

# ASA에서 인증서 인증을 사용하여 AnyConnect VPN Phone 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[전화 인증서 유형](#)

[구성](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 Cisco IP Phone에서 실행되는 AnyConnect 클라이언트에 인증서 인증을 제공하도록 ASA(Adaptive Security Appliance) 및 CallManager 디바이스를 구성하는 방법을 보여 주는 샘플 컨피그레이션을 제공합니다. 이 컨피그레이션이 완료되면 Cisco IP Phone은 통신을 보호하기 위해 인증서를 사용하는 ASA에 VPN 연결을 설정할 수 있습니다.

## 사전 요구 사항

### 요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- AnyConnect Premium SSL 라이선스
- Cisco VPN Phone 라이선스용 AnyConnect

ASA 버전에 따라 ASA 릴리스 8.0.x의 경우 "AnyConnect for Linksys phone" 또는 ASA 릴리스 8.2.x 이상의 경우 "AnyConnect for Cisco VPN Phone"이 표시됩니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ASA - 릴리스 8.0(4) 이상
  - IP Phone 모델 - 7942/7962/7945/7965/7975
  - 전화 - 8961/9951/9971(릴리스 9.1(1) 펌웨어 포함)
  - 전화 - 릴리스 9.0(2)SR1S - SCCP(Skinny Call Control Protocol) 이상
  - Cisco CUCM(Unified Communications Manager) - 릴리스 8.0.1.10000-4 이상
- 이 컨피그레이션 예에 사용된 릴리스에는 다음이 포함됩니다.

- ASA - 릴리스 9.1(1)
- CallManager - 릴리스 8.5.1.10000-26

CUCM 버전에서 지원되는 전화기의 전체 목록을 보려면 다음 단계를 완료하십시오.

1. 다음 URL을 엽니다.<https://<CUCM 서버 IP 주소>:8443/cucreports/systemReports.do>
2. Unified CM Phone Feature List(Unified CM 전화기 기능 목록) > Generate a new report(새 보고서 생성) > Feature(기능)를 선택합니다. 가상 사실망.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 규칙](#)을 참조하십시오.

## 전화 인증서 유형

Cisco는 전화기에서 다음 인증서 유형을 사용합니다.

- MIC(Manufacturer Installed Certificate) - MIC는 모든 7941, 7961 및 최신 모델 Cisco IP 전화에 포함됩니다. MIC는 Cisco CA(Certificate Authority)에서 서명한 2048비트 키 인증서입니다. MIC가 있는 경우 LSC(Locally Significant Certificate)를 설치할 필요가 없습니다. CUCM이 MIC 인증서를 신뢰하기 위해 인증서 신뢰 저장소에서 사전 설치된 CA 인증서 CAP-RTP-001, CAP-RTP-002 및 Cisco\_Manufacturing\_CA를 활용합니다.
- LSC - LSC는 인증 또는 암호화를 위해 디바이스 보안 모드를 구성한 후 CUCM과 전화기 간의 연결을 보호합니다. LSC는 CUCM CAPF(Certificate Authority Proxy Function) 개인 키에 의해 서명된 Cisco IP 전화의 공개 키를 보유합니다. 관리자가 수동으로 프로비저닝한 Cisco IP 전화만 CTL 파일을 다운로드하고 확인할 수 있으므로 MIC를 사용하는 대신 이 방법을 사용하는 것이 좋습니다. **참고:** 보안 위험이 증가함에 따라 Cisco는 LSC 설치에만 MIC를 사용하는 것이 좋으며, 계속 사용할 수는 없습니다. TLS(Transport Layer Security) 인증 또는 다른 용도로 MIC를 사용하도록 Cisco IP 전화기를 구성하는 고객은 위험을 감수해야 합니다.

## 구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

**참고:** [Command Lookup Tool\(등록된\)](#) 고객만 해당)을 사용하여 이 섹션에서 사용하는 명령에 대한 자세한 정보를 얻을 수 있습니다.

## 구성

이 문서에서는 다음 컨피그레이션에 대해 설명합니다.

- ASA 컨피그레이션
- CallManager 구성
- CallManager의 VPN 컨피그레이션
- IP 전화에 인증서 설치

### ASA 컨피그레이션

ASA의 컨피그레이션은 AnyConnect 클라이언트 컴퓨터를 ASA에 연결할 때와 거의 동일합니다. 그러나 이러한 제한 사항은 다음과 같습니다.

- 터널 그룹에는 group-url이 있어야 합니다. 이 URL은 VPN 게이트웨이 URL의 CM에서 구성됩니다.
- 그룹 정책에는 스플릿 터널이 포함되지 않아야 합니다.

이 컨피그레이션에서는 ASA 디바이스의 SSL(Secure Socket Layer) 신뢰 지점에서 이전에 구성 및 설치된 ASA(자체 서명 또는 타사) 인증서를 사용합니다. 자세한 내용은 다음 문서를 참조하십시오.

- [디지털 인증서 구성](#)
- [ASA 8.x Manually Install third Party Vendor Certificates for use with WebVPN Configuration 예](#)
- [ASA 8.x: 자체 서명 인증서 컨피그레이션을 사용하여 AnyConnect VPN 클라이언트를 통한 VPN 액세스 예](#)

ASA의 관련 컨피그레이션은 다음과 같습니다.

```
ip local pool SSL_Pool 10.10.10.1-10.10.10.254 mask 255.255.255.0
group-policy GroupPolicy_SSL internal
group-policy GroupPolicy_SSL attributes
split-tunnel-policy tunnelall
vpn-tunnel-protocol ssl-client
```

```
tunnel-group SSL type remote-access
tunnel-group SSL general-attributes
address-pool SSL_Pool
default-group-policy GroupPolicy_SSL
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.0.3054-k9.pkg
anyconnect enable
```

```
ssl trust-point SSL outside
```

### CallManager 구성

ASA에서 인증서를 내보내고 CallManager에 Phone-VPN-Trust 인증서로 인증서를 가져오려면 다음 단계를 완료하십시오.

1. 생성된 인증서를 CUCM에 등록합니다.
2. SSL에 사용되는 인증서를 확인합니다.

```
ASA(config)#show run ssl
```

ssl trust-point SSL outside

### 3. 인증서를 내보냅니다.

ASA(config)#crypto ca export SSL identity-certificate

PEM(Privacy Enhanced Mail) 인코딩 ID 인증서는 다음과 같습니다.

```
-----BEGIN CERTIFICATE-----ZHUXFjAUBgkqhkiG9w0BCQIWB0FTQTU1NDAwHhcNMTMwMTMwMTM1MzEwWhcNMjMw
MTI4MTM1MzEwWjAmMQwwCgYDVQQDEwNlZHUXFjAUBgkqhkiG9w0BCQIWB0FTQTU1
NDAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMYcrysJZ+MawKBx8Zk69SW4AR
FSpV6FPcUL7xsovhw6hsJE/2VDgd3pkawc5jc15vkcpTkhjbf2xC4C1q6ZQwpahde22sdf1
wsidpQWq1DDrJD1We83L/oqmhkWJO7QfNrGZh0Lv9xOpR7BFpZd1yFyzwAPkoB11
-----END CERTIFICATE-----
```

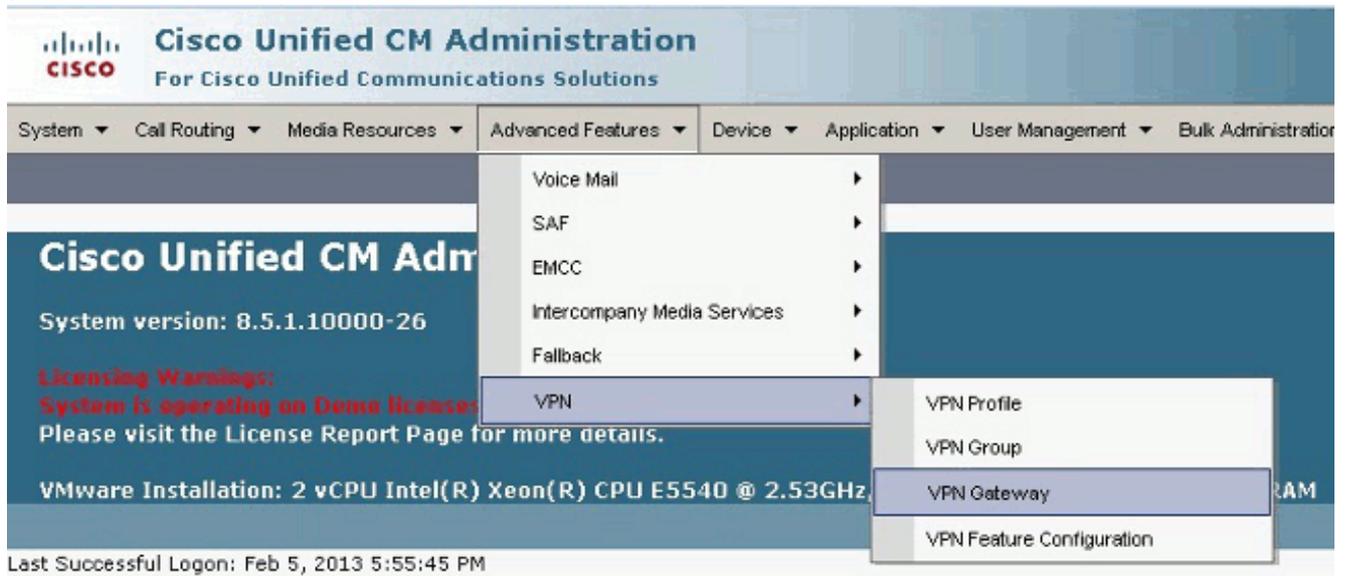
### 4. 터미널에서 텍스트를 복사하고 .pem 파일로 저장합니다.

### 5. CallManager에 로그인하고 Unified OS Administration(Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Upload Certificate(인증서 업로드) > Select Phone-VPN-trust(Phone-VPN-trust)를 선택하여 이전 단계에 저장된 인증서 파일을 업로드합니다.

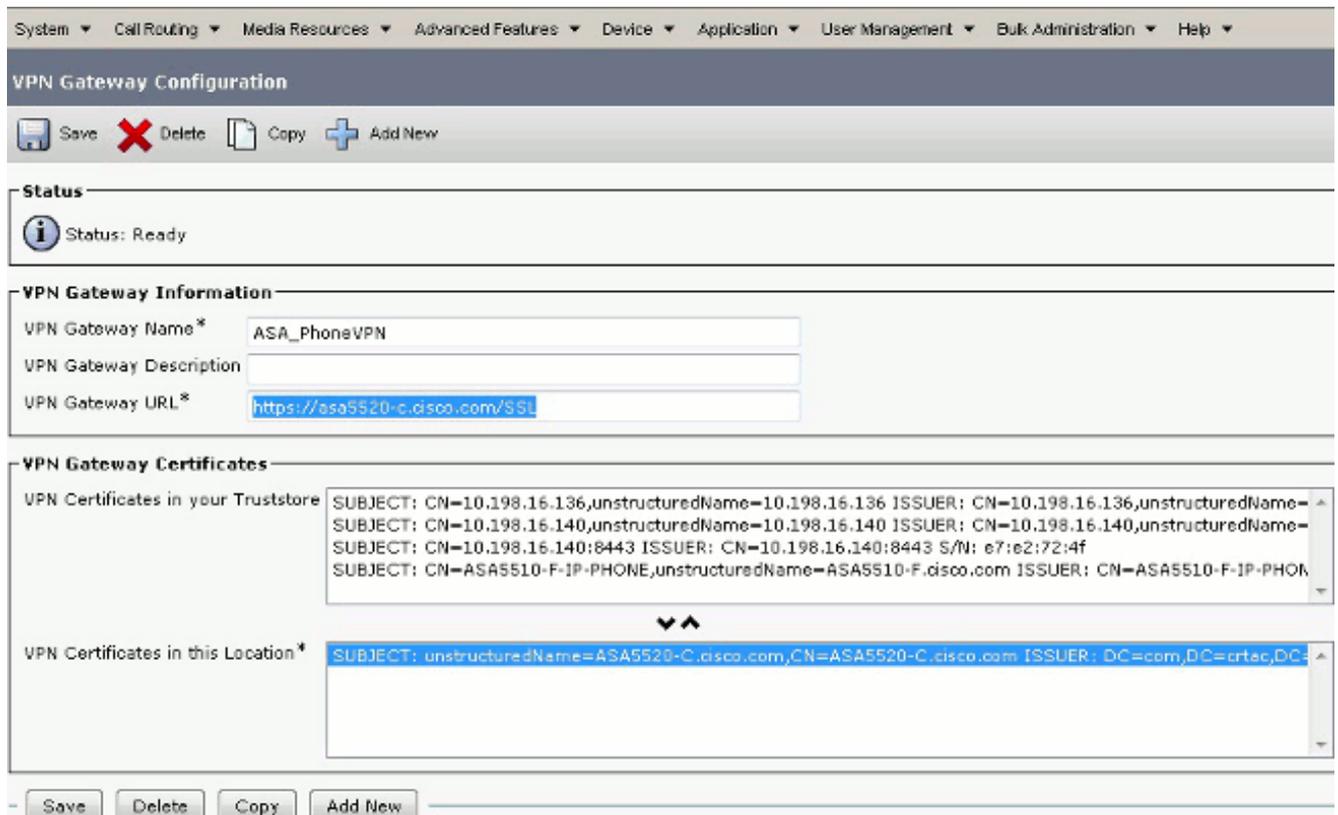
## CallManager의 VPN 컨피그레이션

### 1. Cisco Unified CM Administration(Cisco Unified CM 관리)으로 이동합니다.

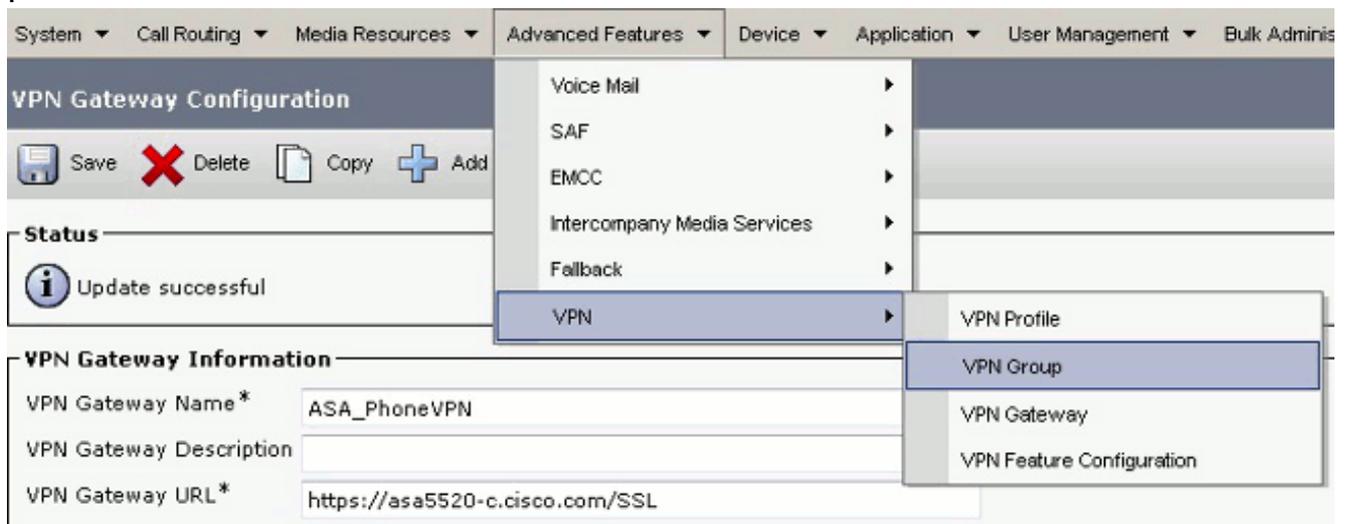
### 2. 메뉴 모음에서 Advanced Features(고급 기능) > VPN > VPN Gateway(VPN 게이트웨이)를 선택합니다



### 3. VPN Gateway Configuration(VPN 게이트웨이 컨피그레이션) 창에서 다음 단계를 완료합니다 .VPN Gateway Name 필드에 이름을 입력합니다.이 이름은 모든 이름이 될 수 있습니다.VPN Gateway Description(VPN 게이트웨이 설명) 필드에 설명(선택 사항)을 입력합니다.VPN Gateway URL 필드에 ASA에 정의된 group-url을 입력합니다.이 위치의 VPN Certificates(VPN 인증서) 필드에서 이전에 CallManager에 업로드된 인증서를 선택하여 신뢰 저장소에서 이 위치로 이동합니다



4. 메뉴 모음에서 Advanced Features(고급 기능) > VPN > VPN Group(VPN 그룹)을 선택합니다



5. All Available VPN Gateways(사용 가능한 모든 VPN 게이트웨이) 필드에서 이전에 정의한 VPN 게이트웨이를 선택합니다.선택한 게이트웨이를 이 VPN Group(이 VPN 그룹) 필드의 Selected VPN Gateway(선택한 VPN 게이트웨이)로 이동하려면 아래쪽 화살표를 클릭합니다

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Manag

## VPN Group Configuration

Save Delete Copy Add New

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN

VPN Group Description

**VPN Gateway Information**

All Available VPN Gateways

**Move the Gateway down**

Selected VPN Gateways in this VPN Group\* ASA\_PhoneVPN

6. 메뉴 모음에서 Advanced Features(고급 기능) > VPN > VPN Profile(VPN 프로파일)을 선택합니다

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administ

## VPN Group Configuration

Save Delete Copy Add

**Status**

Status: Ready

**VPN Group Information**

VPN Group Name\* ASA\_PhoneVPN

VPN Group Description

- Voice Mail ▸
- SAF ▸
- EMCC ▸
- Intercompany Media Services ▸
- Fallback ▸
- VPN ▸**
  - VPN Profile**
  - VPN Group
  - VPN Gateway
  - VPN Feature Configuration

7. VPN 프로파일을 구성하려면 별표(\*)로 표시된 모든 필드를 완료합니다

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

## VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

---

**Status**

 Status: Ready

---

**VPN Profile Information**

Name\*

Description

Enable Auto Network Detect

---

**Tunnel Parameters**

MTU\*

Fail to Connect\*

Enable Host ID Check

---

**Client Authentication**

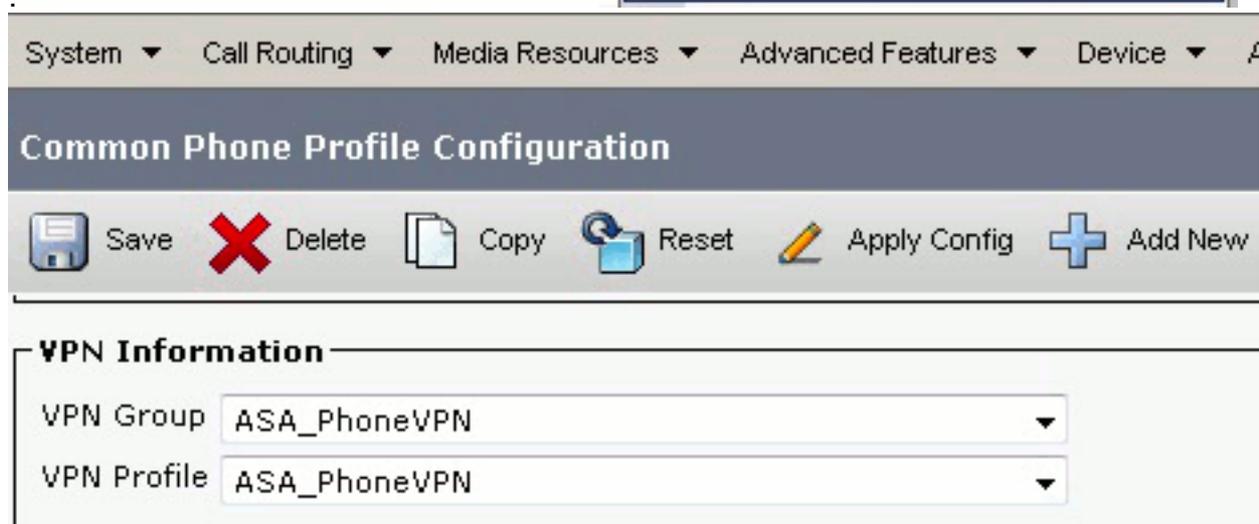
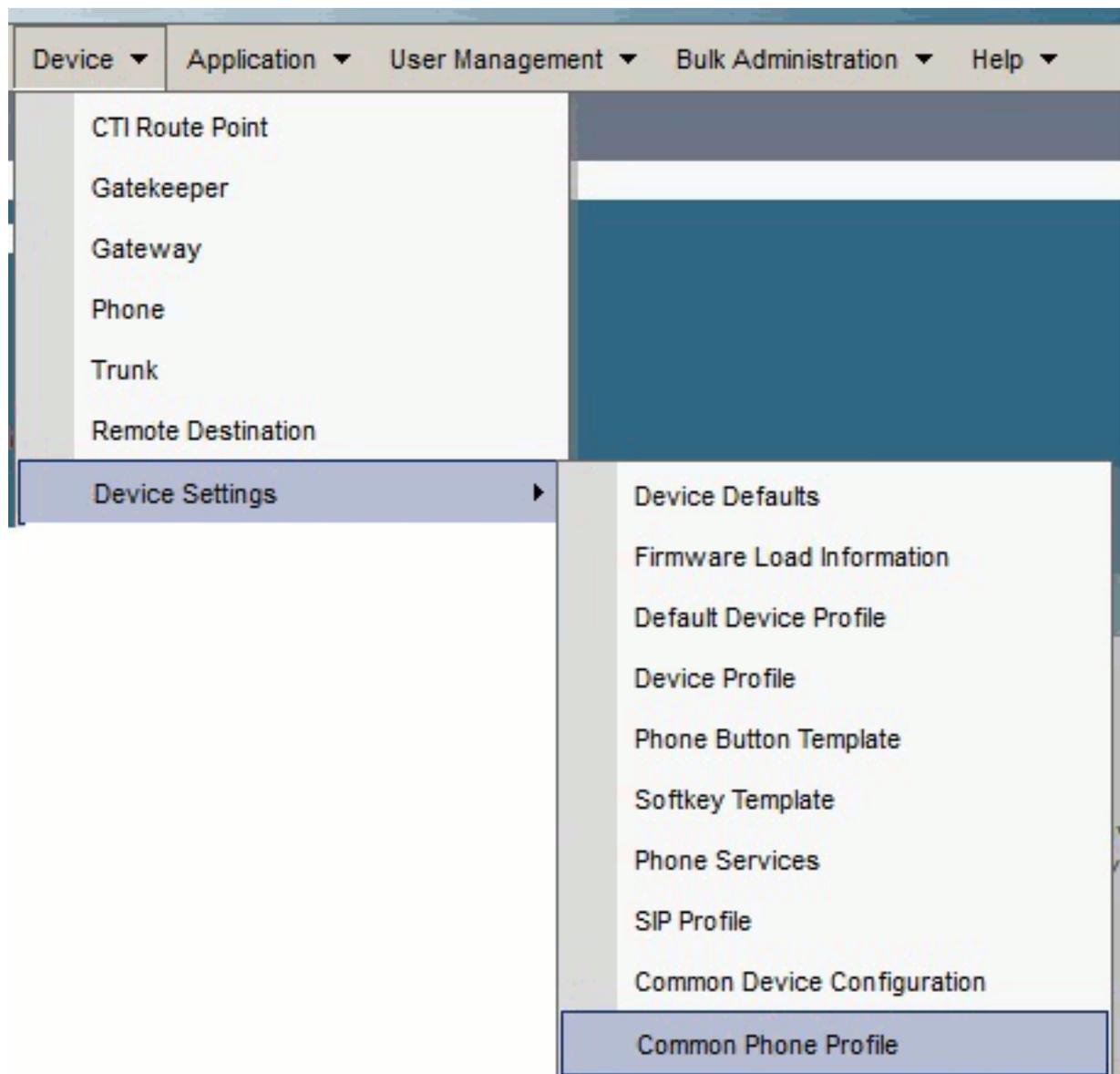
Client Authentication Method\*

Enable Password Persistence

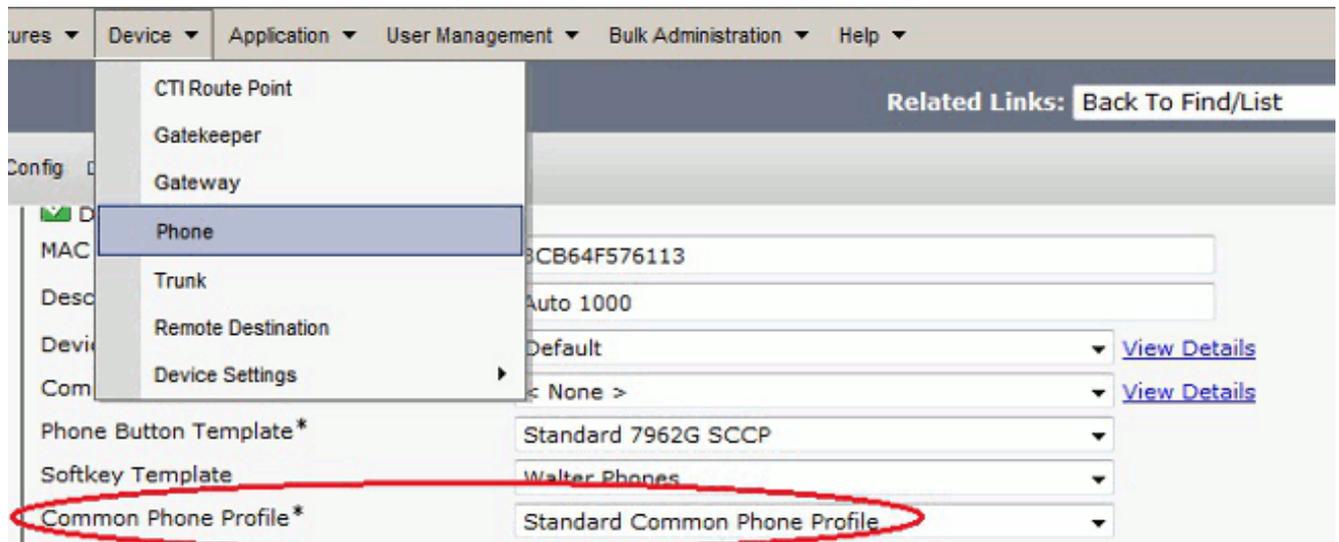
---

**자동 네트워크 탐지 사용:**활성화된 경우 VPN 전화기는 TFTP 서버를 ping하고 응답이 수신되지 않으면 VPN 연결을 자동으로 시작합니다.**호스트 ID 확인 사용:**활성화된 경우 VPN 전화기는 VPN 게이트웨이 URL의 FQDN과 인증서의 CN/SAN을 비교합니다.일치하지 않거나 별표 (\*)가 있는 와일드카드 인증서를 사용하는 경우 클라이언트가 연결하지 못합니다.**비밀번호 지속성 사용:**그러면 VPN 전화에서 다음 VPN 시도에 대한 사용자 이름 및 비밀번호를 캐시할 수 있습니다.

8. Common Phone Profile Configuration(일반 전화기 프로필 컨피그레이션) 창에서 **Apply Config(컨피그레이션 적용)**를 클릭하여 새 VPN 컨피그레이션을 적용합니다."Standard Common Phone Profile(표준 일반 전화기 프로필)"을 사용하거나 새 프로필을 생성할 수 있습니다



9. 특정 전화/사용자에 대한 새 프로필을 생성한 경우 Phone Configuration(전화기 컨피그레이션) 창으로 이동합니다.Common Phone Profile(일반 전화기 프로파일) 필드에서 **Standard Common Phone Profile(표준 일반 전화기 프로파일)**을 선택합니다



10. 새 구성을 다운로드하려면 CallManager에 전화기를 다시 등록하십시오.

### 인증서 인증 컨피그레이션

인증서 인증을 구성하려면 CallManager 및 ASA에서 다음 단계를 완료합니다.

1. 메뉴 모음에서 Advanced Features(고급 기능) > VPN > VPN Profile(VPN 프로파일)을 선택합니다.
2. Client Authentication Method(클라이언트 인증 방법) 필드가 Certificate(인증서)로 설정되어 있는지 **확인합니다**

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾

## VPN Profile Configuration

 Save
  Delete
  Copy
  Add New

---

**Status**

 Status: Ready

---

**VPN Profile Information**

Name\*

Description

Enable Auto Network Detect

---

**Tunnel Parameters**

MTU\*

Fail to Connect\*

Enable Host ID Check

---

**Client Authentication**

Client Authentication Method\*

Enable Password Persistence

3. CallManager에 로그인합니다.메뉴 모음에서 Unified OS Administration > Security > Certificate Management > Find를 선택합니다.

4. 선택한 인증서 인증 방법에 대한 올바른 인증서를 내보냅니다.MIC:Cisco\_Manufacturing\_CA - MIC로 IP Phone 인증

Find Certificate List where File Name ▾ begins with ▾  Find Clear Filter  

Certificate Name	Certificate Type	.PEM File
tomcat	certs	<a href="#">tomcat.pem</a>
ipsec	certs	<a href="#">ipsec.pem</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>
ipsec-trust	trust-certs	<a href="#">CUCM85.pem</a>
CallManager	certs	<a href="#">CallManager.pem</a>
CAPF	certs	<a href="#">CAPF.pem</a>
TVS	certs	<a href="#">TVS.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-001.pem</a>
CallManager-trust	trust-certs	<a href="#">Cisco Root CA 2048.pem</a>
CallManager-trust	trust-certs	<a href="#">CAPF-18cf046e.pem</a>
CallManager-trust	trust-certs	<a href="#">CAP-RTP-002.pem</a>

LSC:Cisco CAPF(Certificate Authority Proxy Function) - LSC로 IP Phone 인증

Certificate Name	Certificate Type	.PEM File	.DER File
tomcat	certs	<a href="#">tomcat.pem</a>	<a href="#">tomcat.der</a>
psec	certs	<a href="#">ipsec.pem</a>	<a href="#">ipsec.der</a>
tomcat-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
psec-trust	trust-certs	<a href="#">CUCM85.pem</a>	<a href="#">CUCM85.der</a>
CallManager	certs	<a href="#">CallManager.pem</a>	<a href="#">CallManager.der</a>
CAPF	certs	<a href="#">CAPF.pem</a>	<a href="#">CAPF.der</a>
TVS	certs	<a href="#">TVS.pem</a>	<a href="#">TVS.der</a>
CallManager-trust	trust-certs	<a href="#">Cisco_Manufacturing_CA.pem</a>	

5. Cisco\_Manufacturing\_CA 또는 CAPF 인증서를 찾습니다..pem 파일을 다운로드하고 .txt 파일로 저장합니다.
6. ASA에서 새 신뢰 지점을 생성하고 이전 저장된 인증서로 신뢰 지점을 인증합니다.base-64로 인코딩된 CA 인증서를 묻는 메시지가 표시되면 다운로드한 .pem 파일의 텍스트를 선택하고 BEGIN 및 END 행과 함께 붙여넣습니다.예를 들면 다음과 같습니다.

```
ASA (config)#crypto ca trustpoint CM-Manufacturing
ASA(config-ca-trustpoint)#enrollment terminal
ASA(config-ca-trustpoint)#exit
ASA(config)#crypto ca authenticate CM-Manufacturing
ASA(config)#
```

```
<base-64 encoded CA certificate>
```

```
quit
```

7. 터널 그룹의 인증이 인증서 인증으로 설정되었는지 확인합니다.

```
tunnel-group SSL webvpn-attributes
authentication certificate
group-url https://asa5520-c.cisco.com/SSL enable
```

## IP 전화에 인증서 설치

IP Phone은 MIC 또는 LSC에서 작동할 수 있지만 각 인증서에 대해 구성 프로세스가 다릅니다.

### MIC 설치

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

**참고:**LSC 설치에만 MIC를 사용하는 것이 좋습니다.Cisco는 CUCM을 사용하여 TLS 연결을 인증하는 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.

### LSC 설치

1. CUCM에서 CAPF 서비스를 활성화합니다.
2. CAPF 서비스가 활성화되면 CUCM에서 LSC를 생성하기 위해 전화 지침을 할당합니다.Cisco Unified CM Administration(Cisco Unified CM 관리)에 로그인하고 Device(디바이스) > **Phone(전화기)**을 선택합니다.구성한 전화기를 선택합니다.
3. Certificate Authority Proxy Function (CAPF) Information(CAPF(인증 기관 프록시 기능) 정보) 섹션에서 모든 설정이 올바르게 작업이 향후 날짜로 설정되어 있는지 확인합니다

**Certification Authority Proxy Function (CAPF) Information**

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Size (Bits)\*

Operation Completes By     (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

4. Authentication Mode(인증 모드)가 Null String(null 문자열) 또는 Existing Certificate(기존 인증서)로 설정된 경우 추가 작업이 필요하지 않습니다.
5. Authentication Mode(인증 모드)가 문자열로 설정된 경우 전화기 콘솔에서 **Settings(설정) > Security Configuration(보안 컨피그레이션) > \*\*# > LSC > Update(업데이트)**를 수동으로 선택합니다.

## 다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

### ASA 확인

```
ASA5520-C(config)#show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : CP-7962G-SEPXXXXXXXXXXXXX
Index : 57
Assigned IP : 10.10.10.2 Public IP : 172.16.250.15
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium, AnyConnect for Cisco VPN Phone
Encryption : AnyConnect-Parent: (1)AES128 SSL-Tunnel: (1)AES128
DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)SHA1 SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1Bytes Tx : 305849
Bytes Rx : 270069Pkts Tx : 5645
Pkts Rx : 5650Pkts Tx Drop : 0
Pkts Rx Drop : 0Group Policy :
GroupPolicy_SSL Tunnel Group : SSL
Login Time : 01:40:44 UTC Tue Feb 5 2013
Duration : 23h:00m:28s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

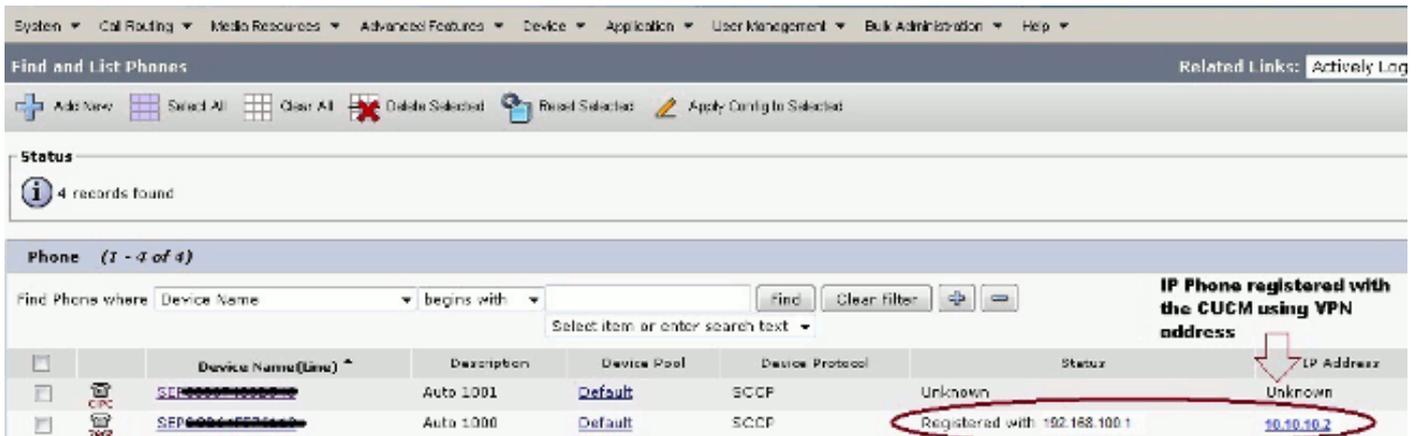
```
AnyConnect-Parent:
Tunnel ID : 57.1
```

Assigned IP : 10.10.10.2 Public IP : 172.16.250.15  
 Encryption : AES128 Hashing : SHA1  
 Encapsulation: TLSv1.0 TCP Dst Port : 443  
 Auth Mode : Certificate  
 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
 Client Type : AnyConnect Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)  
 Bytes Tx : 1759 Bytes Rx : 799  
 Pkts Tx : 2 Pkts Rx : 1  
 Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:  
 Tunnel ID : 57.2  
 Public IP : 172.16.250.15  
 Encryption : AES128 Hashing : SHA1  
 Encapsulation: TLSv1.0 TCP Src Port : 50529  
 TCP Dst Port : 443 Auth Mode : Certificate  
 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
 Client Type : SSL VPN Client  
 Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)  
 Bytes Tx : 835 Bytes Rx : 0  
 Pkts Tx : 1 Pkts Rx : 0  
 Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:  
 Tunnel ID : 57.3  
 Assigned IP : 10.10.10.2 Public IP : 172.16.250.15  
 Encryption : AES128 Hashing : SHA1  
 Encapsulation: DTLSv1.0 UDP Src Port : 51096  
 UDP Dst Port : 443 Auth Mode : Certificate  
 Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
 Client Type : DTLS VPN Client  
 Client Ver : Cisco SVC IPPhone Client v1.0 (1.0)  
 Bytes Tx : 303255 Bytes Rx : 269270  
 Pkts Tx : 5642 Pkts Rx : 5649  
 Pkts Tx Drop : 0 Pkts Rx Drop : 0

## CUCM 확인



## 문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

### 관련 버그

- Cisco 버그 ID [CSCtf09529](#), CUCM에서 8961, 9951, 9971 전화에 대한 VPN 기능 추가 지원
- Cisco 버그 ID [CSCuc71462](#), IP 전화 VPN 장애 조치 소요 시간 8분

- Cisco 버그 ID [CSCtz42052](#), 기본이 아닌 포트 번호에 대한 IP Phone SSL VPN 지원
- Cisco 버그 ID [CSCth96551](#), 전화 VPN 사용자 + 비밀번호 로그인 중에 일부 ASCII 문자가 지원되지 않습니다.
- Cisco 버그 ID [CSCuj71475](#), IP Phone VPN에 필요한 수동 TFTP 항목
- Cisco 버그 ID [CSCum10683](#), 부재 중, 발신 또는 수신된 전화를 로깅하지 않는 IP 전화

## 관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)