

CUCM과 CUC 간의 보안 통합 구성 및 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[다이어그램](#)

[구성 - 보안 SIP 트렁크](#)

[CUC 구성](#)

[1. SIP 인증서 추가](#)

[2. 새 전화 시스템 생성 또는 기본 전화 시스템 수정](#)

[3. 새 포트 그룹 추가](#)

[4. 서버 수정](#)

[5. 포트 그룹 재설정](#)

[6. 음성 메일 포트 추가](#)

[7. CUC 루트 인증서 다운로드](#)

[CUCM 구성](#)

[1. CUC로 트렁크에 대한 SIP 트렁크 보안 프로파일 구성](#)

[2. SIP 프로파일 구성](#)

[3. SIP 트렁크 생성](#)

[4. 경로 패턴 생성](#)

[5. 음성 메일 파일럿 생성](#)

[6. 음성 메일 프로필 만들기](#)

[7. DN에 음성 메일 프로필 할당](#)

[8. CUC 루트 인증서를 CallManager-trust로 업로드](#)

[보안 SCCP 포트 구성](#)

[CUC 구성](#)

[1. CUC 루트 인증서를 다운로드합니다.](#)

[2. 전화 시스템 생성/존재하는 전화기 시스템 수정](#)

[3. 새 SCCP 포트 그룹 추가](#)

[4. 서버 수정](#)

[5. 보안 SCCP 포트 추가](#)

[CUCM 구성](#)

[1. 포트 추가](#)

[2. CUC 루트 인증서를 CallManager-trust로 업로드](#)

[3. MWI\(Message Waiting Information\) On/Off Extensions 구성](#)

[4. 음성 메일 파일럿 생성](#)

[5. 음성 메일 프로필 생성](#)

[6. DN에 음성 메일 프로필 할당](#)

[7. 음성 메일 헌트 그룹 만들기](#)

[다음을 확인합니다.](#)

[SCCP 포트 확인](#)

[보안 SIP 트렁크 확인](#)

[보안 RTP 통화 확인](#)

[문제 해결](#)

[1. 일반적인 문제 해결 팁](#)

[2. 수집 추적](#)

[일반적인 문제](#)

[사례 1:보안 연결을 설정할 수 없음\(알 수 없는 CA 경고\)](#)

[사례 2:CUCM TFTP에서 CTL 파일을 다운로드할 수 없음](#)

[사례 3:포트가 등록되지 않음](#)

[결함](#)

소개

이 문서에서는 Cisco CUCM(Unified Communication Manager)과 CUC(Cisco Unity Connection) 서버 간의 보안 연결의 컨피그레이션, 확인 및 트러블슈팅에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 CUCM에 대해 알고 있는 것이 좋습니다.

자세한 내용은 [Cisco Unified Communications Manager 보안 가이드](#)를 참조하십시오.

참고:보안 통합이 올바르게 작동하려면 혼합 모드로 설정해야 합니다.

Unity Connection 11.5(1) SU3 이상에 대해 암호화를 활성화해야 합니다.

CLI 명령 "utils cuc encryption <enable/disable>"

사용되는 구성 요소

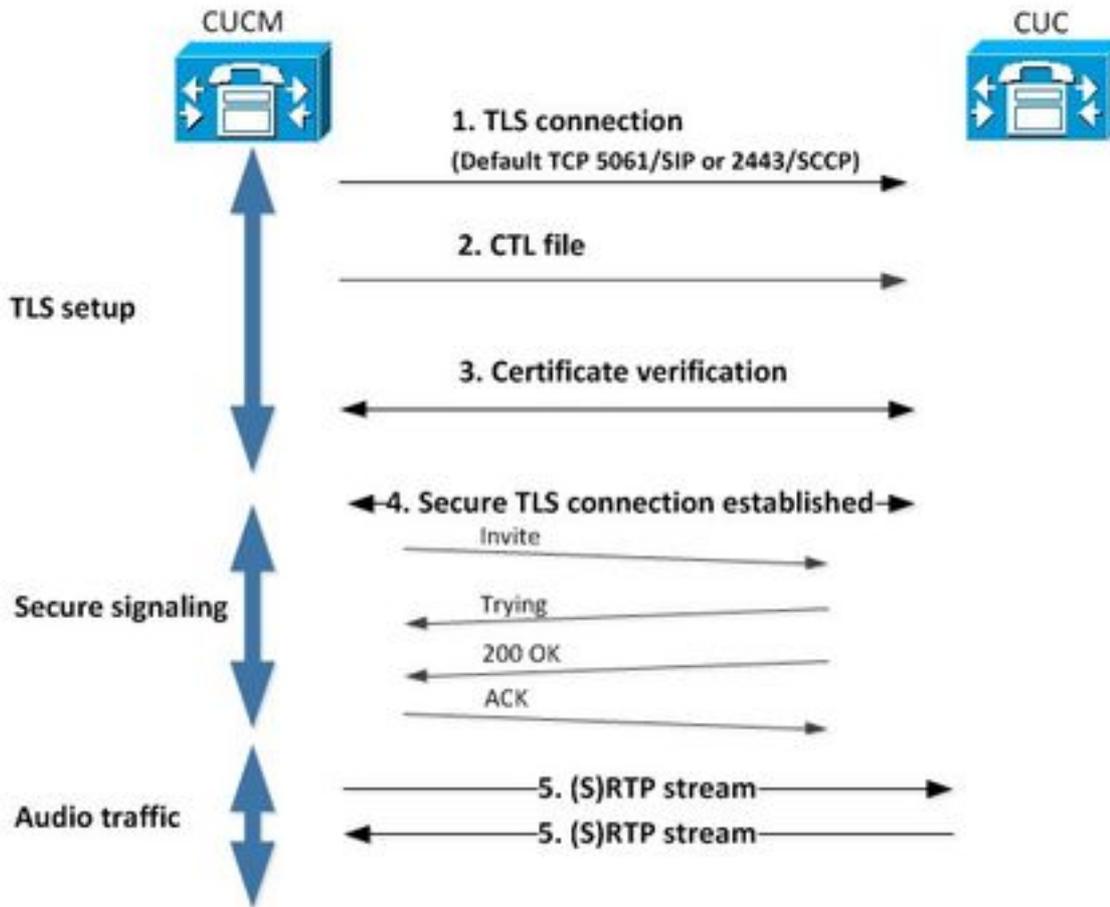
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- CUCM 버전 10.5.2.11900-3.
- CUC 버전 10.5.2.11900-3.

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.

다이아그램

이 다이어그램은 CUCM과 CUC 간의 보안 연결을 설정하는 데 도움이 되는 프로세스에 대해 간략하게 설명합니다.



1. Call Manager는 통합에 사용되는 프로토콜에서 포트 2443 SCCP(Skinny Call Control Protocol) 또는 5061 SIP(Session Initiation Protocol) 기반(SIP)에서 CUC 서버에 대한 TLS(Secure Transport Layer Security) 연결을 설정합니다.

2. CUC 서버는 TFTP 서버(한 번의 프로세스)에서 CTL(Certificate Trust List) 파일을 다운로드하고 CallManager.pem 인증서를 추출하여 저장합니다.

3. CUCM 서버는 이전 단계에서 얻은 CallManager.pem 인증서에 대해 검증된 Callmanager.pem 인증서를 제공합니다. 또한 CUCM 인증서가 CUCM에 저장된 CUC 루트 인증서에 대해 검증되고 있습니다. 루트 인증서는 관리자가 CUCM에 업로드해야 합니다.

4. 인증서 확인이 성공하면 안전한 TLS 연결이 설정됩니다. 이 연결은 암호화된 SCCP 또는 SIP 시그널링을 교환하는 데 사용됩니다.

5. 오디오 트래픽은 실시간 전송 프로토콜(RTP) 또는 SRTP로 교환할 수 있습니다.

참고: TLS 통신을 설정할 때 CUCM 및 CUC는 TLS 상호 인증을 사용합니다. 자세한 내용은 RFC5630을 참조하십시오.

구성 - 보안 SIP 트렁크

CUC 구성

1. SIP 인증서 추가

CUC Administration(CUC 관리) > Telephony Integrations(텔레포니 통합) > Security(보안) > SIP Certificate(SIP 인증서) > Add new(새 추가)로 이동합니다.

- 표시 이름:<의미 있는 이름>
- 주체 이름:<모든 이름(예: SecureConnection)>

참고: 주체 이름은 SIP 트렁크 보안 프로파일의 X.509 주체 이름과 일치해야 합니다(이 문서의 뒷부분에 나오는 CUCM 컨피그레이션의 1단계에서 구성).

참고:인증서가 생성되고 CUC 루트 인증서에 의해 서명됩니다.

2. 새 전화 시스템 생성 또는 기본 전화 시스템 수정

Telephony Integration(텔레포니 통합) > Phone System(전화기 시스템)으로 이동합니다.이미 있는 전화 시스템을 사용하거나 새 전화 시스템을 만들 수 있습니다.

3. 새 포트 그룹 추가

Phone System Basics(전화 시스템 기본 사항) 페이지의 Related Links(관련 링크) 드롭다운 상자에서 Add Port Group(포트 그룹 추가)을 선택하고 Go(이동)를 선택합니다.구성 창에 다음 정보를 입력합니다.

- 전화 시스템:
- 생성 원본: 포트 그룹 유형 SIP
- SIP 보안 프로파일: 5061/TLS

- SIP 인증서:
- 보안 모드: 암호화
- 보안 RTP: 선택
- IPv4 주소 또는 호스트 이름:

저장을 누릅니다.

New Port Group

[Port Group](#) [Reset](#) [Help](#)

New Port Group

Phone System Secure SIP integration ▼

Create From Port Group Type SIP ▼

Port Group ▼

Port Group Description

Display Name*

Authenticate with SIP Server

Authentication Username

Authentication Password

Contact Line Name

SIP Security Profile 5061/TLS ▼

SIP Certificate Secure SIP integration with CUCMv10.5.2 ▼

Security Mode Encrypted ▼

Secure RTP

Primary Server Settings

IPv4 Address or Host Name

IPv6 Address or Host Name

Port

4. 서버 수정

Edit(편집) > Servers(서버)로 이동하고 이 이미지에 표시된 대로 CUCM 클러스터에서 TFTP 서버를 추가합니다.

SIP Servers

<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input type="checkbox"/>	0	10.48.47.110 <input type="button" value="⌵"/>

TFTP Servers

<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input type="checkbox"/>	0	10.48.47.110 <input type="text"/>

참고:올바른 TFTP 주소를 제공해야 합니다.CUC 서버가 이 TFTP에서 CTL 파일을 다운로드 한 경우, 설명된 대로

5. 포트 그룹 재설정

이 이미지에 표시된 대로 **Port Group Basics**(포트 그룹 기본 사항)로 돌아가 시스템에서 프롬프트하는 대로 포트 그룹을 재설정합니다.

Port Group Basics (Secure SIP integration-1)

Port Group Edit Refresh Help

Status

The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

One or more port groups need to be reset.

Port Group

Display Name*

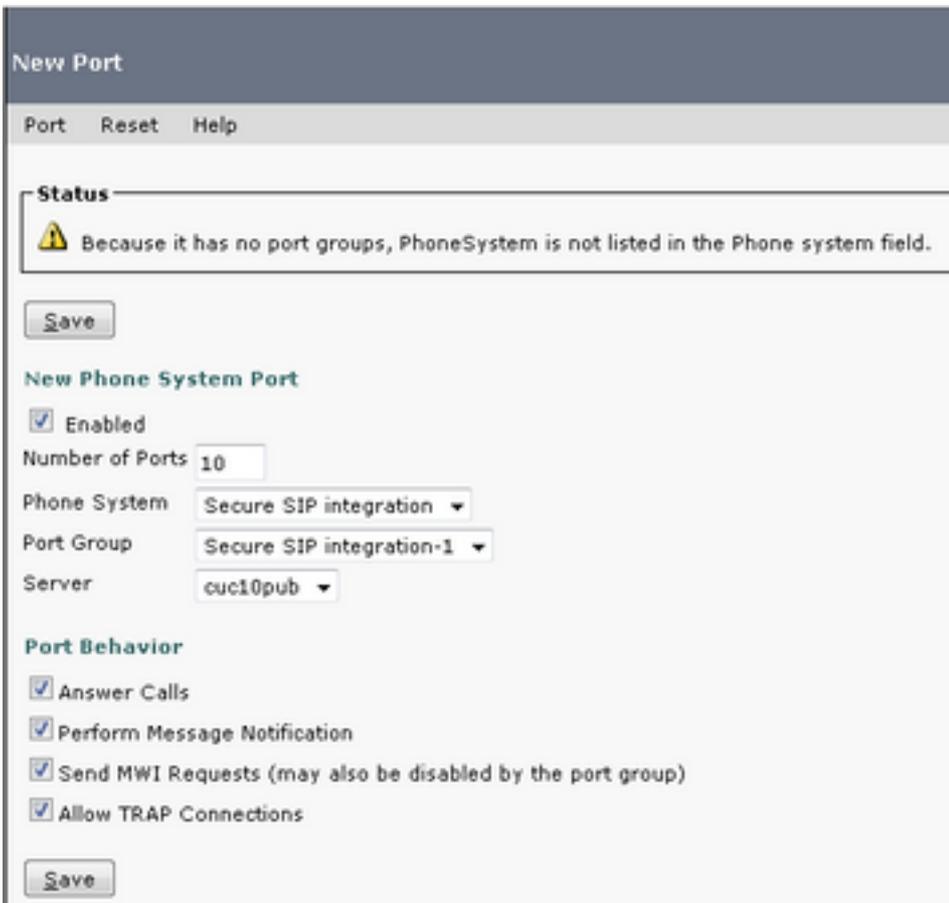
Integration Method

Reset Status

6. 음성 메일 포트 추가

[포트 그룹 기본 사항] 페이지의 [관련 링크] 드롭다운 상자에서 **포트 추가**를 선택하고 **실행**을 선택합니다. 구성 창에 다음 정보를 입력합니다.

- 사용:선택
- 포트 수:
- 전화 시스템:
- 포트 그룹:
- 서버:
- 포트 동작:



7. CUC 루트 인증서 다운로드

Telephony Integrations(텔레포니 통합) > Security(보안) > Root Certificate(루트 인증서)로 이동하고 URL을 마우스 오른쪽 버튼으로 클릭하여 인증서를 <filename>.0(파일 확장자는 .htm이 아니라 .0) 파일로 저장하고 이 이미지에 표시된 대로 저장을 누릅니다.



CUCM 구성

1. CUC로 트렁크에 대한 SIP 트렁크 보안 프로파일 구성

CUCM Administration(CUCM 관리) > System(시스템) > Security(보안) > SIP Trunk Security Profile(SIP 트렁크 보안 프로파일) > Add new(새 추가)로 이동합니다.

다음 필드가 올바르게 입력되었는지 확인합니다.

- 장치 보안 모드: 암호화
- X.509 제목 이름: 보안 연결>
- 대화 상자 외부 참조 수락: 체크
- 요청되지 않은 알림 수락: 체크
- 헤더 바꾸기 수락: 체크

참고:X.509 주체 이름은 Cisco Unity Connection 서버의 SIP 인증서(CUC 컨피그레이션의 1단계에서 구성)에 있는 Subject Name(주체 이름) 필드와 일치해야 합니다.

SIP Trunk Security Profile Information

Name*	Secure_sip_trunk_profile_for_CUC
Description	
Device Security Mode	Encrypted
Incoming Transport Type*	TLS
Outgoing Transport Type	TLS
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	SecureConnection
Incoming Port*	5061
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input checked="" 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

2. SIP 프로파일 구성

특정 설정을 적용해야 하는 경우 **Device > Device Settings > SIP Profile**으로 이동합니다. 그렇지 않으면 표준 SIP 프로필을 사용할 수 있습니다.

3. SIP 트렁크 생성

Device(디바이스) > Trunk(트렁크) > Add new(새로 추가)로 이동합니다. 이 이미지에 표시된 대로 Unity Connection과의 보안 통합에 사용할 SIP 트렁크를 생성합니다.

Trunk Information	
Trunk Type*	SIP Trunk
Device Protocol*	SIP
Trunk Service Type*	None(Default)

트렁크 컨피그레이션의 Device Information(디바이스 정보) 섹션에서 다음 정보를 입력합니다.

- 장치 이름:
- 장치 풀:
- SRTP 허용: 선택

참고: CallManager 그룹(장치 풀 컨피그레이션)에 CUC(포트 그룹 > 편집 > 서버)에 구성된 모든 서버가 포함되어 있는지 확인합니다.

Trunk Configuration	
Save	
Status Status: Ready	
Device Information	
Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	SecureSIPtoCUC
Description	Trunk for secure integration with CUC
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	< None >
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	None
Packet Capture Duration	0
<input type="checkbox"/> Media Termination Point Required	
<input checked="" type="checkbox"/> Retry Video Call as Audio	
<input type="checkbox"/> Path Replacement Support	
<input type="checkbox"/> Transmit UTF-8 for Calling Party Name	
<input type="checkbox"/> Transmit UTF-8 Names in QSIG APDU	
<input type="checkbox"/> Unattended Port	
<input checked="" type="checkbox"/> 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
<input type="checkbox"/> PSTN Access	
<input type="checkbox"/> Run On All Active Unified CM Nodes	

트렁크 컨피그레이션의 Inbound Calls 섹션에 다음 정보를 입력합니다.

- 발신 검색 공간:
- 전환 헤더 전달 리디렉션 - 인바운드: 선택

Inbound Calls

Significant Digits* All

Connected Line ID Presentation* Default

Connected Name Presentation* Default

Calling Search Space AllPhones

AAR Calling Search Space < None >

Prefix DN

Redirecting Diversion Header Delivery - Inbound

아웃바운드에서 트렁크 컨피그레이션의 통화 섹션에서 다음 정보를 입력합니다.

- 전환 헤더 전달 리디렉션 - 아웃바운드:체크

Outbound Calls

Called Party Transformation CSS < None >

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS < None >

Use Device Pool Calling Party Transformation CSS

Calling Party Selection* Originator

Calling Line ID Presentation* Default

Calling Name Presentation* Default

Calling and Connected Party Info Format* Deliver DN only in connected party

Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS < None >

Use Device Pool Redirecting Party Transformation CSS

트렁크 컨피그레이션의 SIP Information(SIP 정보) 섹션에 다음 정보를 입력합니다.

- 대상 주소:
- SIP 트렁크 보안 프로파일:
- 발신 검색 공간 재라우팅:
- 통화 중 검색 공간 참조:
- SIP 프로필:

SIP Information

Destination

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	10.48.47.124		5061

MTP Preferred Originating Codec* 711ulaw

BLF Presence Group* Standard Presence group

SIP Trunk Security Profile* Secure_sip_trunk_profile_for_CUC

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile* Standard SIP Profile [View Details](#)

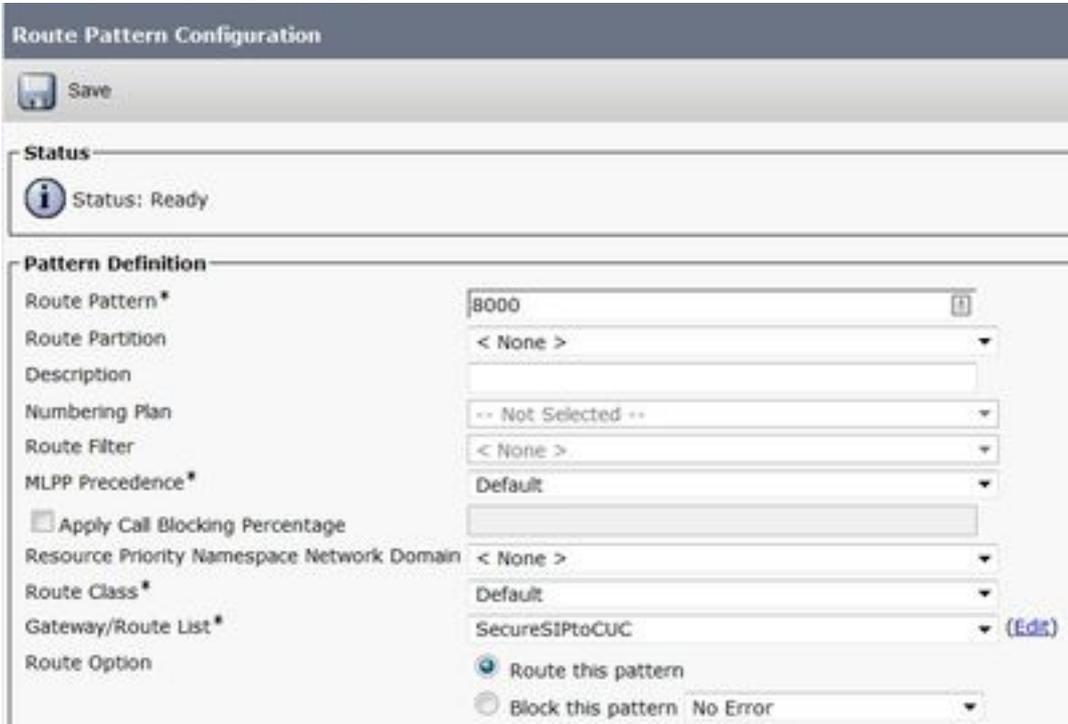
DTMF Signaling Method* No Preference

요구 사항에 따라 다른 설정을 조정합니다.

4. 경로 패턴 생성

구성된 트렁크를 가리키는 경로 패턴을 생성합니다(Call Routing(통화 라우팅) > Route/Hunt(경로 /헌트) > Route Pattern(경로 패턴)). 경로 패턴 번호로 입력한 내선 번호를 음성 메일 파일럿으로 사용할 수 있습니다.다음 정보를 입력합니다.

- 경로 패턴:
- 게이트웨이/경로 목록:



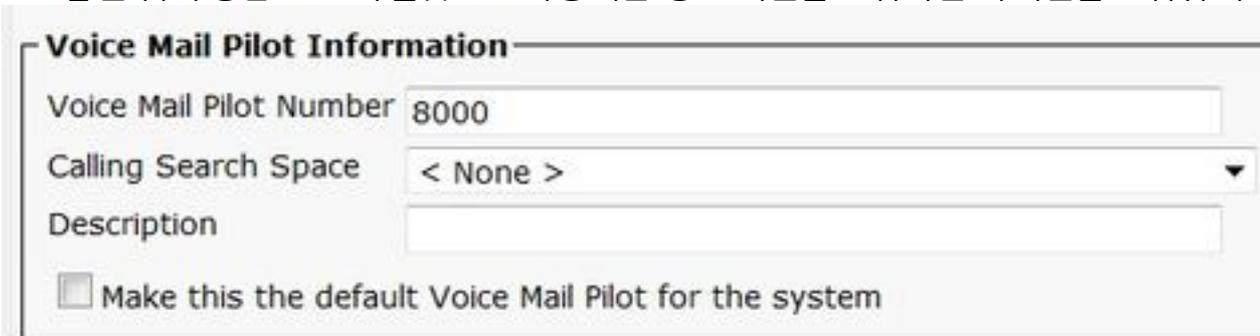
The screenshot shows the 'Route Pattern Configuration' window. At the top, there is a 'Save' button. Below it, the 'Status' section shows 'Status: Ready'. The main 'Pattern Definition' section contains the following fields:

Route Pattern *	8000
Route Partition	< None >
Description	
Numbering Plan	-- Not Selected --
Route Filter	< None >
MLPP Precedence *	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class *	Default
Gateway/Route List *	SecureSIPtoCUC (Eds)
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern No Error

5. 음성 메일 파일럿 생성

통합을 위한 음성 메일 파일럿(고급 기능 > 음성 메일 > 음성 메일 파일럿)을 생성합니다. 다음 값을 입력합니다.

- 음성 메일 파일럿 번호:
- 발신 검색 공간: 파일럿으로 사용되는 경로 패턴을 포함하는 파티션을 포함합니다.>



The screenshot shows the 'Voice Mail Pilot Information' window. It contains the following fields:

Voice Mail Pilot Number	8000
Calling Search Space	< None >
Description	
<input type="checkbox"/> Make this the default Voice Mail Pilot for the system	

6. 음성 메일 프로필 만들기

모든 설정을 함께 연결하려면 음성 메일 프로필을 만듭니다(Advanced Features > Voice Mail > Voice Mail Profile). 다음 정보를 입력합니다.

- 음성 메일 파일럿:
- 음성 사서함 마스크:

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

Make this the default Voice Mail Profile for the System

7. DN에 음성 메일 프로필 할당

보안 통합을 사용할 DN에 음성 메일 프로필을 할당합니다. DN 설정을 변경한 후 'Apply Config' 버튼을 클릭하는 것을 잊지 마십시오.

다음으로 이동: **통화 라우팅 > 디렉터리 번호**를 변경하고 다음을 변경합니다.

- 음성 메일 프로필: Secure_SIP_통합

Directory Number Configuration

Save Delete Reset Apply Config Add New

Directory Number Settings

Voice Mail Profile Secure_SIP_Integration (Choose <None> to use system default)

Calling Search Space < None >

BLF Presence Group* Standard Presence group

User Hold MOH Audio Source < None >

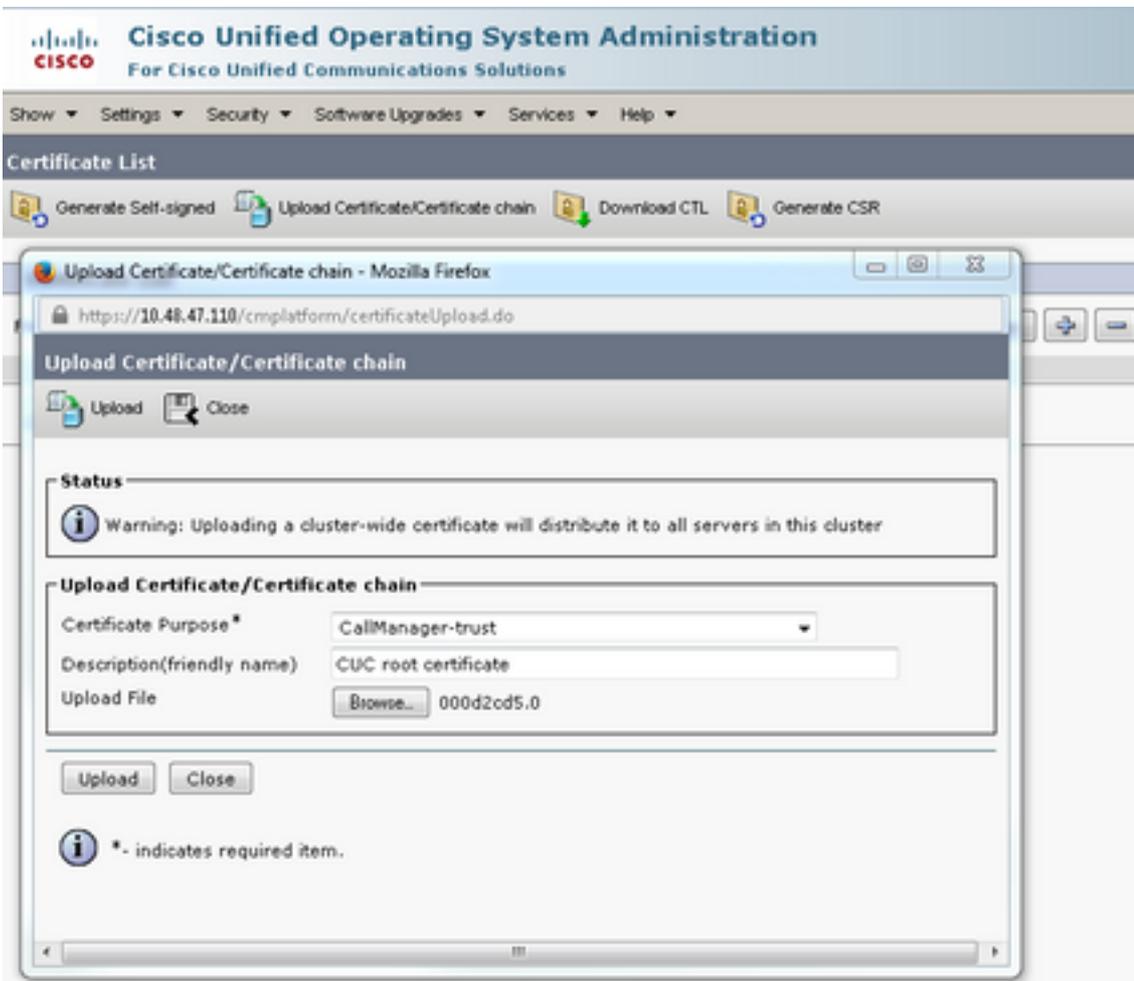
Network Hold MOH Audio Source < None >

Auto Answer* Auto Answer Off

Reject Anonymous Calls

8. CUC 루트 인증서를 CallManager-trust로 업로드

OS Administration(OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Upload Certificate/Certificate Chain(인증서/인증서 체인 업로드)으로 이동하고 CUC 루트 인증서를 CUC 서버와 통신하도록 구성된 모든 노드에서 CallManager-trust로 업로드합니다.



참고: 인증서를 적용하려면 인증서가 업로드된 후 Cisco CallManager 서비스를 다시 시작해야 합니다.

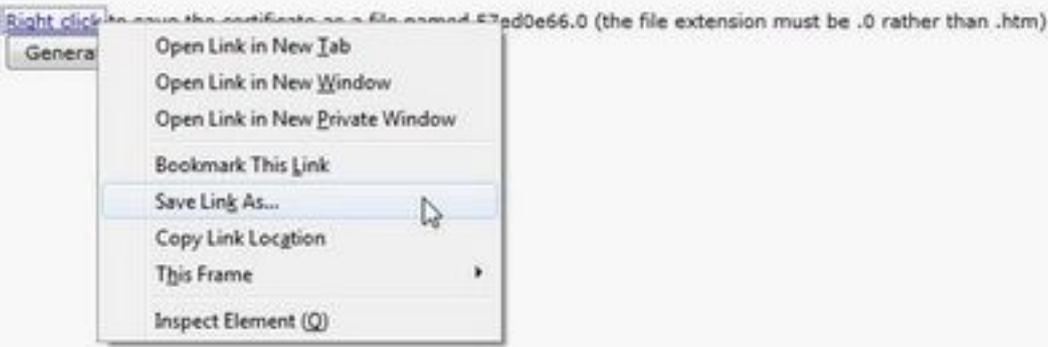
보안 SCCP 포트 구성

CUC 구성

1. CUC 루트 인증서 다운로드

CUC Administration(CUC 관리) > Telephony Integration(텔레포니 통합) > Security(보안) > Root Certificate(루트 인증서)로 이동합니다. 인증서를 <filename>.0(파일 확장명은 .htm이 아닌 .0) 파일로 저장하려면 URL을 마우스 오른쪽 버튼으로 클릭하고 저장:

Root Certificate for Cisco Unified Communications Manager Authentication and Encryption	
Subject	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Issuer	CN=CiscoUnity-5dad32eb-cafa-4559-978f-56f2c6850d41
Valid From	Tue Mar 31 08:59:34 CEST 2015
Valid Until	Fri Apr 01 08:59:34 CEST 2022
Version	2
File Name	57ed0e66.0
Serial Number	f6b8fb3369144dd39f18e064893aec42
Certificate Text	<pre>-----BEGIN CERTIFICATE----- MIICPDCCAaWgAwIBAgIRAPa4+zNpFE3TnxjgZ1k67E1wDQYJKoZIhvcNAQEFBQAw OjE4MDYGA1UEAwwvQ2lyZ29Vbml0eS01ZGFkMzJlYy1jYWZlLnQ1NTktOTc0Zi01 NmYyYzY4NTBkNDEwHhcNMjUwMzY1OTM0WWhcNMjUwMzY1OTM0WjA6MTgw NgYDVQQLDDBkaXNjb1VuaXR5LTUyYzY1YzY1YzY1YzY1YzY1YzY1YzY1YzY1 Njg1MGQ0MTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAoBOBg/qh8cWQx457 Q47eGUWcR2jeyE726RTO40GkdhDYI4Km6ouSeMiGbs757WpvtspKp+zeSDjVm2j4 B1lxG9wM3XgPPwM+3QIMh0NQPLARuJdm9g2/5uiHB6/1k82Po0Wrv2r6Anoragrv Md3ordaCB3mG1u2g0GqXj9GChf0CAwEAaANCMEEAwEgYDVR0TAQH/BAGwBgEB/wIB ADAdBgNVHQ4EFgQU438N5JYGHhgp7qm2dUmu+HGkM8wCwYDVR0PBAQDAgKsMA0G CSqGSIb3DQEBBQUAA4GBAGPhrFt6GH2a0iXV8bnKvC12f5ty1eTeMD6ZzD62P4C6 RtGM88WqGU1IAZw1www0nxdetKzZvJX2z2Ksu2ptVUnFPMzSc+xl0jv7vmJq52px TcD/Ti0efckXlc+vACWlu4wlv20SHxsoto9CiiXqsKQ7e/zyYHu152zTOQeYvAES -----END CERTIFICATE-----</pre>
Private Key	Hk2Pzp3YnX3/9ghz1r8v1VgMpSLr8HZ8XW/VXIL342IudK3G1GwnZ1IMvhzta/zEseh2ELON



2. 전화 시스템 생성/존재하는 전화기 시스템 수정

Telephony Integration > Phone system으로 이동합니다. 이미 있는 전화 시스템을 사용하거나 새 전화 시스템을 만들 수 있습니다.

Phone System Basics (PhoneSystem)

Phone System Edit Refresh Help

Save Delete Previous Next

Status

The phone system cannot take calls until a port group is set. Use the Related Links to add a port group.

Phone System

Phone System Name*

Default TRAP Phone System

3. 새 SCCP 포트 그룹 추가

Phone System Basics(전화 시스템 기본 사항) 페이지의 Related Links(관련 링크) 드롭다운 상자에서 Add Port Group(포트 그룹 추가)을 선택하고 Go(이동)를 선택합니다. 구성 창에 다음 정보를 입력합니다.

- 전화 시스템:
- 포트 그룹 유형: SCCP
- 장치 이름 접두사*: CiscoUM1-VI
- MWI On 확장:
- MWI 끄기 확장:

참고:이 컨피그레이션은 CUCM의 컨피그레이션과 일치해야 합니다.

Status

 The phone system cannot take calls if it has no ports. Use the Related Links to add ports.

 Created Port Group(s)

Port Group

Display Name*

Integration Method

Device Name Prefix*

Reset Status

Message Waiting Indicator Settings

Enable Message Waiting Indicators

MWI On Extension

MWI Off Extension

Delay between Requests milliseconds

Maximum Concurrent Requests

Retries After Successful Attempt

Retry Interval After Successful Attempt milliseconds

Fields marked with an asterisk (*) are required.

4. 서버 수정

Edit(편집) > Servers(서버)로 이동하고 CUCM 클러스터에서 TFTP 서버를 추가합니다.

SIP Servers

<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input type="checkbox"/>	0	10.48.47.110 <input type="button" value="📄"/>

TFTP Servers

<input type="checkbox"/>	Order	IPv4 Address or Host Name
<input type="checkbox"/>	0	10.48.47.110 <input type="text"/>

참고:올바른 TFTP 주소를 제공해야 합니다.CUC 서버가 이 TFTP에서 CTL 파일을 다운로드 한 경우, 설명된 대로

5. 보안 SCCP 포트 추가

[포트 그룹 기본 사항] 페이지의 [관련 링크] 드롭다운 상자에서 포트 추가를 선택하고 실행을 선택합니다. 구성 창에 다음 정보를 입력합니다.

- 사용:체크
- 포트 수:
- 전화 시스템:
- 포트 그룹:
- 서버:
- 포트 동작:
- 보안 모드: **암호화**

Status

 Because it has no port groups, PhoneSystem is not listed in the Phone system field.

New Phone System Port

Enabled

Number of Ports

Phone System

Port Group

Server

Port Behavior

Answer Calls

Perform Message Notification

Send MWI Requests (may also be disabled by the port group)

Allow TRAP Connections

Security Mode

CUCM 구성

1. 포트 추가

다음으로 이동 CUCM Administration > Advanced features > Voice Mail Port Configuration > Add New를 선택합니다.

SCCP 음성 메일 포트를 평소와 같이 구성합니다.유일한 차이점은 Encrypted Voice Mail Port(암호화된 음성 메일 포트) 옵션을 선택해야 하는 포트 컨피그레이션 아래의 Device Security Mode(디바이스 보안 모드)입니다.

Voice Mail Port Configuration

Save ~~Delete~~ Copy Reset Apply Config Add New

Status

Status: Ready

Device Information

Registration: Registered with Cisco Unified Communications Manager 10.48.46.182
 IPv4 Address: 10.48.46.184
 Device is trusted
 Port Name* CiscoUM1-VI1
 Description VM-sccp-secure-ports
 Device Pool* Default
 Common Device Configuration < None >
 Calling Search Space < None >
 AAR Calling Search Space < None >
 Location* Hub_None
 Device Security Mode* Encrypted Voice Mail Port
 Use Trusted Relay Point* Default
 Geolocation < None >

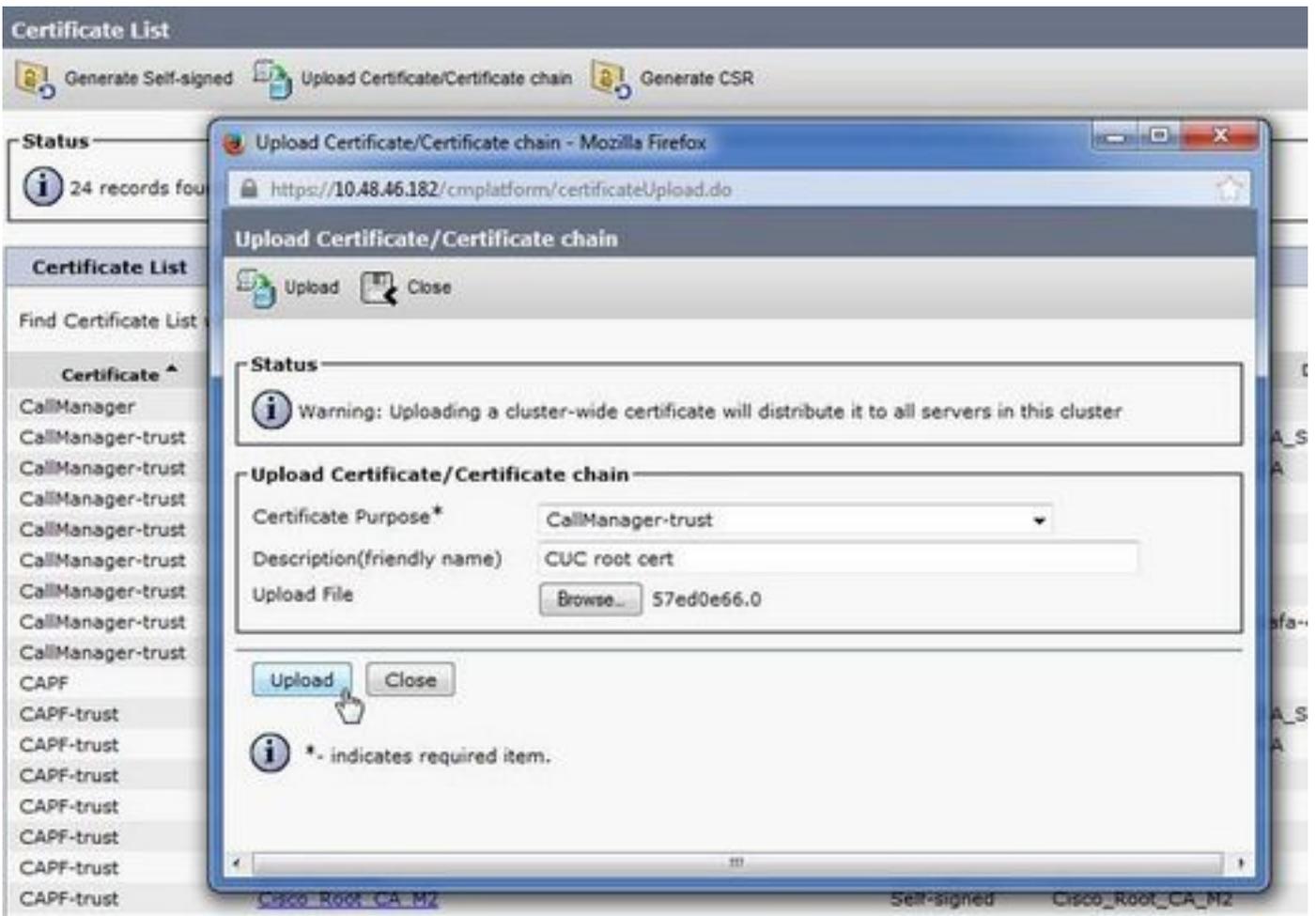
Directory Number Information

Directory Number* 999001
 Partition < None >
 Calling Search Space < None >
 AAR Group < None >
 Internal Caller ID Display VoiceMail
 Internal Caller ID Display (ASCII format) VoiceMail
 External Number Mask

Save Delete Copy Reset Apply Config Add New

2. CUC 루트 인증서를 CallManager-trust로 업로드

OS Administration(OS 관리) > Security(보안) > Certificate Management(인증서 관리) > Upload Certificate/Certificate Chain(인증서/인증서 체인 업로드)으로 이동하고 CUC 루트 인증서를 CUC 서버와 통신하도록 구성된 모든 노드에서 CallManager-trust로 업로드합니다.



참고: 인증서를 적용하려면 인증서가 업로드된 후 Cisco CallManager 서비스를 다시 시작해야 합니다.

3 . MWI(Message Waiting Information) On/Off Extensions 구성

CUCM Administration(CUCM 관리) > Advanced Features(고급 기능) > Voice Mail Port Configuration(음성 메일 포트 컨피그레이션)으로 이동하고 MWI On/Off Extensions(MWI 켜기/끄기 확장)를 구성합니다.MWI 번호는 CUC 컨피그레이션과 일치해야 합니다.

Message Waiting Information

Message Waiting Number*

Partition

Description

Message Waiting Indicator* On Off

Calling Search Space

Message Waiting Information

Message Waiting Number* 999990

Partition < None >

Description MWI off

Message Waiting Indicator* On Off

Calling Search Space < None >

Save

4. 음성 메일 파일럿 생성

통합을 위한 음성 메일 파일럿(고급 기능 > 음성 메일 > 음성 메일 파일럿)을 생성합니다. 다음 값을 입력합니다.

- 음성 메일 파일럿 번호:
- 발신 검색 공간: 파일럿으로 사용되는 경로 패턴을 포함하는 파티션을 포함합니다.>

Voice Mail Pilot Information

Voice Mail Pilot Number 8000

Calling Search Space < None >

Description

Make this the default Voice Mail Pilot for the system

5. 음성 메일 프로필 생성

모든 설정을 함께 연결하려면 음성 메일 프로필을 만듭니다(Advanced Features > Voice Mail > Voice Mail Profile). 다음 정보를 입력합니다.

- 음성 메일 파일럿:
- 음성 사서함 마스크:

Voice Mail Profile Information

Voice Mail Profile Name* Voicemail-profile-8000

Description Secure Voicemail

Voice Mail Pilot** 8000/< None >

Voice Mail Box Mask

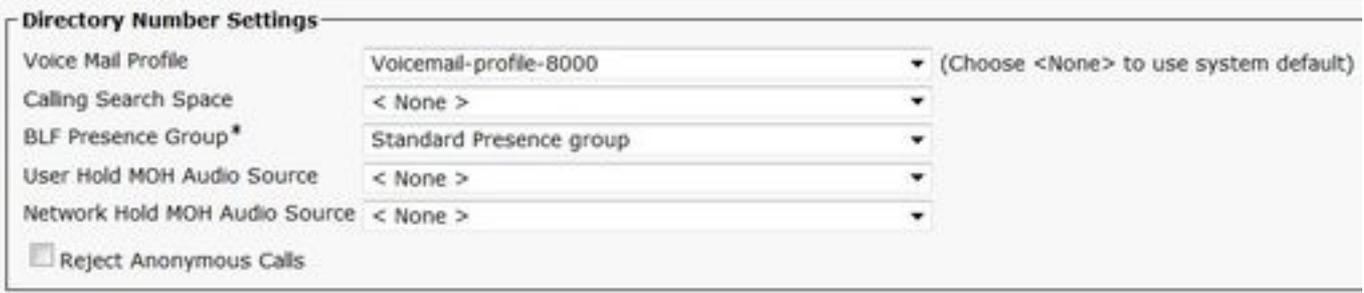
Make this the default Voice Mail Profile for the System

6. DN에 음성 메일 프로필 할당

보안 통합을 사용할 DN에 음성 메일 프로필을 할당합니다. DN 설정이 변경된 후 Apply Config 버튼을 클릭합니다.

Call Routing(통화 라우팅) > Directory number(디렉토리 번호)로 이동하고 다음으로 변경합니다.

- 음성 메일 프로필: 음성 메일 프로필-8000



Directory Number Settings

Voice Mail Profile	Voicemail-profile-8000	(Choose <None> to use system default)
Calling Search Space	< None >	
BLF Presence Group*	Standard Presence group	
User Hold MOH Audio Source	< None >	
Network Hold MOH Audio Source	< None >	

Reject Anonymous Calls

7. 음성 메일 헌트 그룹 만들기

a) 새 라인 그룹을 추가합니다(Call Routing(통화 라우팅) > Route/Hunt(경로/헌트) > Line group(라인 그룹)).



- Line Group Information

Line Group Name*	voicemail-ig
RNA Reversion Timeout*	10
Distribution Algorithm*	Longest Idle Time

b) 새 음성 메일 헌트 목록(Call Routing(통화 라우팅) > Route/Hunt(경로/헌트) > Hunt List(헌트 목록)) 추가



Hunt List Information

Device is trusted

Name*	voicemail-hi
Description	
Cisco Unified Communications Manager Group*	Default

Enable this Hunt List (change effective on Save; no reset required)

For Voice Mail Usage

c) 새 헌트 파일럿 추가(Call Routing(통화 라우팅) > Route/Hunt(경로/헌트) > Hunt Pilot(헌트 파일럿))

Pattern Definition

Hunt Pilot*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence*

Hunt List* (Edit)

Call Pickup Group

Alerting Name

ASCII Alerting Name

Route Option Route this pattern
 Block this pattern

다음을 확인합니다.

SCCP 포트 확인

CUCM Administration(CUCM 관리) > Advance Features(고급 기능) > Voice Mail(음성 메일) > Voice Mail Ports(음성 메일 포트)로 이동하고 포트 등록을 확인합니다.

Find and List Voice Mail Ports

Find Voice Mail Port where: Device Name begins with Find Clear Filter

Status: 0 records found

Voice Mail Port (1 - 8 of 8)

Device Name	Description	Device Pool	Device Security Mode	Calling Search Space	Extension	Partition	Status	IP Address	Clear
CUCM575-101	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999001		Registered with 10.48.46.182	10.48.46.184	
CUCM575-102	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999002		Registered with 10.48.46.182	10.48.46.184	
CUCM575-103	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999003		Registered with 10.48.46.182	10.48.46.184	
CUCM575-104	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999004		Registered with 10.48.46.182	10.48.46.184	
CUCM575-105	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999005		Registered with 10.48.46.182	10.48.46.184	
CUCM575-106	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999006		Registered with 10.48.46.182	10.48.46.184	
CUCM575-107	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999007		Registered with 10.48.46.182	10.48.46.184	
CUCM575-108	VN-ecp-secure-ports	Default	Encrypted Voice Mail Port		999008		Registered with 10.48.46.182	10.48.46.184	

전화기의 음성 메일 단추를 눌러 음성 메일을 호출합니다.사용자의 내선 번호가 Unity Connection 시스템에 구성되지 않은 경우 시작 인사말을 들어야 합니다.

보안 SIP 트렁크 확인

전화기의 음성 메일 단추를 눌러 음성 메일을 호출합니다.사용자의 내선 번호가 Unity Connection 시스템에 구성되지 않은 경우 시작 인사말을 들어야 합니다.

또는 SIP OPTIONS keepalive를 활성화하여 SIP 트렁크 상태를 모니터링할 수 있습니다.이 옵션은 SIP 트렁크에 할당된 SIP 프로파일에서 활성화할 수 있습니다.이 기능이 활성화되면 이 이미지에 표시된 대로 Device(디바이스) > Trunk(트렁크)를 통해 Sip 트렁크 상태를 모니터링할 수 있습니다.

Trunks (1 - 1 of 1)

Find Trunks where: Device Name begins with Find Clear Filter

Name	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Status	SIP Trunk Duration
SecureSIPtoCUC			Default					SIP Trunk	No Service	Time not in Full Service: 0 day 0 hour 0 minute

보안 RTP 통화 확인

Unity Connection 통화에 자물쇠 아이콘이 있는지 확인합니다. 이는 RTP 스트림이 이 이미지에 표시된 대로 암호화됨을 의미합니다(장치 보안 프로파일이 작동하려면 안전해야 함).



문제 해결

1. 일반적인 문제 해결 팁

보안 통합 문제를 해결하려면 다음 단계를 수행하십시오.

- 구성 확인.
- 모든 관련 서비스가 실행 중인지 확인합니다.(CUCM - CallManager, TFTP, CUC - 대화 관리자)
- 서버 간의 보안 통신에 필요한 포트가 네트워크에서 열려 있는지 확인합니다(SCCP 통합에는 TCP 포트 2443, SIP 통합에는 TCP 5061).
- 이 모든 것이 올바른 경우 추적 수집을 계속 진행합니다.

2. 수집 추적

이러한 추적을 수집하여 보안 통합 문제를 해결합니다.

- CUCM 및 CUC에서 패킷 캡처
- CallManager 추적
- Cisco Conversation Manager 추적

다음에 대한 자세한 내용은 다음 리소스를 참조하십시오.

CUCM에서 패킷 캡처를 수행하는 방법:

<http://www.cisco.com/c/en/us/support/docs/voice-unified-communications/unified-communications-manager-version-50/112040-packet-capture-cucm-00.html>

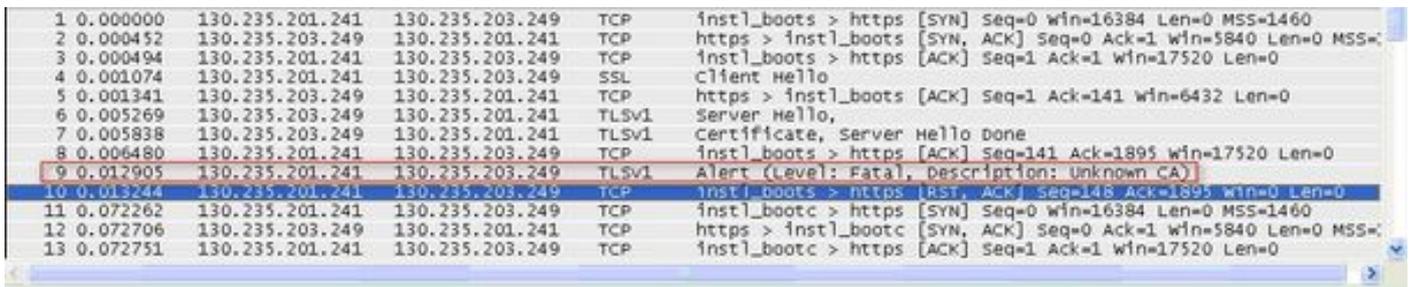
CUC 서버에서 추적을 활성화하는 방법:

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/troubleshooting/guide/10xcuctsgx/10xcuctsg010.html

일반적인 문제

사례 1:보안 연결을 설정할 수 없음(알 수 없는 CA 경고)

서버 중 하나에서 패킷 캡처가 수집되면 TLS 세션이 설정됩니다.



클라이언트가 서버에서 보낸 인증서를 확인할 수 없기 때문에 클라이언트가 서버에 대해 알 수 없는 CA라는 치명적인 오류와 함께 경고를 발행했습니다.

두 가지 가능성이 있습니다.

1) CUCM에서 경고 전송 알 수 없는 CA

- 현재 CUC 루트 인증서가 CUC 서버와 통신하는 서버에 업로드되었는지 확인합니다.
- 해당 서버에서 CallManager 서비스가 다시 시작되는지 확인합니다.

2) CUC에서 Unknown CA(알 수 없는 CA)라는 경고 전송

- TFTP IP 주소가 CUC 서버의 **Port Group(포트 그룹) > Edit(편집) > Servers(서버)** 컨피그레이션에 올바르게 입력되었는지 확인합니다.
- 연결 서버에서 CUCM TFTP 서버에 연결할 수 있는지 확인합니다.
- CUCM TFTP의 CTL 파일이 최신인지 확인합니다(OS Admin 페이지에 표시된 것처럼 "show ctf"의 출력을 인증서와 비교). 그렇지 않으면 CTLClient를 다시 실행합니다.
- CUCM 서버를 재부팅하거나 포트 그룹을 삭제하고 다시 생성하여 CUCM TFTP에서 CTL 파일을 다시 다운로드합니다.

사례 2:CUCM TFTP에서 CTL 파일을 다운로드할 수 없음

이 오류는 대화 관리자 추적에 표시됩니다.

```
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server certificates.
MiuGeneral,25,Error executing tftp command 'tftp://10.48.47.189:69/CTLFile.tlv' res=68 (file not found on server)
MiuGeneral,25,FAILED Port group 'PhoneSystem-1' attempt set InService(true), error retrieving server certificates.
Arbiter,-1,Created port PhoneSystem-1-001 objectId='7c2e86b8-2d86-4403-840e-16397b3c626b' as ID=1
```

```
MiuGeneral,25,Port group object 'b1c966e5-27fb-4eba-a362-56a5fe9c2be7' exists
MiuGeneral,25,FAILED SetInService=true parent port group is out of service:
```

해결책:

1. TFTP 서버가 Port group(포트 그룹) > Edit(편집) > Servers(서버) 컨피그레이션에서 올바른지 다시 확인합니다.
2. CUCM 클러스터가 보안 모드인지 확인합니다.
3. CTL 파일이 CUCM TFTP에 있는지 확인합니다.

사례 3:포트가 등록되지 않음

이 오류는 대화 관리자 추적에 표시됩니다.

```
MiuSkinny,23,Failed to retrieve Certificate for CCM Server <CUCM IP Address>
MiuSkinny,23,Failed to extract any CCM Certificates - Registration cannot proceed. Starting
retry timer -> 5000 msec
MiuGeneral,24,Found local CTL file [/tmp/aaaaaaaa-xxxx-xxxx-xxxx-xxxxxxxxxxxxx.tlv]
MiuGeneral,25,CCMCertificateCache::RetrieveServerCertificates() failed to find CCM Server '<CUCM
IP Address>' in CTL File
```

해결책:

1. CUCM 및 CUC의 재생성 결과 CTL 파일의 md5 체크섬이 일치하지 않기 때문일 가능성이 가장 높습니다.

인증서.CTL 파일을 새로 고치려면 CUC 서버를 다시 시작합니다.

Cisco 내부 정보

또는 다음과 같이 루트에서 CTL 파일을 제거할 수 있습니다.

/tmp/ 폴더에서 CTL 파일을 삭제하고 포트 그룹을 재설정합니다.파일에서 md5 체크섬을 수행할 수 있습니다.

삭제하기 전에 비교합니다.

```
CUCM: [root@vfrscucm1 trust-certs]# md5sum /usr/local/cm/tftp/CTLFile.tlv
e5bf2ab934a42f4d8e6547dfd8cc82e8 /usr/local/cm/tftp/CTLFile.tlv

CUC: [root@vstscuc1 tmp]# cd /tmp

[root@vstscuc1 tmp]# ls -al *tlv
-rw-rw-r--. 1 cucsmgr 고객 서비스 6120년 2월 5일 15:29 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

[root@vstscuc1 tmp]# md5sum a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv
```

e5bf2ab934a42f4d8e6547dfd8cc82e8 a31cefe5-9359-4cbc-a0f3-52eb870d976c.tlv

또한 다음 트러블슈팅 가이드를 참조할 수 있습니다.

결합

[CSCum48958](#) - CUCM 10.0(IP 주소 길이가 올바르지 않음)

[CSCtn87264](#) - 보안 SIP 포트에 대한 TLS 연결 실패

[CSCur10758](#) - 취소된 인증서를 제거할 수 없습니다. Unity 연결

[CSCur10534](#) - Unity Connection 10.5 TLS/PKI inter-op redundant CUCM

[CSCve47775](#) - CUC에서 CUCM의 CTLFile을 업데이트하고 검토하는 방법에 대한 기능 요청