VPN 전화 구성 및 문제 해결

목차

소개

이 문서에서는 Cisco IP Phone 및 Cisco Unified Communications Manager의 VPN Phone 기능을 구성하고 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco CUCM(Unified Communications Manager)
- Cisco ASA(Adaptive Security Appliance)
- AnyConnect VPN(Virtual Private Network)
- Cisco IP Phone

사용되는 구성 요소

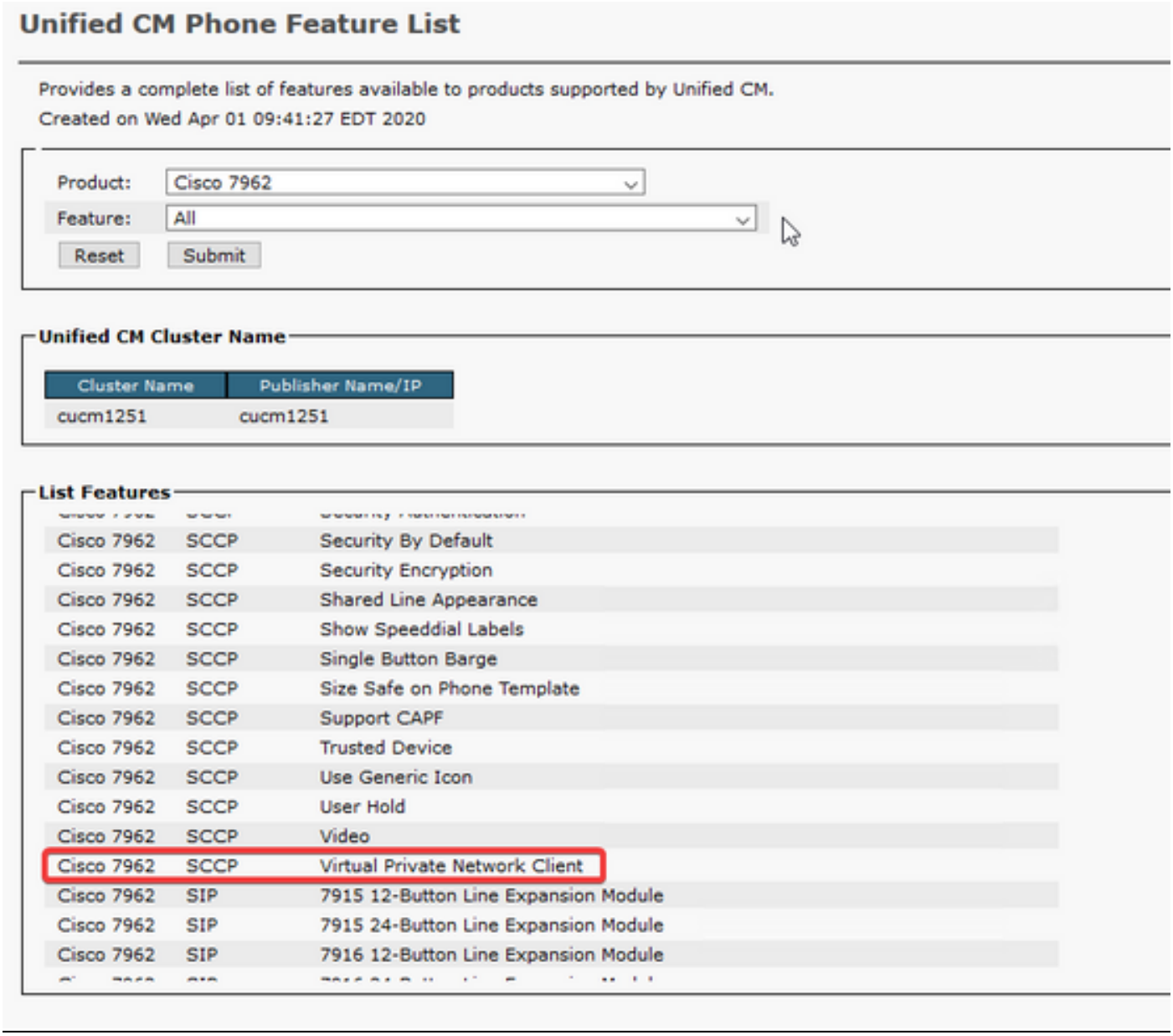
- 8861 14-0-1-0101-145
- ASAv 9.12(2)9

- CUCM 11.5.1.21900-40

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

이 문서의 테스트 환경에는 8861, ASAv 및 CUCM 11.5.1이 포함되지만 사용할 수 있는 다양한 제품이 있습니다. 전화기 모델이 VPN 기능을 지원하는지 확인하려면 CUCM의 Phone Feature List(전화기 기능 목록)를 선택해야 합니다. 전화 기능 목록을 사용하려면 브라우저에서 CUCM 게시자에 액세스하여 **Cisco Unified Reporting > Unified CM Phone Feature List로 이동합니다**. 새 보고서를 생성한 다음 드롭다운에서 전화기 모델을 선택합니다. 그런 다음 이미지에 표시된 대로 List Features(기능 목록) 섹션에서 Virtual Private Network Client(가상 사설망 클라이언트)를 검색해야 합니다.



구성

VPN 전화기에 ASA 및 CUCM에 적절한 컨피그레이션이 있어야 합니다. 먼저 두 제품 중 하나로 시

작할 수 있지만 이 문서에서는 먼저 ASA 컨피그레이션을 다룹니다.

ASA 컨피그레이션

1단계. VPN 전화에 대해 AnyConnect를 지원하도록 ASA에 라이센스가 부여되었는지 확인합니다. ASA의 **show version** 명령을 사용하여 **Cisco VPN Phone용 Anyconnect**가 다음 코드 단편에 표시된 대로 활성화되었는지 확인할 수 있습니다.

```
[output omitted]
Licensed features for this platform:
Maximum VLANs : 50
Inside Hosts : Unlimited
Failover : Active/Standby
Encryption-DES : Enabled
Encryption-3DES-AES : Enabled
Security Contexts : 0
Carrier : Enabled
AnyConnect Premium Peers : 250
AnyConnect Essentials : Disabled
Other VPN Peers : 250
Total VPN Peers : 250
AnyConnect for Mobile : Enabled
AnyConnect for Cisco VPN Phone : Enabled
Advanced Endpoint Assessment : Enabled
Shared License : Disabled
Total TLS Proxy Sessions : 500
Botnet Traffic Filter : Enabled
Cluster : Disabled
```

이 기능이 활성화되지 않은 경우 라이센스 팀과 함께 적절한 라이센스를 받아야 합니다. 이제 ASA가 VPN 폰을 지원함을 확인했으므로 컨피그레이션을 시작할 수 있습니다.

> **참고:** 구성 섹션의 밑줄이 그어진 모든 항목은 변경할 수 있는 구성 가능한 이름입니다. 이러한 이름의 대부분은 컨피그레이션의 다른 곳에서 참조되므로 나중에 필요하므로 이러한 섹션(그룹 정책, 터널 그룹 등)에서 사용하는 이름을 기억해야 합니다.

2단계. VPN 클라이언트에 대한 IP 주소 풀을 생성합니다. 이는 IP 전화기가 ASA에 연결할 때 이 풀에서 IP 주소를 수신한다는 점에서 DHCP 풀과 유사합니다. ASA에서 다음 명령을 사용하여 풀을 생성할 수 있습니다.

ip 로컬 풀 vpn-phone-pool 10.10.1.1-10.10.1.254 마스크 255.255.255.0

또한 다른 네트워크 또는 서브넷 마스크를 선호할 경우 변경할 수도 있습니다. 풀이 생성되면 그룹 정책(ASA와 IP 전화 간 연결을 위한 매개변수 집합)을 구성해야 합니다.

group-policy vpn-phone-policy internal

group-policy vpn-phone-policy 특성

스플릿 터널 정책 터널all

vpn-tunnel-protocol ssl-client

3단계. AnyConnect가 아직 활성화되지 않은 경우 활성화해야 합니다. 이렇게 하려면 외부 인터페이스의 이름을 알아야 합니다. 일반적으로 이 인터페이스 이름은 **outside**(코드 조각에 표시된 것처

럼)이지만 구성 가능하므로 올바른 인터페이스가 있는지 확인합니다. **show ip**를 실행하여 인터페이스 목록을 확인합니다.

```
sckiewer-ASAv# show ip
System IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
Current IP Addresses:
Interface Name IP address Subnet mask Method
GigabitEthernet0/0 outside 172.16.1.250 255.255.255.0 CONFIG
GigabitEthernet0/1 inside 172.16.100.250 255.255.255.0 CONFIG
```

이 환경에서는 외부 인터페이스의 이름이 **outside**로 지정되므로 이러한 명령은 해당 인터페이스에서 AnyConnect를 활성화합니다.

webvpn
외부 사용
anyconnect 활성화

4단계. 특정 URL에 연결하는 클라이언트에 이전에 생성된 그룹 정책을 적용하려면 새 터널 그룹을 구성합니다. 코드 조각의 3번째 및 4번째 행에서 이전에 생성한 IP 주소 풀 및 그룹 정책의 이름에 대한 참조를 확인합니다. IP 주소 풀 또는 그룹 정책의 이름을 수정한 경우 잘못된 값을 수정된 이름으로 바꿔야 합니다.

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
address-pool vpn-phone-pool
default-group-policy vpn-phone-policy
tunnel-group vpn-phone-group webvpn-attributes
인증 인증서
group-url https://asav.sckiewer.lab/phone 활성화

group-url의 이름 대신 IP 주소를 사용할 수 있습니다. 이는 일반적으로 전화기에 ASA의 FQDN(Fully Qualified Domain Name)을 확인할 수 있는 DNS 서버에 액세스할 수 없는 경우에 수행됩니다. 또한 이 예에서는 인증서 기반 인증을 사용하는 것을 확인할 수 있습니다. 사용자 이름/비밀번호 인증도 사용할 수 있지만 이 문서의 범위를 벗어나는 ASA에 대한 더 많은 요구 사항이 있습니다.

이 예에서 DNS 서버에는 A 레코드인 asav.**sckiewer.lab - 172.16.1.250**이 있으며 **outside**라는 인터페이스에 172.16.1.250이 구성된 **show ip** 출력에서 확인할 수 있습니다. 따라서 다음과 같은 구성이 가능합니다.

crypto ca trustpoint asa-identity-cert

등록 자체

subject-name CN=asav.sckiewer.lab

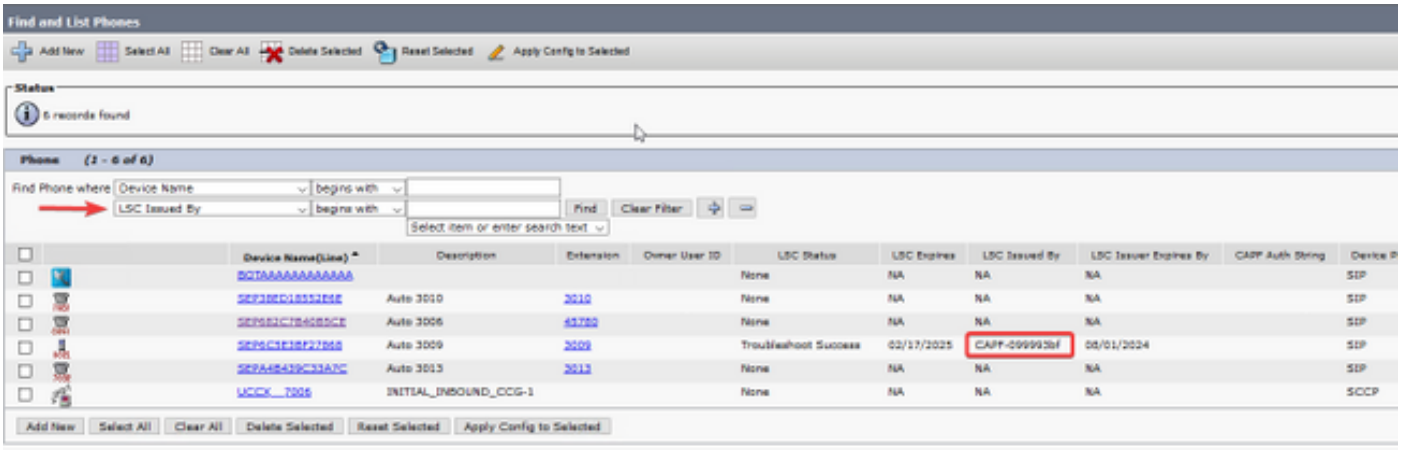
crypto ca enroll asa-identity-cert

ssl trust-point asa-identity-cert outside

몇 가지 유의할 사항은 다음과 같습니다.

1. asa-identity-cert라는 새 신뢰 지점이 생성되었으며 주체 이름이 적용되었습니다. 이렇게 하면 이 신뢰 지점에서 생성된 인증서가 지정된 주체 이름을 사용합니다
2. 다음으로, 'crypto ca enroll asa-identity-cert' 명령을 사용하면 ASA에서 자체 서명 인증서를 생성하여 해당 신뢰 지점에 저장할 수 있습니다
3. 마지막으로, ASA는 신뢰 지점의 인증서를 외부 인터페이스에 연결하는 디바이스에 제공합니다

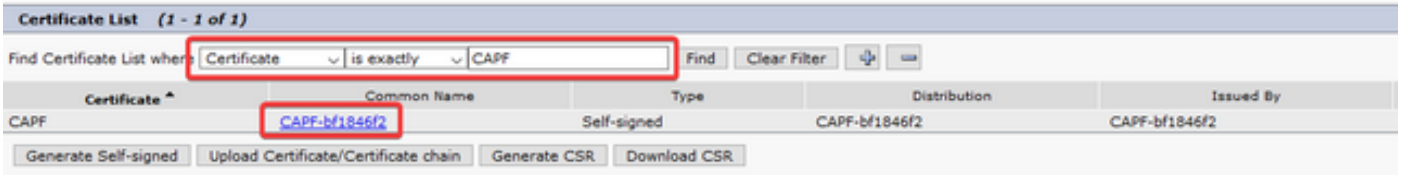
5단계. ASA가 IP 전화의 인증서를 신뢰할 수 있도록 필요한 신뢰 지점을 생성합니다. 먼저 IP 전화에서 MIC(Manufacturer Installed Certificate) 또는 LSC(Locally Significant Certificate)를 사용하는지 확인해야 합니다. 기본적으로 모든 전화기에 LSC가 설치되어 있지 않으면 보안 연결에 MIC를 사용합니다. CUCM 11.5.1 이상에서 Unified **CM Administration(Unified CM 관리) > Device(디바이스) > Phone(전화기)**에 있는 검색을 실행하여 LSC가 설치되어 있는지 확인하고 이전 버전의 CUCM에서는 각 전화기의 보안 설정을 물리적으로 확인해야 합니다. CUCM 11.5.1에서 필터를 추가하거나 기본 필터를 LSC Issued By로 변경해야 **합니다**. LSC Issued **By(LSC 발급** 기준) **열**에 **NA**가 있는 디바이스는 LSC가 설치되어 있지 않으므로 MIC를 사용합니다.



전화기가 이미지에서 강조 표시된 것과 같이 보일 경우 ASA가 보안 연결을 위해 전화기의 인증서를 검증하려면 CUCM Publisher의 CAPF 인증서를 ASA에 업로드해야 합니다. LSC가 설치되지 않은 장치를 사용하려면 Cisco Manufacturing 인증서를 ASA에 업로드해야 합니다. 이러한 인증서는 **Cisco Unified OS 관리 > 보안 > 인증서 관리**의 CUCM 게시자에서 찾을 수 있습니다.

> **참고:** 이러한 인증서 중 일부는 여러 신뢰 저장소(CallManager-trust 및 CAPF-trust)에서 확인할 수 있습니다. 이러한 정확한 이름을 가진 인증서를 선택하기만 하면 어떤 신뢰 저장소에서 인증서를 다운로드하든 상관없습니다.

- Cisco_Root_CA_2048 < MIC SHA-1 Root
- Cisco_Manufacturing_CA < MIC SHA-1 Intermediate
- Cisco_Root_CA_M2 < MIC SHA-256 Root
- Cisco_Manufacturing_CA_SHA2 < MIC SHA-256 Intermediate
- CUCM 게시자의 CAPF < LSC



MIC에 대해 79xx 및 99xx 시리즈와 같은 이전 전화기 모델은 SHA-1 인증서 체인을 사용하는 반면, 88xx 시리즈와 같은 최신 전화기 모델은 SHA-256 인증서 체인을 사용합니다. 전화기가 사용하는 인증서 체인을 ASA에 업로드해야 합니다.

필요한 인증서가 있으면 다음으로 신뢰 지점을 생성할 수 있습니다.

crypto ca trustpoint cert1

등록 터미널

crypto ca authenticate cert1

첫 번째 명령은 cert1이라는 신뢰 지점을 생성하고 **crypto ca authenticate** 명령을 사용하면 base64 인코딩 인증서를 CLI에 붙여넣을 수 있습니다. ASA에서 적절한 신뢰 지점을 가져오기 위해 필요한 만큼 이 명령을 여러 번 실행할 수 있지만 각 인증서에 대해 새 신뢰 지점 이름을 사용해야 합니다.

6단계. 다음 명령을 실행하여 ASA ID 인증서의 복사본을 얻습니다.

crypto ca export asa-identity-cert identity-certificate

이렇게 하면 asa-identity-cert라는 신뢰 지점에 대한 ID 인증서가 내보내집니다. 4단계에서 생성한 신뢰 지점과 일치하도록 이름을 조정하십시오.

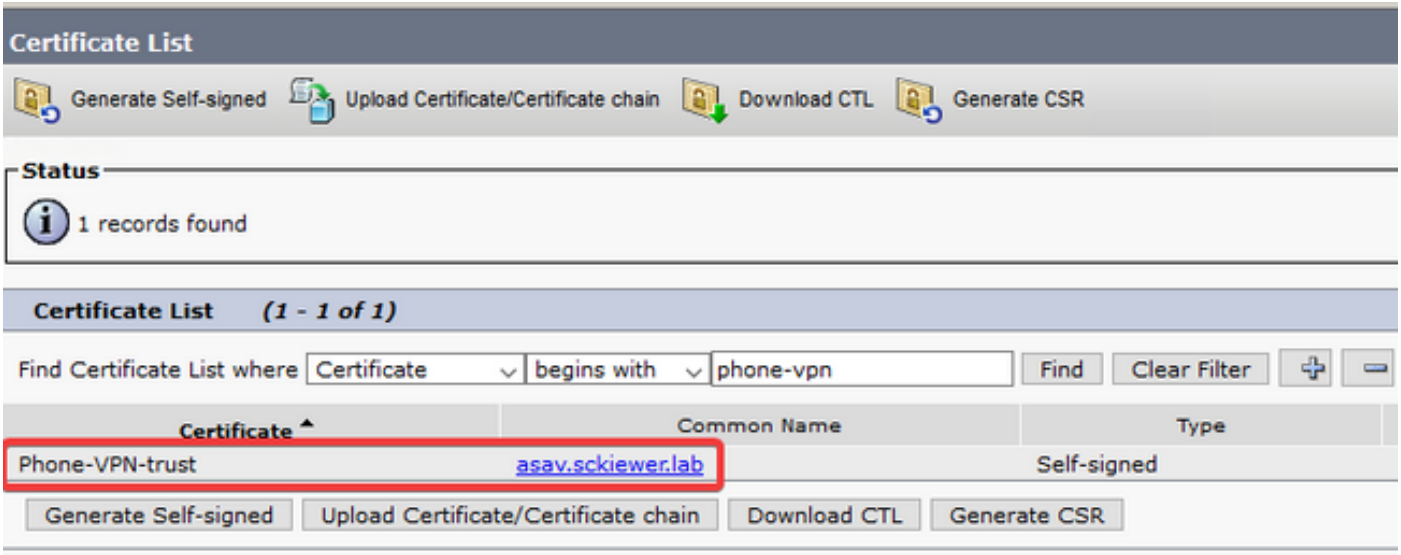
다음은 ASA에 대한 전체 랩 컨피그레이션입니다.

```
ip local pool vpn-phone-pool 10.10.1.1-10.10.1.254 mask 255.255.255.0

group-policy vpn-phone-policy internal
group-policy vpn-phone-policy attributes
     split-tunnel-policy tunnelall
     vpn-tunnel-protocol ssl-client

webvpn
     enable outside
     anyconnect enable

tunnel-group vpn-phone-group type remote-access
tunnel-group vpn-phone-group general-attributes
     address-pool vpn-phone-pool
     default-group-policy vpn-phone-policy

tunnel-group vpn-phone-group webvpn-attributes
     authentication certificate
     group-url https://asav.sckiewer.lab/phone enable

ssl trust-point asa-identity-cert outside
```

이 시점에서 ASA 컨피그레이션이 완료되었으며 CUCM 컨피그레이션을 계속 진행할 수 있습니다. 방금 수집한 ASA 인증서 사본과 tunnel-group 섹션에서 구성한 URL이 있어야 합니다.

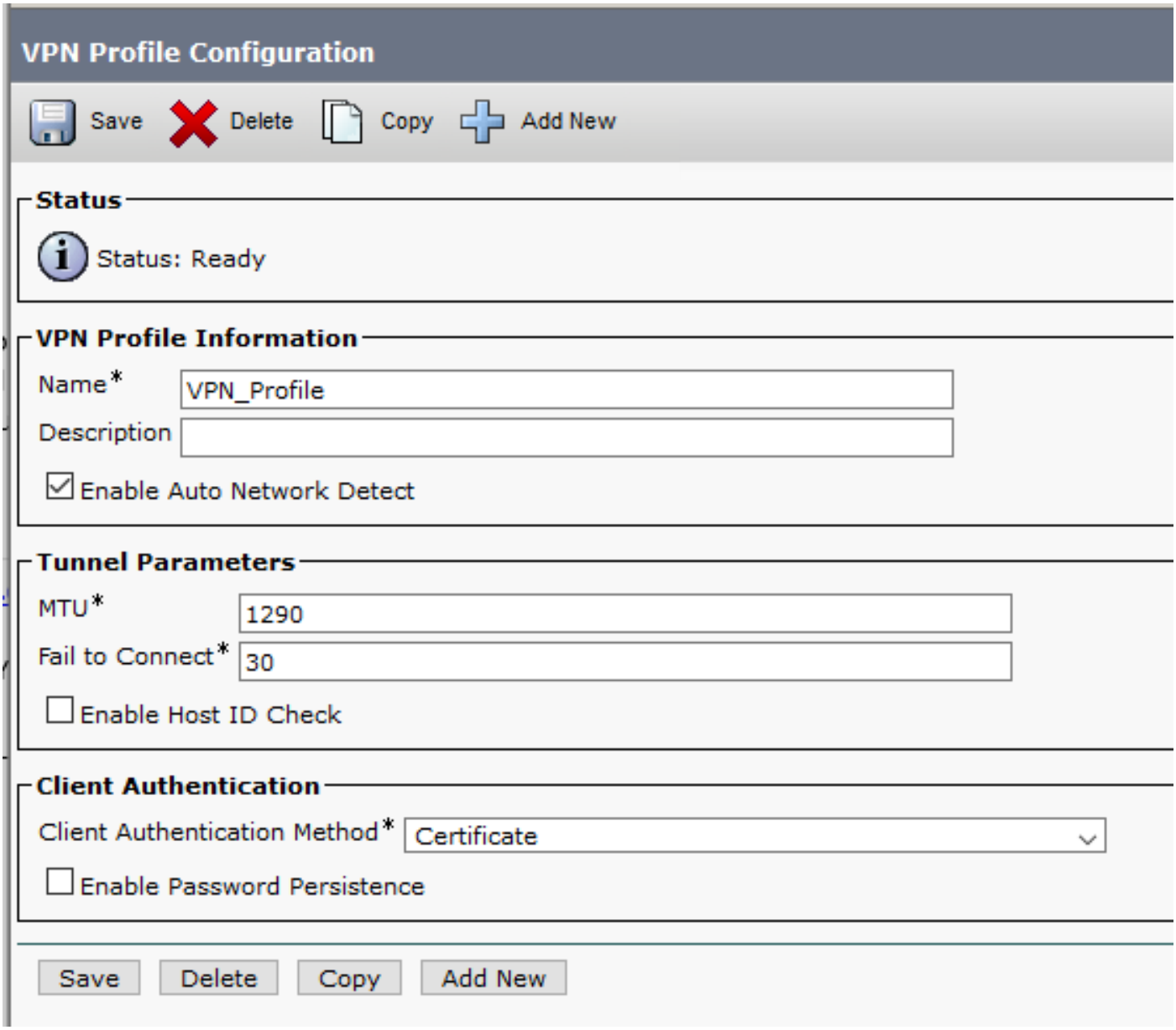
CUCM 컨피그레이션

1단계. CUCM에서 **Cisco Unified OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리)로 이동하고** ASA 인증서를 **phone-vpn-trust**로 **업로드합니다**.

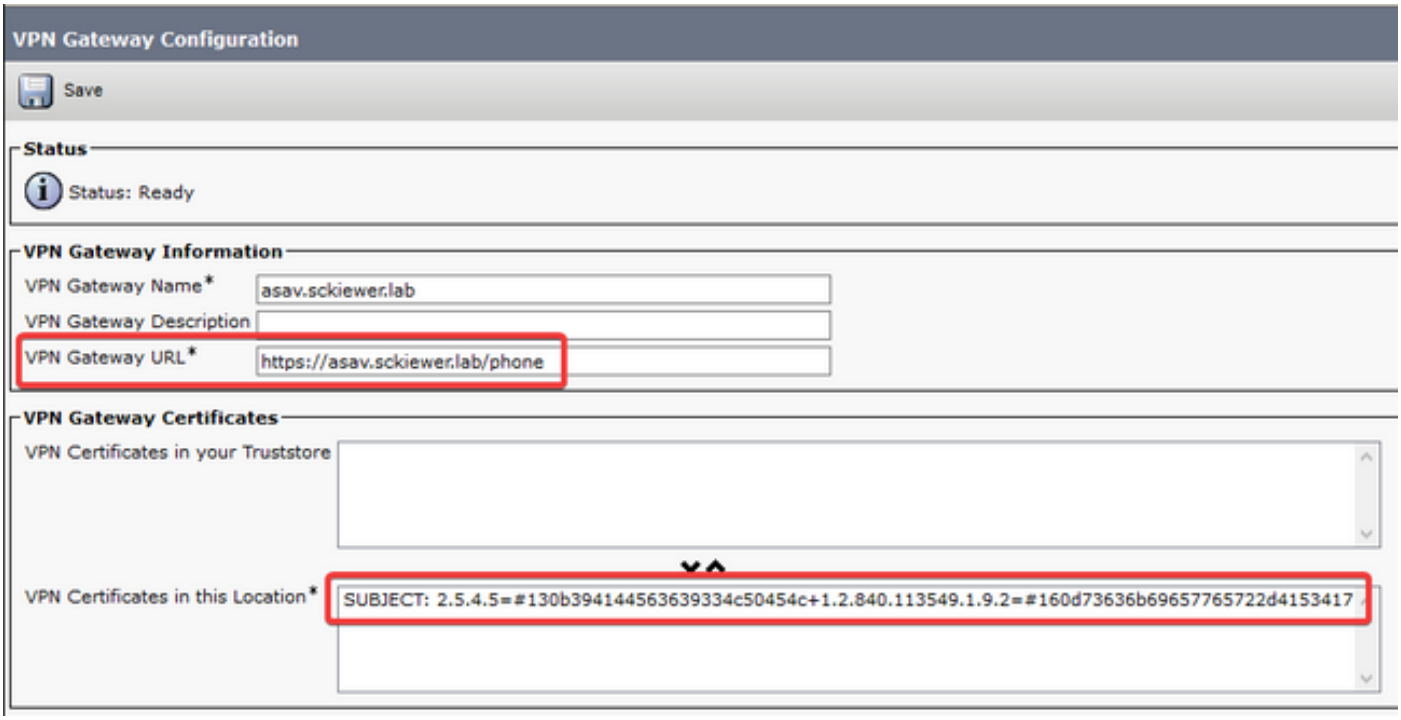


2단계. 이 작업이 완료되면 **Cisco Unified CM Administration(Cisco Unified CM 관리) > Advanced Features(고급 기능) > VPN > VPN Profile(VPN 프로파일)로 이동하여** 새 프로파일을 생성합니다. 이 섹션에는 옳고 그름이 없으므로 각 설정의 목적을 이해하는 것이 중요합니다.

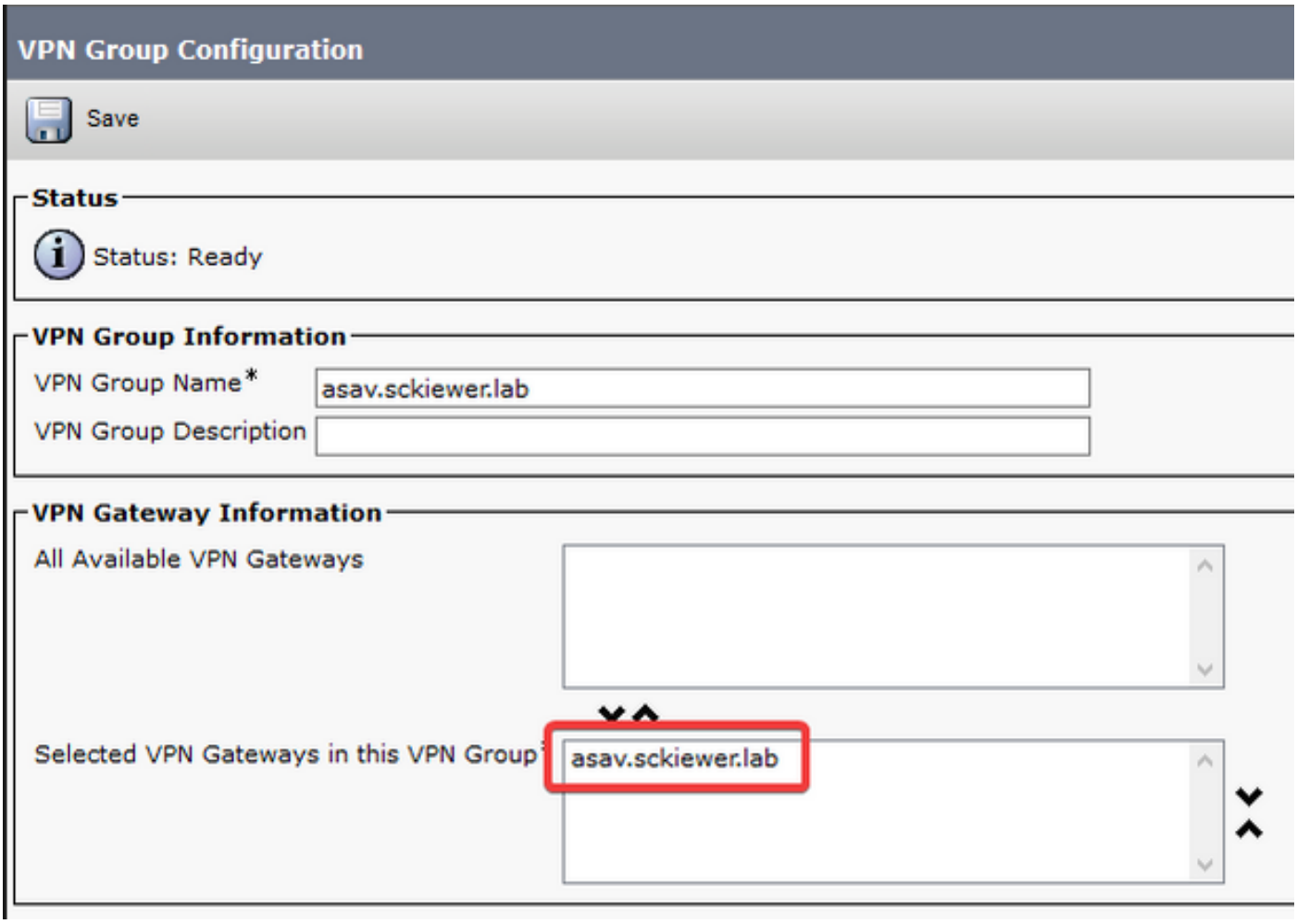
1. **Enable Auto Network Detect(자동 네트워크 탐지** 활성화) - 이 기능이 활성화되면 전화기가 TFTP 서버를 켜면 해당 TFTP 서버를 ping합니다. 이 ping에 대한 응답을 받으면 VPN을 활성화하지 않습니다. 전화기에서 이 ping에 대한 응답을 받지 못하면 VPN을 활성화합니다. 이 설정을 사용하면 VPN을 수동으로 활성화할 수 없습니다.
2. **호스트 ID 확인** - 이 기능이 활성화되면 전화기는 해당 구성 파일 (https://asav.sckiewer.lab/phone은 이 문서에서 사용됨)에서 VPN URL을 검사하고, 호스트 이름 또는 FQDN이 ASA에서 제공하는 인증서의 CN(Common Name) 또는 SAN 항목과 일치하는지 확인합니다.
3. **Authentication Method** - ASA와의 연결에 사용되는 인증 방법 유형을 제어합니다. 이 문서의 컨피그레이션 예에서는 인증서 기반 인증이 사용됩니다.
4. **Password Persistence**(비밀번호 지속성) - 이 옵션을 활성화하면 실패한 로그인 시도가 발생할 때까지 클라이언트의 비밀번호가 전화기에 저장되고, 클라이언트가 수동으로 비밀번호를 지우거나 전화기가 재설정됩니다.



3단계. 다음으로, **Cisco Unified CM Administration(Cisco Unified CM 관리) > Advanced Features(고급 기능) > VPN > VPN Gateway(VPN 게이트웨이)로 이동합니다**. VPN 게이트웨이 URL이 ASA 컨피그레이션과 일치하는지, 이미지에 표시된 것처럼 상단 상자에서 아래쪽 상자로 인증서를 이동해야 합니다.

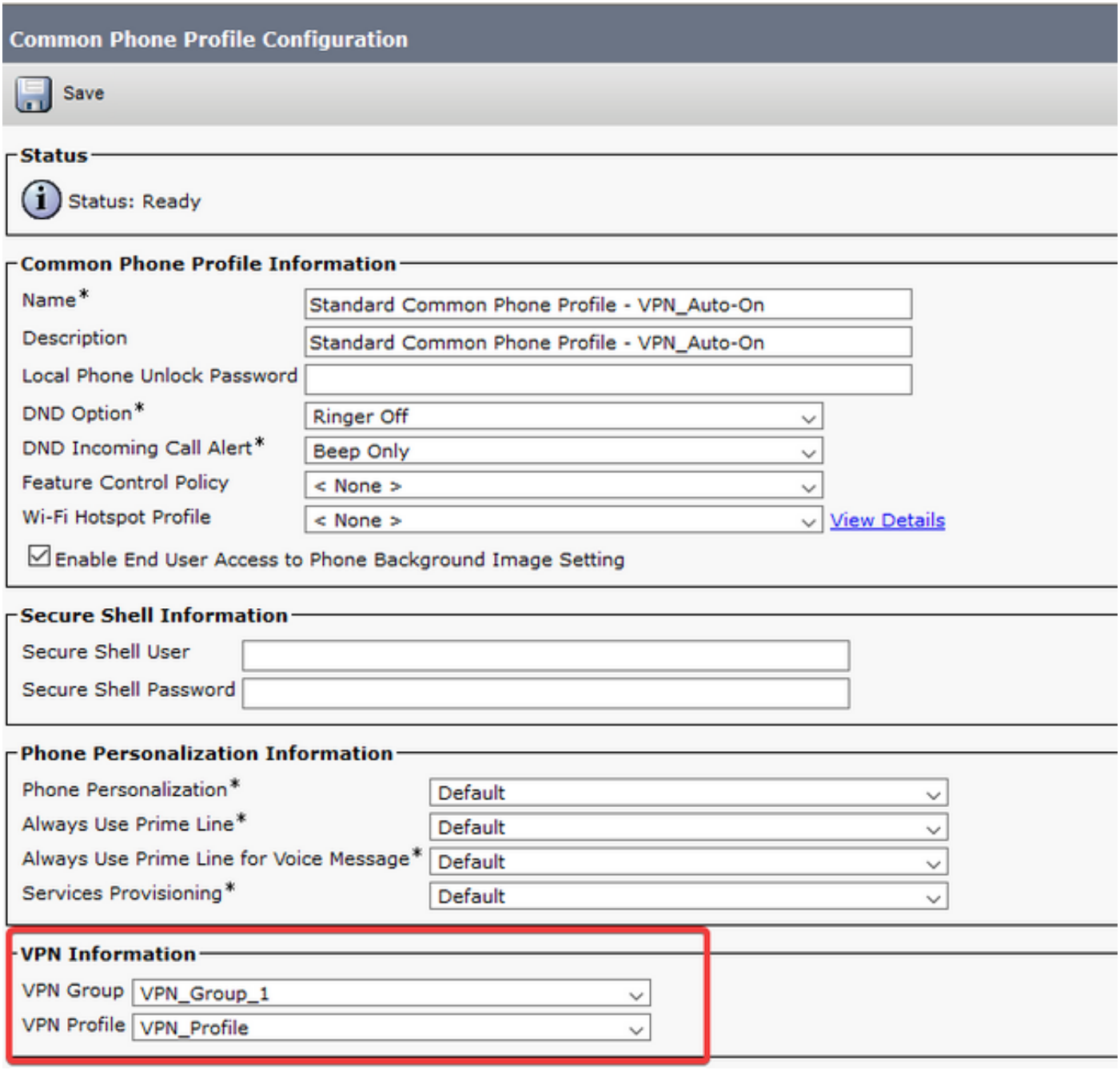


4단계. 이 정보가 저장되면 **Cisco Unified CM Administration(Cisco Unified CM 관리) > Advanced Features(고급 기능) > VPN > VPN Group(VPN 그룹)으로 이동하고** 생성한 게이트웨이를 'Selected VPN Gateways in this VPN Group(이 VPN 그룹의 선택한 VPN 게이트웨이)' 상자로 이동해야 합니다.



5단계. 이제 VPN 설정이 구성되었으므로 **Cisco Unified CM Administration(Cisco Unified CM 관리) > Device(디바이스) > Device Settings(디바이스 설정) > Common Phone Profile(일반 전화기 프로**

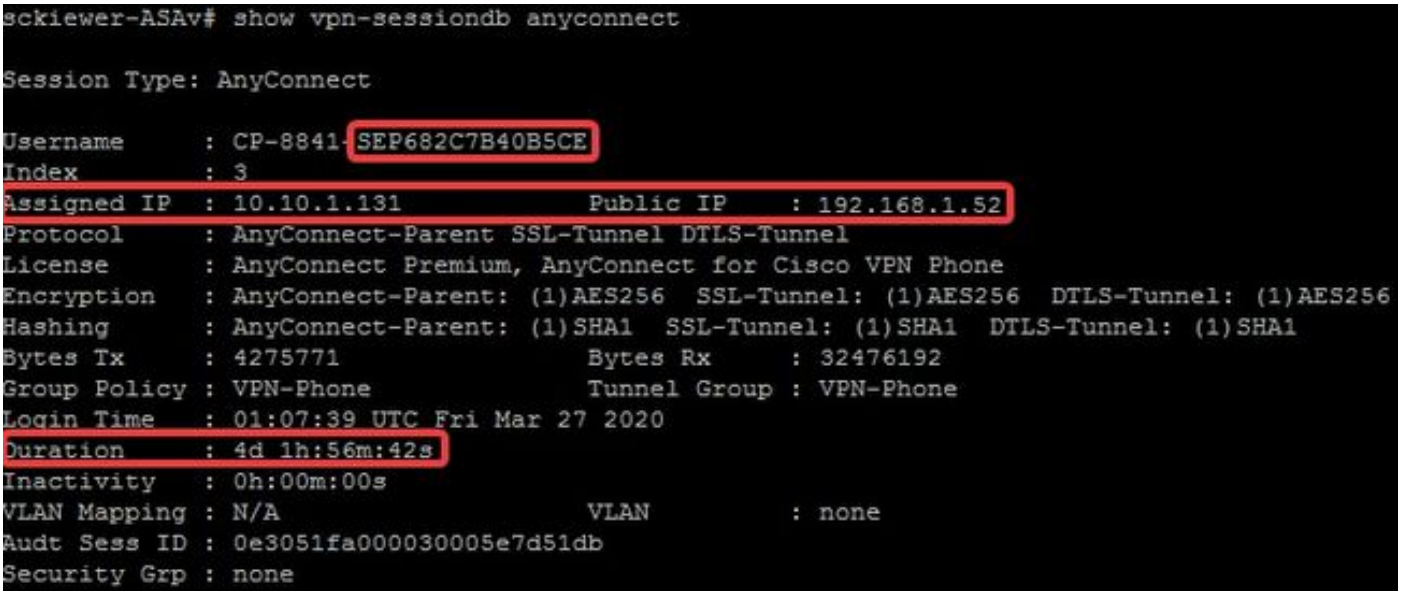
파일)으로 이동해야 합니다. 여기서 원하는 VPN 전화기에서 사용하는 프로필을 복사하고 이름을 바꾸고 VPN 그룹 및 VPN 프로필을 선택한 다음 새 프로필을 저장해야 합니다.



6단계. 마지막으로 이 새 프로필을 휴대폰에 적용한 다음 내부 네트워크에 있는 동안 전화기를 재설정해야 합니다. 이렇게 하면 전화기에서 ASA 인증서 해시 및 VPN URL과 같은 모든 새 컨피그레이션을 수신할 수 있습니다.

> **참고:** 전화기를 테스트하기 전에 전화기에 '대체 TFTP' 서버가 구성되어 있는지 확인해야 합니다. ASA는 전화기에 옵션 150을 제공하지 않으므로 전화기에 TFTP IP를 수동으로 구성해야 합니다.

7단계. VPN 전화기를 테스트하고 ASA에 성공적으로 연결하여 등록할 수 있는지 확인합니다. 터널이 ASA에서 VPN-sessiondb anyconnect와 함께 작동 중인지 확인할 수 **있습니다**.



문제 해결

수집할 데이터

VPN Phone 문제를 해결하려면 다음 데이터를 사용하는 것이 좋습니다.

- ASA 디버그: 버퍼된 디버그 로깅디버그 추적 로깅디버그 암호화 ca 트랜잭션 255디버그 암호화 ca 메시지 255디버그 암호화 ca 255디버그 webvpn 255debug webvpn anyconnect 255
- Phone Console 로그(또는 전화기에서 지원하는 경우 PRT) - 추가 정보 여기)

디버그가 활성화된 상태로 문제를 재현한 후에는 디버그 출력에는 항상 711001이 포함되므로 이 명령으로 출력을 볼 수 있습니다.

로그 표시 | i 711001

일반적인 문제

> **참고:** 이 섹션에서는 VPN 전화기로 구축된 가장 일반적인 전화 시리즈 중 하나이므로 로그 조각이 8861 전화기에서 가져온 것입니다. 다른 모델에서는 로그에 서로 다른 메시지를 쓸 수 있습니다.

ASA 자체 서명 ID 인증서 업데이트

ASA ID 인증서가 만료되기 전에 새 인증서를 생성하여 전화기에 푸시해야 합니다. VPN 전화기에 영향을 주지 않고 이 작업을 수행하려면 다음 프로세스를 사용합니다.

1단계. 새 ID 인증서에 대한 새 신뢰 지점을 만듭니다.

crypto ca trustpoint asa-identity-cert-2

등록 자체

subject-name CN=asav.sckiewer.lab

crypto ca enroll asa-identity-cert-2

2단계. 이 시점에서는 ASA에 대한 새 ID 인증서가 있지만 아직 어떤 인터페이스에서도 사용되지 않습니다. 이 새 인증서를 내보내고 CUCM에 업로드해야 합니다.

crypto ca export asa-identity-cert-2 identity-certificate

3단계. 새 ID 인증서가 있으면 **Cisco Unified OS Administration(Cisco Unified OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Upload(업로드)**에서 CUCM 노드 중 하나에 해당 인증서를 **phone-VPN-trust로 업로드합니다**.

> **참고:** 현재 phone-VPN-trust 인증서는 원래 업로드된 CUCM 노드에만 있습니다(일부 인증서와 같은 다른 노드에 자동으로 전파되지 않음). CUCM 버전이 CSCuo58506의 영향을 받는 경우 새 ASA 인증서를 다른 노드에 업로드해야 합니다.

4단계. 새 인증서가 클러스터의 노드에 업로드되면 CUCM Publisher에서 **Cisco Unified CM Administration(Cisco Unified CM 관리) > Advanced Features(고급 기능) > VPN > VPN Gateway(VPN 게이트웨이)**로 이동합니다.

5단계. 적절한 게이트웨이를 선택합니다.

6단계. 맨 위 상자에서 인증서를 선택하고(방금 업로드한 인증서) 아래쪽 화살표를 선택하여 맨 아래로 이동합니다(이렇게 하면 TFTP에서 VPN 전화의 컨피그레이션 파일에 인증서를 추가할 수 있음). 그런 다음 Save(저장)를 선택합니다.

7단계. 작업이 완료되면 모든 VPN 전화기를 재설정합니다. 이 프로세스에서 ASA는 여전히 이전 인증서를 제공하므로 폰은 연결할 수 있지만 새 인증서와 이전 인증서가 모두 포함된 새 컨피그레이션 파일을 가져옵니다.

8단계. 이제 새 인증서를 ASA에 적용할 수 있습니다. 이렇게 하려면 새 신뢰 지점의 이름 및 외부 인터페이스의 이름이 필요한 다음 해당 정보로 이 명령을 실행합니다.

ssl trust-point asa-identity-cert-2 outside

> **참고:** 브라우저에서 webvpn URL로 이동하여 ASA가 새 인증서를 제공하는지 확인할 수 있습니다. 외부 전화기에 연결할 수 있도록 해당 주소에 공개적으로 연결할 수 있어야 하므로 PC도 연결할 수 있습니다. 그런 다음 ASA가 브라우저에 제공하는 인증서를 확인하고 새 인증서인지 확인할 수 있습니다.

9단계. ASA가 새 인증서를 사용하도록 구성되면 테스트 전화기를 재설정하고 ASA에 연결하여 등록할 수 있는지 확인합니다. 전화기가 성공적으로 등록되면 모든 전화기를 재설정하고 ASA에 연결하여 등록할 수 있는지 확인할 수 있습니다. 인증서 변경 후 ASA에 연결된 전화기가 연결된 상태로 유지되기 때문에 권장되는 프로세스입니다. 한 전화기에서 인증서 업데이트를 먼저 테스트할 경우 컨피그레이션 문제가 많은 전화기에 미치는 영향을 줄일 수 있습니다. 첫 번째 VPN 폰에서 ASA에 연결할 수 없는 경우, 다른 전화기가 연결된 상태에서 문제를 해결하기 위해 전화기 및/또는 ASA에서 로그를 수집할 수 있습니다.

10단계. 전화기가 새 인증서에 연결하고 등록할 수 있는지 확인한 후에는 CUCM에서 이전 인증서를 제거할 수 있습니다.

ASA에서 EC(Elliptic Curve) 암호를 선택

ASA는 9.4(x)부터 EC(Elliptic Curve) 암호화를 지원하므로, ASA를 9.4(x) 이상으로 업그레이드한 후 이전에 작동하는 VPN 전화에서 장애가 발생하는 경우가 일반적입니다. 이는 ASA가 최신 폰 모델과의 TLS 핸드셰이크 중에 EC 암호를 선택했기 때문입니다. 일반적으로 이전 ASA 버전에서 EC를 지원하지 않았기 때문에 전화기가 연결되는 인터페이스와 연결된 RSA 인증서가 있습니다. 이 시점에서 ASA는 EC 암호를 선택했으므로 연결에 RSA 인증서를 사용할 수 없으므로, RSA가 아닌 EC 알고리즘으로 생성하는 임시 자체 서명 인증서를 생성하여 전화기를 전송합니다. 이 임시 인증서는 전화기에서 인식되지 않으므로 연결이 실패합니다. 88xx 전화 로그에서 이 문제가 매우 간단한지 확인할 수 있습니다.

```
2101 NOT Mar 30 12:23:21.331861 (393:393) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2102 NOT Mar 30 12:23:21.331871 (393:393) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
```

전화 로그에는 ASA가 이 연결에 대해 EC 암호를 선택했음을 보여줍니다. '새 암호' 회선에 EC 암호가 포함되어 있어 연결이 실패합니다.

AES가 선택된 시나리오에서 다음이 표시됩니다.

```
2691 NOT Mar 30 12:18:19.016923 (907:907) VPNC: -protocol_handler: current cipher -> ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA
2690 NOT Mar 30 12:18:19.016943 (907:907) VPNC: -protocol_handler: new cipher -> AES256-SHA:AES128-SHA
```

이에 대한 자세한 내용은 CSCuu02848을 참조하십시오.

이 문제를 해결하려면 전화기에서 사용하는 TLS 버전에 대해 ASA에서 EC 암호를 비활성화해야 합니다. 각 전화기 모델이 지원하는 TLS 버전에 대한 자세한 내용은 여기에서 확인할 수 있습니다.

Table 6 lists the TLS versions supported by the Cisco IP phones.

Table 6. TLS version support

	Phone Models			
Version	7900	6900, 8900, 9900	7811, 7821, 7841, 7861	8811, 8821, 8841, 8845, 8851, 8861, 8865
TLS 1.0	Yes	Yes	Yes	Yes
TLS 1.2	No	No	Yes	Yes
Disable TLS 1.0 and TLS 1.1 with https for web access*	No	No	Yes	Yes
Selectively Disable TLS cipher suites used by TLS connection or handshake**	No	No	Yes	Yes

* With 12.1 firmware
** With 12.5 firmware

https://www.cisco.com/c/dam/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-8800-series/white-paper-c11-739097.pdf

환경에서 어떤 TLS 버전이 관련되는지 알게 되면 ASA에서 다음 명령을 실행하여 해당 버전에 대해 EC 암호를 비활성화할 수 있습니다.

```
ssl cipher tlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher tlsv1.2 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
ssl cipher dtlsv1 custom "AES256-SHA:AES128-SHA:AES256-GCM-SHA384:AES256-SHA256:AES128-GCM-
SHA256:AES128-SHA256:AES256-SHA"
```

IP 전화에서는 기본적으로 DTLS(Datagram Transport Layer Security)를 사용하므로 DTLS에 대한 암호 문과 전화에 대한 관련 TLS 버전을 실행해야 합니다. 또한 이러한 변경 사항이 ASA의 전역 변경 사항임을 이해하는 것이 중요합니다. 따라서 이러한 TLS 버전을 사용하는 다른 AnyConnect 클라이언트에서 EC 암호를 협상하는 것을 방지할 수 있습니다.

DTLS 연결 실패

경우에 따라 VPN 전화기는 DTLS를 사용하는 ASA에 연결할 수 없습니다. 전화기에서 DTLS를 사용하려고 시도했지만 실패해도 DTLS가 활성화되었음을 알고 있으므로 전화기는 계속해서 DTLS를 반복해서 시도하지만 실패함 88xx 전화 로그에서 이를 확인할 수 있습니다.

```
3249 ERR Mar 29 15:22:38.949354 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
fatal:illegal parameter
3250 NOT Mar 29 15:22:38.951428 (385:385) VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000
status: 0x0 error: 0x0
3251 ERR Mar 29 15:22:38.951462 (385:385) VPNC: -alert_err: DTLS write alert: code 47, illegal
parameter
3252 ERR Mar 29 15:22:38.951489 (385:385) VPNC: -create_dtls_connection: SSL_connect ret -1,
error 1
3253 ERR Mar 29 15:22:38.951506 (385:385) VPNC: -DTLS: SSL_connect: SSL_ERROR_SSL (error 1)
3254 ERR Mar 29 15:22:38.951552 (385:385) VPNC: -DTLS: SSL_connect: error:140920C5:SSL
routines:ssl3_get_server_hello:old session cipher not returned
3255 ERR Mar 29 15:22:38.951570 (385:385) VPNC: -create_dtls_connection: DTLS setup failure,
cleanup
3256 WRN Mar 29 15:22:38.951591 (385:385) VPNC: -dtls_state_cb: DTLSv0.9: write: alert:
warning:close notify
3257 ERR Mar 29 15:22:38.951661 (385:385) VPNC: -do_dtls_connect: create_dtls_connection failed
3258 ERR Mar 29 15:22:38.951722 (385:385) VPNC: -protocol_handler: connect: do_dtls_connect
failed
3259 WRN Mar 29 15:22:38.951739 (385:385) VPNC: -protocol_handler: connect : err: SSL success
DTLS fail
```

이는 ASA Selecting Elliptic Curve (EC) Cipher(EC(Elliptic Curve) Cipher(EC(Elliptic Curve) 암호 선택) 섹션에 언급된 동일한 문제로 인해 발생할 수 있으므로 DTLS에 대해 EC 암호를 비활성화해야 합니다. 이 외에도 VPN 전화기에서 TLS를 대신 사용하도록 하는 DTLS를 모두 비활성화할 수 있습니다. 이는 모든 트래픽이 오버헤드를 추가하는 UDP 대신 TCP를 사용한다는 의미이므로 이상적인 것은 아닙니다. 그러나 일부 시나리오에서는 적어도 대부분의 컨피그레이션이 정상이며 문제가 DTLS에만 해당된다는 것을 확인하는 좋은 테스트입니다. 이를 테스트하려면 관리자가 일반적으로 VPN 전화에 대해 고유한 그룹 정책을 사용하므로 다른 클라이언트에 영향을 주지 않고 변경 사항을 테스트할 수 있으므로 그룹 정책 수준에서 실행하는 것이 좋습니다.

group-policy vpn-phone-policy 특성
webvpn
anyconnect ssl dtls 없음

DTLS 연결에 성공할 수 없는 또 다른 일반적인 구성 문제는 전화기가 동일한 암호를 사용하여 TLS 및 DTLS 연결을 설정할 수 없는 경우입니다. 예시 로그:

```
%%%%% TLS Ciphers Offered
3905 NOT Apr 01 20:14:22.741838 (362:362) VPNC: -protocol_handler: new cipher -> ECDHE-RSA-
AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:AES256-SHA:AES128-SHA

%%%%% DTLS Ciphers Offered
4455 NOT Apr 01 20:14:23.405417 (362:362) VPNC: -process_connect: x-dtls-ciphersuite: AES128-SHA
4487 NOT Apr 01 20:14:23.523994 (362:362) VPNC: -create_dtls_connection: cipher list: AES128-SHA

%%%%% DTLS connection failure
4496 WRN Apr 01 20:14:53.547046 (362:474) VPNC: -vpnc_control: conn timer expired at:1585772093,
to abort connect
4497 NOT Apr 01 20:14:53.547104 (362:474) VPNC: -abort_connect: in dtls setup phase
```

코드 단본의 첫 줄에 제공되는 TLS 암호를 확인할 수 있습니다. 양측이 지원하는 가장 안전한 옵션이 선택됩니다(로그는 선택 사항을 표시하지 않지만 로그 조각에서 적어도 AES-256임을 추론할 수 있습니다). 제공되는 유일한 DTLS 암호는 AES128입니다. 선택한 TLS 암호를 DTLS에 사용할 수 없으므로 연결이 실패합니다. 이 시나리오의 수정 사항은 ASA 컨피그레이션에서 TLS 및 DTLS에 동일한 암호를 사용하도록 허용하는지 확인하는 것입니다.

인증서 업데이트 후 전화기에서 ASA에 연결할 수 없음

전화기가 이 새 인증서에 대한 해시를 획득할 수 있도록 CUCM에서 phone-vpn-trust로 새 ASA ID 인증서를 업로드하는 것이 매우 중요합니다. 이 프로세스를 수행하지 않으면 업데이트 후 VPN 전화기가 ASA에 연결을 시도할 때 전화기에 신뢰할 수 없는 인증서가 표시되므로 연결이 실패합니다. 인증서가 변경될 때 전화기의 연결이 끊기지 않기 때문에 ASA 인증서 업데이트 후 며칠 또는 몇 주가 지나도 이 문제가 발생할 수 있습니다. ASA가 전화기에서 keepalive를 계속 수신하는 경우 VPN 터널이 작동 상태로 유지됩니다. 따라서 ASA 인증서가 업데이트되었지만 새 인증서가 먼저 CUCM에 저장되지 않은 경우 두 가지 옵션이 있습니다.

1. 이전 ASA ID 인증서가 여전히 유효한 경우 ASA를 이전 인증서로 되돌린 다음 이 문서에서 제공된 프로세스를 따라 인증서를 업데이트합니다. 새 인증서를 이미 생성한 경우 인증서 생성 섹션을 건너뛸 수 있습니다.
2. 이전 ASA ID 인증서가 만료된 경우 새 ASA 인증서를 CUCM에 업로드하고 전화기를 내부 네트워크에 다시 가져와 새 인증서 해시로 업데이트된 컨피그레이션 파일을 받아야 합니다.

DNS를 통해 ASA URL을 확인할 수 없는 전화

일부 시나리오에서는 관리자가 IP 주소가 아닌 호스트 이름으로 VPN URL을 구성합니다. 이 작업을 수행하면 DNS 서버가 있어야 이름을 IP 주소로 확인할 수 있습니다. 코드 조각에서 전화기가 두 개의 DNS 서버(192.168.1.1 및 192.168.1.2)으로 이름을 확인하려고 하지만 응답을 받지 않음을 확인할 수 있습니다. 30초 후 전화기에서 'DnsLookupErr:'을 인쇄합니다.

```
3816 NOT Mar 3 15:38:03.819168 VPNC: -do_login: URL -> https://asav.sckiewer.lab/phone
...
3828 INF Mar 3 15:38:03.834915 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3829 INF Mar 3 15:38:03.835004 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3830 INF Mar 3 15:38:03.835030 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3831 INF Mar 3 15:38:17.845305 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3832 INF Mar 3 15:38:17.845352 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3833 INF Mar 3 15:38:17.845373 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3834 INF Mar 3 15:38:31.854834 dnsmasq[322]: query[A] asav.sckiewer.lab from 127.0.0.1
3835 INF Mar 3 15:38:31.854893 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.1
3836 INF Mar 3 15:38:31.855213 dnsmasq[322]: forwarded asav.sckiewer.lab to 192.168.1.2
3837 ERR Mar 3 15:38:32.864376 VPNC: -parse_url: gethostbyname failed <asav.sckiewer.lab>
```

```
3838 NOT Mar 3 15:38:32.864435 VPNC: -vpnc_set_notify_netsd : cmd: 0x5 event: 0x40000 status:
0x0 error: 0x0
3839 ERR Mar 3 15:38:32.864464 VPNC: -do_login: parse URL failed ->
https://asav.sckiewer.lab/phone
3840 NOT Mar 3 15:38:32.864482 VPNC: -vpn_stop: de-activating vpn
3841 NOT Mar 3 15:38:32.864496 VPNC: -vpn_set_auto: auto -> auto
3842 NOT Mar 3 15:38:32.864509 VPNC: -vpn_set_active: activated -> de-activated
3843 NOT Mar 3 15:38:32.864523 VPNC: -set_login_state: LOGIN: 1 (TRYING) --> 3 (FAILED)
3844 NOT Mar 3 15:38:32.864538 VPNC: -set_login_state: VPNC : 1 (LoggingIn) --> 3 (LoginFailed)
3845 NOT Mar 3 15:38:32.864561 VPNC: -vpnc_send_notify: notify type: 1 [LoginFailed]
3846 NOT Mar 3 15:38:32.864580 VPNC: -vpnc_send_notify: notify code: 32 [DnsLookupErr]
3847 NOT Mar 3 15:38:32.864611 VPNC: -vpnc_send_notify: notify desc: [url hostname lookup err]
```

이는 일반적으로 다음 중 하나를 나타냅니다.

1. 전화기에 잘못된 DNS 서버가 있습니다.
2. 전화기에서 DHCP를 통해 DNS 서버를 받지 못했거나 수동으로 구성되지 않았습니다.

이 문제를 해결하려면 두 가지 옵션이 있습니다.

1. 전화기의 컨피그레이션을 확인하여 DHCP 서버가 외부일 때 DNS 서버를 수신하는지 확인하고 전화기의 DNS 서버가 ASA 컨피그레이션에 사용된 이름을 확인할 수 있는지 확인합니다.
2. DNS가 필요하지 않도록 ASA 컨피그레이션의 URL 및 CUCM을 IP 주소로 변경합니다.

전화기가 VPN을 활성화하지 않음

이 문서의 앞부분에서 언급한 대로, Auto Network Detect는 전화기에서 TFTP 서버에 ping을 수행하고 응답을 확인합니다. 전화기가 내부 네트워크에 있는 경우 VPN 없이 TFTP 서버에 연결할 수 있으므로 전화기에서 ping에 대한 응답을 받을 때 VPN을 활성화하지 않습니다. 전화기가 내부 네트워크에 있지 않으면 ping이 실패하므로 전화기가 VPN을 활성화하고 ASA에 연결합니다. 클라이언트의 홈 네트워크는 DHCP를 통해 옵션 150을 전화기에 제공하도록 구성되지 않을 가능성이 있으며 ASA는 옵션 150을 제공할 수 없으므로 '대체 TFTP'는 VPN 전화기에 대한 요구 사항입니다.

로그에서 몇 가지 사항을 확인합니다.

1. 전화기가 CUCM TFTP 서버 IP에 대해 ping을 수행합니까?
2. 전화기에서 전화에 대한 응답을 받습니까?
3. 전화기에서 ping에 대한 응답을 받지 못한 후 VPN을 활성화합니까?

이 순서대로 이러한 항목을 보는 것이 중요합니다. 전화기가 잘못된 IP를 ping하고 응답을 수신하는 경우 전화기가 VPN을 활성화하지 않으므로 ASA에서 디버그를 활성화하면 의미가 없습니다. 불필요한 로그 분석을 방지할 수 있도록 이러한 3가지 사항을 이 순서로 검증합니다. ping이 실패하고 이후에 VPN이 활성화된 경우 88xx 전화 로그에서 이를 확인할 수 있습니다.

```
5645 NOT Mar 27 11:32:34.630109 (574:769) JAVA-vpnAutoDetect: ping time out
5647 DEB Mar 27 11:32:34.630776 (710:863) JAVA-configmgr MQThread|cip.vpn.VpnStateHandler:? -
VpnStateHandler: handleVPN_ENABLED_STATE()
```

전화 등록이 등록되지만 통화 기록을 표시할 수 없음

전화기에 Alternate TFTP가 활성화되었고 올바른 TFTP IP가 구성되었는지 확인합니다. ASA는 옵션 150을 제공할 수 없으므로 대체 TFTP는 VPN 전화기의 요구 사항입니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems