(**설정**) > Network Configuration(**네트워크 컨피그레이션**) > IPv**4 Configuration(IPv4 컨피그레이션)으로 이동합니다**.
2. Alternate TFTP 옵션으로 스크롤합니다.
3. 전화기에서 대체 TFTP 서버를 사용하려면 Yes(예) 소프트키를 누릅니다.그렇지 않으면 No(아니요) 소프트키를 누릅니다.옵션이 잠겨 있는 경우 * * #을 눌러 잠금을 해제합니다.
4. 저장 소프트키를 누릅니다.
5. TFTP Server 1 옵션에서 Alternate TFTP Server를 적용합니다.

웹 브라우저 또는 전화기 메뉴에서 상태 메시지를 직접 검토하여 전화기가 올바른 정보를 수신하고 있는지 확인합니다.통신이 올바르게 설정되면 다음과 같은 메시지가 표시됩니다.




전화기에서 TFTP 서버에서 정보를 검색할 수 없는 경우 TFTP 오류 메시지가 표시됩니다.


## ASA SSL 인증서 갱신

기능적 AnyConnect VPN 전화 설정이 있지만 ASA SSL 인증서가 곧 만료될 예정인 경우 전화기에 새 SSL 인증서를 삽입하기 위해 모든 IP 전화기를 기본 사이트로 가져올 필요가 없습니다.VPN이 연결된 동안 새 인증서를 추가할 수 있습니다.

ASA의 루트 CA 인증서를 ID 인증서 대신 내보내거나 가져온 경우 이 갱신 중에 동일한 벤더(CA)를 계속 사용하려면 CUCM에서 인증서가 동일하게 유지되므로 인증서를 변경할 필요가 없습니다.그러나 ID 인증서를 사용한 경우 이 절차가 필요합니다.그렇지 않으면 ASA와 IP 전화 간의 해시 값이 일치하지 않으며 전화기에서 연결을 신뢰할 수 없습니다.

1. ASA에서 인증서를 갱신합니다.
   **참고:**자세한 내용은 ASA 8.x:ASDM을 사용하여 SSL 인증서를 갱신하고 설치합니다.별도의 신뢰 지점을 생성하고 모든 VPN IP 전화에 인증서를 적용할 때까지 **ssl trustpoint <name> outside** 명령을 사용하여 이 새 인증서를 적용하지 마십시오.

2. 새 인증서를 내보냅니다.

3. CUCM에 Phone-VPN-Trust 인증서로 새 인증서를 가져옵니다.
   **참고:**Phone-VPN-trust에서 **동일한 CN으로 인증서를 업로드하면 이전 인증서를 덮어쓰게 됩니다.**
4. CUCM에서 VPN Gateway Configuration(VPN 게이트웨이 컨피그레이션)으로 이동하여 새 인증서를 적용합니다.이제 두 인증서가 모두 있습니다.곧 만료될 인증서와 ASA에 아직 적용되지 않은 새 인증서.

5. 이 새 컨피그레이션을 IP 전화기에 적용합니다.VPN 터널을 통해 IP 전화에 새 컨피그레이션 변경 사항을 삽입하려면 Apply Config > Reset > Restart로 이동합니다.모든 IP 전화기가 VPN을 통해 연결되어 있고 터널을 통해 TFTP 서버에 연결할 수 있는지 확인합니다.

6. TFTP를 사용하여 상태 메시지 및 컨피그레이션 파일을 확인하여 IP Phone이 변경 사항과 함께 컨피그레이션 파일을 받았는지 확인합니다.

7. ASA에 새 SSL 신뢰 지점을 적용하고 이전 인증서를 교체합니다.

**참고:**ASA SSL 인증서가 이미 만료되었고 IP 전화가 AnyConnect를 통해 연결할 수 없는 경우 변경 사항(예: 새 ASA 인증서 해시)을 IP 전화기에 푸시할 수 있습니다.IP 전화기에서 정보를 검색할 수 있도록 IP 전화기의 TFTP를 공용 IP 주소로 수동으로 설정합니다.공용 TFTP 서버를 사용하여 컨피그레이션 파일을 호스팅합니다.한 가지 예는 ASA에서 포트 전달을 생성하고 트래픽을 내부 TFTP 서버로 리디렉션하는 것입니다.