Contact Center Enterprise에서 Secure SIP Signaling 구성

목차

소개

이 문서에서는 CCE(Contact Center Enterprise) 포괄적인 통화 흐름에서 SIP(Session Initiation Protocol) 신호 처리를 보호하는 방법에 대해 설명합니다.

사전 요구 사항

인증서 생성 및 가져오기는 이 문서의 범위에 포함되지 않으므로 Cisco Unified Communication Manager(CUCM), Customer Voice Portal(CVP) 통화 서버, Cisco Virtual Voice Browser(CVVB) 및 Cisco Unified Border Element(CUBE)용 인증서를 생성하여 해당 구성 요소로 가져와야 합니다. 자체 서명 인증서를 사용하는 경우 서로 다른 구성 요소 간에 인증서를 교환해야 합니다.

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CCE
- CVP
- 입방체
- CUCM
- CVVB

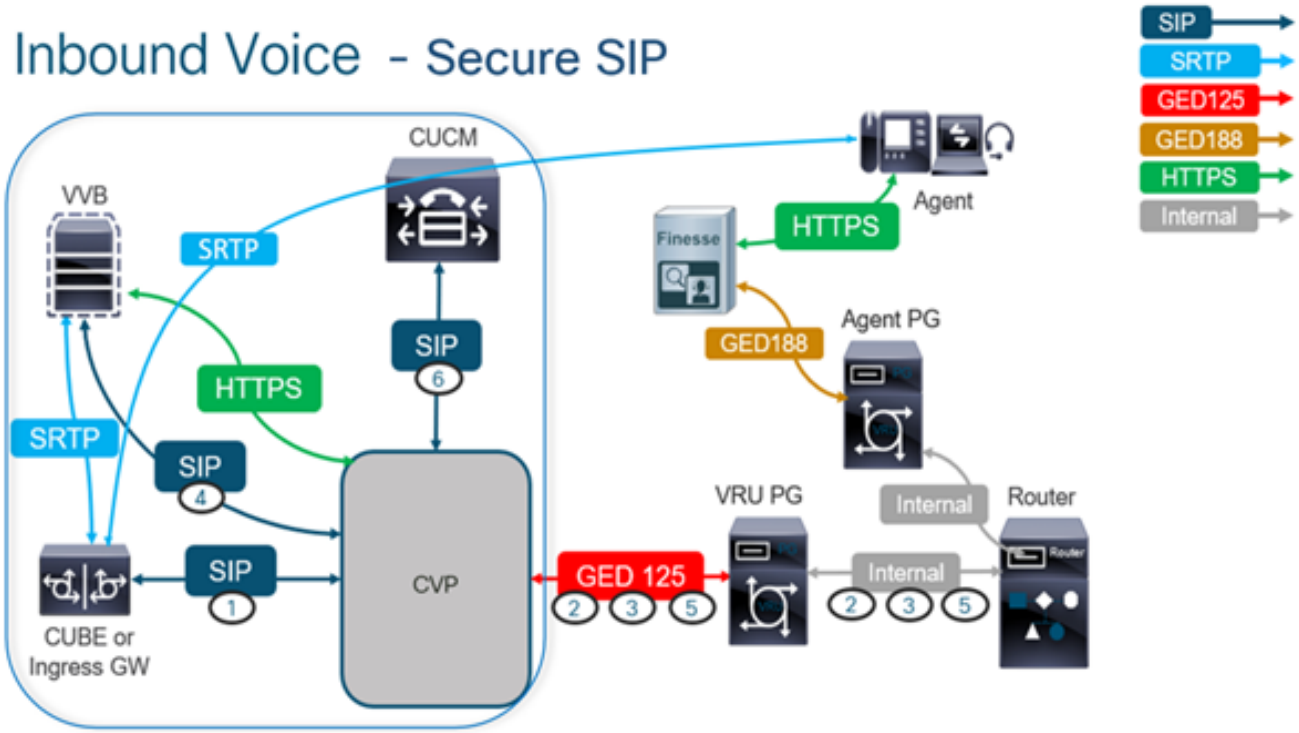
사용되는 구성 요소

이 문서의 정보는 PCCE(Package Contact Center Enterprise), CVP, CVVB 및 CUCM 버전 12.6을 기반으로 하지만 이전 버전에도 적용됩니다.

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

구성

다음 다이어그램은 컨택 센터의 포괄적인 통화 흐름에서 SIP 시그널링과 관련된 구성 요소를 보여줍니다. 음성 통화가 시스템에 도착하면 먼저 인그레스 게이트웨이 또는 CUBE를 통해 제공되므로 CUBE에서 보안 SIP 컨피그레이션을 시작합니다. 다음으로 CVP, CVVB 및 CUCM을 구성합니다.



작업 1. CUBE 보안 컨피그레이션

이 작업에서는 SIP 프로토콜 메시지를 보호하도록 CUBE를 구성합니다.

필수 구성:

- SIP UA(사용자 에이전트)에 대한 기본 신뢰 지점 구성
- TLS(Transport Layer Security)를 사용하도록 다이얼 피어 수정

단계:

1. CUBE에 대한 SSH(Secure Shell) 세션을 엽니다.
2. SIP 스택에서 CUBE의 CA(Certificate Authority) 인증서를 사용하도록 하려면 다음 명령을 실행합니다. CUBE는 CUCM(198.18.133.3) 및 CVP(198.18.133.13)와 SIP TLS 연결을 설정합니다.

```
conf t sip-ua transport tcp tls v1.2 crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name exit
```

```
CC-VCUBE(config)#sip-ua
CC-VCUBE(config-sip-ua)#transport tcp tls v1.2
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.3 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#crypto signaling remote-addr 198.18.133.13 255.255.255.255 trustpoint ms-ca-name
CC-VCUBE(config-sip-ua)#exit
CC-VCUBE(config)#
```

3. CVP로의 발신 다이얼 피어에서 TLS를 활성화하려면 다음 명령을 실행합니다. 이 예에서는 다이얼 피어 태그(6000)를 사용하여 통화를 CVP로 라우팅합니다.

Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls exit

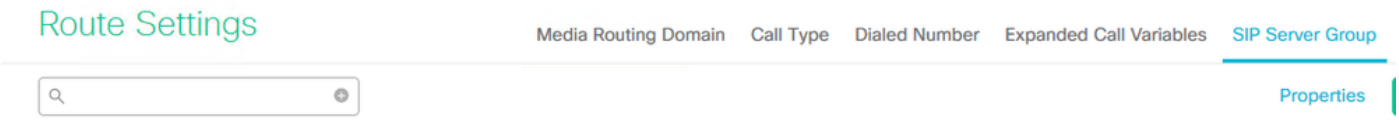
```
CC-VCUBE#
CC-VCUBE#Conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CC-VCUBE(config)#dial-peer voice 6000 voip
CC-VCUBE(config-dial-peer)#session target ipv4:198.18.133.13:5061
CC-VCUBE(config-dial-peer)#session transport tcp tls
CC-VCUBE(config-dial-peer)#
CC-VCUBE(config-dial-peer)#exit
CC-VCUBE(config)#
```

작업 2. CVP 보안 컨피그레이션

이 작업에서 SIP 프로토콜 메시지(SIP TLS)를 보호하도록 CVP 통화 서버를 구성합니다.

단계:

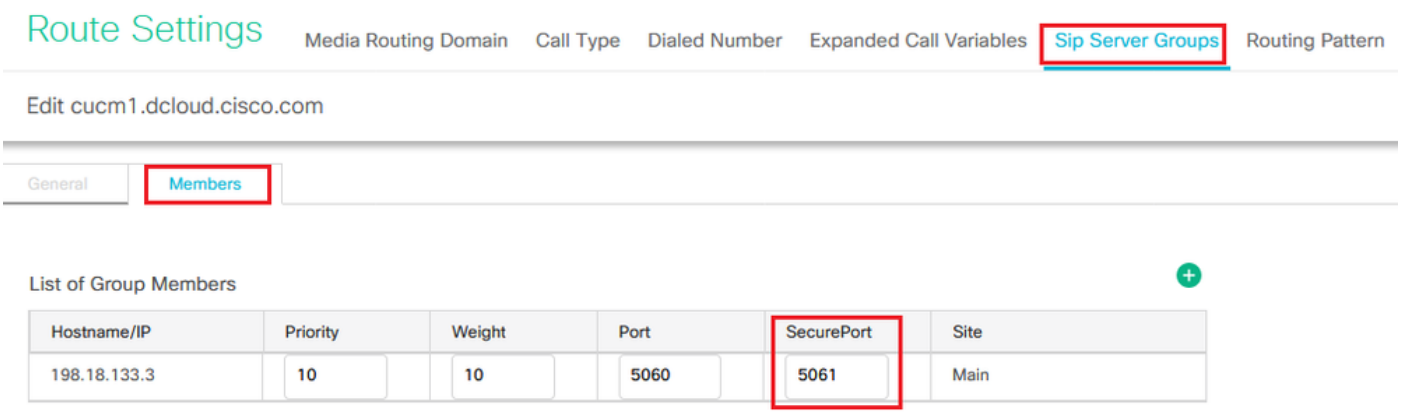
1. 다음에 로그인:UCCE Web Administration.
2. 탐색 Call Settings > Route Settings > SIP Server Group.



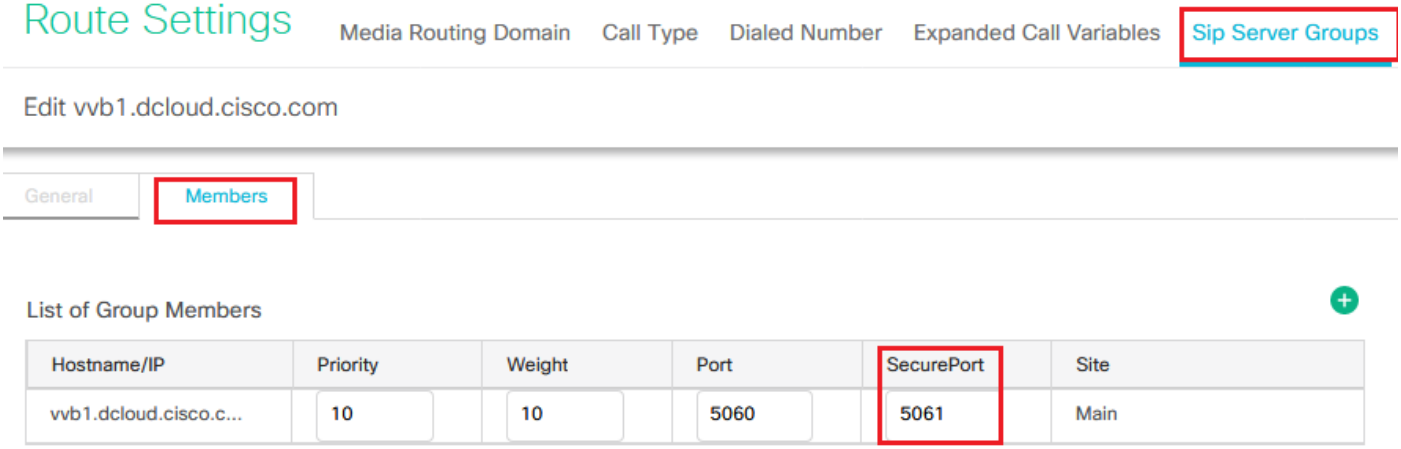
구성에 따라 CUCM, CVVB 및 CUBE에 대해 구성된 SIP 서버 그룹이 있습니다. 보안 SIP 포트 전체를 5061로 설정해야 합니다. 이 예에서는 다음 SIP 서버 그룹이 사용됩니다.

- cucm1.dcloud.cisco.com CUCM용
- vvb1.dcloud.cisco.com CVVB용
- cube1.dcloud.cisco.com CUBE용

3. 클릭 cucm1.dcloud.cisco.com Cisco의 **Members** 탭 - SIP 서버 그룹 컨피그레이션의 세부사항을 표시합니다. 설정 SecurePort 수신 5061 을 클릭하고 Save .



4. 클릭 vvb1.dcloud.cisco.com Cisco의 **Members** 탭을 클릭합니다. 보안 포트 설정 5061 을 클릭하고 Save.

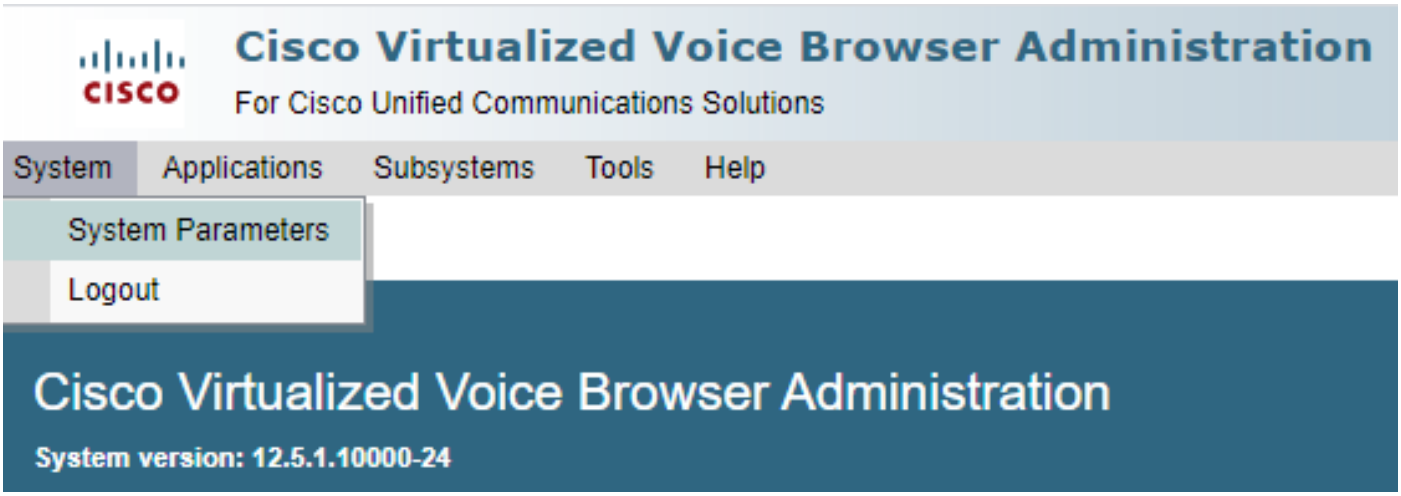


작업 3. CVVB 보안 컨피그레이션

이 작업에서 SIP 프로토콜 메시지(SIP TLS)를 보호하도록 CVVB를 구성합니다.

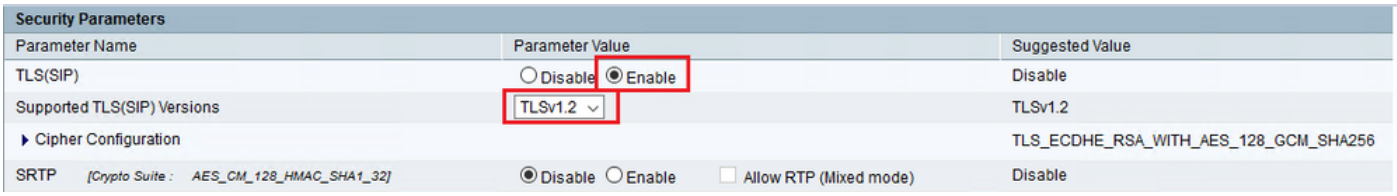
단계:

1. 다음에 로그인: **Cisco VVB Administration** 페이지를 참조하십시오.
2. 탐색 System > System Parameters.

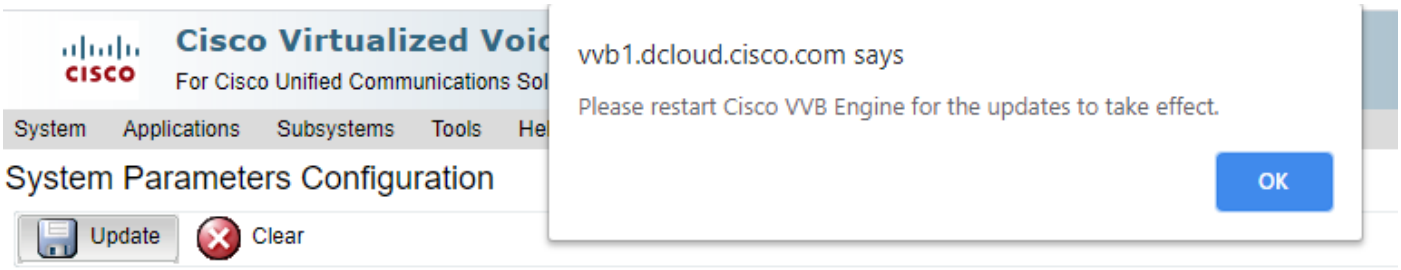


3. 의 Security Parameters 섹션, 선택 Enable 대상: TLS(SIP) . 유지 Supported TLS(SIP) version 다음으로

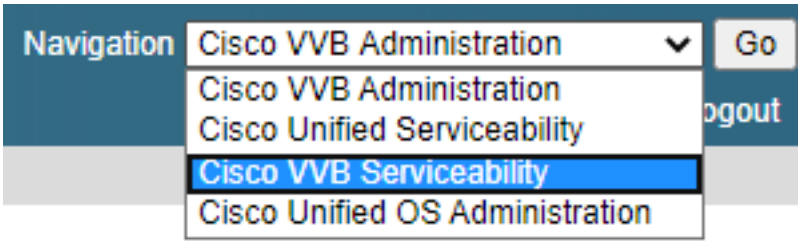
TLSv1.2.



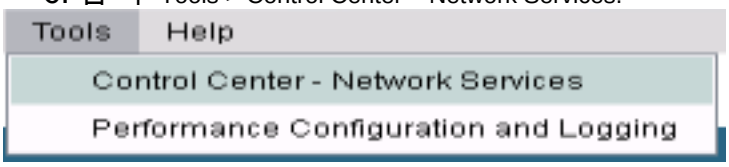
4. 업데이트를 **클릭합니다**. 클릭 Ok CVVB 엔진을 다시 시작하라는 프롬프트가 표시되면



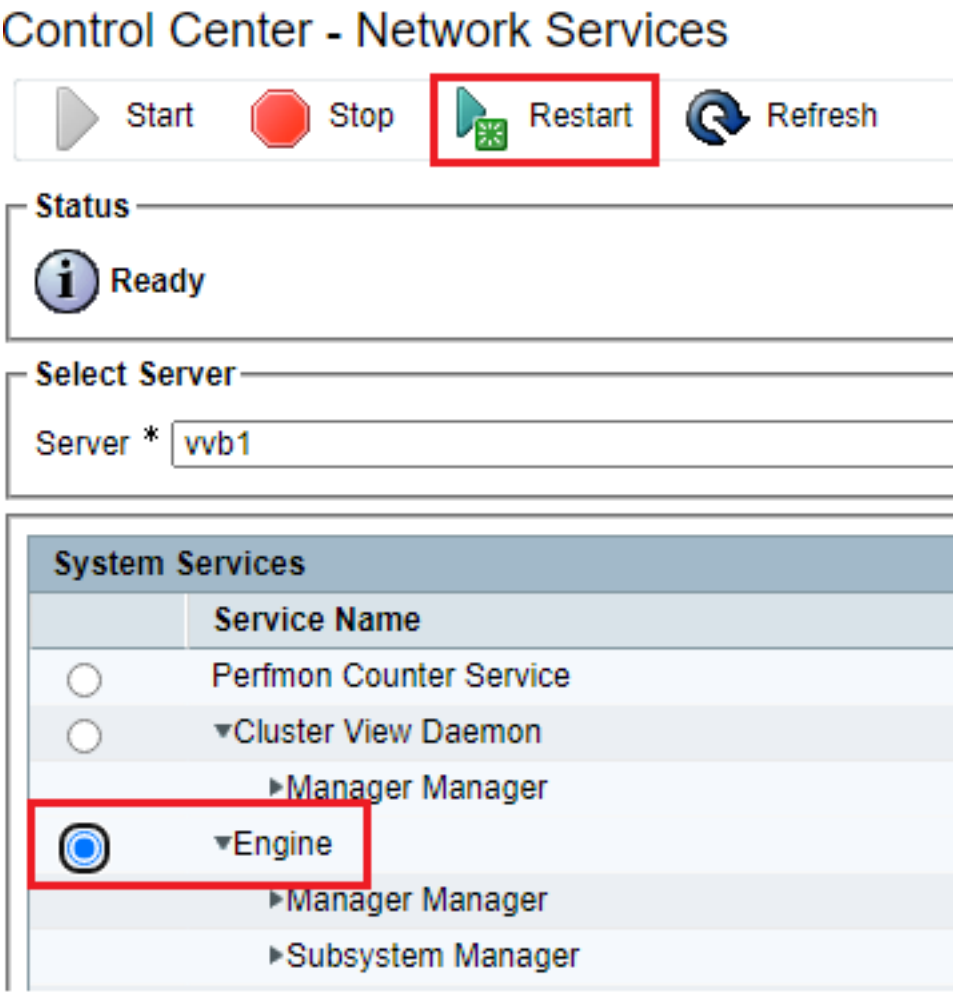
5. 이러한 변경 사항을 적용하려면 Cisco VVB 엔진을 다시 시작해야 합니다. VVB 엔진을 다시 시작하려면 Cisco VVB Serviceability 그런 다음 **Go**.



6. 탐색 Tools > Control Center – Network Services.



7. 선택 Engine 을 클릭하고 Restart.



작업 4. CUCM 보안 컨피그레이션

CUCM에서 SIP 메시지를 보호하려면 다음 컨피그레이션을 수행합니다.

- CUCM 보안 모드를 혼합 모드로 설정
- CUBE 및 CVP에 대한 SIP 트렁크 보안 프로필 구성
- SIP 트렁크 보안 프로필을 각 SIP 트렁크에 연결
- 보안 에이전트의 CUCM과의 디바이스 통신

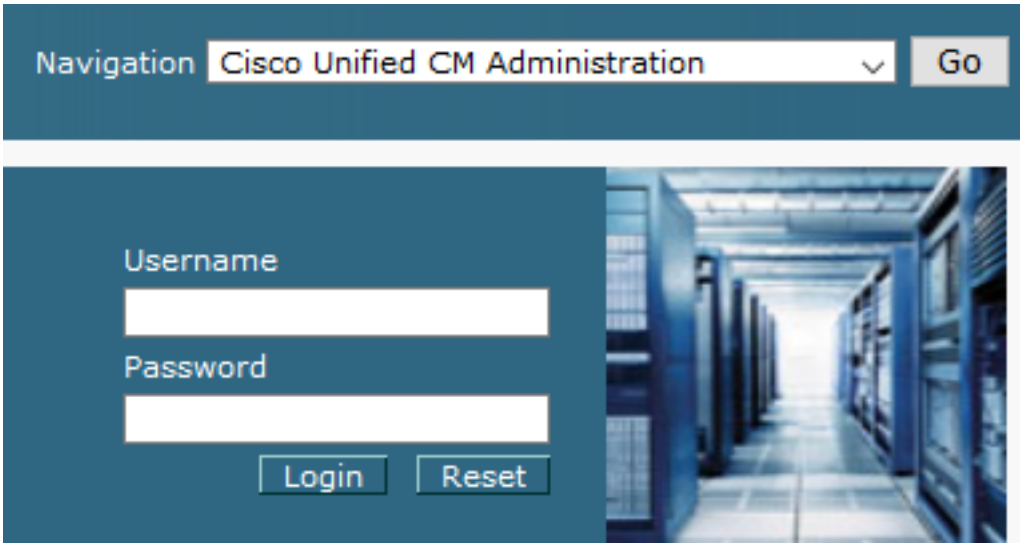
CUCM 보안 모드를 혼합 모드로 설정

CUCM은 2가지 보안 모드를 지원합니다.

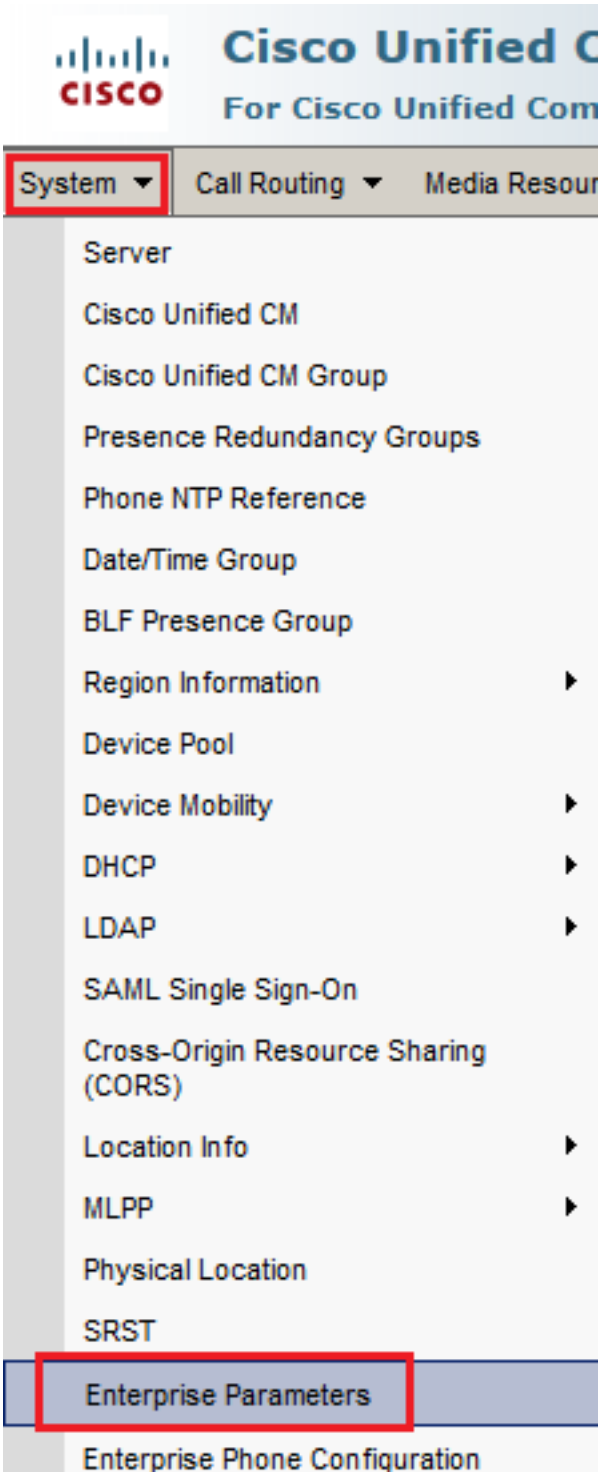
- 비보안 모드(기본 모드)
- 혼합 모드(보안 모드)

단계:

1. 보안 모드를 혼합 모드로 설정하려면 Cisco Unified CM Administration 인터페이스입니다.



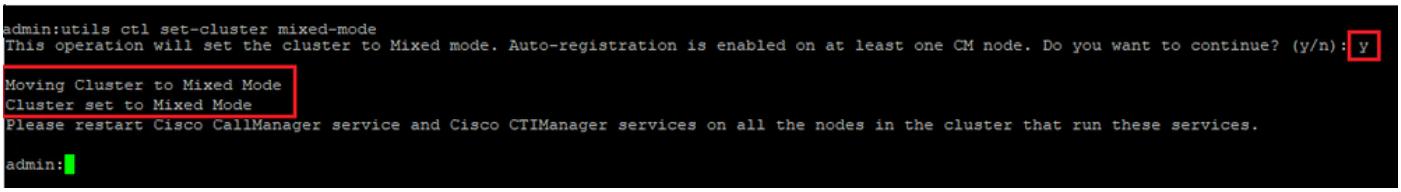
2. CUCM에 성공적으로 로그인했으면 System > Enterprise Parameters.



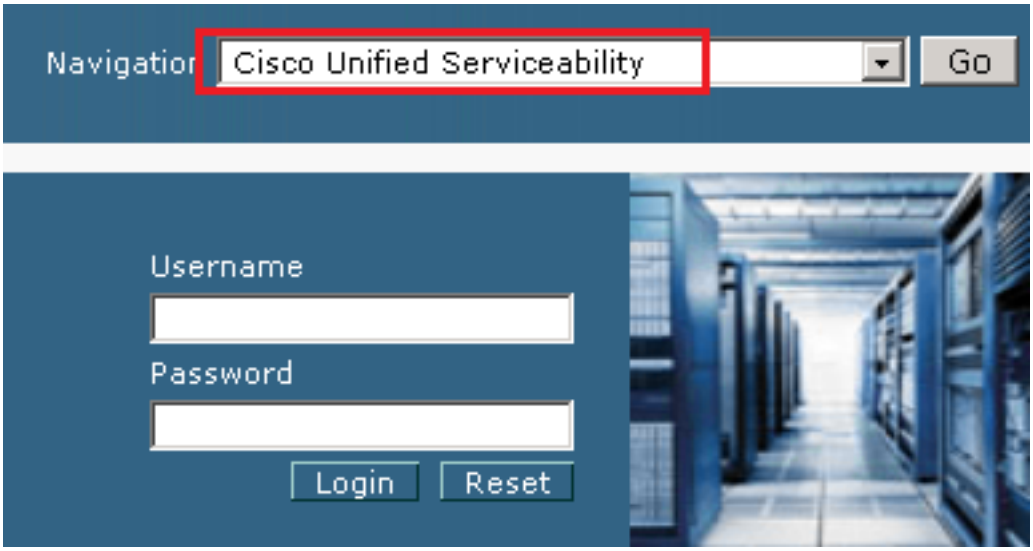
3. Cisco의 Security Parameters 섹션, 확인 Cluster Security Mode 다음으로 설정됨 **0**.

4. Cluster Security Mode(클러스터 보안 모드)가 0으로 설정된 경우, 이는 클러스터 보안 모드가 비보안으로 설정되었음을 의미합니다. CLI에서 혼합 모드를 활성화해야 합니다.
5. CUCM에 대한 SSH 세션을 엽니다.
6. SSH를 통해 CUCM에 성공적으로 로그인한 후 다음 명령을 실행합니다. utils ctl set-cluster mixed-mode

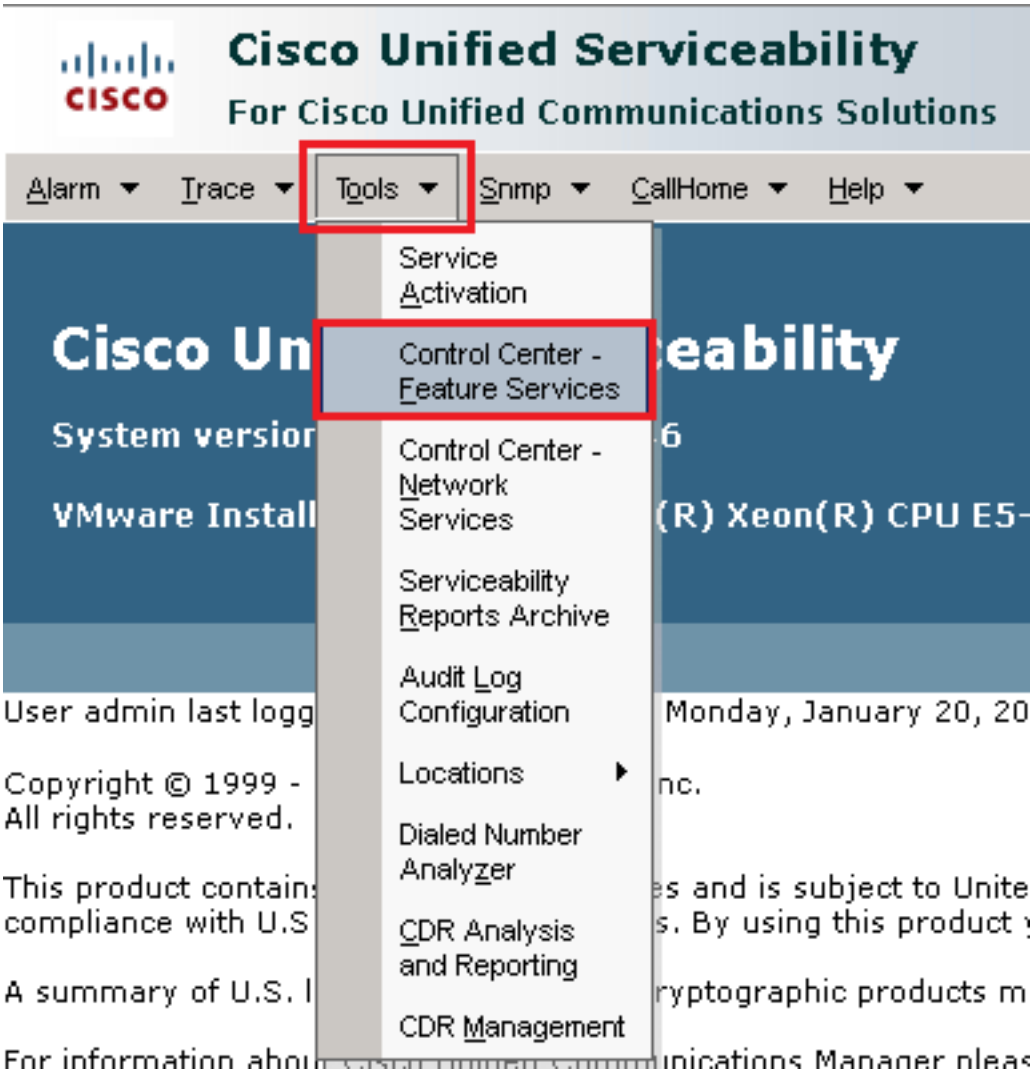
7. 유형 y 프롬프트가 표시되면 **Enter**를 클릭합니다. 이 명령은 클러스터 보안 모드를 혼합 모드로 설정합니다.



8. 변경 사항을 적용하려면 다시 시작하십시오. Cisco CallManager 및 Cisco CTIManager services.
9. 서비스를 다시 시작하려면 다음으로 이동하여 로그인합니다. Cisco Unified Serviceability.

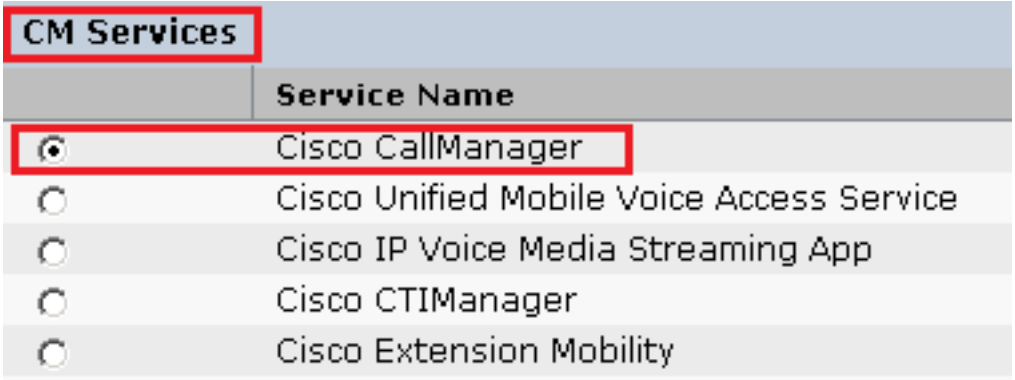


10. 성공적으로 로그인했으면 Tools > Control Center – Feature Services.

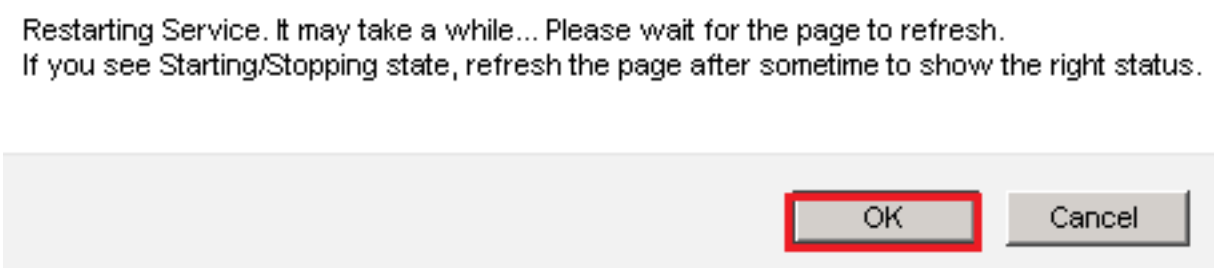


11. 서버를 선택한 다음 Go.

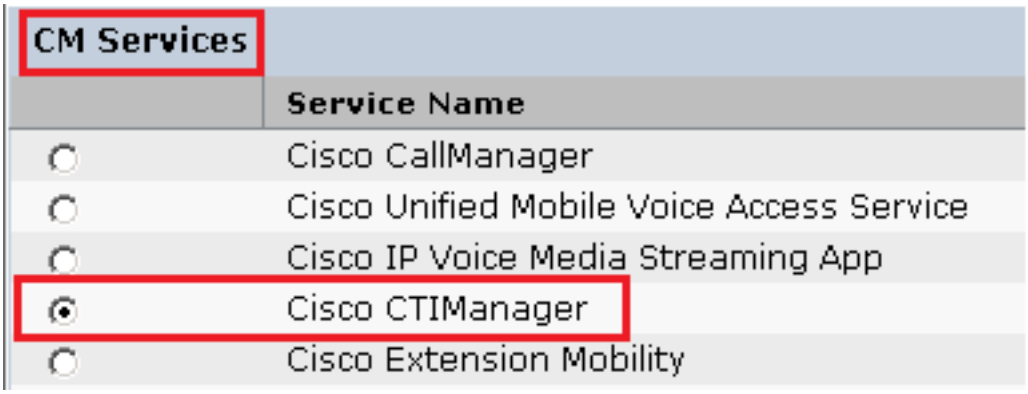
12. CM 서비스 아래에서 Cisco CallManager 그런 다음 Restart 버튼을 클릭합니다.



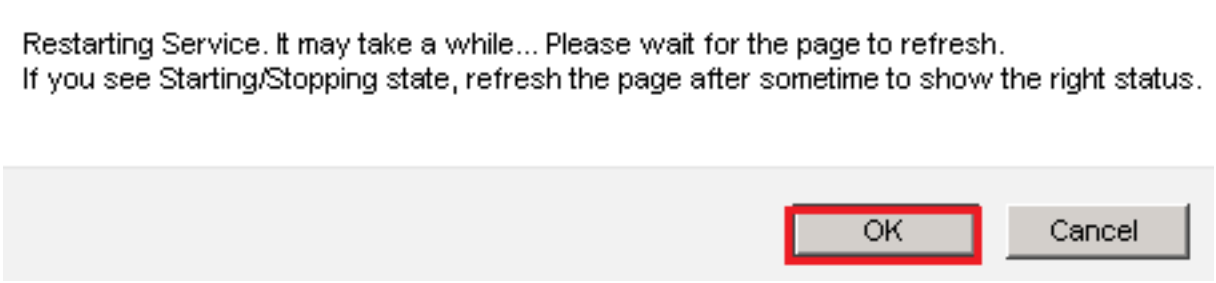
13. 팝업 메시지를 확인하고 OK. 서비스가 성공적으로 다시 시작될 때까지 기다립니다.



14. 을(를) 성공적으로 재시작한 후 Cisco CallManager, Cisco 선택 **CTIManager** 그런 다음 Restart 단추를 클릭하여 다시 시작합니다. Cisco CTIManager 서비스.



15. 팝업 메시지를 확인하고 **OK**. 서비스가 성공적으로 다시 시작될 때까지 기다립니다.

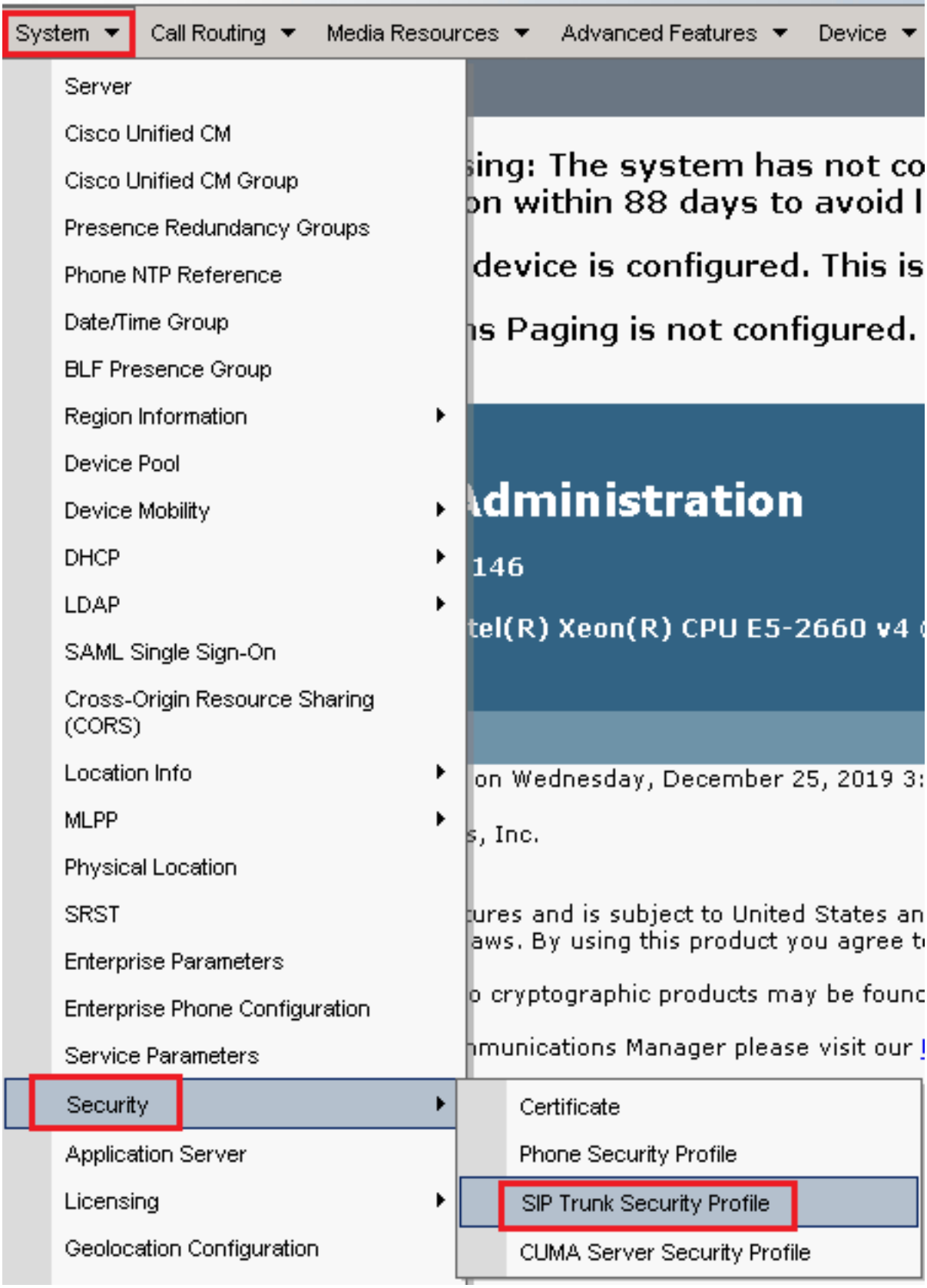


16. 서비스를 성공적으로 다시 시작한 후 클러스터 보안 모드가 혼합 모드로 설정되어 있는지 확인하고 5단계에서 설명한 대로 CUCM 관리로 이동한 다음 **Cluster Security Mode**. 이제 다음으로 설정되어야 합니다. **1**.

CUBE 및 CVP에 대한 SIP 트렁크 보안 프로필 구성

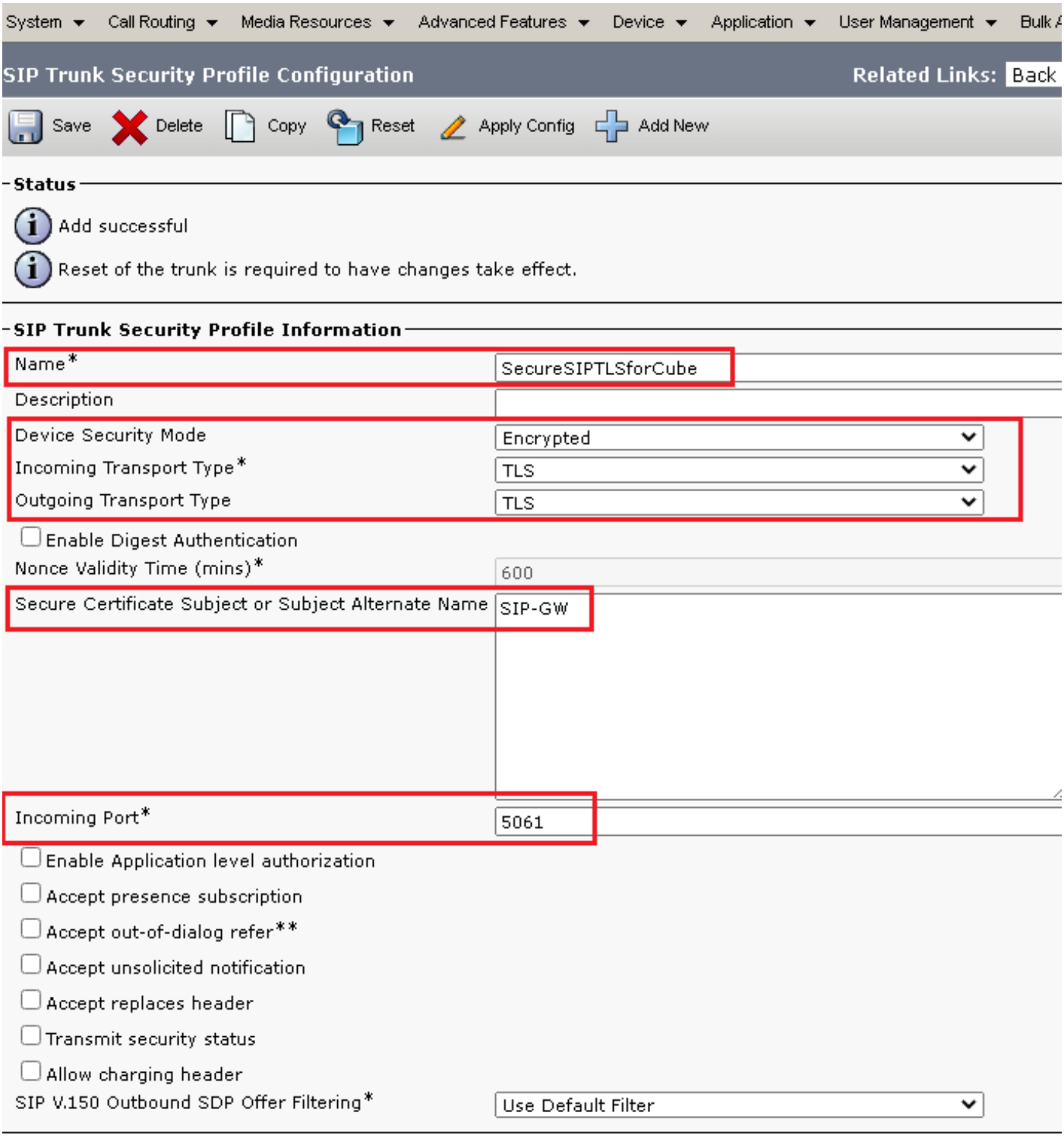
단계:

1. 다음에 로그인: CUCM administration 인터페이스입니다.
2. CUCM에 성공적으로 로그인했으면 System > Security > SIP Trunk Security Profile CUBE에 대한 디바이스 보안 프로필을 생성하려면



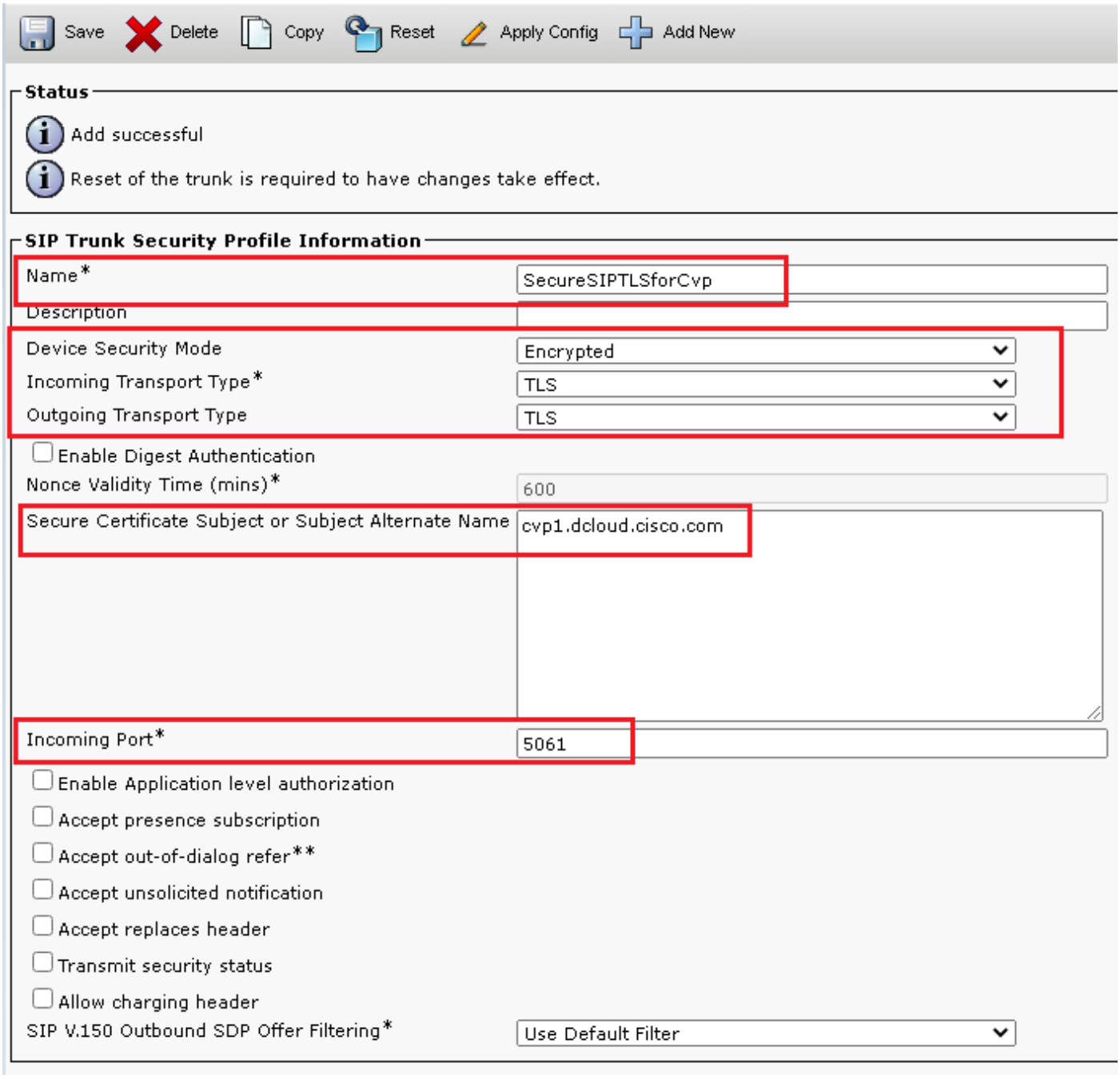
3. 왼쪽 상단에서 Add New 새 프로필을 추가합니다.

4. 구성 SIP Trunk Security Profile 이 그림에 표시된 대로 Save 페이지의 왼쪽 하단에서 Save 그렇습니다.



5. 다음을 설정합니다 Secure Certificate Subject or Subject Alternate Name CUBE 인증서의 CN(Common Name)과 일치해야 합니다.

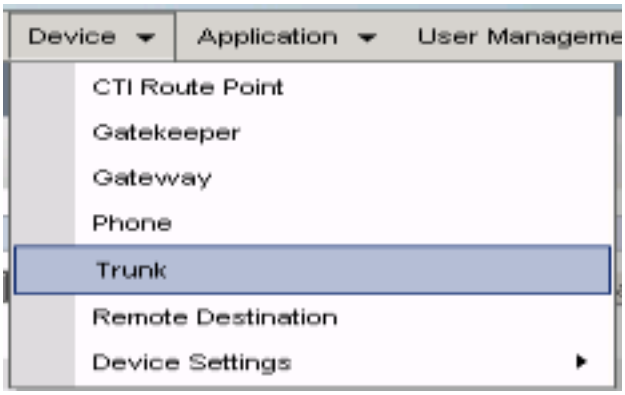
6. 클릭 Copy 버튼을 클릭하고 Name 수신 SecureSipTLSforCVP 및 Secure Certificate Subject 일치해야 하므로 CVP 통화 서버 인증서의 CN에 연결합니다. 클릭 Save 버튼을 클릭합니다.



SIP 트렁크 보안 프로필을 각 SIP 트렁크에 연결

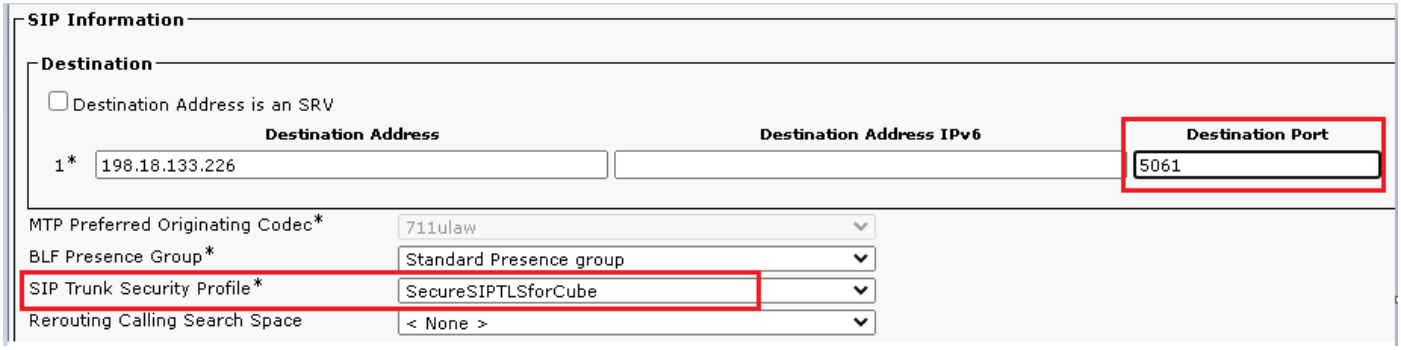
단계:

1. CUCM Administration(CUCM 관리) 페이지에서 Device > Trunk.

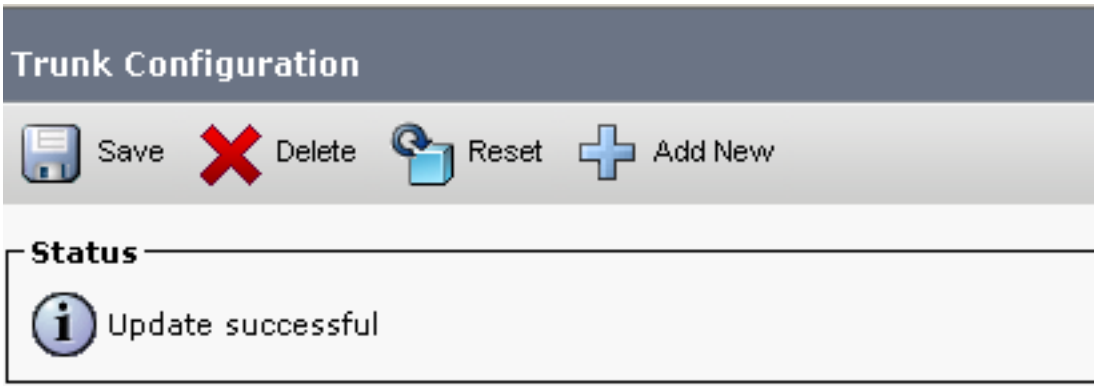


2. CUBE 트렁크를 검색합니다. 이 예에서 CUBE 트렁크 이름은 vCube . 클릭 **Find**.

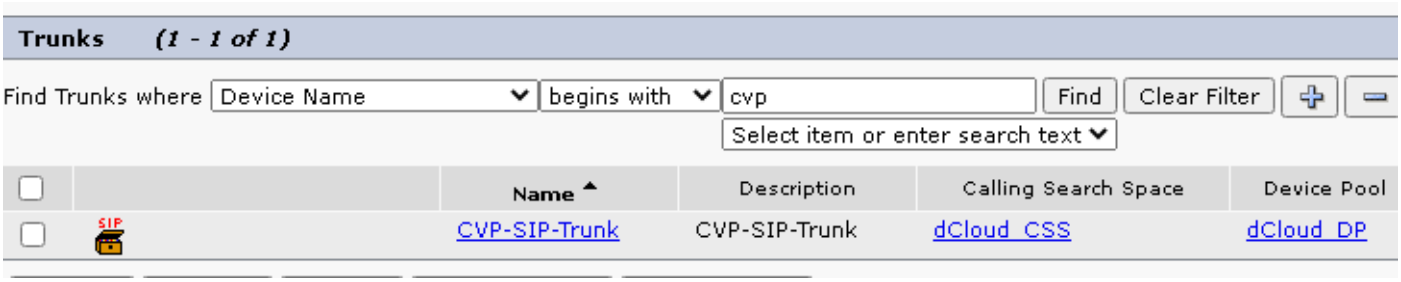
3. vCUBE를 눌러 vCUBE 트렁크 컨피그레이션 페이지를 엽니다.
4. 아래로 스크롤하여 SIP Information 섹션 및 변경 Destination Port 수신 5061.
5. 변경 SIP Trunk Security Profile 수신 SecureSIPTLSForCube.



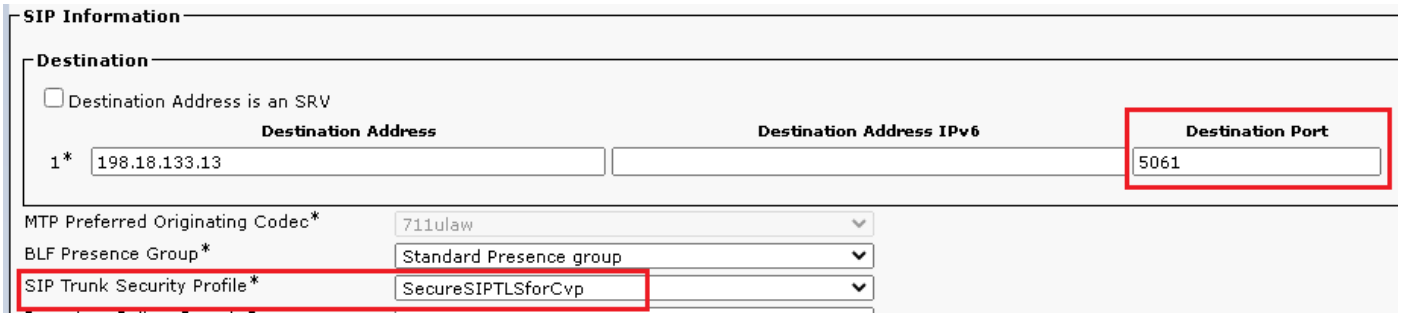
6. 클릭 Save 그런 다음 Rest 를 위해 Save 변경 사항을 적용합니다.



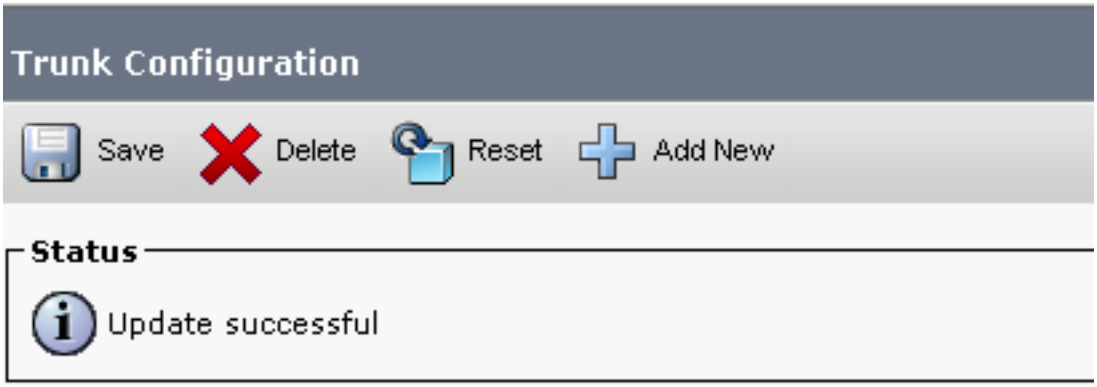
7. 탐색 Device > Trunk를 누르고 CVP 트렁크를 검색합니다. 이 예에서 CVP 트렁크 이름은 cvp-SIP-Trunk . 클릭 **Find.**



8. 클릭 CVP-SIP-Trunk CVP 트렁크 컨피그레이션 페이지를 열려면
9. 아래로 스크롤하여 SIP Information 섹션 및 변경 Destination Port 수신 5061 .
10. 변경 SIP Trunk Security Profile 수신 SecureSIPTLSForCvp.



11. 클릭 Save 그런 다음 Rest 를 위해 save 변경 사항을 적용합니다.



보안 에이전트의 CUCM과의 디바이스 통신

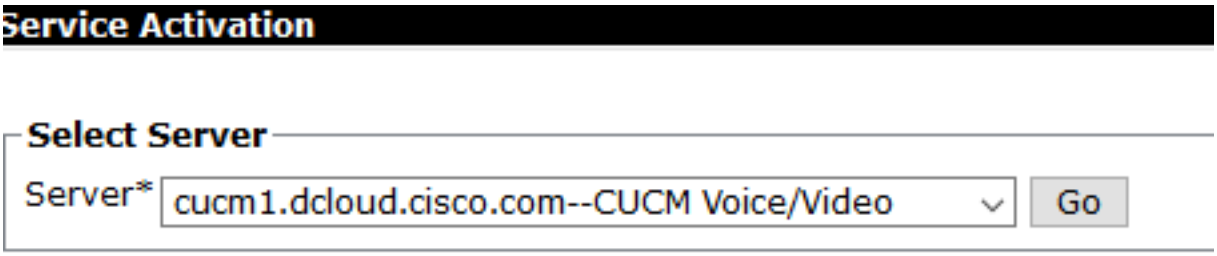
디바이스에 보안 기능을 활성화하려면 LSC(Locally Significant Certificate)를 설치하고 해당 디바이

스에 보안 프로파일을 할당해야 합니다. LSC는 CAPF(Certificate Authority Proxy Function) 개인 키로 서명된 엔드포인트의 공개 키를 보유합니다. 기본적으로 전화기에는 설치되지 않습니다.

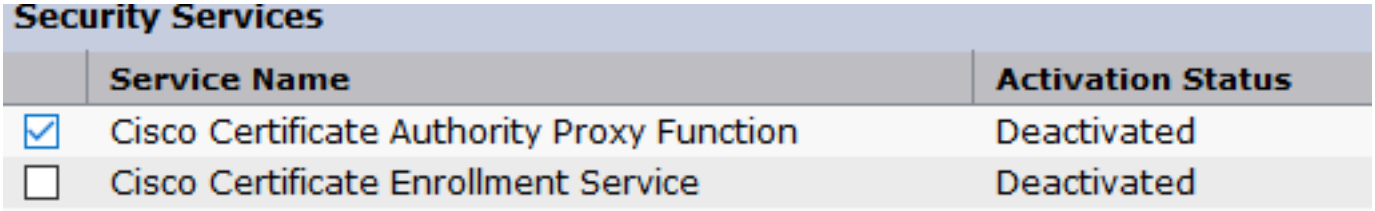
단계:

1. 다음에 로그인: Cisco Unified Serviceability Interface.
2. 탐색 Tools > Service Activation.

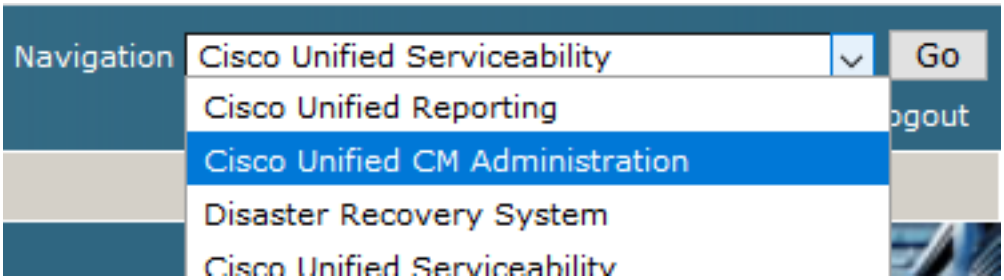
3. CUCM 서버를 선택하고 Go .



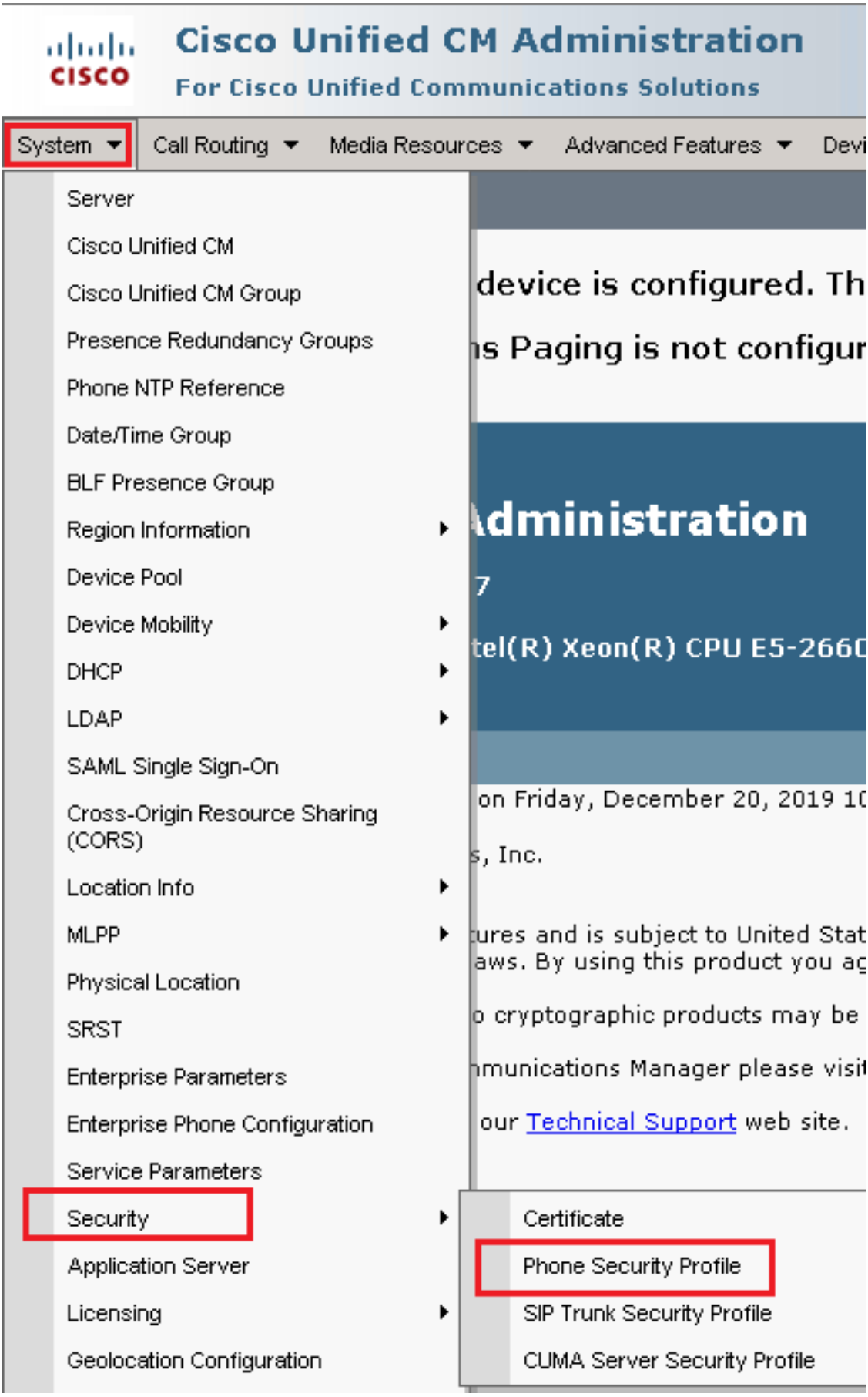
4. 수표 Cisco Certificate Authority Proxy Function 을 클릭하고 Save 서비스를 활성화합니다. 클릭 Ok 확인합니다.



5. 서비스가 활성화되었는지 확인한 다음 Cisco Unified CM Administration.

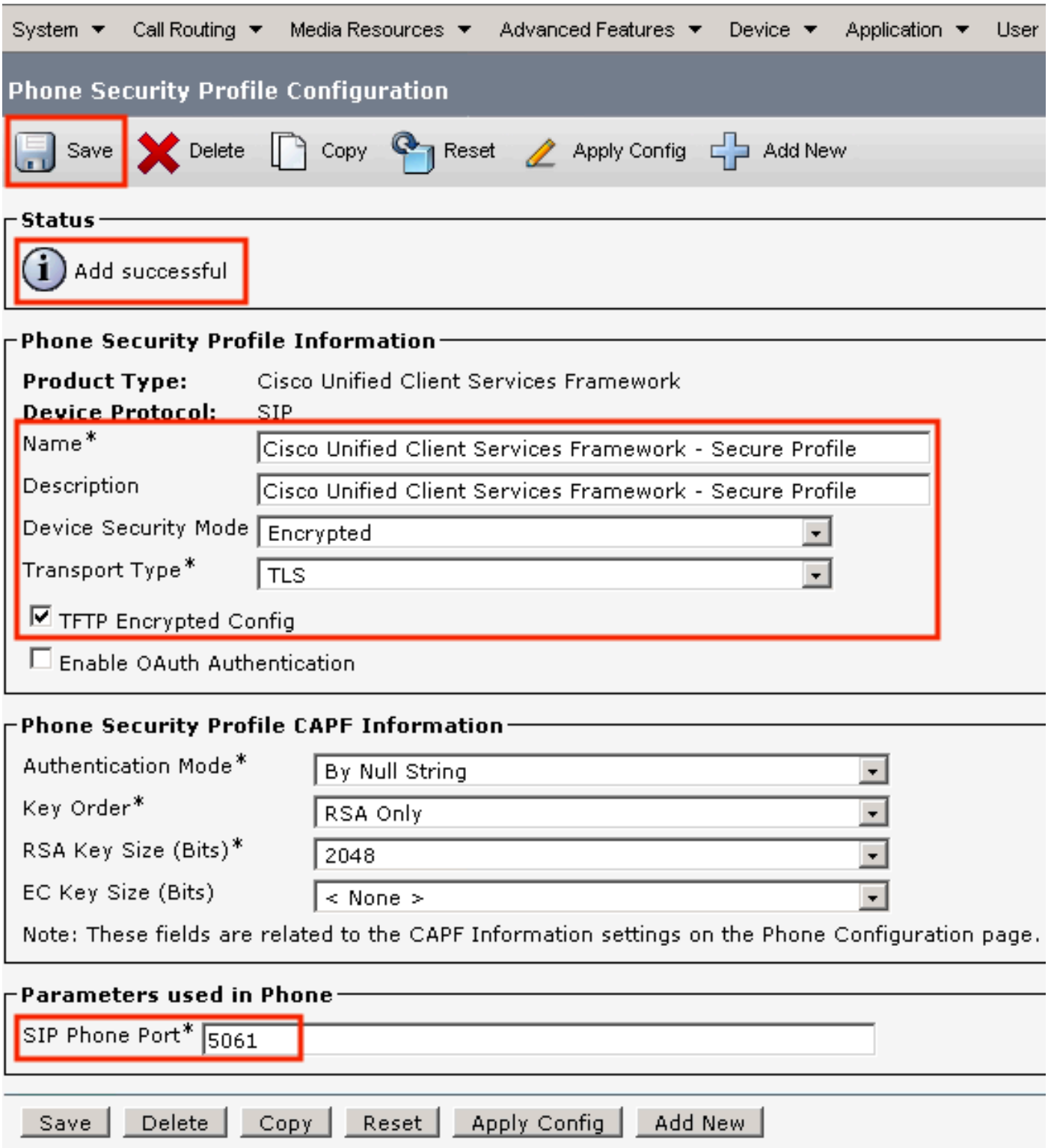


6. CUCM 관리에 로그인했으면 System > Security > Phone Security Profile 상담원 장치에 대한 장치 보안 프로필을 만듭니다.

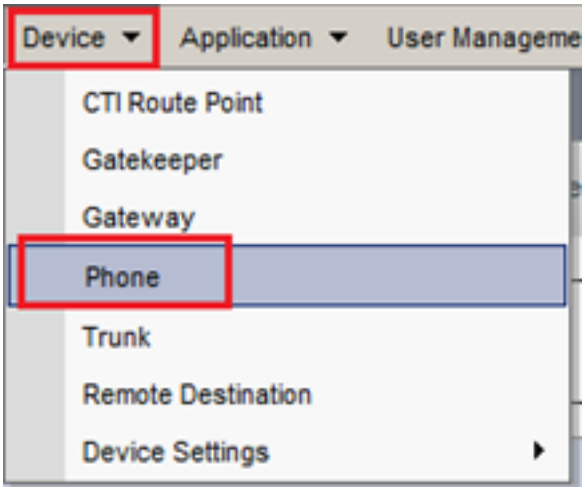


7. 상담원 장치 유형에 해당하는 보안 프로파일을 찾습니다. 이 예에서는 소프트폰을 사용하므로 Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile . 클릭 Copy 이 프로파일을 복사하려면

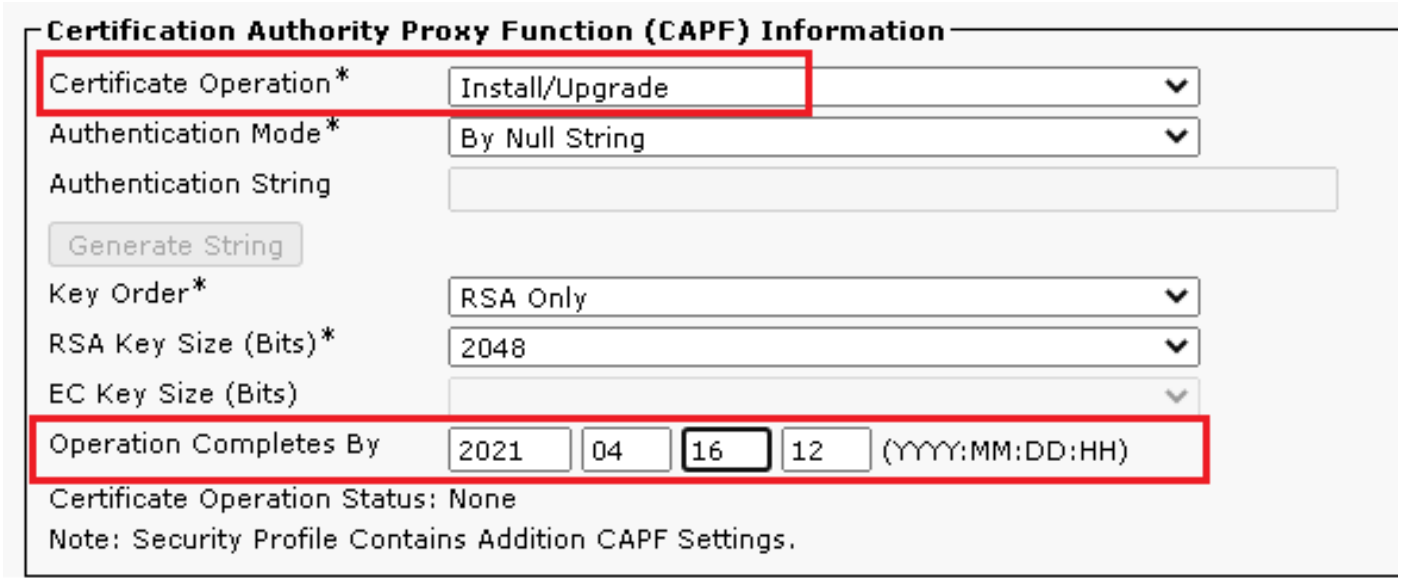
8. 프로파일 이름을 다음으로 변경 Cisco Unified Client Services Framework - Secure Profile이 이미지에 표시된 대로 매개변수를 변경한 다음 Save 페이지의 왼쪽 상단에 있습니다.



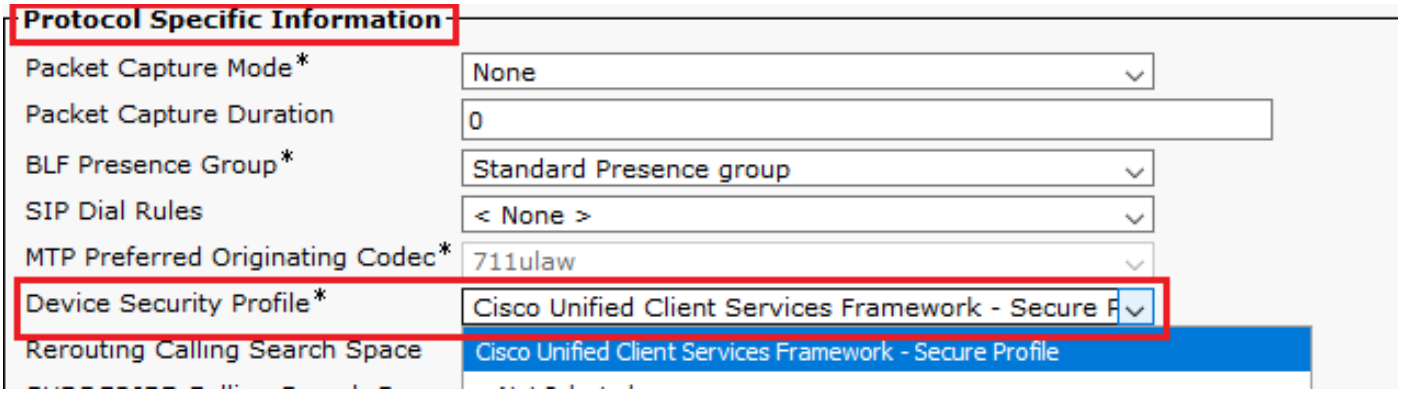
9. 전화기 디바이스 프로필을 성공적으로 생성한 후 Device > Phone.



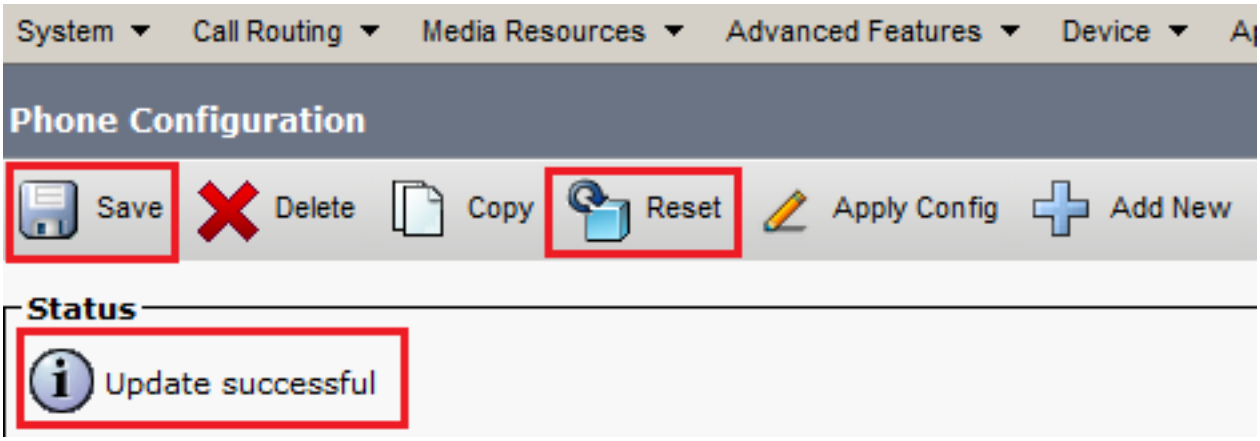
10. 클릭 Find 사용 가능한 모든 전화기를 나열하려면 에이전트 전화기를 클릭합니다.
11. 에이전트 폰 컨피그레이션 페이지가 열립니다. 찾기 Certification Authority Proxy Function (CAPF) Information 섹션을 참조하십시오. LSC를 설치하려면 Certificate Operation 수신 Install/Upgrade 및 Operation Completes by 향후 날짜로 변경합니다.



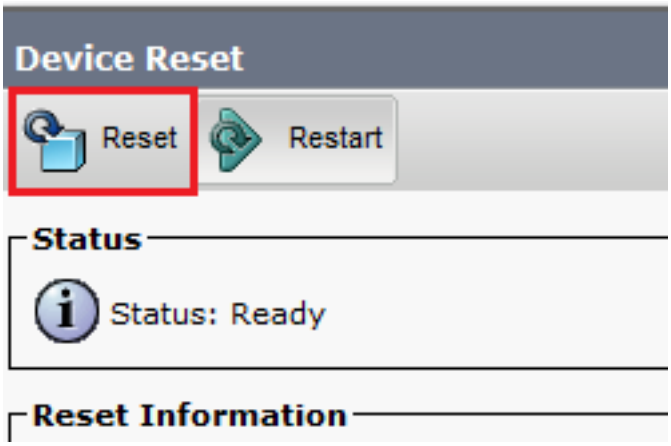
12. 찾기 Protocol Specific Information 섹션을 참조하십시오. 변경 Device Security Profile 수신 Cisco Unified Client Services Framework – Secure Profile.



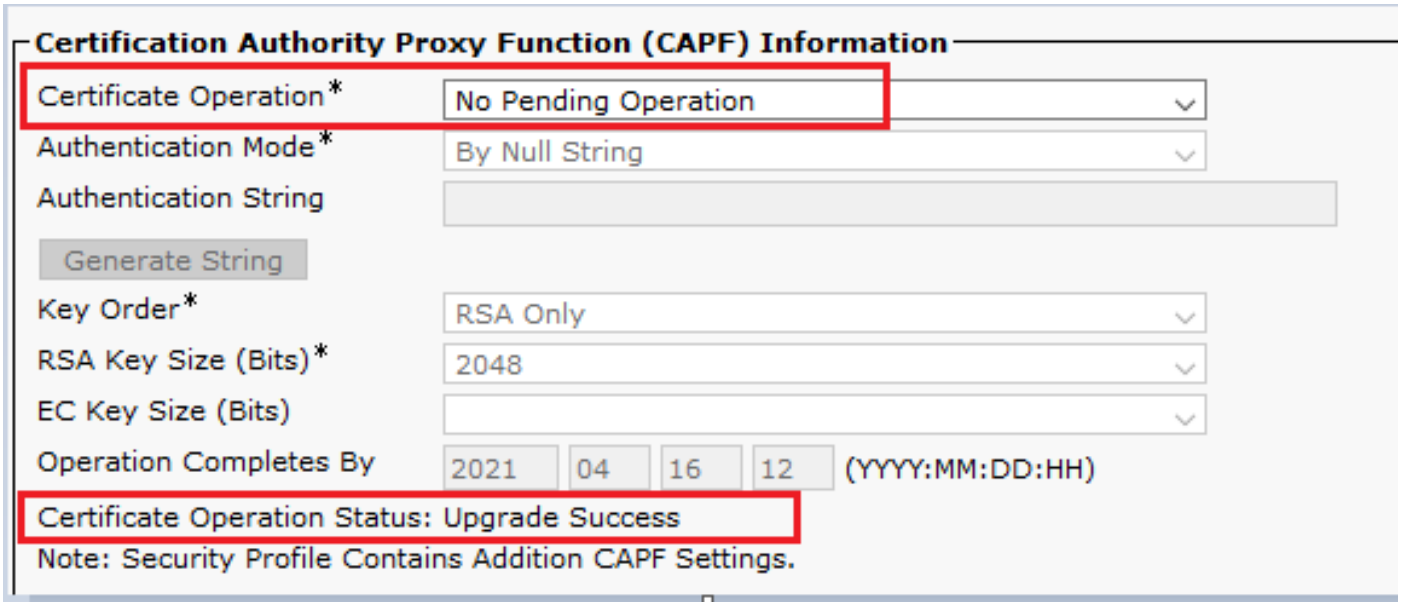
13. 클릭 Save 페이지의 왼쪽 상단에 있습니다. 변경 사항이 성공적으로 저장되었는지 확인하고 Reset.



14. 팝업 창이 열리고 Reset 을 눌러 작업을 확인합니다.



15. 에이전트 디바이스가 CUCM에 다시 한 번 등록되면 현재 페이지를 새로 고치고 LSC가 성공적으로 설치되었는지 확인합니다. 수표 Certification Authority Proxy Function (CAPF) Information 섹션 , Certificate Operation 다음으로 설정되어야 합니다. No Pending Operation 및 Certificate Operation Status 다음으로 설정됨 Upgrade Success .

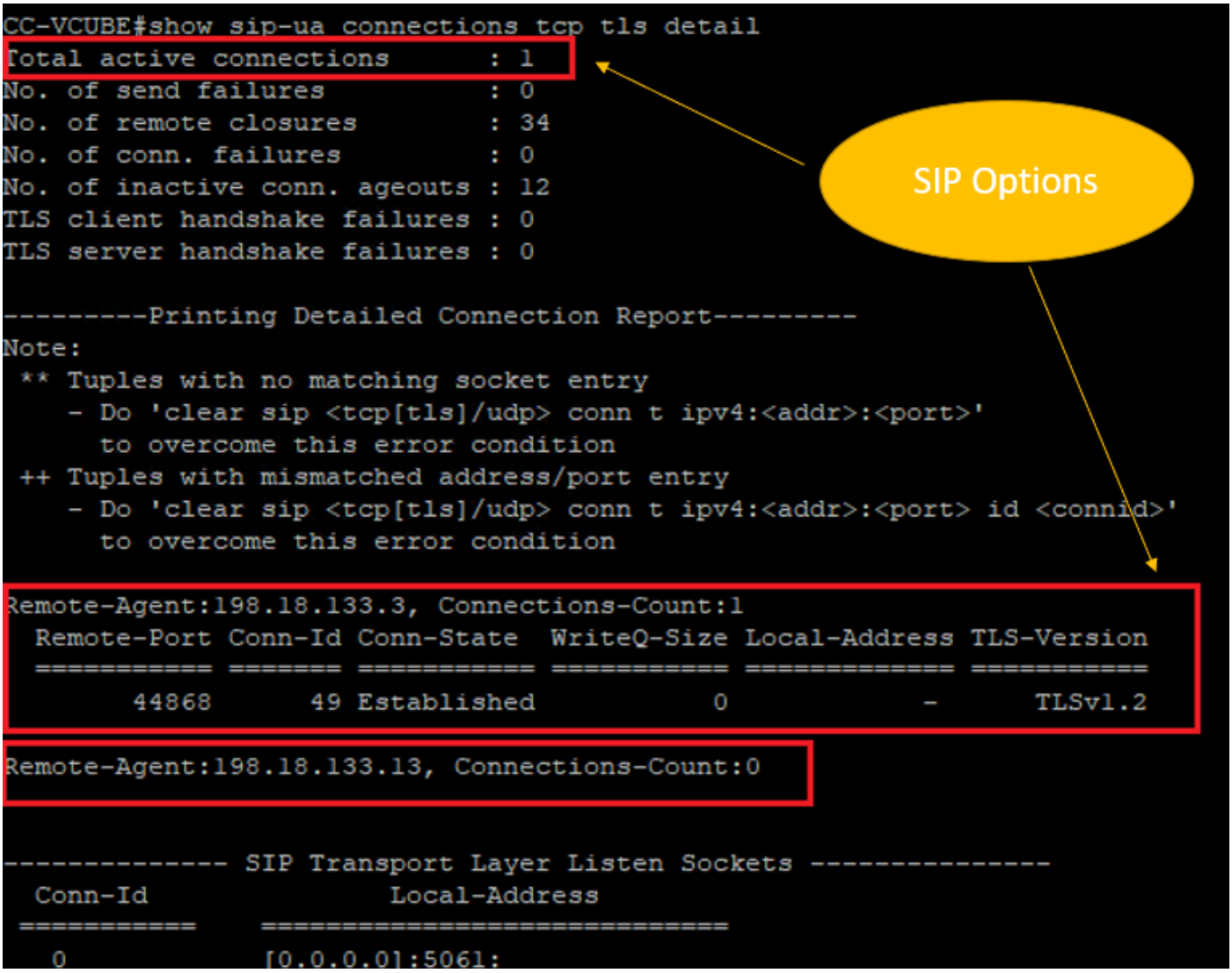


16. 단계를 참조하십시오. CUCM을 사용하여 SIP를 보호하는 데 사용할 다른 에이전트 디바이스를 보호하기 위해 7-13

다음을 확인합니다.

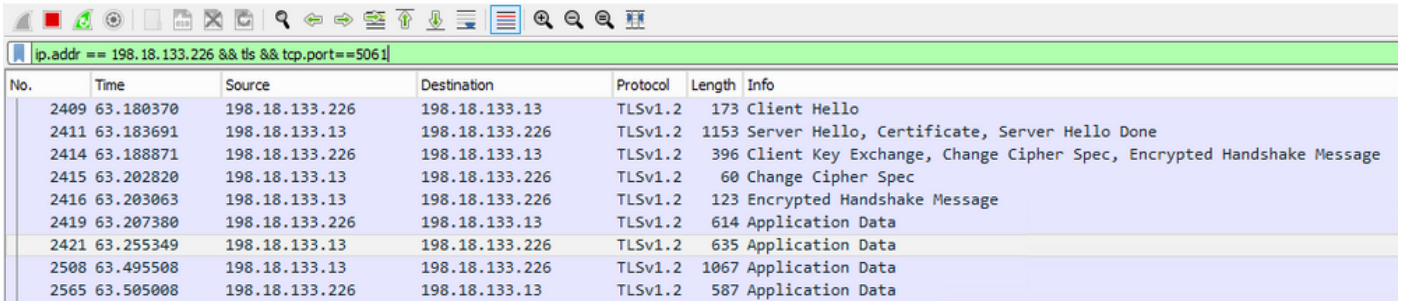
SIP 신호 처리가 제대로 보호되어 있는지 확인하려면 다음 단계를 수행하십시오.

1. vCUBE에 대한 SSH 세션을 열고 명령을 실행합니다 show sip-ua connections tcp tls detail 를 클릭하고 현재 CVP(198.18.133.13)를 사용하여 설정된 TLS 연결이 없음을 확인합니다.



참고: 현재 CUCM(198.18.133.3)에서는 SIP 옵션에 대한 활성 TLS 세션이 하나만 활성화되어 있습니다. 활성화된 SIP 옵션이 없으면 SIP TLS 연결이 없습니다.

2. CVP에 로그인하고 Wireshark를 시작합니다.
3. 컨택 센터 번호로 테스트 전화를 겁니다.
4. CVP 세션으로 이동합니다. Wireshark에서 이 필터를 실행하여 CUBE의 SIP 신호 처리를 확인합니다.
   ip.addr == 198.18.133.226 && tls && tcp.port==5061



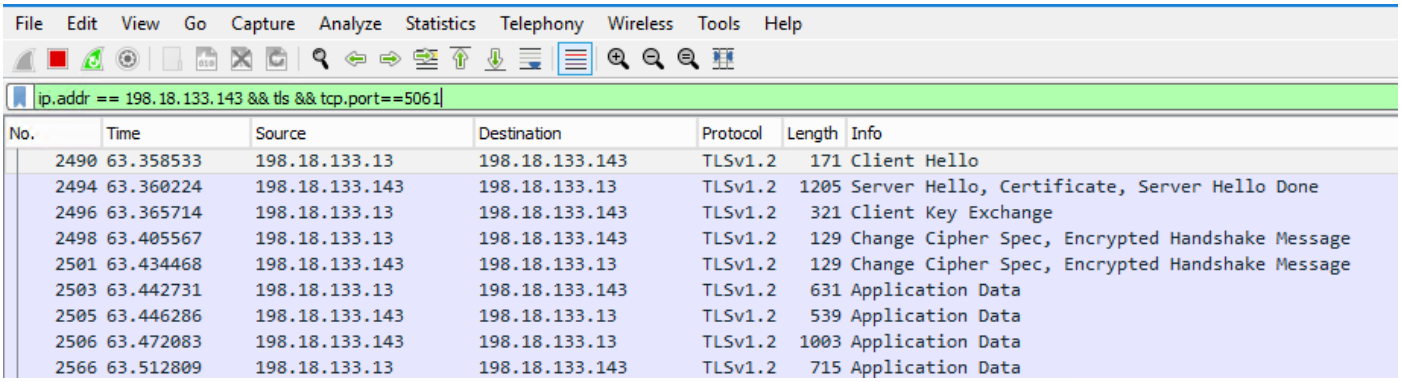
ip.addr == 198.18.133.226 && tls && tcp.port==5061

No.	Time	Source	Destination	Protocol	Length	Info
2409	63.180370	198.18.133.226	198.18.133.13	TLSv1.2	173	Client Hello
2411	63.183691	198.18.133.13	198.18.133.226	TLSv1.2	1153	Server Hello, Certificate, Server Hello Done
2414	63.188871	198.18.133.226	198.18.133.13	TLSv1.2	396	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2415	63.202820	198.18.133.13	198.18.133.226	TLSv1.2	60	Change Cipher Spec
2416	63.203063	198.18.133.13	198.18.133.226	TLSv1.2	123	Encrypted Handshake Message
2419	63.207380	198.18.133.226	198.18.133.13	TLSv1.2	614	Application Data
2421	63.255349	198.18.133.13	198.18.133.226	TLSv1.2	635	Application Data
2508	63.495508	198.18.133.13	198.18.133.226	TLSv1.2	1067	Application Data
2565	63.505008	198.18.133.226	198.18.133.13	TLSv1.2	587	Application Data

확인: SIP over TLS 연결이 설정되었습니까? 대답이 "예"인 경우 CVP와 CUBE 간의 SIP 신호가 안전하다는 것이 출력에 확인됩니다.

5. CVP와 CVVB 간의 SIP TLS 연결을 확인합니다. 동일한 Wireshark 세션에서 다음 필터를 실행합니다.

ip.addr == 198.18.133.143 && tls && tcp.port==5061



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 198.18.133.143 && tls && tcp.port==5061

No.	Time	Source	Destination	Protocol	Length	Info
2490	63.358533	198.18.133.13	198.18.133.143	TLSv1.2	171	Client Hello
2494	63.360224	198.18.133.143	198.18.133.13	TLSv1.2	1205	Server Hello, Certificate, Server Hello Done
2496	63.365714	198.18.133.13	198.18.133.143	TLSv1.2	321	Client Key Exchange
2498	63.405567	198.18.133.13	198.18.133.143	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2501	63.434468	198.18.133.143	198.18.133.13	TLSv1.2	129	Change Cipher Spec, Encrypted Handshake Message
2503	63.442731	198.18.133.13	198.18.133.143	TLSv1.2	631	Application Data
2505	63.446286	198.18.133.143	198.18.133.13	TLSv1.2	539	Application Data
2506	63.472083	198.18.133.143	198.18.133.13	TLSv1.2	1003	Application Data
2566	63.512809	198.18.133.13	198.18.133.143	TLSv1.2	715	Application Data

확인: SIP over TLS 연결이 설정되었습니까? 대답이 예일 경우, 출력은 CVP와 CVVB 사이의 SIP 신호가 안전함을 확인한다.

6. CUBE의 CVP를 사용하여 SIP TLS 연결을 확인할 수도 있습니다. vCUBE SSH 세션으로 이동하고 다음 명령을 실행하여 보안 sip 신호를 확인합니다.

show sip-ua connections tcp tls detail

```
CC-VCUBE#show sip-ua connections tcp tls detail
Total active connections      : 2
No. of send failures          : 0
No. of remote closures        : 0
No. of conn. failures         : 0
No. of inactive conn. ageouts : 0
TLS client handshake failures : 0
TLS server handshake failures : 0

---------Printing Detailed Connection Report---------
Note:
 ** Tuples with no matching socket entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port>'
      to overcome this error condition
 ++ Tuples with mismatched address/port entry
    - Do 'clear sip <tcp[tls]/udp> conn t ipv4:<addr>:<port> id <connid>'
      to overcome this error condition

Remote-Agent:198.18.133.3, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= ========== ========== ============= ===========
        38896       2 Established          0             -      TLSv1.2

Remote-Agent:198.18.133.13, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size Local-Address TLS-Version
  =========== ======= ========== ========== ============= ===========
         5061       3 Established          0             -      TLSv1.2


-------------- SIP Transport Layer Listen Sockets ---------------
  Conn-Id                Local-Address
 ===========    ================================
   0             [0.0.0.0]:5061:
```

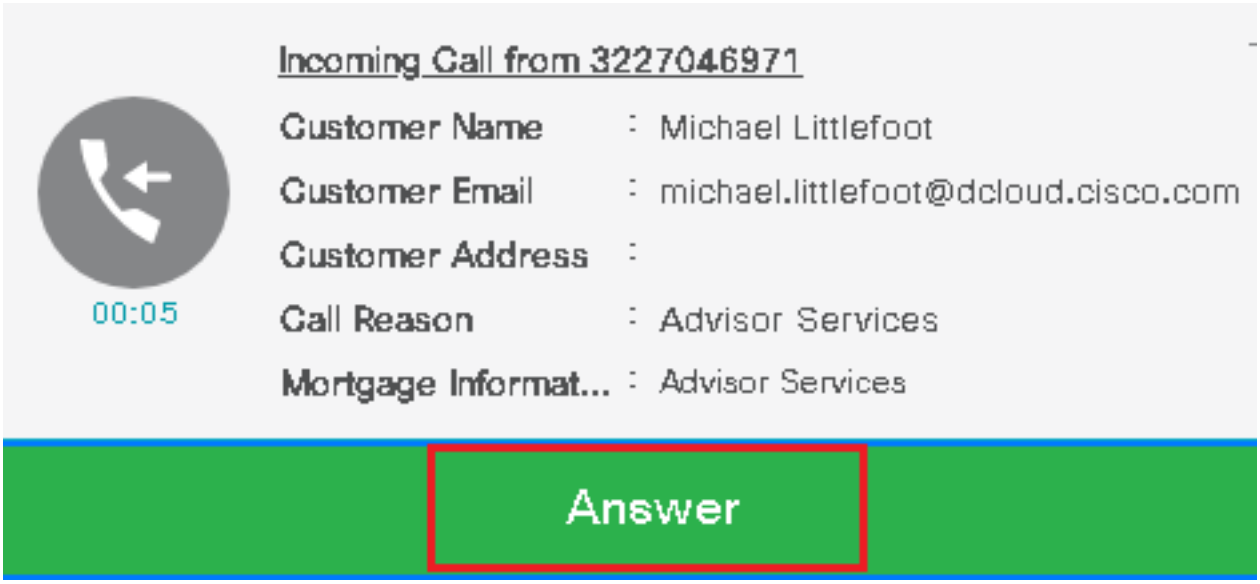
확인: CVP와 SIP over TLS 연결이 설정됩니까? 대답이 "예"인 경우 CVP와 CUBE 간의 SIP 신호가 안전하다는 것이 출력에 확인됩니다.

7. 현재 통화가 활성 상태이며, 통화에 응답할 수 있는 상담원이 없으므로 MOH(대기 중 음악)가 재생됩니다.

8. 상담원이 전화를 받을 수 있도록 합니다.

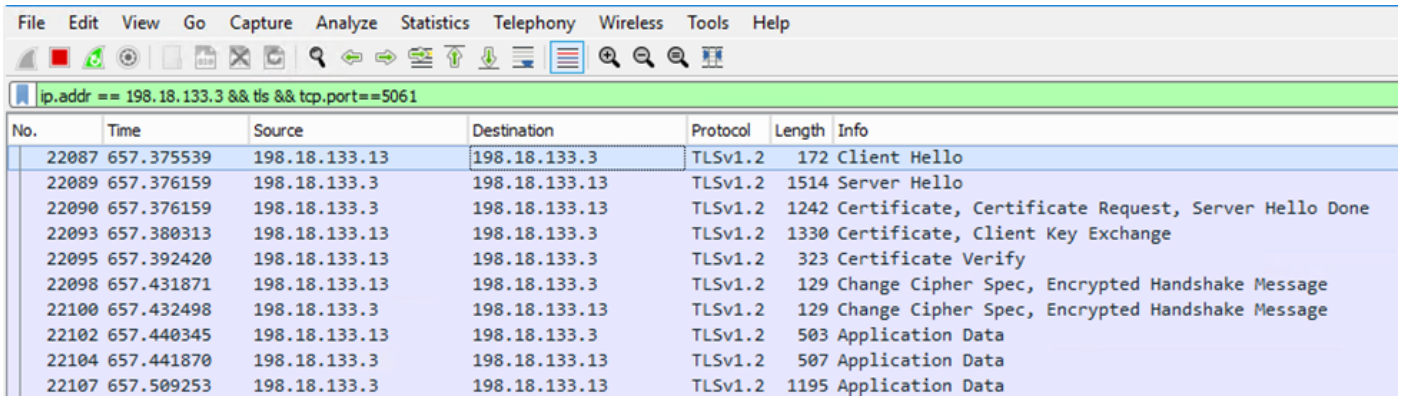
.

9. 상담원이 예약되고 통화가 상담원에게 라우팅됩니다. 클릭 Answer 전화를 받을 수 있습니다



10. 통화가 상담원에게 연결됩니다.

11. CVP와 CUCM 간의 SIP 신호를 확인하려면 CVP 세션으로 이동하여 Wireshark에서 이 필터를 실행합니다.
ip.addr == 198.18.133.3 && tls && tcp.port==5061



> **확인**: 모든 SIP 통신이 TLS를 통해 CUCM(198.18.133.3)과 통신합니까? 대답이 "예"인 경우 CVP와 CUCM 간의 SIP 신호가 안전하다는 것이 출력에 확인됩니다.

문제 해결

TLS가 설정되지 않은 경우 CUBE에서 다음 명령을 실행하여 디버그 TLS를 활성화하여 문제를 해결합니다.

- Debug ssl openssl errors
- Debug ssl openssl msg
- Debug ssl openssl states

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.