

# Contact Center Enterprise에서 보안 RTP 구성

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[작업 1: CUBE 보안 컨피그레이션](#)

[작업 2: CVP 보안 컨피그레이션](#)

[작업 3: CVVB 보안 컨피그레이션](#)

[작업 4: CUCM 보안 컨피그레이션](#)

[CUCM 보안 모드를 혼합 모드로 설정](#)

[CUBE 및 CVP에 대한 SIP 트렁크 보안 프로필 구성](#)

[SIP 트렁크 보안 프로필을 각 SIP 트렁크에 연결하고 SRTP 활성화](#)

[보안 에이전트의 CUCM과의 디바이스 통신](#)

[다음을 확인합니다.](#)

## 소개

이 문서에서는 CCE(Contact Center Enterprise) 종합 통화 흐름에서 SRTP(Real-Time Transport Protocol) 트래픽을 보호하는 방법을 설명합니다.

## 사전 요구 사항

인증서 생성 및 가져오기는 이 문서의 범위에 포함되지 않으므로 Cisco Unified Communication Manager(CUCM), Customer Voice Portal(CVP) Call Server, 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.

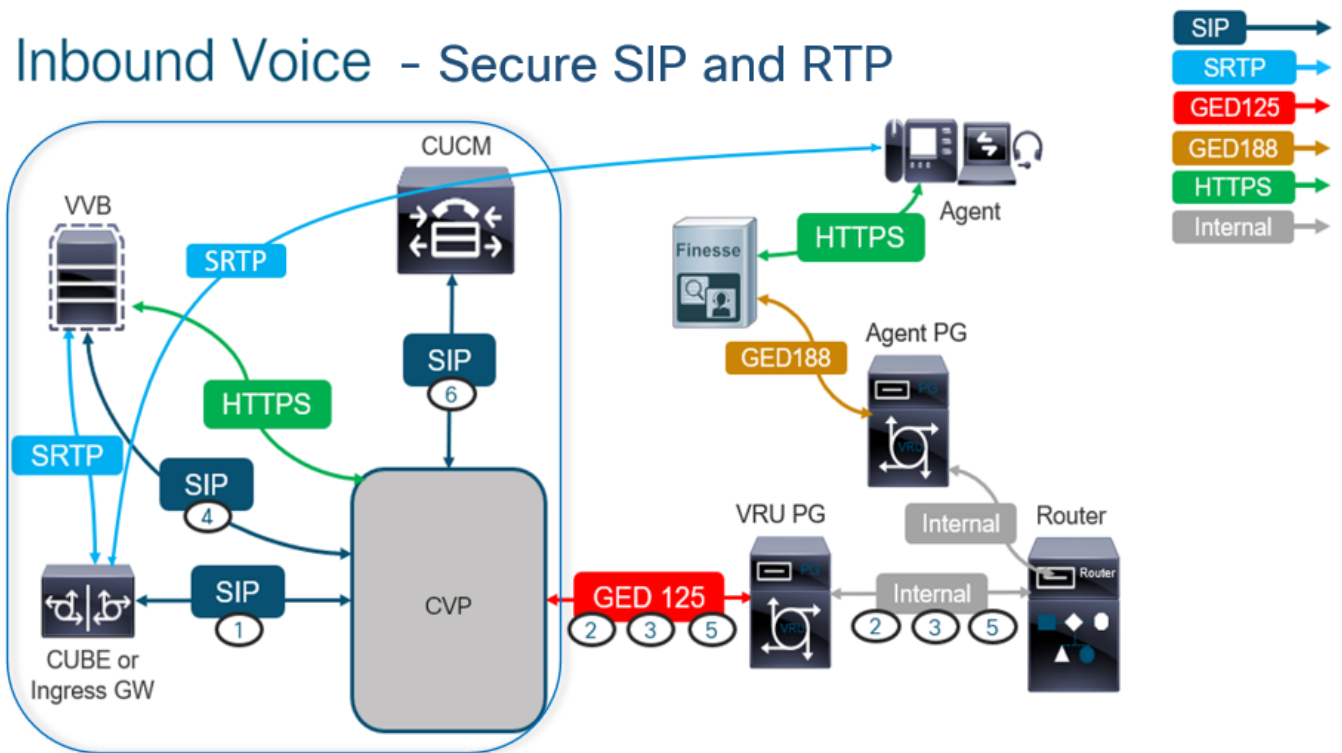
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

**참고:** 컨택 센터의 포괄적인 통화 흐름에서 보안 RTP를 활성화하려면 보안 SIP 신호를 활성화해야 합니다. 따라서 이 문서의 컨피그레이션은 보안 SIP 및 SRTP를 모두 활성화합니다.

다음 다이어그램에는 컨택 센터의 포괄적인 통화 흐름에서 SIP 신호 및 RTP와 관련된 구성 요소가 나와 있습니다. 음성 통화가 시스템에 수신되면 먼저 인그레스 게이트웨이 또는 CUBE를 통해 수신되므로 CUBE에서 컨피그레이션을 시작합니다. 다음으로 CVP, CVVB 및 CUCM을 구성합니다.

### Inbound Voice - Secure SIP and RTP



### 작업 1: CUBE 보안 컨피그레이션

이 작업에서는 SIP 프로토콜 메시지 및 RTP를 보호하도록 CUBE를 구성합니다.

필수 구성:

- SIP UA에 대한 기본 신뢰 지점 구성
- TLS 및 SRTP를 사용하도록 다이얼 피어 수정

단계:

1. CUBE에 대한 SSH 세션을 엽니다.
2. SIP 스택에서 CUBE의 CA 인증서를 사용하도록 하려면 다음 명령을 실행합니다. CUBE는

CUCM(198.18.133.3) 및 CVP(198.18.133.13)에서/로 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 6000을 사용하여 통화를 CVP로 라우팅합니다.

```
Conf t dial-peer voice 6000 voip session target ipv4:198.18.133.13:5061 session transport tcp tls srtp 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) #SRTP
CC-VCUBE (config-dial-peer) #exit
CC-VCUBE (config) #
CC-VCUBE (config) #
```

## 작업 2: CVP 보안 컨피그레이션

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

단계:

1. 에 로그인합니다 UCCE Web Administration.
2. 탐색 Call Settings > Route Settings > SIP Server Group.

### Route Settings

Media Routing Domain Call Type Dialed Number Expanded Call Variables SIP Server Group

Properties

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, 그리고 Members SIP 서버 그룹 컨피그레이션의 세부사항을 표시하는 탭입니다. 설정 SecurePort 수신 5061 을 클릭하고 Save.

Edit cucm1.dcloud.cisco.com

General

Members

List of Group Members



Hostname/IP	Priority	Weight	Port	SecurePort	Site
198.18.133.3	10	10	5060	5061	Main

4. 클릭 vvb1.dcloud.cisco.com CISCO의 Members 탭, SecurePort 수신 5061 을 클릭하고 Save.

Edit vvb1.dcloud.cisco.com

General

Members

List of Group Members



Hostname/IP	Priority	Weight	Port	SecurePort	Site
vvb1.dcloud.cisco.c...	10	10	5060	5061	Main

### 작업 3: CVVB 보안 컨피그레이션

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

단계:

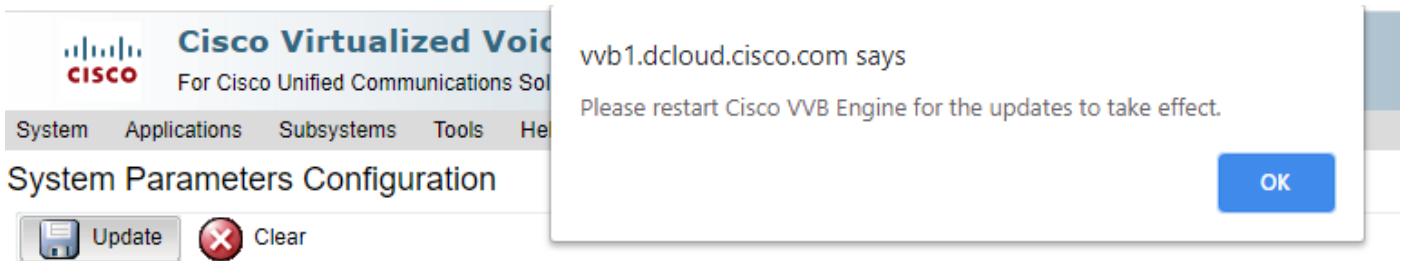
1. 열기 Cisco VVB Admin 페이지를 참조하십시오.
2. 탐색 System > System Parameters.

The screenshot shows the Cisco Virtualized Voice Browser Administration interface. The top navigation bar includes System, Applications, Subsystems, Tools, and Help. The System Parameters menu is highlighted, showing a dropdown with System Parameters and Logout options. The main header displays the Cisco logo and the text 'Cisco Virtualized Voice Browser Administration For Cisco Unified Communications Solutions'. The system version is noted as 12.5.1.10000-24.

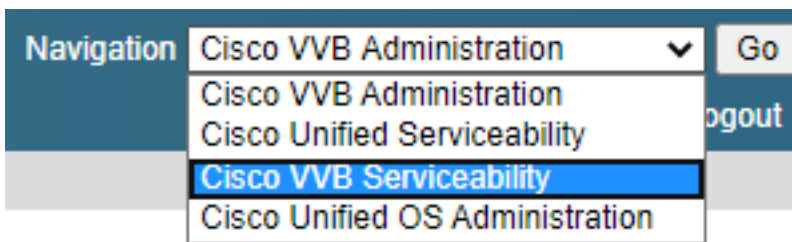
3. 에 Security Parameters 섹션, 선택 Enable 대상: TLS (SIP) . 유지 Supported TLS(SIP) version as TLSv1.2 선택 Enable 대상: SRTP.

Security Parameters		
Parameter Name	Parameter Value	Suggested Value
TLS(SIP)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable	Disable
Supported TLS(SIP) Versions	TLSv1.2	TLSv1.2
▶ Cipher Configuration		TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
SRTP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable <input type="checkbox"/> Allow RTP (Mixed mode)	Disable

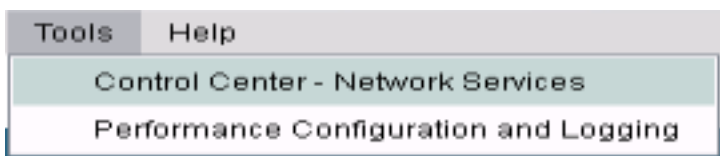
4. 클릭 Update. 클릭 ok CVVB 엔진을 다시 시작하라는 메시지가 나타나면



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



6. 탐색 Tools > Control Center – Network Services.




7. 선택 Engine 을 클릭하고 Restart.

## Control Center - Network Services



### Status

 Ready

### Select Server

Server \*

System Services	
	Service Name
<input type="radio"/>	Perfmon Counter Service
<input type="radio"/>	▼Cluster View Daemon
	▶Manager Manager
<input checked="" type="radio"/>	▼Engine
	▶Manager Manager
	▶Subsystem Manager

## 작업 4: CUCM 보안 컨피그레이션

CUCM에서 SIP 메시지 및 RTP를 보호하려면 다음 컨피그레이션을 수행합니다.

- CUCM 보안 모드를 혼합 모드로 설정
- CUBE 및 CVP에 대한 SIP 트렁크 보안 프로파일 구성
- SIP 트렁크 보안 프로필을 각 SIP 트렁크에 연결하고 SRTP 활성화
- CUCM과의 보안 에이전트 장치 통신

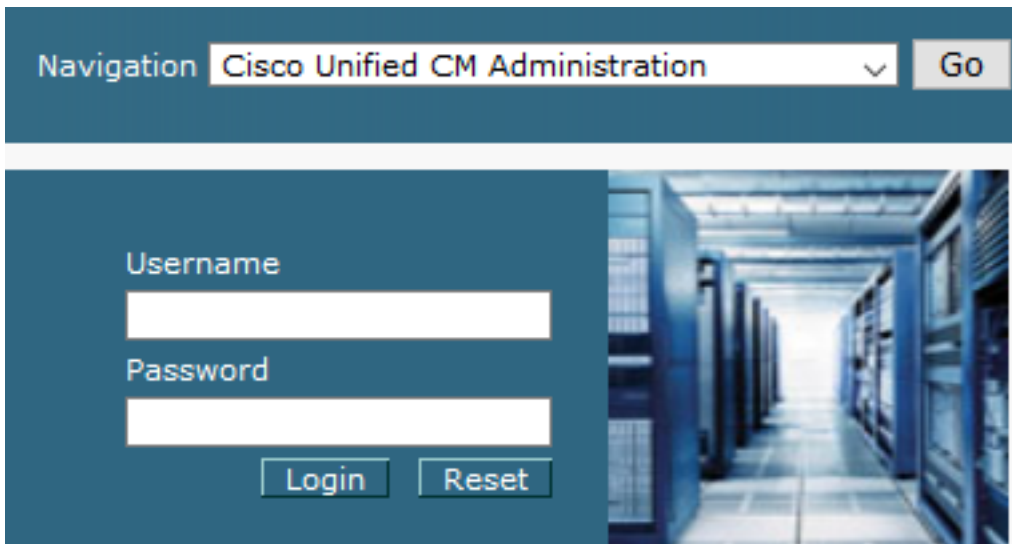
### CUCM 보안 모드를 혼합 모드로 설정

CUCM은 2가지 보안 모드를 지원합니다.

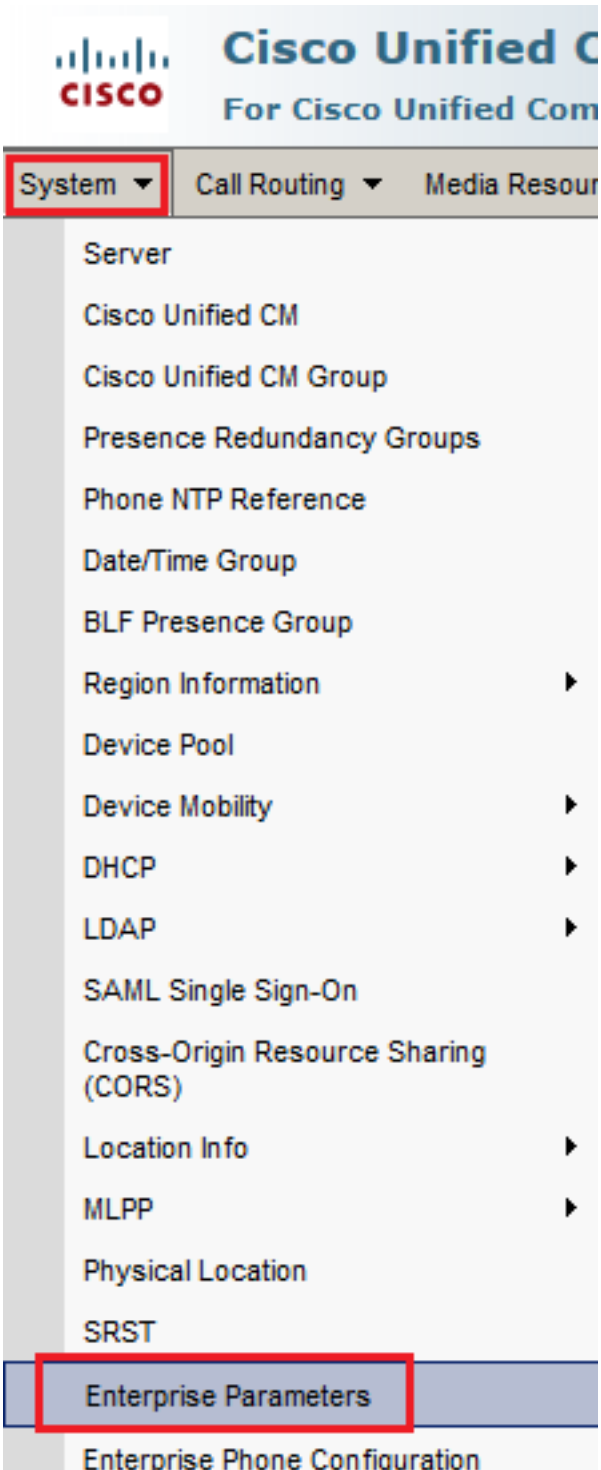
- 비보안 모드(기본 모드)
- 혼합 모드(보안 모드)

단계:

1. CUCM 관리 인터페이스에 로그인합니다.



2. CUCM에 로그인하면 System > Enterprise Parameters.



3. 아래 Security Parameters 섹션, 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 로그인하면 다음 명령을 실행합니다.

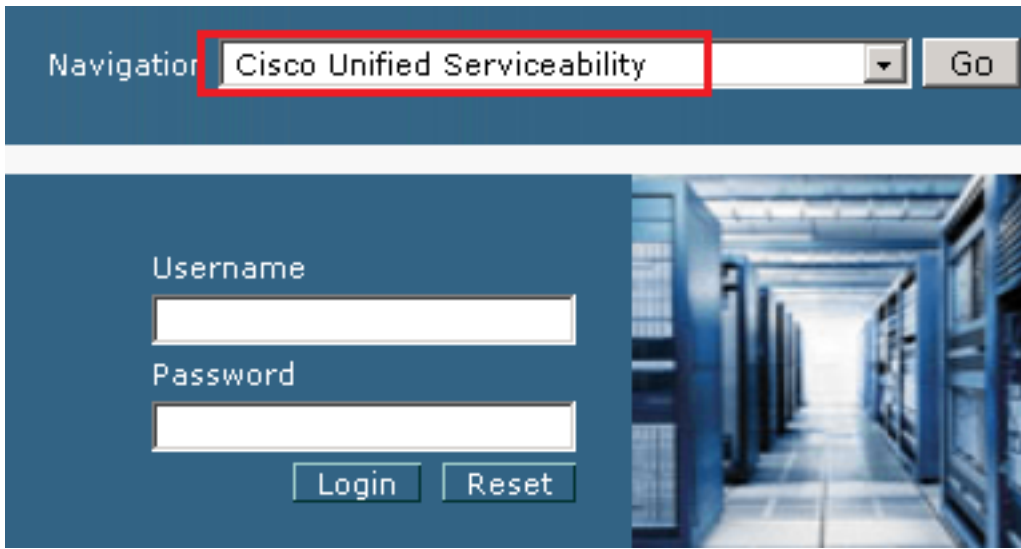
`utils ctl set-cluster 혼합 모드`



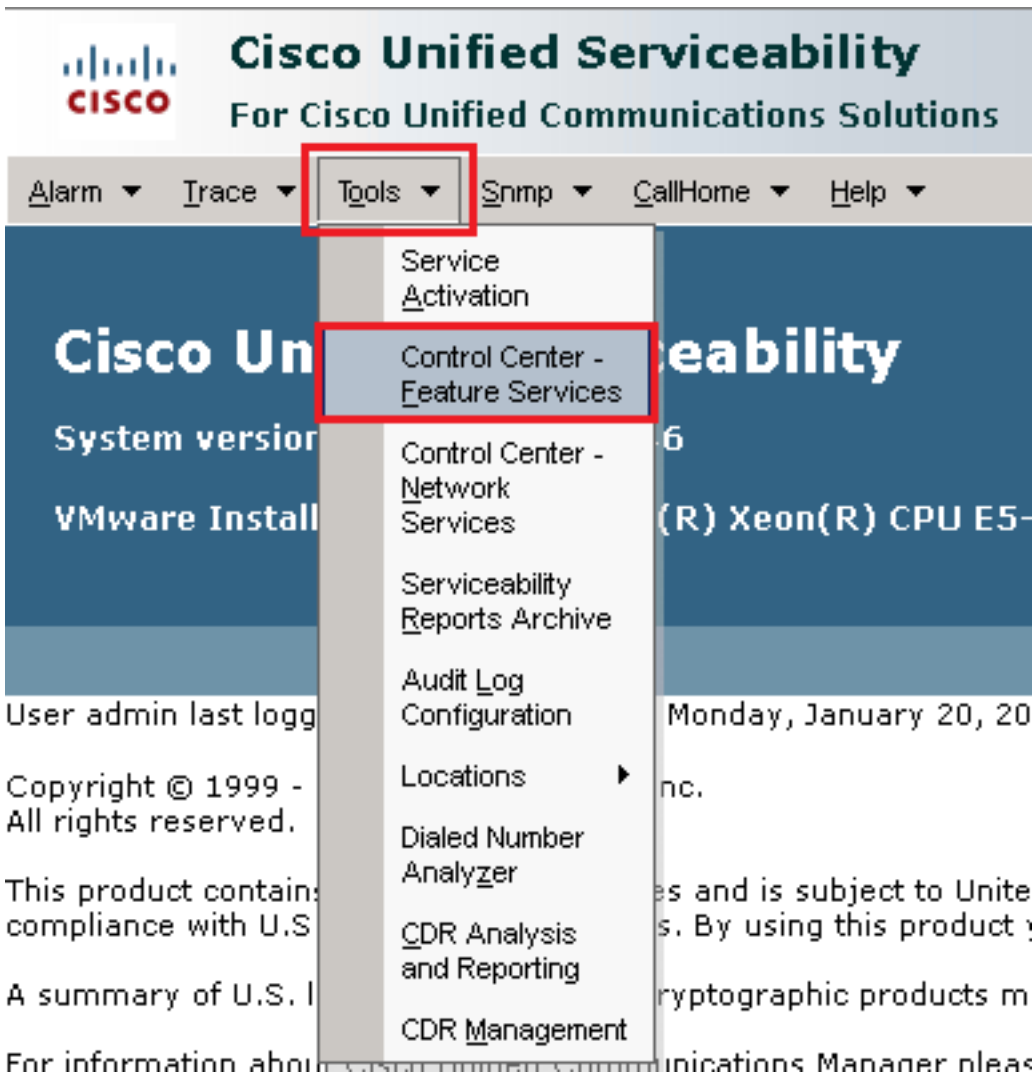
7. 유형 y 을 클릭하고 Enter 프롬프트가 표시되면 이 명령은 클러스터 보안 모드를 혼합 모드로 설정합니다.

```
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y
Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.
admin:
```

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



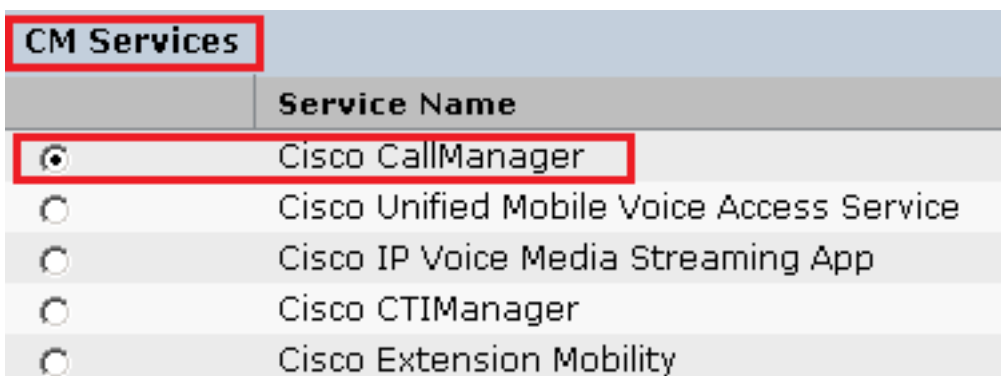
10. 로그인에 성공하면 Tools > Control Center – Feature Services.



11. 서버를 선택한 다음 Go.



12. CM 서비스 아래에서 Cisco CallManager 를 클릭한 다음 Restart 버튼을 클릭합니다.



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

Restarting Service. It may take a while... Please wait for the page to refresh.  
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



14. 을(를) 성공적으로 재시작한 후 Cisco CallManager을 선택합니다. Cisco CTIManager 그런 다음 Restart 단추를 클릭하여 다시 시작합니다. Cisco CTIManager 서비스.

CM Services	
	Service Name
<input type="radio"/>	Cisco CallManager
<input type="radio"/>	Cisco Unified Mobile Voice Access Service
<input type="radio"/>	Cisco IP Voice Media Streaming App
<input checked="" type="radio"/>	Cisco CTIManager
<input type="radio"/>	Cisco Extension Mobility

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

Restarting Service. It may take a while... Please wait for the page to refresh.  
If you see Starting/Stopping state, refresh the page after sometime to show the right status.



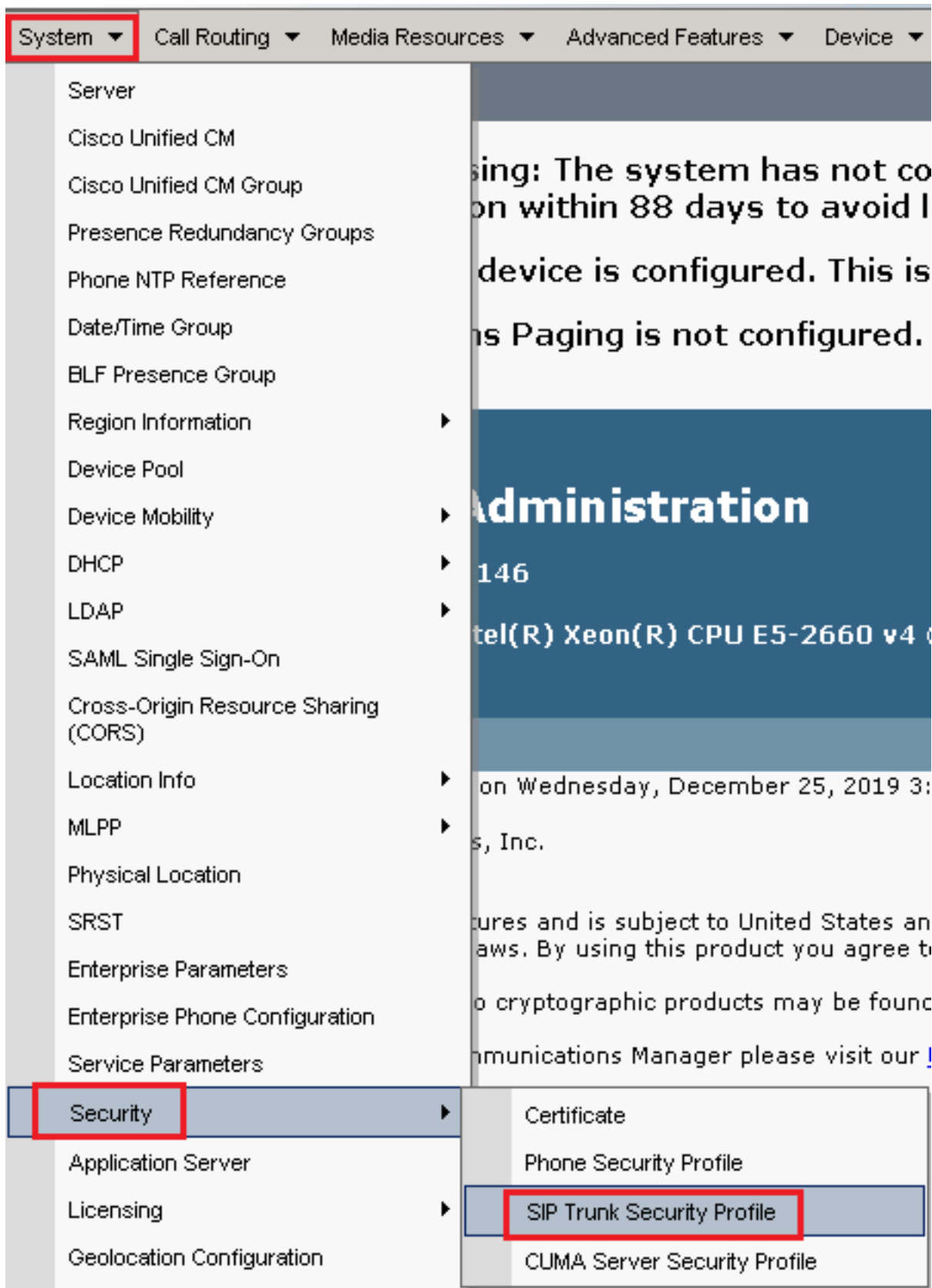
16. 서비스를 성공적으로 다시 시작한 후 클러스터 보안 모드가 혼합 모드로 설정되어 있는지 확인하려면 5단계에서 설명한 대로 CUCM 관리로 이동한 다음 Cluster Security Mode. 이제 다음으로 설정되어야 합니다. 1.

Security Parameters	
<u>Cluster Security Mode</u> *	1
<u>Cluster SIPOAuth Mode</u> *	Disabled

## CUBE 및 CVP에 대한 SIP 트렁크 보안 프로필 구성

단계:

1. CUCM 관리 인터페이스에 로그인합니다.
2. CUCM에 성공적으로 로그인했다면 System > Security > SIP Trunk Security Profile CUBE에 대한 디바이스 보안 프로필을 생성하려면



3. 왼쪽 상단에서 Add **New**(새로 추가)를 클릭하여 새 프로필을 추가합니다.

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features

## Find and List SIP Trunk Security Profiles







 Add New
  Select All
  Clear All
  Delete Selected

4. 구성 SIP Trunk Security Profile 이 이미지로 이동한 다음 Save 페이지의 왼쪽 하단에 있습니다.



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

## SIP Trunk Security Profile Configuration

Related Links: [Back](#)

 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New

**- Status**

-  Add successful
-  Reset of the trunk is required to have changes take effect.

**- SIP Trunk Security Profile Information**

Name*	SecureSIPTLSforCube
Description	
Device Security Mode	Encrypted ▾
Incoming Transport Type*	TLS ▾
Outgoing Transport Type	TLS ▾
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
Secure Certificate Subject or Subject Alternate Name	SIP-GW
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter ▾

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. 변경 Secure Certificate Subject 일치해야 하므로 CVP 통화 서버 인증서의 CN에 연결합니다. 클릭 Save 버튼을 클릭합니다.

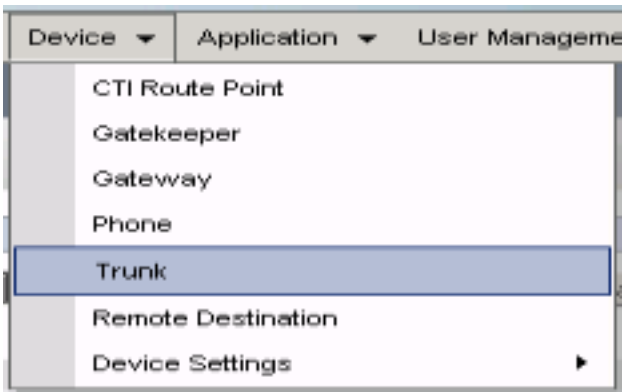
The screenshot displays the configuration interface for a SIP Trunk Security Profile. At the top, there is a toolbar with icons for Save, Delete, Copy, Reset, Apply Config, and Add New. Below the toolbar, the 'Status' section shows two informational messages: 'Add successful' and 'Reset of the trunk is required to have changes take effect.' The main section is titled 'SIP Trunk Security Profile Information' and contains several fields and options:

- Name\***: SecureSIPTLSforCvp
- Description**: (Empty)
- Device Security Mode**: Encrypted
- Incoming Transport Type\***: TLS
- Outgoing Transport Type**: TLS
- Enable Digest Authentication
- Nonce Validity Time (mins)\***: 600
- Secure Certificate Subject or Subject Alternate Name**: cvp1.dcloud.cisco.com
- Incoming Port\***: 5061
- Enable Application level authorization
- Accept presence subscription
- Accept out-of-dialog refer\*\*
- Accept unsolicited notification
- Accept replaces header
- Transmit security status
- Allow charging header
- SIP V.150 Outbound SDP Offer Filtering\***: Use Default Filter

SIP 트렁크 보안 프로필을 각 SIP 트렁크에 연결하고 SRTP 활성화

단계:

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



2. CUBE 트렁크를 검색합니다. 이 예에서 CUBE 트렁크 이름은 vCube 를 클릭한 다음 Find.

Trunks (1 - 5 of 5)

Find Trunks where Device Name begins with vCube Find Clear Filter

	Name ^	Description	Calling Search Space	Device Pool	Route Pattern	Partition
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	cloudcherry.sip.twilio.com	dCloud_PT
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	7800	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	6016	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	7019	PSTN_Incoming_Numbers
<input type="checkbox"/>	vCUBE	dCloud_CSS	dCloud_DP	dCloud_DP	44413XX	Robot Agent Remote Destinations

3. 클릭 vCUBE vCUBE 트렁크 컨피그레이션 페이지를 엽니다.

4. 수신 Device Information 섹션, SRTP Allowed SRTP를 활성화하려면 확인란을 선택합니다.

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information. Consider Traffic on This Trunk Secure\*

When using both sRTP and TLS

Route Class Signaling Enabled\* Default

Use Trusted Relay Point\* Default

5. 아래로 스크롤하여 SIP Information 섹션 및 변경 Destination Port 수신 5061.

6. 변경 SIP Trunk Security Profile 수신 SecureSIPTLSForCube.

SIP Information

Destination

Destination Address is an SRV

1\* Destination Address 198.18.133.226 Destination Address IPv6 Destination Port 5061

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* SecureSIPTLSforCube

Rerouting Calling Search Space < None >

7. 클릭 Save 그런 다음 Rest 수신 save 변경 사항을 적용합니다.

## Trunk Configuration



Save



Delete



Reset



Add New

### Status



Update successful

The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

OK

8. 탐색 Device > Trunk, CVP 트렁크를 검색합니다. 이 예에서는 CVP 트렁크 이름이 cvp-SIP-Trunk. 클릭 Find.

### Trunks (1 - 1 of 1)

Find Trunks where  begins with

<input type="checkbox"/>	Name ^	Description	Calling Search Space	Device Pool
<input type="checkbox"/>	CVP-SIP-Trunk	CVP-SIP-Trunk	dCloud_CSS	dCloud_DP

9. 클릭 CVP-SIP-Trunk 를 눌러 CVP 트렁크 컨피그레이션 페이지를 엽니다.
10. 수신 Device Information 섹션, 확인 SRTP Allowed SRTP를 활성화하려면 확인란을 선택합니다.

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information. Consider Traffic on This Trunk Secure\*

Route Class Signaling Enabled\*

Use Trusted Relay Point\*

11. 아래로 스크롤하여 SIP Information 섹션, 변경 Destination Port 수신 5061.
12. 변경 SIP Trunk Security Profile 수신 SecureSIPTLSForCvp.

### SIP Information

**Destination**

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 198.18.133.13		5061

MTP Preferred Originating Codec\*

BLF Presence Group\*

SIP Trunk Security Profile\*

13. 클릭 Save 그런 다음 Rest 수신 save 변경 사항을 적용합니다.



The configuration changes will not take effect on the trunk until a reset is performed. Use the Reset button or Job Scheduler to execute the reset.

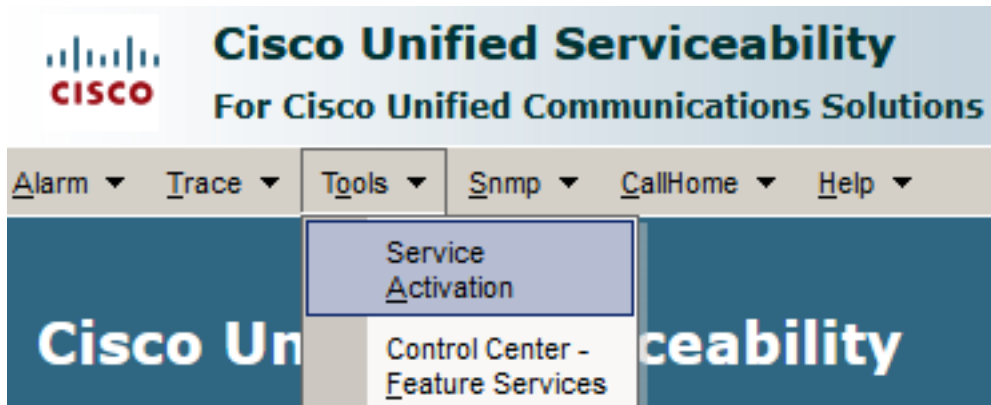
OK

## 보안 에이전트의 CUCM과의 디바이스 통신

디바이스에 보안 기능을 활성화하려면 LSC(Locally Significant Certificate)를 설치하고 해당 디바이스에 보안 프로파일을 할당해야 합니다. LSC는 CUCM CAPF 개인 키로 서명된 엔드포인트의 공개 키를 보유하고 있습니다. 기본적으로 전화기에는 설치되지 않습니다.

단계:

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



3. CUCM 서버를 선택하고 Go.

### Service Activation

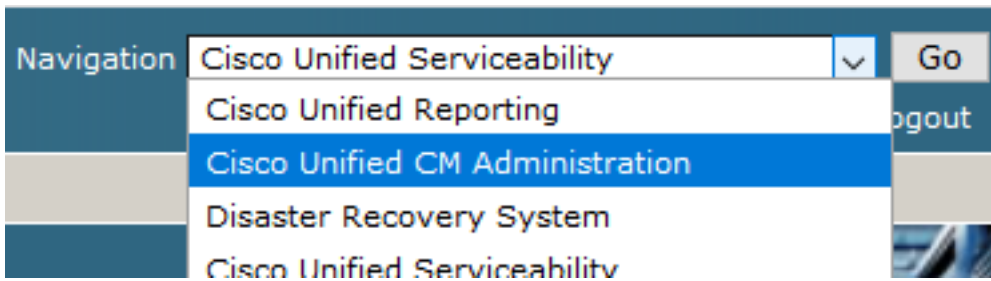
Select Server

Server\*

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

Security Services		
	Service Name	Activation Status
<input checked="" type="checkbox"/>	Cisco Certificate Authority Proxy Function	Deactivated
<input type="checkbox"/>	Cisco Certificate Enrollment Service	Deactivated

5. 서비스가 활성화되었는지 확인한 다음 CUCM administration(CUCM 관리)으로 이동합니다.



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



# Cisco Unified CM Administration

For Cisco Unified Communications Solutions

System ▾

Call Routing ▾

Media Resources ▾

Advanced Features ▾

Devi

Server

Cisco Unified CM

Cisco Unified CM Group

Presence Redundancy Groups

Phone NTP Reference

Date/Time Group

BLF Presence Group

Region Information ▶

Device Pool

Device Mobility ▶

DHCP ▶

LDAP ▶

SAML Single Sign-On

Cross-Origin Resource Sharing (CORS)

Location Info ▶

MLPP ▶

Physical Location

SRST

Enterprise Parameters

Enterprise Phone Configuration

Service Parameters

Security ▶

Application Server

Licensing ▶

Geolocation Configuration

device is configured. The  
as Paging is not configur

## Administration

7

tel(R) Xeon(R) CPU E5-2660

on Friday, December 20, 2019 10  
s, Inc.

ures and is subject to United Stat  
aws. By using this product you ac

o cryptographic products may be

munications Manager please visit


our [Technical Support](#) web site.

Certificate

Phone Security Profile

SIP Trunk Security Profile

CUMA Server Security Profile

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

Phone Security Profile (1 - 1 of 1) Rows per Page 50

Find Phone Security Profile where Name contains client Find Clear Filter + -

Name	Description	Copy
Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	Cisco Unified Client Services Framework - Standard SIP Non-Secure Profile	

8. 프로파일 이름을 다음으로 변경 Cisco Unified Client Services Framework - Secure Profile. C0이 그림과 같이 매개변수를 변경한 다음 Save 페이지의 왼쪽 상단에 있습니다.

System Call Routing Media Resources Advanced Features Device Application User

### Phone Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

**Status**

Add successful

**Phone Security Profile Information**

**Product Type:** Cisco Unified Client Services Framework  
**Device Protocol:** SIP

Name\* Cisco Unified Client Services Framework - Secure Profile  
 Description Cisco Unified Client Services Framework - Secure Profile  
 Device Security Mode Encrypted  
 Transport Type\* TLS

TFTP Encrypted Config  
 Enable OAuth Authentication

**Phone Security Profile CAPF Information**

Authentication Mode\* By Null String  
 Key Order\* RSA Only  
 RSA Key Size (Bits)\* 2048  
 EC Key Size (Bits) < None >

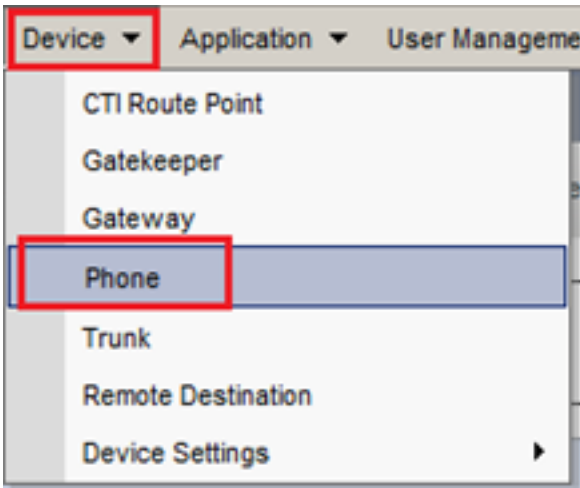
Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

**Parameters used in Phone**

SIP Phone Port\* 5061

Save Delete Copy Reset Apply Config Add New

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.

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

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Null String
Authentication String	<input type="text"/>
<input type="button" value="Generate String"/>	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	<input type="text"/>
Operation Completes By	2021 04 16 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None  
 Note: Security Profile Contains Addition CAPF Settings.

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







**Protocol Specific Information**

Packet Capture Mode*	None
Packet Capture Duration	0
BLF Presence Group*	Standard Presence group
SIP Dial Rules	< None >
MTP Preferred Originating Codec*	711ulaw
Device Security Profile*	Cisco Unified Client Services Framework - Secure F
Rerouting Calling Search Space	Cisco Unified Client Services Framework - Secure Profile

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


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

## Phone Configuration

 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New



---

### Status

 Update successful


14. 팝업 창이 열리고 Reset 을 눌러 작업을 확인합니다.

## Device Reset

 Reset
  Restart

---

### Status

 Status: Ready

---

### Reset Information

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.

## Certification Authority Proxy Function (CAPF) Information

Certificate Operation\*

Authentication Mode\*

Authentication String

Key Order\*

RSA Key Size (Bits)\*

EC Key Size (Bits)

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

**Certificate Operation Status: Upgrade Success**

Note: Security Profile Contains Addition CAPF Settings.

16. 단계의 동일한 단계를 참조하십시오. 7 - 13 - CUCM에서 보안 SIP 및 RTP를 사용하려는 다른 에이전트의 디바이스를 보호합니다.

# 다음을 확인합니다.

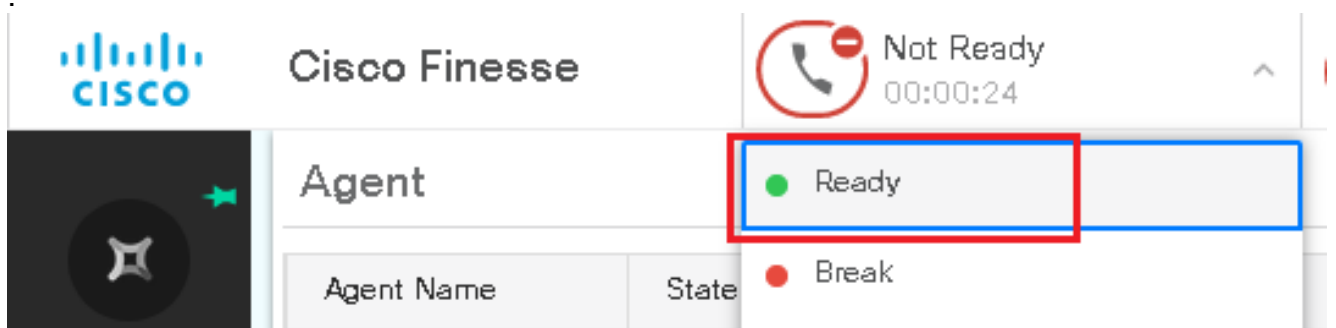
RTP가 올바르게 보호되어 있는지 확인하려면 다음 단계를 수행하십시오.

1. 컨택 센터에 테스트 전화를 걸고 IVR 프롬프트를 청취합니다.
2. 동시에 vCUBE에 대한 SSH 세션을 열고 다음 명령을 실행합니다.  
show call active voice brief

```
Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:674ECD1639ED7A710000ABF910000178
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 active
dur 00:00:26 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.143:25346 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:674ECD1639ED7A710000ABF910000178
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:
```

**팁:** SRTP가 on CUBE와 VVB(198.18.133.143) 사이의 숫자입니다. 대답이 "예"인 경우 CUBE와 VVB 간의 RTP 트래픽이 안전함을 확인합니다.

3. 상담원이 전화를 받을 수 있도록 합니다.



4. 상담원이 예약되고 통화가 상담원에게 라우팅됩니다. 전화를 받습니다.
5. 통화가 상담원에게 연결됩니다. vCUBE SSH 세션으로 돌아가 다음 명령을 실행합니다.  
show call active voice brief

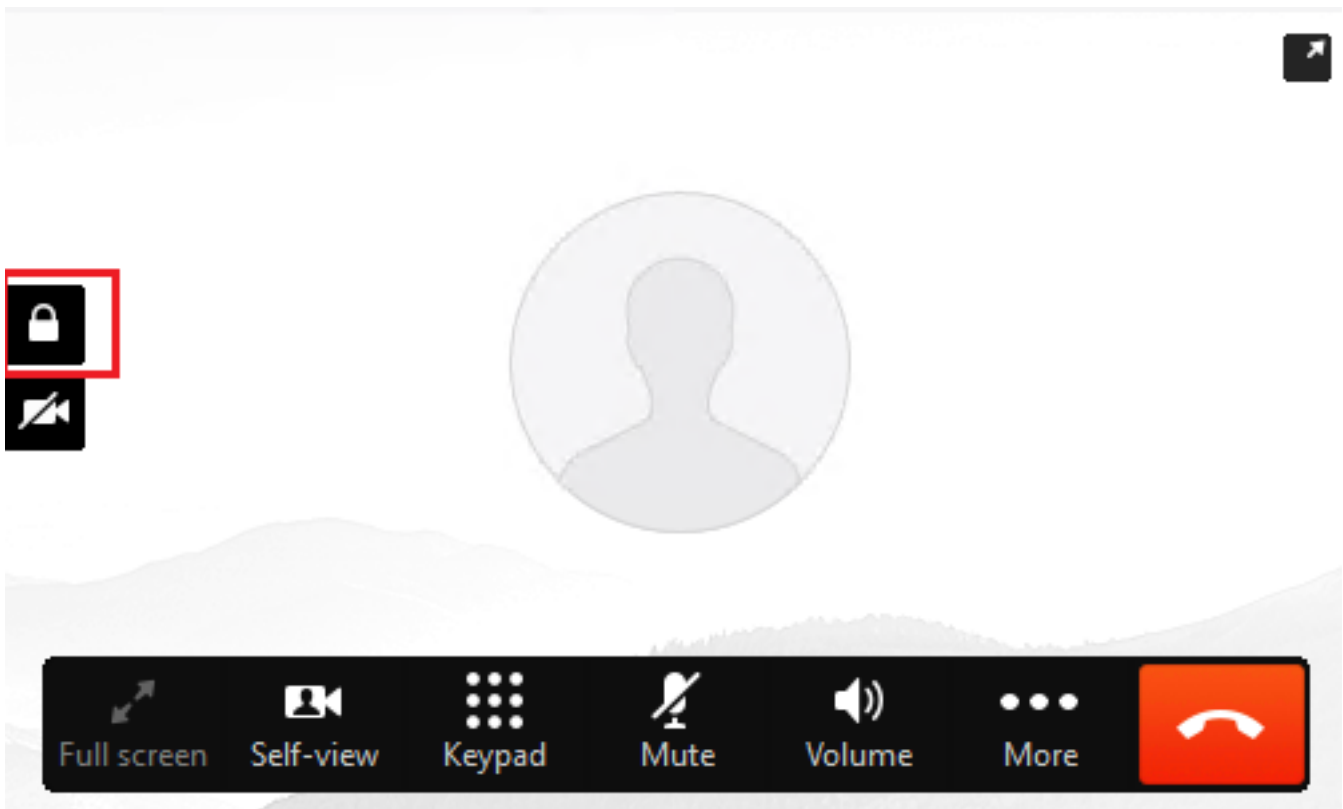
```

Total call-legs: 2
1E85 : 100642 465092660ms.1 (02:55:19.809 UTC Thu Mar 25 2021) +1090 pid:6000100 Answer 3227046971 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.76:5062 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:4865626844c25f248e19a95a65b0ad50
RemoteUUID:00003e7000105000a000005056a06cb8
VRF:
1E85 : 100643 465093670ms.1 (02:55:20.819 UTC Thu Mar 25 2021) +70 pid:6000 Originate 6016 connected
dur 00:04:01 tx:0/0 rx:0/0 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 198.18.133.75:24648 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off Transcoded: No ICE: Off
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a
LostPacketRate:0.00 OutOfOrderRate:0.00
LocalUUID:00003e7000105000a000005056a06cb8
RemoteUUID:4865626844c25f248e19a95a65b0ad50
VRF:

```

**팁:** SRTP가 on CUBE와 상담원 전화 간(198.18.133.75) 대답이 "예"인 경우 CUBE와 Agent 간의 RTP 트래픽이 안전한지 확인합니다.

6. 또한 통화가 연결되면 에이전트 디바이스에 보안 잠금이 표시됩니다. 또한 RTP 트래픽이 안전한지 확인합니다.



SIP 신호가 제대로 보호되는지 확인하려면 Configure Secure SIP Signaling(보안 SIP 신호 [구성](#)) [문서](#)를 참조하십시오.



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.