VPN 클라이언트

VPN 클라이언트 개요

Cisco Unified IP Phone의 Cisco VPN 클라이언트는 재택 근무하는 직원에 대한 보안 VPN 연결을 생성합니다. Cisco VPN 클라이언트의 모든 설정은 Cisco Unified Communications Manager Administration를 통해 구성됩니다. 엔터프라이즈 내에서 전화기를 구성한 후에는 사용자가 인스턴트 연결을 위해 해당 디바이스를 광대역 라우터에 연결할 수 있습니다.

참고 Unified Communications Manager의 미국 수출 무제한 버전에서는 VPN 메뉴 및 관련 옵션을 사용할 수 없습니다.

VPN 클라이언트 사전 요건

전화기를 사전 준비하고 회사 네트워크 내에서 초기 연결을 설정하여 전화기 구성을 검색합니다. 전화기에서 구성이 이미 검색되었으므로 VPN을 사용하여 후속 연결을 설정할 수 있습니다.

VPN 클라이언트 구성 작업 흐름

전화기를 사전 준비하고 회사 네트워크 내에서 초기 연결을 설정하여 전화기 구성을 검색합니다. 전화기에서 구성이 이미 검색되었으므로 VPN을 사용하여 후속 연결을 설정할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	전체 Cisco IOS 사전 요건, 3 페이지	전체 Cisco IOS 사전 요건 Cisco IOS VPN을 구성하려는 경우 이 작업을 수행합니다.
단계 **2**	IP 전화기를 지원하도록 Cisco IOS SSL VPN 구성 , 3 페이지	IP 전화기에서 VPN 클라이언트용 Cisco IOS를 구성합니다. Cisco IOS VPN을 구성하려는 경우 이 작업을 수행합니다.
단계 **3**	AnyConnect에 대한 전체 ASA 사전 요건, 5 페이지	AnyConnect에 대한 전체 ASA 사전 요건 ASA VPN을 구성하려면 이 작업을 수행합니다.
단계 **4**	IP 전화기에서 VPN 클라이언트에 대한 ASA 구성, 6 페이지	IP 전화기에서 VPN 클라이언트에 대한 ASA를 구성합니다. ASA VPN을 구성하려면 이 작업을 수행합니다.
단계 **5**	각 VPN 게이트웨이에 대한 VPN 집중 디바이스를 구성합니다.	사용자가 원격 전화기에서 펌웨어 또는 구성 정보를 업그레이드할 때 오랜 지연이 발생하지 않도록 하려면 네트워크에서 TFTP 또는 Unified Communications Manager 서버에 VPN 집중 디바이스 닫기를 설정합니다. 네트워크에서 이 방법이 적합하지 않은 경우에는 VPN 집중 디바이스 옆에 있는 대체 TFTP 또는 로드 서버를 설정할 수 있습니다.
단계 **6**	VPN 집중 디바이스 인증서 업로드, 8 페이지	VPN 집중 디바이스 인증서를 업로드합니다.
단계 **7**	VPN 게이트웨이 구성, 9 페이지	VPN 게이트웨이를 구성합니다.
단계 **8**	VPN 그룹 구성, 10 페이지	VPN 그룹을 만든 후에는 방금 구성한 VPN 게이트웨이 중 하나를 여기 추가할 수 있습니다.
단계 **9**	다음 중 하나를 수행합니다. • VPN 프로파일 구성, 11 페이지 • VPN 기능 매개 변수 구성, 12 페이지	여러 VPN 그룹이 있는 경우에만 VPN 프로파일을 구성해야 합니다. VPN 프로파일 필드는 VPN 기능 구성 필드보다 우선합니다.
단계 **10**	일반 전화 프로파일에 VPN 세부 정보 추가, 14 페이지	VPN 그룹 및 VPN 프로파일을 일반 전화 프로파일에 추가합니다.
단계 **11**	VPN을 지원하는 버전으로 Cisco Unified IP Phone의 펌웨어를 업그레이드합니다.	Cisco VPN 클라이언트를 실행하려면 지원되는 Cisco Unified IP Phone에서 펌웨어 릴리스 9.0(2) 이상을 실행하고 있어야합니다. 펌웨어 업그레이드에 대한 자세한 내용은 해당 Cisco Unified IP Phone 모델에 대한 Unified Communications Manager의 *Cisco Unified IP Phone* 관리 지침서를 참조하십시오.

	명령 또는 동작	목적
단계 **12**	지원되는 Cisco Unified IP Phone을(를) 사용하여 VPN 연결을 설정합니다.	Cisco Unified IP Phone을(를) VPN에 연결합니다.

전체 **Cisco IOS** 사전 요건

이 절차를 사용하여 Cisco IOS 사전 요건을 완료합니다.

프로시저

단계 **1** Cisco IOS 소프트웨어 버전 15.1(2)T 이상을 설치합니다.

기능 집합/라이센스: IOS ISR-G2 및 ISR-G3에 대한 유니버설(데이터와 보안 및 UC)

기능 집합/라이센스: IOS ISR에 대한 고급 보안

단계 **2** SSL VPN 라이센스를 활성화합니다.

IP 전화기를 지원하도록 **Cisco IOS SSL VPN** 구성

이 절차를 사용하여 IP 전화기를 지원하기 위해 Cisco IOS SSL VPN을 완료할 수 있습니다.

프로시저

단계 **1** Cisco IOS를 로컬로 구성합니다.

a) 네트워크 인터페이스를 구성합니다.

예:

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) 다음 명령을 사용하여 정적 및 기본 라우트를 구성합니다.

router(config)# **ip route** <*dest_ip*> < *mask*> < *gateway_ip*>

예:

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

단계 **2** CAPF 인증서를 생성 및 등록하여 LSC를 사용하여 IP 전화기를 인증합니다.

단계 **3** Unified Communications Manager에서 CAPF 인증서를 가져옵니다.

a) Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.

참고 이 위치는 Unified Communications Manager 버전을 기반으로 변경됩니다.

b) Cisco_Manufacturing_CA 및 CAPF 인증서를 찾습니다. .pem 파일을 다운로드하고 .txt 파일로 저장합니다.

c) Cisco IOS 소프트웨어에서 트러스트 포인트를 생성합니다.

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

Base64 인코딩 CA 인증서를 묻는 메시지가 나타나면 다운로드한 .pem 파일에 BEGIN 및 END 라인과 함께 텍스트를 복사하여 붙여넣습니다. 다른 인증서에 대해 절차를 반복합니다.

d) 다음 Cisco IOS 자체 서명 인증서를 생성하고 Unified Communications Manager로 등록하거나 CA에서 가져오는 인증서로 대체합니다.

- SSC(자가서명 인증서)를 생성합니다.

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Unified Communications Manager의 VPN 프로파일에서 호스트 ID 확인을 활성화한 상태에서 SSC(자가서명 인증서)를 생성합니다.

  예:

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- 생성된 인증서를 Unified Communications Manager에 등록합니다.

  예:

```
Router(config)# crypto pki export <name> pem terminal
```

  터미널에서 텍스트를 복사하여 .pem 파일로 저장하고 Cisco Unified OS 관리를 사용하여 Unified Communications Manager에 업로드합니다.

단계 **4** Cisco IOS에 AnyConnect를 설치합니다.

cisco.com에서 Anyconnect 패키지를 다운로드하고 플래시에 설치합니다.

예:

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

단계 **5** VPN 기능을 구성합니다.

참고 인증서 및 암호 인증과 함께 전화기를 사용하려면 전화기 MAC 주소를 사용하여 사용자를 만듭니다. 사용자 이름 일치는 대/소문자를 구분합니다. 예:

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

AnyConnect에 대한 전체 ASA 사전 요건

이 절차를 사용하여 AnyConnect에 대한 ASA 사전 요건을 완료합니다.

프로시저

단계 **1** ASA 소프트웨어(버전 8.0.4 이상)와 호환되는 ASDM을 설치합니다.

단계 **2** 호환되는 AnyConnect 패키지를 설치합니다.

단계 **3** 라이선스를 활성화합니다.

a) 다음 명령을 사용하여 현재 라이센스의 기능을 확인합니다.

show activation-key detail

b) 필요한 경우 추가 SSL VPN 세션을 사용하여 새 라이센스를 받고 Linksys 전화기를 활성화합니다.

단계 **4** 다음과 같이 기본이 아닌 URL을 사용하여 터널 그룹을 구성해야 합니다.

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

기본값이 아닌 URL을 구성하는 경우 다음 사항을 고려하십시오.

- 서버의 IP 주소에 공용 DNS 항목이 있는 경우 FQDN(정규화된 도메인 이름)으로 바꿀 수 있습니다.
- Unified Communications Manager의 VPN 게이트웨이에서는 단일 URL(FQDN 또는 IP 주소)만 사용할 수 있습니다.
- 인증서 CN 또는 주체 대체 이름이 group-url의 FQDN 또는 IP 주소와 일치하는 것이 좋습니다.
- ASA 인증서 CN 또는 SAN이 FQDN 또는 IP 주소와 일치하지 않으면 Unified Communications Manager에서 호스트 ID 확인란의 선택을 취소합니다.

IP 전화기에서 VPN 클라이언트에 대한 ASA 구성

이 절차를 사용하여 IP 전화기의 VPN 클라이언트에 대해 ASA를 구성합니다.

참고 ASA 인증서를 대체하면 Unified Communications Manager를 사용할 수 없게 됩니다.

프로시저

단계 **1** 로컬 구성

a) 네트워크 인터페이스를 구성합니다.

예:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) 정적 경로 및 기본 경로를 구성합니다.

ciscoasa(config)# **route** <interface_name> <ip_address> <netmask> <gateway_ip>

예:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) DNS를 구성합니다.

예:

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

단계 **2** Unified Communications Manager 및 ASA에 필요한 인증서를 생성하고 등록합니다.

Unified Communications Manager에서 다음 인증서를 가져옵니다.

- CallManager - TLS 핸드셰이크 중 Cisco UCM을 인증합니다(혼합 모드 클러스터에만 필요).
- Cisco_Manufacturing_CA - 제조업체에서 설치한 인증서(MIC)를 사용하여 IP 전화기를 인증합니다.
- CAPF - LSC를 사용하여 IP 전화기를 인증합니다.

Unified Communications Manager 인증서를 가져오려면 다음을 수행합니다.

a) Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
b) 인증서 Cisco_Manufacturing_CA 및 CAPF를 찾습니다. `.Pem` 파일을 다운로드하고, asa`.txt` 파일로 저장합니다.

c) ASA에 트러스트 포인트를 만듭니다.

예:

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

Base 64 인코딩 CA 인증서를 입력하라는 메시지가 표시되면 다운로드한 .pem 파일의 텍스트를 BEGIN 및 END 줄과 함께 복사합니다. 다른 인증서에 대해 절차를 반복합니다.

d) 다음의 ASA 자체 서명 인증서를 생성하고 이를 사용하여 Unified Communications Manager에 등록하거나 CA에서 가져오는 인증서로 대체합니다.

- SSC(자가서명 인증서)를 생성합니다.

  예:

  ```
  ciscoasa> enable
  ciscoasa# configure terminal
  ciscoasa(config)# crypto key generate rsa general-keys label <name>
  ciscoasa(config)# crypto ca trustpoint <name>
  ciscoasa(ca-trustpoint)# enrollment self
  ciscoasa(ca-trustpoint)# keypair <name>
  ciscoasa(config)# crypto ca enroll <name>
  ciscoasa(config)# end
  ```

- Unified Communications Manager의 VPN 프로파일에서 호스트 ID 확인을 활성화한 상태에서 SSC(자가서명 인증서)를 생성합니다.

  예:

  ```
  ciscoasa> enable
  ciscoasa# configure terminal
  ciscoasa(config)# crypto key generate rsa general-keys label <name>
  ciscoasa(config)# crypto ca trustpoint <name>
  ciscoasa(ca-trustpoint)# enrollment self
  ciscoasa(ca-trustpoint)# fqdn <full domain name>
  ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
  ciscoasa(config)# crypto ca enroll <name>
  ciscoasa(config)# end
  ```

- 생성된 인증서를 Unified Communications Manager에 등록합니다.

  예:

  ```
  ciscoasa(config)# crypto ca export <name> identity-certificate
  ```

  터미널에서 텍스트를 복사하여 .pem 파일로 저장하고 Unified Communications Manager에 업로드합니다.

단계 **3** VPN 기능을 구성합니다. 아래 샘플 ASA 구성 요약을 사용하여 구성을 안내할 수 있습니다.

참고 인증서 및 암호 인증과 함께 전화기를 사용하려면 전화기 MAC 주소를 사용하여 사용자를 만듭니다. 사용자 이름 일치는 대/소문자를 구분합니다. 예:

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9
encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA 인증서 구성

ASA 인증서 구성에 대한 자세한 내용은 ASA에서 인증서 인증을 사용하여 Anyconnect VPN 전화기 구성을 참조하십시오.

VPN 집중 디바이스 인증서 업로드

VPN 기능을 지원하도록 설정하는 경우에는 인증서가 ASA에서 생성됩니다. 생성 된 인증서를 PC 또는 워크스테이션에 다운로드한 다음 Unified Communications Manager가 이 섹션의 절차를 사용하여 업로드합니다. Unified Communications Manager는 전화기-VPN-신뢰 목록에 인증서를 저장합니다.

ASA는 이 인증서를 SSL 핸드셰이크 중에 전송되며, Cisco Unified IP Phone은 이 인증서를 전화기-VPN-신뢰 목록에 저장 된 값과 비교합니다.

LSC (로컬 중요 인증서)가 Cisco Unified IP Phone에 설치된 경우 LSC가 기본적으로 전송됩니다.

디바이스 수준 인증서 인증을 사용하려면 Cisco Unified IP Phone를 신뢰할 수 있도록 ASA에 루트 MIC 또는 CAPF 인증서를 설치합니다.

Unified Communications Manager에 인증서를 업로드하려면 Cisco 통합 OS 관리를 사용하십시오.

프로시저

단계 **1** Cisco Unified OS 관리에서 다음을 선택합니다. 보안 > 인증서 관리.

단계 **2** 인증서 업로드를 클릭합니다.

단계 **3** 인증서 용도 드롭다운 목록에서 전화기-**VPN**-신뢰를 선택합니다.

단계 **4** 찾아보기를 클릭하여 업로드할 파일을 선택합니다.

단계 **5** 파일 업로드를 클릭합니다.

단계 **6** 업로드할 다른 파일을 선택하거나 닫기를 클릭합니다.

자세한 내용은 인증서 관리 장을 참조하십시오.

VPN 게이트웨이 구성

각 VPN 게이트웨이에 대해 VPN 집중 디바이스를 구성했는지 확인합니다. VPN 집중 디바이스를 구성한 후 VPN 집중 디바이스 인증서를 업로드합니다. 자세한 내용은 VPN 집중 디바이스 인증서 업로드, 8 페이지를 참고하십시오.

이 절차를 사용하여 VPN 프로파일을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다. 고급 기능 > **VPN** > **VPN** 게이트웨이

단계 **2** 다음 작업 중 하나를 수행합니다.

a) 새로 추가를 클릭하여 새 프로파일을 구성합니다.

b) 복사하려는 VPN 게이트웨이 옆에 있는 복사를 클릭합니다.

c) 적절한 VPN 게이트웨이를 찾고 설정을 수정하여 기존 프로파일을 업데이트합니다.

단계 **3** **VPN** 게이트웨이 구성 창에서 필드를 구성합니다. 자세한 정보는 VPN 클라이언트용 VPN 게이트웨이 필드, 9 페이지를 참조하십시오.

단계 **4** 저장을 클릭합니다.

VPN 클라이언트용 VPN 게이트웨이 필드

이 표는 VPN 클라이언트에 대한 VPN 게이트웨이 필드를 설명합니다.

표 ***1: VPN*** 클라이언트용 ***VPN*** 게이트웨이 필드

필드	설명
VPN 게이트웨이 이름	VPN 게이트웨이의 이름을 입력합니다.
VPN 게이트웨이 설명	VPN 게이트웨이에 대한 설명을 입력합니다.
VPN 게이트웨이 URL	게이트웨이의 기본 VPN 집중기에 대한 URL을 입력합니다. 참고 그룹 URL을 사용하여 VPN 집중기를 구성하고 이 URL을 게이트웨이 URL로 사용해야 합니다. 구성 정보는 다음과 같은 VPN 집중기에 대한 설명서를 참조하십시오. • *ASDM*을 사용하여 *ASA*에 *SVC(SSL VPN* 클라이언트*)* 구성 예제

필드	설명
이 게이트웨이의 VPN 인증서	위쪽 및 아래쪽 화살표 키를 사용하여 게이트웨이에 인증서를 할당합니다. 게이트웨이에 대한 인증서를 할당하지 않으면 VPN 클라이언트가 해당 집중기에 연결하는 데 실패합니다. 참고 VPN 게이트웨이에 최대 10개의 인증서를 할당할 수 있으며 각 게이트웨이에 하나 이상의 인증서를 할당해야 합니다. 전화기 -VPN-신뢰 역할과 연결된 인증서만 사용 가능한 VPN 인증서 목록에 표시됩니다.

VPN 그룹 구성

이 절차를 사용하여 VPN 그룹을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다. 고급 기능 > **VPN** > **VPN** 그룹

단계 **2** 다음 작업 중 하나를 수행합니다.

a) 새로 추가를 클릭하여 새 프로파일을 구성합니다.

b) 기존 VPN 그룹을 복사할 VPN 그룹 옆에 있는 복사를 클릭합니다.

c) 적절한 VPN 그룹을 찾고 설정을 수정하여 기존 프로파일을 업데이트합니다.

단계 **3** **VPN** 그룹 구성 창에서 필드를 구성합니다. 자세한 내용은 VPN 클라이언트용 VPN 게이트웨이 필드, 9 페이지의 필드 설명 세부 정보를 참조하십시오.

단계 **4** 저장을 클릭합니다.

VPN 클라이언트용 VPN 그룹 필드

이 표는 VPN 클라이언트에 대한 VPN 그룹 필드를 설명합니다.

표 ***2: VPN*** 클라이언트용 ***VPN*** 그룹 필드

필드	정의
VPN 그룹 이름	VPN 그룹의 이름을 입력합니다.
VPN 그룹 설명	VPN 그룹에 대한 설명을 입력합니다.
사용 가능한 모든 VPN 게이트웨이	스크롤하여 사용 가능한 모든 VPN 게이트웨이를 확인합니다.

필드	정의
이 VPN 그룹에서 선택한 VPN 게이트웨이	위쪽 및 아래쪽 화살표 버튼을 사용하여 사용 가능한 VPN 게이트웨이를 이 VPN 그룹의 내부 및 외부로 이동합니다. VPN 클라이언트에 심각한 오류가 발생하고 특정 VPN 게이트웨이에 연결할 수 없는 경우 목록에 있는 다음 VPN 게이트웨이로 이동하려고 시도합니다. 참고 최대 3개의 VPN 게이트웨이를 VPN 그룹에 추가할 수 있습니다. 또한 VPN 그룹의 총 인증서 수는 10개를 초과할 수 없습니다.

VPN 프로파일 구성

이 절차를 사용하여 VPN 프로파일을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다. 고급 기능 > **VPN** > **VPN** 프로파일

단계 **2** 다음 작업 중 하나를 수행합니다.

a) 새로 추가를 클릭하여 새 프로파일을 구성합니다.
b) 기존 프로파일을 복사하려는 VPN 프로파일 옆에 있는 복사를 클릭합니다.
c) 기존 프로파일을 업데이트하려면 **VPN** 프로파일 위치 찾기에서 해당 필터를 지정하고 찾기를 클릭한 다음 설정을 수정합니다.

단계 **3** **VPN** 프로파일 구성 창에서 필드를 구성합니다. 자세한 내용은 VPN 클라이언트용 VPN 프로파일 필드, 11 페이지의 필드 설명 세부 정보를 참조하십시오.

단계 **4** 저장을 클릭합니다.

VPN 클라이언트용 VPN 프로파일 필드

이 표는 VPN 프로파일 필드 세부 정보를 설명합니다.

표 ***3: VPN*** 프로파일 필드 세부 정보

필드	정의
이름	VPN 프로파일의 이름을 입력합니다.
설명	VPN 프로파일에 대한 설명을 입력합니다.

필드	정의
자동 네트워크 감지 활성화	이 확인란을 선택하는 경우 VPN 클라이언트가 회사 네트워크 외부에 있다는 것을 감지하는 경우에만 실행될 수 있습니다. 기본값: 비활성화됨
MTU	MTU(최대 전송 단위) 크기(바이트)를 입력합니다. 기본값: 1290바이트
연결 실패	이 필드는 시스템이 VPN 터널을 생성하는 동안 로그인 또는 연결 작업이 완료될 때까지 기다리는 시간을 지정합니다. 기본값: 30초
호스트 ID 확인 활성화	이 확인란을 선택하는 경우 게이트웨이 인증서 subjectAltName 또는 CN이 VPN 클라이언트가 연결된 URL과 일치해야 합니다. 기본값: 활성화됨
클라이언트 인증 방법	드롭다운 목록에서 클라이언트 인증 방법을 선택합니다. • 사용자 및 암호 • 암호 전용 • 인증서(LSC 또는 MIC)
암호 지속성 활성화	이 확인란을 선택하면 실패한 로그인 시도가 발생하거나, 사용자가 수동으로 암호를 지우거나, 전화기가 재설정되거나, 전화기 전원이 유실될 때까지 사용자 암호가 전화기에 저장됩니다.

VPN 기능 매개 변수 구성

프로시저

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다. 고급 기능 > **VPN** > **VPN** 기능 구성.

단계 **2** **VPN** 그룹 구성 창에서 필드를 구성합니다. 자세한 정보는 VPN 기능 매개 변수, 13 페이지를 참조하십시오.

단계 **3** 저장을 클릭합니다.

다음 작업을 수행하십시오.

- Cisco Unified IP Phone에 대한 펌웨어를 VPN을 지원하는 버전으로 업그레이드합니다. 펌웨어 업그레이드에 대한 자세한 내용은 해당 Cisco Unified IP Phone 모델에 대한 *Cisco Unified IP Phone* 관리 지침서를 참조하십시오.

• 지원되는 Cisco Unified IP Phone을(를) 사용하여 VPN 연결을 설정합니다.

VPN 기능 매개 변수

이 표는 VPN 기능 매개 변수를 설명합니다.

표 *4: VPN* 기능 매개 변수

필드	기본값
자동 네트워크 감지 활성화	참이면 VPN 클라이언트가 회사 네트워크 외부에 있다는 것을 감지하는 경우에만 실행될 수 있습니다. 기본값: 거짓
MTU	이 필드는 최대 전송 단위를 지정합니다. 기본값: 1290바이트 최소값: 256바이트 최대값: 1406바이트
연결 유지	이 필드는 시스템이 연결 유지 메시지를 전송하는 레이트를 지정합니다. 참고 0이 아니고 Unified Communications Manager에 지정된 값보다 작은 경우 VPN 집중기의 연결 유지 설정이 이 설정을 덮어씁니다. 기본값: 60초 최소값: 0 최대값: 120초
연결 실패	이 필드는 시스템이 VPN 터널을 생성하는 동안 로그인 또는 연결 작업이 완료될 때까지 기다리는 시간을 지정합니다. 기본값: 30초 최소값: 0 최대값: 600초
클라이언트 인증 방법	드롭다운 목록에서 클라이언트 인증 방법을 선택합니다. • 사용자 및 암호 • 암호 전용 • 인증서(LSC 또는 MIC) 기본값: 사용자 및 암호

필드	기본값
암호 지속성 활성화	참(True)일 때 사용자 암호는 전화기에 저장됩니다(재설정 버튼 또는 "**#**"가 재설정에 사용되는 경우). 전화기의 전원이 끊기거나 공장 재설정을 초기화할 경우 암호가 저장되지 않고 전화기에서 자격 증명을 요청합니다. 기본값: 거짓
호스트 ID 확인 활성화	참인 경우 게이트웨이 인증서 subjectAltName 또는 CN이 VPN 클라이언트가 연결된 URL과 일치해야 합니다. 기본값: 참

일반 전화 프로파일에 VPN 세부 정보 추가

이 절차를 사용하여 VPN 세부 정보를 일반 전화 프로파일에 추가합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다. 디바이스 > 디바이스 설정 > 일반 전화 프로파일
단계 **2** 찾기를 클릭하고 VPN 세부 정보를 추가할 일반 전화 프로파일을 선택합니다.
단계 **3** **VPN** 정보 섹션에서 적절한 **VPN** 그룹 및 **VPN** 프로파일을 선택합니다.
단계 **4** 저장 및 구성 적용을 클릭합니다.
단계 **5** 구성 적용 창에서 확인을 클릭합니다.