Cisco IOS 라우터 컨피그레이션에 대한 AnyConnect VPN Phone 연결 예

목차

소개

이 문서에서는 Cisco IP Phone에서 Cisco IOS 라우터에 대한 VPN 연결을 설정할 수 있도록 Cisco IOS® 라우터 및 Call Manager 디바이스를 구성하는 방법에 대해 설명합니다. 다음 두 클라이언트 인증 방법 중 하나와의 통신을 보호하려면 이러한 VPN 연결이 필요합니다.

- AAA(Authentication, Authorization, and Accounting) 서버 또는 로컬 데이터베이스
- 전화 인증서

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 하드웨어 및 소프트웨어 버전을 기반으로 합니다.

- Cisco IOS 15.1(2)T 이상
- 기능 집합/라이센스: Cisco IOS ISR(Integrated Service Router)-G2용 범용(데이터 및 보안, UC)
- 기능 집합/라이센스: Cisco IOS ISR을 위한 고급 보안
- Cisco Unified Communications Manager(CUCM) 릴리스 8.0.1.100000-4 이상
- IP Phone Release 9.0(2)SR1S - SCCP(Skinny Call Control Protocol) 이상

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 사설 네트워크.

이 컨피그레이션 예에서 사용되는 릴리스는 다음과 같습니다.

- Cisco IOS Router 릴리스 15.1(4)M4
- Call Manager 릴리스 8.5.1.10000-26
- IP Phone 릴리스 9.1(1)SR1S

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.

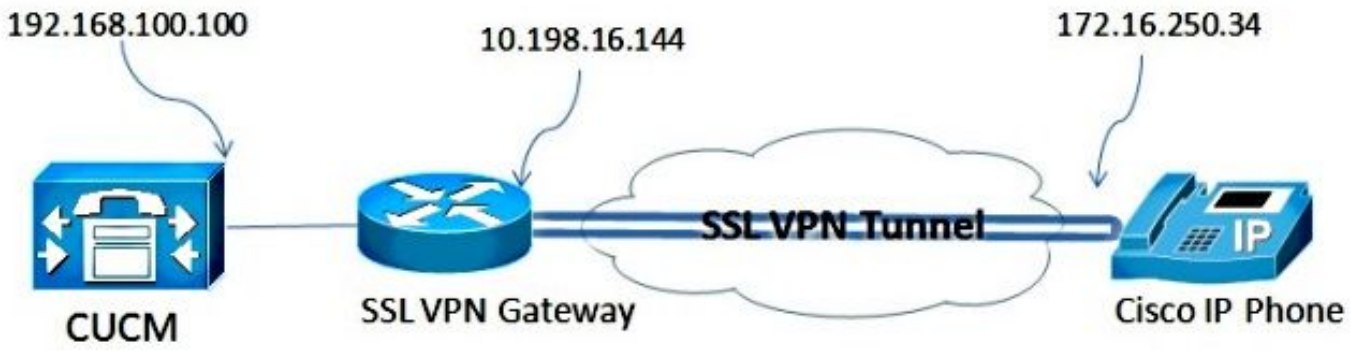
구성

이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 필요한 정보를 다룹니다.

> 참고: 이 섹션에 사용된 명령에 대한 자세한 내용을 가져오려면 명령 조회 툴(등록 고객 전용)을 사용하십시오.

네트워크 토폴로지

이 문서에 사용된 토폴로지에는 Cisco IP Phone 1개, Cisco IOS Router as the Secure Sockets Layer (SSL) VPN Gateway, CUCM as the voice gateway가 포함됩니다.



SSL VPN 서버 컨피그레이션

이 섹션에서는 인바운드 SSL VPN 연결을 허용하기 위해 Cisco IOS 헤드엔드를 구성하는 방법에 대해 설명합니다.

공통 컨피그레이션 단계

1. 길이가 1024바이트인 RSA(Rivest-Shamir-Adleman) 키를 생성합니다.

```
<#root>

Router(config)#

crypto key generate rsa general-keys label SSL modulus 1024
```

2. 자체 서명 인증서에 대한 신뢰 지점을 생성하고 SSL RSA 키를 연결합니다.

```
<#root>

Router(config)#

crypto pki trustpoint server-certificate


 enrollment selfsigned
 usage ssl-server
 serial-number
 subject-name CN=10.198.16.144
 revocation-check none
 rsakeypair SSL
```

3. 신뢰 지점이 구성되면 다음 명령을 사용하여 자체 서명 인증서를 등록합니다.

```
<#root>

Router(config)#
```

```
crypto pki enroll

server-certificate


% Include an IP address in the subject name? [no]: no
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

4. 헤드엔드에서 올바른 AnyConnect 패키지를 활성화합니다. 전화기 자체에서 이 패키지를 다운로드하지 않습니다. 그러나 패키지가 없으면 VPN 터널이 설정되지 않습니다. Cisco.com에서 사용할 수 있는 최신 클라이언트 소프트웨어 버전을 사용하는 것이 좋습니다. 이 예에서는 버전 3.1.3103을 사용합니다.

   이전 Cisco IOS 버전에서는 패키지를 활성화하기 위한 명령입니다.

   ```
   <#root>

   Router(config)#

   webvpn install svc flash:anyconnect-win-3.1.03103-k9.pkg
   ```

   그러나 최신 Cisco IOS 버전에서는 다음 명령을 사용합니다.

   ```
   <#root>

   Router(config)#

   crypto vpn anyconnect flash:/webvpn/anyconnect-win-
   3.1.03103-k9.pkg sequence 1
   ```

5. VPN 게이트웨이를 구성합니다. WebVPN 게이트웨이는 사용자로부터의 SSL 연결을 종료하는 데 사용됩니다.

   ```
   webvpn gateway SSL
   ip address 10.198.16.144 port 443
    ssl encryption 3des-sha1 aes-sha1
    http-redirect port 80
    ssl trustpoint server-certificate
    inservice
   ```

   참고: 여기서 사용하는 IP 주소는 전화기가 연결되는 인터페이스와 동일한 서브넷에 있거나, 게이트웨이는 라우터의 인터페이스에서 직접 소싱해야 합니다. 게이트웨이는 라우터가 클라이언트에 대한 인증을 위해 어떤 인증서를 사용할지를 정의하는 데에도 사용됩니다.

   ---

6. 클라이언트가 연결할 때 IP 주소를 클라이언트에 할당하기 위해 사용되는 로컬 풀을 정의합니다.

```
ip local pool ap_phonevpn 192.168.100.1 192.168.100.254
```

AAA 인증을 사용한 컨피그레이션

이 섹션에서는 AAA 서버 또는 로컬 데이터베이스를 구성하여 전화기를 인증하는 데 필요한 명령에 대해 설명합니다. 전화기에 대해 인증서 전용 인증을 사용하려는 경우 다음 섹션으로 진행합니다.

사용자 데이터베이스 구성

라우터의 로컬 데이터베이스 또는 외부 AAA 서버를 인증에 사용할 수 있습니다.

- 로컬 데이터베이스를 구성하려면 다음을 입력합니다.

```
aaa new-model
aaa authentication login SSL local
username phones password 0 phones
```

- 인증을 위해 원격 AAA RADIUS 서버를 구성하려면 다음을 입력합니다.

```
aaa new-model
aaa authentication login SSL group radius
radius-server host 192.168.100.200 auth-port 1812 acct-port 1813
radius-server key cisco
```

가상 컨텍스트 및 그룹 정책 구성

가상 컨텍스트는 다음과 같이 VPN 연결을 제어하는 특성을 정의하는 데 사용됩니다.

- 연결할 때 사용할 URL
- 클라이언트 주소를 할당하기 위해 사용할 풀
- 사용할 인증 방법

다음 명령은 클라이언트에 대해 AAA 인증을 사용하는 컨텍스트의 예입니다.

```
webvpn context SSL
 aaa authenticate list SSL
 gateway SSL domain SSLPhones
 !
 ssl authenticate verify all
 inservice
 !
 policy group phones
  functions svc-enabled
```

```
  svc address-pool "ap_phonevpn" netmask 255.255.255.0
  svc keep-client-installed
default-group-policy phones
```

클라이언트 인증을 위한 IP Phone LSC(Locally Significant Certificate)를 사용한 컨피그레이션

이 섹션에서는 전화기에 대한 인증서 기반 클라이언트 인증을 구성하는 데 필요한 명령에 대해 설명합니다. 그러나 이를 위해서는 다양한 유형의 전화 인증서에 대한 지식이 필요합니다.

- MIC(Manufacturer Installed Certificate) - 모든 7941, 7961 및 최신 모델 Cisco IP Phone에 MIC가 포함되어 있습니다. MIC는 Cisco CA(Certificate Authority)에서 서명한 2,048비트 키 인증서입니다. CUCM에서 MIC 인증서를 신뢰하려면 인증서 신뢰 저장소에 사전 설치된 CA 인증서 CAP-RTP-001, CAP-RTP-002 및 Cisco_Manufacturing_CA를 사용합니다. 이 인증서는 이름에 표시된 대로 제조업체 자체에서 제공되므로 클라이언트 인증에 이 인증서를 사용하지 않는 것이 좋습니다.
- LSC - 인증 또는 암호화를 위해 디바이스 보안 모드를 구성한 후 LSC가 CUCM과 전화기 간의 연결을 보호합니다. LSC는 CUCM CAPF(Certificate Authority Proxy Function) 개인 키로 서명된 Cisco IP Phone의 공개 키를 보유합니다. 이것이 더 안전한 방법입니다(MIC 사용과 반대).

주의: 보안 위험이 증가함에 따라 MIC는 계속 사용하지 않고 LSC 설치에만 사용하는 것이 좋습니다. TLS(Transport Layer Security) 인증 또는 기타 용도로 MIC를 사용하기 위해 Cisco IP Phone을 구성하는 고객은 위험을 감수하고 이를 수행합니다.

이 컨피그레이션 예에서는 LSC를 사용하여 전화기를 인증합니다.

팁: 전화기에 연결하는 가장 안전한 방법은 인증서와 AAA 인증을 결합한 이중 인증을 사용하는 것입니다. 각 가상 컨텍스트에 사용되는 명령을 하나의 가상 컨텍스트로 결합할 경우 이를 구성할 수 있습니다.

클라이언트 인증서를 검증하기 위해 신뢰 지점 구성

IP 전화에서 LSC를 검증하려면 라우터에 CAPF 인증서가 설치되어 있어야 합니다. 인증서를 가져와 라우터에 설치하려면 다음 단계를 완료하십시오.

1. CUCM Operating System (OS) Administration(CUCM 운영 체제(OS) 관리) 웹 페이지로 이동합니다.
2. Security(보안) > Certificate Management(인증서 관리)를 선택합니다.

참고: 이 위치는 CUCM 버전에 따라 변경될 수 있습니다.

---

3. CAPF라는 레이블이 지정된 인증서를 찾아 .pem 파일을 다운로드합니다. 파일을 .txt 파일로 저장
4. 인증서가 추출되면 여기에 표시된 것처럼 라우터에 새 신뢰 지점을 생성하고 CAPF를 사용하여 신뢰 지점을 인증합니다. Base64 인코딩 CA 인증서를 묻는 메시지가 표시되면 다운로드

한 .pem 파일의 텍스트를 BEGIN 및 END 행과 함께 선택하여 붙여넣습니다.
<#root>

```
Router(config)#

crypto pki trustpoint CAPF


 enrollment terminal
 authorization username subjectname commonname
 revocation-check none
Router(config)#

crypto pki authenticate CAPF


Router(config)#









 quit
```

참고 사항:

- 인증서가 라우터에 수동으로 설치되어야 하므로 등록 방법은 터미널입니다.
- 클라이언트가 연결을 수행할 때 사용자 이름으로 사용할 것을 라우터에 알려주려면 authorization username 명령이 필요합니다. 이 경우 CN(Common Name)을 사용합니다.
- 전화 인증서에 정의된 CRL(Certificate Revocation List)이 없으므로 해지 검사를 비활성화해야 합니다. 따라서 비활성화되지 않으면 연결이 실패하고 PKI(Public Key Infrastructure) 디버깅에 이 출력이 표시됩니다.

<#root>

```
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076)

 Starting CRL revocation check


Jun 17 21:49:46.695: CRYPTO_PKI:

Matching CRL not found


Jun 17 21:49:46.695: CRYPTO_PKI: (A0076)

 CDP does not exist. Use SCEP to
query CRL.


Jun 17 21:49:46.695: CRYPTO_PKI: pki request queued properly
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation check is complete, 0
Jun 17 21:49:46.695: CRYPTO_PKI: Revocation status = 3
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: poll CRL
```

```
Jun 17 21:49:46.695: CRYPTO_PKI: Remove session revocation service providers
CRYPTO_PKI: Bypassing SCEP capabilies request 0
Jun 17 21:49:46.695: CRYPTO_PKI: status = 0: failed to create GetCRL
Jun 17 21:49:46.695: CRYPTO_PKI: enrollment url not configured
Jun 17 21:49:46.695: CRYPTO_PKI: transaction GetCRL completed
Jun 17 21:49:46.695: CRYPTO_PKI: status = 106: Blocking chain verification
callback received status
Jun 17 21:49:46.695: CRYPTO_PKI: (A0076)

Certificate validation failed
```

가상 컨텍스트 및 그룹 정책 구성

컨피그레이션의 이 부분은 두 점을 제외하고 이전에 사용한 컨피그레이션과 유사합니다.

- 인증 방법
- 컨텍스트에서 전화기를 인증하기 위해 사용하는 신뢰 지점

명령은 다음과 같습니다.

```
webvpn context SSL
 gateway SSL domain SSLPhones
 authentication certificate
 ca trustpoint CAPF
 !
 ssl authenticate verify all
 inservice
 !
 policy group phones
 functions svc-enabled
 svc address-pool "ap_phonevpn" netmask 255.255.255.0
 svc keep-client-installed
 default-group-policy phones
```

Call Manager 구성

이 섹션에서는 Call Manager 컨피그레이션 단계에 대해 설명합니다.

라우터에서 CUCM으로 자체 서명 또는 ID 인증서 내보내기

라우터에서 인증서를 내보내고 Call Manager로 Phone-VPN-Trust 인증서로 인증서를 가져오려면 다음 단계를 완료하십시오.

1. SSL에 사용된 인증서를 확인합니다.

```
<#root>

Router#

show webvpn gateway SSL
```

```
SSL Trustpoint: server-certificate
```

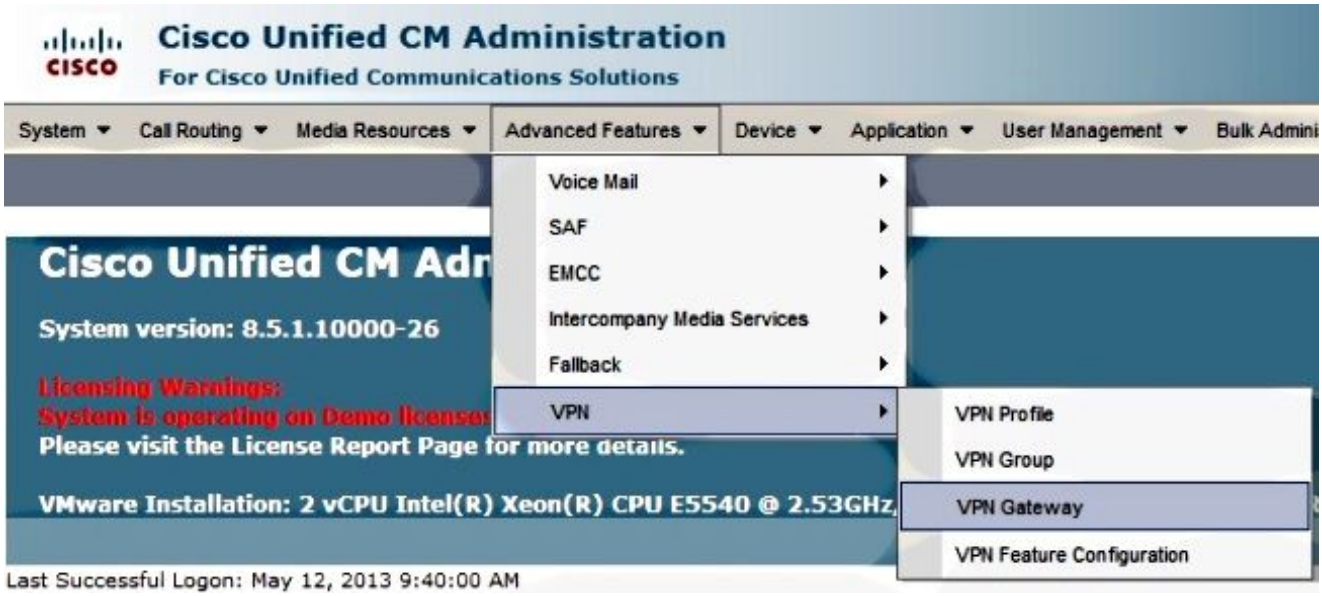
2. 인증서 내보내기

```
<#root>

Router(config)#

crypto pki export server-certificate pem terminal


The Privacy Enhanced Mail (PEM) encoded identity certificate follows:
-----BEGIN CERTIFICATE-----

<output removed>

-----END CERTIFICATE-----
```

3. 터미널에서 텍스트를 복사하여 .pem 파일로 저장합니다.
4. Call Manager에 로그인하고 Unified OS Administration > Security > Certificate Management > Upload Certificate > Select Phone-VPN-trust를 선택하여 이전 단계에서 저장된 인증서 파일을 업로드합니다.

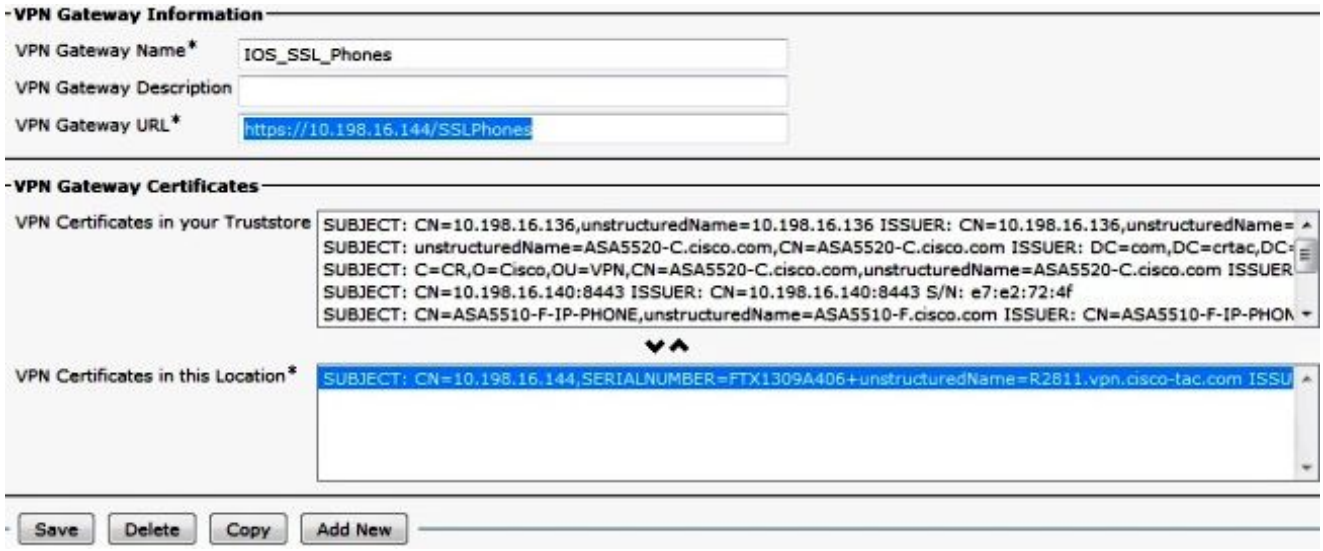
CUCM에서 VPN 게이트웨이, 그룹 및 프로파일 구성

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.



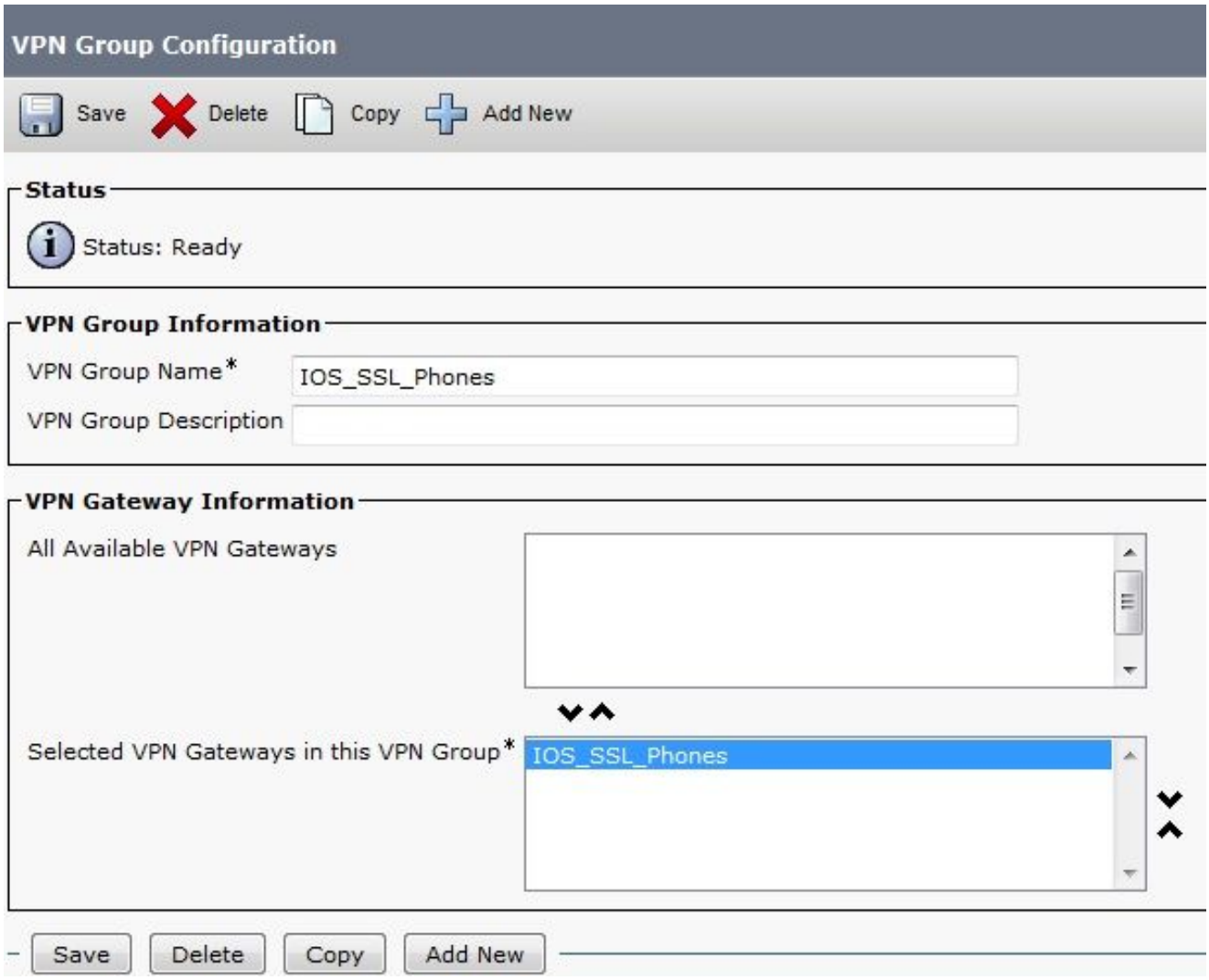
3. VPN Gateway Configuration(VPN 게이트웨이 컨피그레이션) 창에서 다음 단계를 완료합니다.
   - VPN Gateway Name(VPN 게이트웨이 이름) 필드에 이름을 입력합니다. 어떤 이름이든 가능합니다.
   - VPN Gateway Description 필드에 설명(선택 사항)을 입력합니다.

- VPN Gateway URL(VPN 게이트웨이 URL) 필드에 라우터에 정의된 그룹 URL을 입력합니다.
- 이 위치의 VPN Certificates(VPN 인증서) 필드에서 트러스트 저장소에서 이 위치로 이동하기 위해 이전에 Call Manager에 업로드한 인증서를 선택합니다.

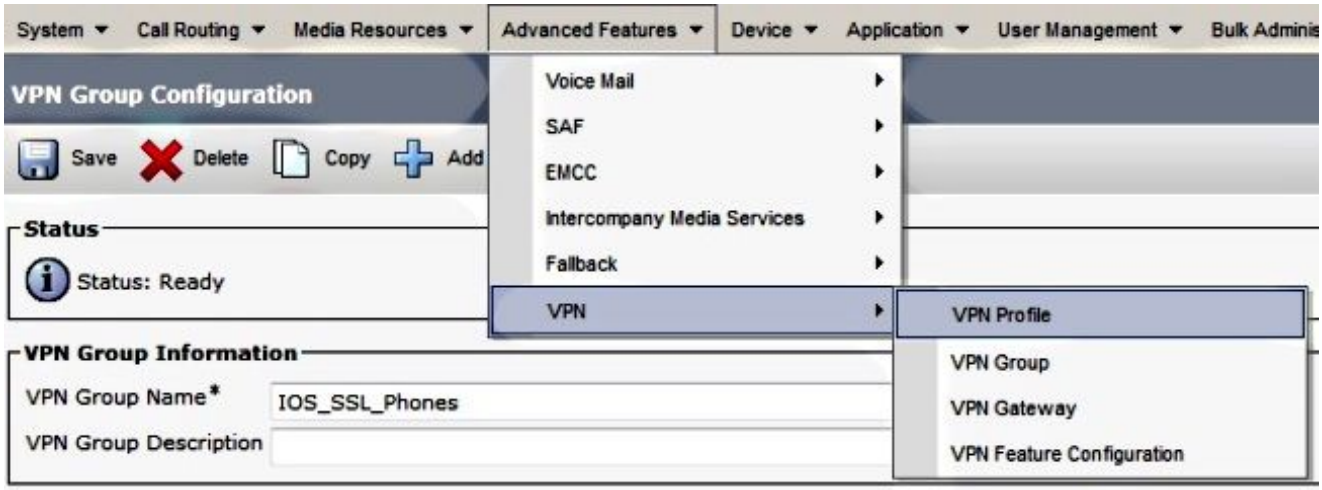


4. 메뉴 모음에서 Advanced Features(고급 기능) > VPN > VPN Group(VPN 그룹)을 선택합니다.

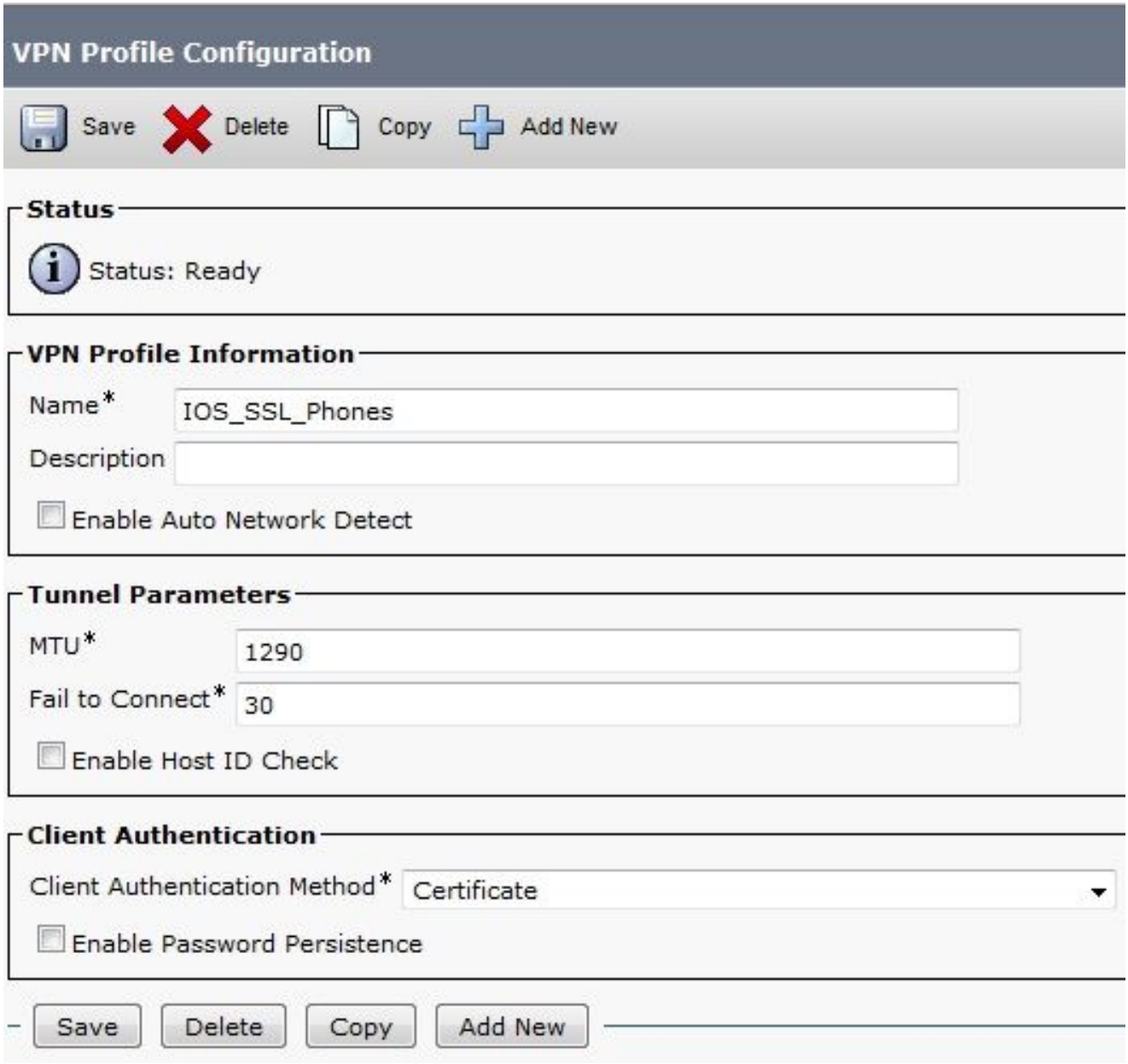
5. All Available VPN Gateways(사용 가능한 모든 VPN 게이트웨이) 필드에서 이전에 정의된 VPN 게이트웨이를 선택합니다. 선택한 게이트웨이를 이 VPN Group(VPN 그룹) 필드에서 Selected VPN Gateways(선택한 VPN 게이트웨이)로 이동하려면 아래쪽 화살표를 클릭합니다.



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



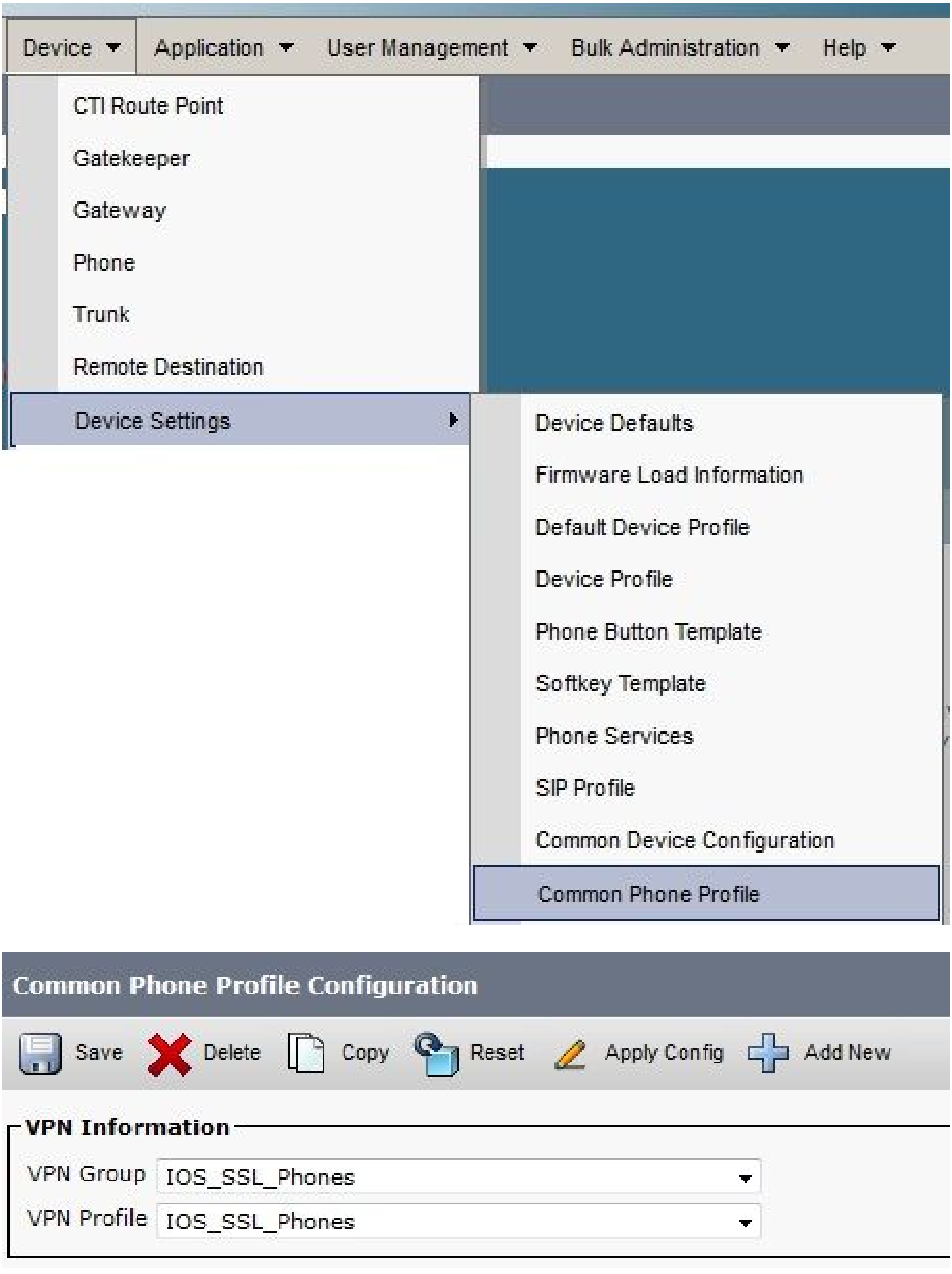
7. VPN 프로필을 구성하려면 별표(*)가 표시된 모든 필드를 작성합니다.



- Auto Network Detect 활성화: 활성화된 경우 VPN 폰이 TFTP 서버에 ping합니다. 응답이 수신되지 않으면 VPN 연결이 자동으로 시작됩니다.
- Enable Host ID Check(호스트 ID 확인 활성화): 활성화된 경우 VPN 전화기는 VPN 게이트웨이 URL의 FQDN(정규화된 도메인 이름)을 인증서의 CN/SAN(저장소 영역 네트워크)과 비교합니다. 이러한 항목이 일치하지 않거나 별표(*)가 있는 와일드카드 인증서가 사용되는 경우 클라이언트가 연결하지 못합니다.
- 비밀번호 지속성 활성화: 그러면 VPN 전화기에서 다음 VPN 시도를 위해 사용자 이름과 비밀번호를 캐시할 수 있습니다.

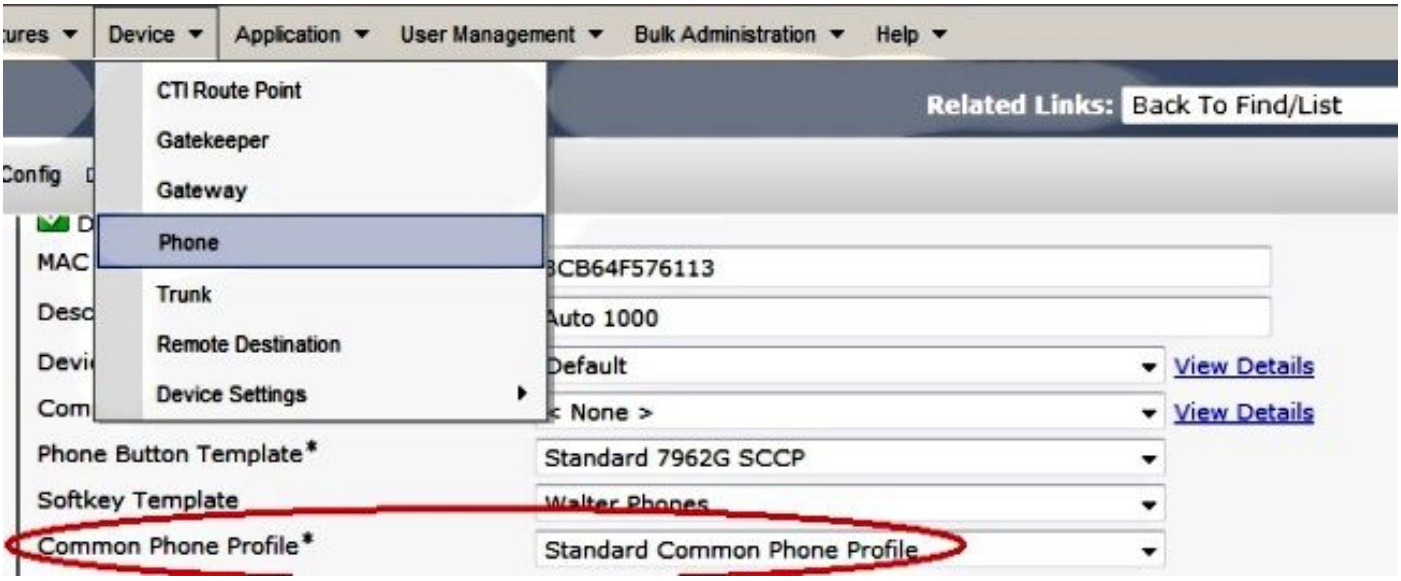
공통 전화기 프로필을 사용하여 IP 전화기에 그룹 및 프로필 적용

새 VPN 컨피그레이션을 적용하려면 Common Phone Profile Configuration(일반 전화기 프로필 컨피그레이션) 창에서 Apply Config(컨피그레이션 적용)를 클릭합니다. 표준 일반 전화기 프로필을 사용하거나 새 프로필을 생성할 수 있습니다.



IP Phone에 일반 전화기 프로필 적용

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



Cisco IP Phone에 LSC(Locally Significant Certificates) 설치

다음 설명서는 Cisco IP Phone에 Locally Significant Certificates를 설치하는 데 사용할 수 있습니다. 이 단계는 LSC를 사용한 인증이 사용되는 경우에만 필요합니다. MIC(Manufacturer Installed Certificate) 또는 사용자 이름과 비밀번호를 사용한 인증에는 LSC를 설치할 필요가 없습니다.

CUCM Cluster Security Mode(CUCM 클러스터 보안 모드)가 Non-Secure(비보안)로 설정된 전화기에 LSC를 설치합니다.

새 구성을 다운로드하려면 Call Manager에 전화를 다시 등록하십시오.

이는 구성 프로세스의 마지막 단계입니다.

다음을 확인합니다.

라우터 확인

라우터에서 VPN 세션의 통계를 확인하려면 다음 명령을 사용하고 사용자 이름과 인증서 인증에 대한 출력(강조 표시)의 차이를 확인할 수 있습니다.

사용자 이름/비밀번호 인증의 경우

<#root>

```
Router#

show webvpn session user phones context SSL

Session Type      : Full Tunnel
```

```
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username          :
```

phones

```
               Num Connection : 1
Public IP         : 172.16.250.34        VRF Name       : None
Context           : SSL                  Policy Group   : SSLPhones
Last-Used         : 00:00:29             Created        : 15:40:21.503 GMT
Fri Mar 1 2013
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : SSL                  MTU Size       : 1290
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 10.10.10.1           Netmask        : 255.255.255.0
Rx IP Packets     : 106                  Tx IP Packets  : 145
CSTP Started      : 00:11:15             Last-Received  : 00:00:29
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Client Ports      : 51534
DTLS Port         : 52768
Router#

Router#
```

show webvpn session context all

```
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
```

phones

```
             172.16.250.34              1         00:30:38  00:00:20
```

인증서 인증:

<#root>

```
Router#
```

show webvpn session user SEP8CB64F578B2C context all

```
Session Type      : Full Tunnel
Client User-Agent : Cisco SVC IPPhone Client v1.0 (1.0)

Username          :
```

SEP8CB64F578B2C

```
      Num Connection : 1
Public IP         : 172.16.250.34        VRF Name       : None
```

CA Trustpoint : CAPF

```
Context           : SSL                  Policy Group   :
```

```
Last-Used         : 00:00:08            Created        : 13:09:49.302 GMT
Sat Mar 2 2013
Session Timeout   : Disabled            Idle Timeout   : 2100
DPD GW Timeout    : 300                 DPD CL Timeout : 300
Address Pool      : SSL                 MTU Size       : 1290
Rekey Time        : 3600                Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 10.10.10.2          Netmask        : 255.255.255.0
Rx IP Packets     : 152                 Tx IP Packets  : 156
CSTP Started      : 00:06:44            Last-Received  : 00:00:08
CSTP DPD-Req sent : 0                   Virtual Access : 1
Msie-ProxyServer  : None                Msie-PxyPolicy : Disabled
Msie-Exception    :
Client Ports      : 50122
DTLS Port         : 52932
```

```
Router#
```

show webvpn session context all

```
WebVPN context name: SSL
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
```

SEP8CB64F578B2C

```
    172.16.250.34              1         3d04h     00:00:16
```

CUCM 확인

IP Phone이 Call Manager에 SSL 연결에 라우터가 제공한 할당된 주소로 등록되어 있는지 확인합니다.

문제 해결

SSL VPN 서버에서 디버깅

<#root>

```
Router#
```

show debug

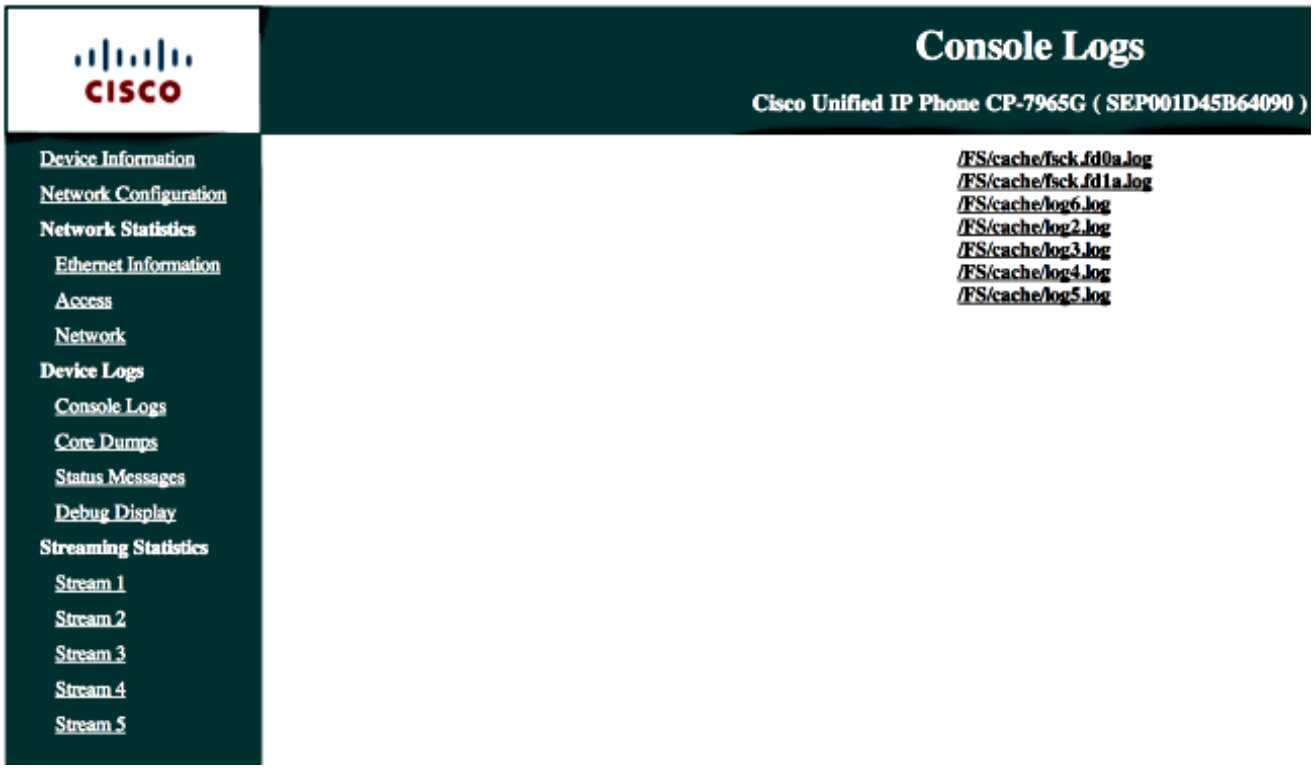
```
WebVPN Subsystem:
 WebVPN (verbose) debugging is on
```

```
 WebVPN HTTP debugging is on
 WebVPN AAA debugging is on
 WebVPN tunnel debugging is on
 WebVPN Tunnel Events debugging is on
 WebVPN Tunnel Errors debugging is on
 Webvpn Tunnel Packets debugging is on


PKI:
 Crypto PKI Msg debugging is on
 Crypto PKI Trans debugging is on
 Crypto PKI Validation Path debugging is on
```

전화에서 디버깅

1. CUCM에서 Device(디바이스) > Phone(전화기)으로 이동합니다.
2. 디바이스 컨피그레이션 페이지에서 Web Access(웹 액세스)를 Enabled(활성화됨)로 설정합니다.
3. Save(저장)를 클릭한 다음 Apply Config(컨피그레이션 적용)를 클릭합니다.

4. 브라우저에서 전화기의 IP 주소를 입력하고 왼쪽의 메뉴에서 Console Logs(콘솔 로그)를 선택합니다.



5. 모든 /FS/cache/log*.log 파일을 다운로드합니다. 콘솔 로그 파일에는 전화기가 VPN에 연결하지 못하는 이유에 대한 정보가 들어 있습니다.

관련 버그

Cisco 버그 ID CSCty46387 , IOS SSLVPN: 컨텍스트가 기본값이 되도록 개선
Cisco 버그 ID CSCty46436 , IOS SSLVPN: 클라이언트 인증서 유효성 검사 동작 개선

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.