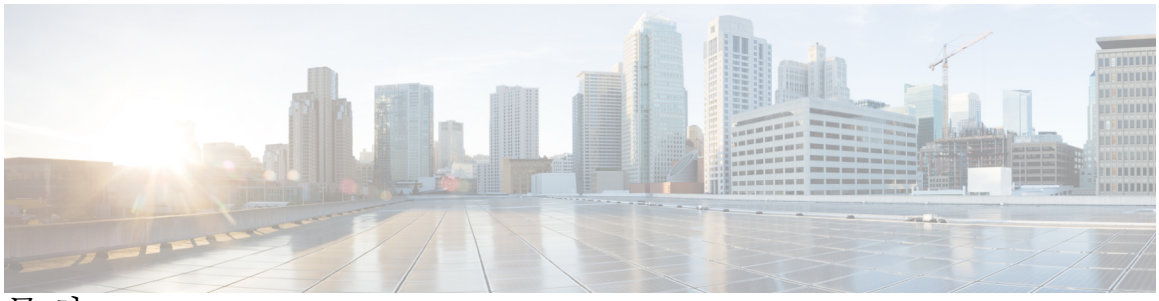
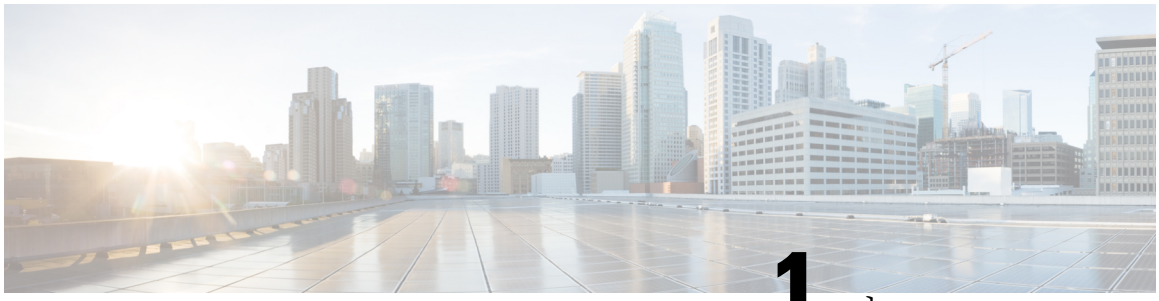
Cisco Unified Communications Manager 시스템 구성 설명서, 릴리스 15

초판: 2023년 12월 18일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

신규 및 변경된 정보

신규 및 변경된 정보

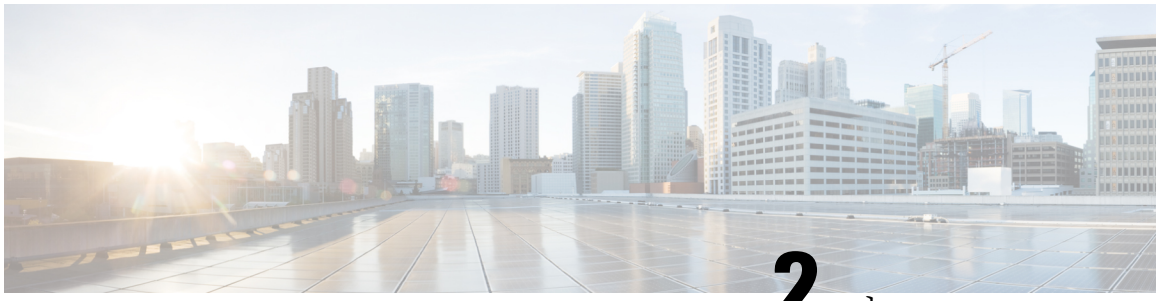
다음 테이블은 현재 릴리스까지 이 가이드의 주요 기능 변경 사항을 소개합니다. 이 테이블은 가이드에 제공된 모든 변경 사항 또는 이 릴리스의 새 기능에 대한 전체 목록을 제공하지 않습니다.

표 *1: Unified Communications Manager* 및 *IM*과 프레즌스 서비스의 새로운 기능 및 변경된 동작

날짜	설명	참고:
2023년 12월 18일	SRTP DTMF 상호 연동 지원에 대한 정보를 제공하는 섹션을 추가했습니다.	SRTP DTMF 상호 연동, 125 페이지
2023년 12월 18일	LPNS(로컬 푸시 알림 서비스) 기능과 관련된 포트 정보를 추가했습니다.	• 공통 서비스 포트, 426 페이지 • 전화기와 Cisco Unified Communications Manager 간 신호, 미디어 및 기타 통신, 430 페이지
2023년 12월 18일	H.323 게이트키퍼 지원 제거에 대한 정보를 추가했습니다.	H.323 트렁크 개요, 96 페이지
2023년 12월 18일	Webex 앱 및 Cisco Jabber 장치 자동 프로비전에 대한 정보를 추가했습니다.	LDAP 디렉터리 동기화 구성, 319 페이지
2023년 12월 18일	업그레이드 조건에 대한 참고 사항을 포함하도록 'Cisco Smart Software Manager' 및 'Cisco Smart Software Manager 위성' 섹션을 업데이트했습니다.	• Smart Software 라이센싱 개요, 7 페이지 • 영구 라이센스 예약 활성화 시스템을 버전 15로 업그레이드, 32 페이지

신규 및 변경된 정보

날짜	설명	참고:
2023년 12월 18일	Oauth에 대한 SSO 및 OAuth 구성 섹션 업데이트 - CUCM 게시자에 대한 새로 고침 토큰 종속성 제거	공통 엔터프라이즈 매개변수, 37 페이지
2023년 12월 18일	새로 고침 토큰을 자동으로 갱신하도록 지원을 위한 SSO 및 OAuth 구성 섹션을 업데이트했습니다.	공통 엔터프라이즈 매개변수, 37 페이지



2 장

소개

시스템 구성 개요

이 문서에는 통화 제어 시스템의 설치 후 설정에 대한 기본 구성 작업이 포함되어 있습니다. 이 문서를 사용하여 시스템 매개변수, 다이얼 플랜 및 콜 라우팅, 미디어 리소스, 애플리케이션 통합 및 엔드유저 및 엔드포인트 프로비저닝을 구성할 수 있습니다. 이 문서를 작성할 때는, 구성된 다이얼 플랜, 콜 라우팅, 미디어 리소스, 대역폭 관리 리소스 및 기본 보안을 포함하는 기본 구성을 갖추고 있어야 합니다. 또한 사용자 및 엔드포인트가 프로비저닝됩니다.

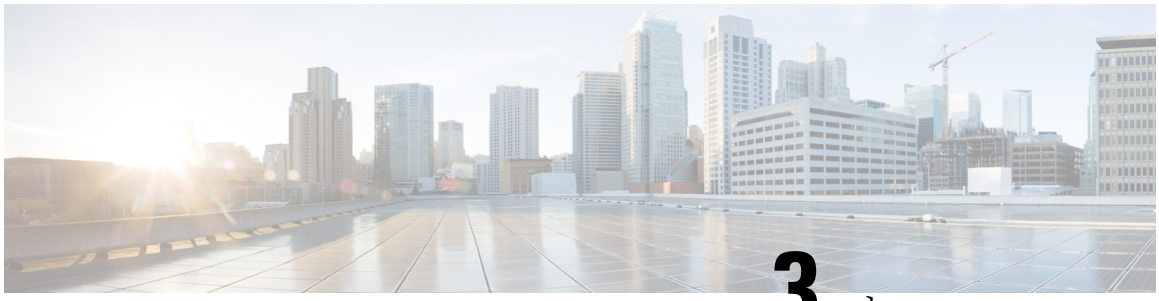
이 문서에는 다음 섹션이 포함되어 있습니다.

- 시스템 구성 요소—시스템 라이센스, 기본 보안, SSO, 디바이스 풀, 트렁크, 게이트웨이, 미디어 리소스 및 콜수락 제어(CAC) 등의 항목을 구성합니다.
- 다이얼 플랜—다이얼 플랜 및 콜 라우팅 요소를 구성합니다.
- 애플리케이션 통합—Cisco Emergency Responder, Cisco Unity Connection 및 Cisco Expressway와 같은 애플리케이션을 통합합니다.
- 사용자 프로비저닝—사용자를 시스템에 추가합니다.
- 디바이스 프로비저닝—사용자에 대한 디바이스를 등록합니다.

이 설명서의 작업을 완료하고 나면, 시스템은 사용자, 디바이스, 기본 보안 및 SSO를 통해 설정됩니다. 그런 다음 계속 진행하여 Cisco 솔루션을 구성할 수 있습니다.

부

시스템 구성 요소



3 장

Smart Software 라이센싱

Smart Software 라이센싱 개요

Cisco Smart Software 라이센싱은 새로운 라이센싱 방식입니다. 이 방식을 사용하는 경우 라이센싱을 더욱 유연하게 활용하고 전사적으로 간편하게 적용할 수 있습니다. 또한 라이센스 소유권 및 소비량도 명확하게 확인할 수 있게 됩니다.

Cisco Smart Software 라이센싱을 사용하면 디바이스에서 자동으로 등록하고 라이센스 소비량을 보고하여 라이센스를 쉽게 확보, 구축 및 관리하여, 제품 활성화 키(PAK)의 필요를 없애 줍니다. 라이센스 엔타이틀먼트를 단일 계정으로 풀링하고 필요로 할 때는 언제든지 네트워크를 통해 자유롭게 라이센스를 이동할 수 있습니다. Cisco 제품에서 활성화되고 직접 클라우드 기반 또는 간접 구축 모델에 의해 관리됩니다.

Cisco Smart Software 라이센싱 서비스는 제품 인스턴스를 등록하고, 라이센스 사용량을 보고하고, Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 필요한 인증을 가져옵니다.

스마트 라이센싱을 사용하여 다음을 수행할 수 있습니다.

- 라이센스 사용량 및 수량 확인
- 각 라이센스 유형의 상태 확인
- Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 사용할 수 있는 제품 라이센스 확인

- Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 라이센스 인증 갱신
- 라이센스 등록 갱신
- Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 등록 해제

참고 라이센스 인증은 최소 30일에 1회 갱신되며 90일간 유효합니다. Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 연결되지 않은 경우, 인증은 90일 후에 만료됩니다.

Cisco Smart Software Manager 위성 옵션을 선택한 경우, 인증을 수행하려면 위성이 Cisco Smart Software Manager와 인터넷으로 연결되어 있어야 합니다. Cisco Smart Software Manager 위성은 두 가지 모드 즉, 연결 시간 구성이 가능한 연결 모드와 수동 동기화가 필요한 연결 중단 모드에서 작동할 수 있습니다.

스마트 라이센싱에 대한 두 가지 메인 구축 옵션이 있습니다.

- Cisco Smart Software Manager
- Cisco Smart Software Manager 위성

Cisco Smart Software Manager

Cisco Smart Software Manager는 시스템 라이센싱을 처리하는 클라우드 기반 서비스입니다. Unified Communications Manager에서 직접 또는 프록시 서버를 통해 cisco.com에 연결할 수 있는 경우, 이 옵션을 사용합니다. Cisco Smart Software Manager을 사용해서 다음을 할 수 있습니다.

- 라이센스 관리 및 추적
- 가상 어카운트 전체에서 라이센스 이동
- 등록된 제품 인스턴스 제거

선택 사항으로, Unified Communications Manager에서 Cisco Smart Software Manager로 바로 연결할 수 없는 경우, 프록시 서버를 구축하여 연결을 관리할 수도 있습니다.

Cisco Smart Software Manager에 대한 자세한 내용은 https://software.cisco.com을 참조하십시오.

Cisco Smart Software Manager 위성

Cisco Smart Software Manager 위성은 Unified Communications Manager에서 보안 또는 사용 가능성을 위해 cisco.com으로 바로 연결할 수 없는 경우 라이센스 요구 사항을 처리할 수 있는 온프레미스 구축입니다. 이 옵션이 구축되면 Unified Communications Manager에서 위성으로 등록되고 라이센스 소비량을 보고합니다. 위성은 cisco.com에 호스팅된 백엔드 Cisco Smart Software Manager와 데이터베이스를 정기적으로 동기화합니다.

cisco.com에 직접 연결할 수 있는지 여부에 따라, Cisco Smart Software Manager 위성을 연결 또는 연결 끊김 모드로 구축할 수 있습니다.

- 연결—Smart Software Manager 위성에서 직접 cisco.com에 연결할 수 있는 경우 사용합니다. 스마트 어카운트 동기화는 자동으로 발생합니다.
- 연결 끊김—Smart Software Manager에서 cisco.com에 연결할 수 없는 경우 사용합니다. 스마트 어카운트 동기화를 수동으로 업로드하고 다운로드해야 합니다.

참고 듀얼 스택 모드에서 실행되는 Unified CM에서 IPv4 및 IPv6 주소를 사용하여 구성된 위성을 지원합니다.

Cisco Smart Software Manager 위성 정보 및 설명서는 https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html을 참조하십시오.

라이센스 유형

다음과 같은 라이센스 유형을 사용하여 요구 사항을 처리할 수 있습니다.

Cisco Unified Workspace Licensing

CUWL(Cisco Unified Workspace Licensing)은 가장 보편적인 Cisco Collaboration 애플리케이션과 서비스를 비용 효율적이고 간단한 패키지로 제공합니다. 사용자 별로 소프트 클라이언트, 애플리케이션 서버 소프트웨어 및 라이센스가 포함됩니다.

Cisco User Connect Licensing

UCL(User Connect Licensing)은 애플리케이션 서버 소프트웨어, 사용자 라이센스 및 소프트 클라이언트를 포함하는 개별 Cisco Unified Communications 애플리케이션에 대한 단일 사용자 기반 라이센스입니다. 필요한 디바이스 유형 및 디바이스의 수에 따라, UCL은 필수, 기본, 고급 및 고급 플러스 버전으로 제공됩니다.

이러한 라이센스 유형 및 사용 가능한 버전에 대한 자세한 내용은 http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html을 참조하십시오.

Session Management Edition

Session Management Edition은 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 등록할 수 있습니다. Unified Communications Manager와 동일한 프로세스를 사용하여 Session Management Edition을 등록하 고, Cisco Unified Communications Manager가 등록된 가상 어카운트 또는 별도의 가상 어카운트에 등록하고, 최소 라이센스 요구 사항 세트를 충족할 수 있습니다.

참고 특정 라이센스 예약(SLR)에 등록된 SME에서는 SLR 인증 코드를 생성하는 동안 CSSM에 예약된 최소 라이센스 세트가 필요합니다.

제품 인스턴스 평가 모드

설치 후 Unified Communications Manager이 90일 평가 기간 동안 실행됩니다. 평가 기간이 끝나면 Unified Communications Manager에서는 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 등록될 때까지 새 사용자 또는 디바이스 추가를 허용하지 않습니다.

참고 평가 기간은 제품이 등록되기 이전입니다.

참고 90일 평가 기간으로 실행 중에는 보안 SIP 트렁크를 구축할 수 없습니다. 보안 SIP 트렁크를 구축하려면, 시스템에서 내보내기 제어 기능 사용 제품 등록 토큰이 선택된 상태로 Smart Software Manager 계정에 등록되어 있어야만 합니다.

시스템 라이센싱 사전 요건

시스템 라이센스 계획

UC(Unified Communications) 라이센싱 구조를 검토하고 이해합니다. 자세한 내용은 http://www.cisco.com/c/en/us/products/unified-communications/unified-communications-licensing/index.html의 내용을 참조하십시오.

다음과 같이 Unified Communications Manager를 Smart Software Manager 서비스에 연결하는 방법을 계획합니다.

- cisco.com에서 Cisco Smart Software Manager에 직접 연결—Unified Communications Manager에서 cisco.com의 Cisco Smart Software Manager에 직접 연결합니다. 이 옵션을 사용하면 `tools.cisco.com`을 해결하는 Unified Communications Manager에서 DNS를 구성해야 합니다.
- 프록시 서버를 통해 Smart Software Manager에 연결—Unified Communications Manager에서 cisco.com의 Cisco Smart Software Manager 서비스에 연결되는 프록시 서버 또는 전송 게이트웨이에 연결합니다. DNS는 Unified Communications Manager에서 필요하지 않지만, `tools.cisco.com`을 해결할 수 있는 프록시 서버에서는 DNS를 구성해야 합니다.
- 온프레미스 Cisco Smart Software Manager 위성에 연결—Unified Communications Manager에서 온프레미스 Smart Software Manager 위성에 연결합니다. Unified Communications Manager에서 DNS는 필요하지 않습니다. Connected 모드를 구축 중인 경우, 위성 서버에서 `tools.cisco.com`을 해결할 수 있는 DN이 필요합니다. Disconnected 모드를 구축 중인 경우, 위성 서버에서 DNS가 필요하지 않습니다.

스마트 라이센싱 등록

스마트 어카운트 및 가상 어카운트 설정 자세한 내용은 https://software.cisco.com/의 내용을 참조하십시오.

(선택 사항) Cisco Smart Software Manager 위성을 배포 하려면 위성을 설치 하 고 설정합니다. 스마트 소프트웨어 관리자 위성 설치 설명서를 포함하여 설명서를 참조하십시오. https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html에서 설명서를 찾을 수 있습니다.

스마트 소프트웨어 라이센싱 작업 플로우

이들 작업을 완료하여 Unified Communications Manager에 대한 시스템 라이센싱을 설정합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	제품 인스턴스 등록 토큰 받기, 11 페이지.	이를 사용하여 가상 어카운트에 대한 제품 인스턴스 등록 토큰을 생성합니다.
단계 **2**	Smart Software 라이센싱에 대한 연결 구성, 12 페이지	Unified Communications Manager에서 스마트 소프트웨어 라이센싱 서비스에 연결하는 전송 설정을 선택합니다. 직접 옵션이 기본값으로 선택되어 있어, 제품이 Cisco 라이센싱 서버와 바로 통신합니다.
단계 **3**	Cisco Smart Software Manager로 등록, 13 페이지.	이 단계를 수행하여 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 Unified Communications Manager를 등록합니다.

제품 인스턴스 등록 토큰 받기

시작하기 전에

Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 제품 인스턴스 등록 토큰을 가져와서 제품 인스턴스를 등록합니다. 토큰은 내보내기 제어 기능의 활성화와 무고나하게 생성할 수 있습니다.

프로시저

단계 **1** Smart Software Manager 또는 Smart Software Manager 위성에서 스마트 어카운트에 로그인합니다.

단계 **2** Unified Communications Manager 클러스터와 연결하려는 가상 어카운트을 탐색합니다.

단계 **3** “제품 인스턴스 등록 토큰”을 생성합니다.

참고 이 토큰으로 등록된 제품에 대해 내보내기 제어 기능을 허용 확인란에 체크 표시하여, 이 스마트 어카운트에서 원하는 제품 인스턴스 토큰의 내보내기 제어 기능을 켭니다. 이 확인란에 체크 표시하고 조건에 동의하여, 이 등록 토큰으로 등록된 제품에 대해 더 높은 수준의 제품 암호화를 활성화합니다. 기본적으로 이 확인란은 선택되어 있습니다. 이 토큰을 사용하여 내보내기 제어 기능을 사용하는 것을 허용하지 않으려는 경우, 이 확인란에 체크 표시할 수 있습니다.

주의 이 옵션은 내보내기 제어 기능을 준수하는 경우에만 사용하십시오.

참고 이 토큰으로 등록된 제품에 대해 내보내기 제어 기능을 허용 확인란은 내보내기 제어 기능을 사용하도록 허용되지 않는 스마트 계정의 경우 표시되지 않습니다.

단계 **4** 토큰을 복사하거나 다른 위치에 저장합니다.

자세한 내용은 https://software.cisco.com/의 내용을 참조하십시오.

Smart Software 라이센싱에 대한 연결 구성

이 작업을 완료하여 Unified Communications Manager를 Smart Software 라이센싱 서비스에 연결합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 라이센싱 > 라이센스 관리를 선택합니다.
라이센스 관리 창이 나타납니다.

단계 **2** **Smart Software** 라이센싱 섹션에서 **Smart Call Home** 라이센싱 설정 보기/편집 링크를 클릭합니다.
전송 수정 대화 상자가 나타납니다.

단계 **3** Unified Communications Manager를 Smart Licensing 서비스에 연결하는 다음과 같은 방법을 선택합니다.

- 다이렉트—Unified Communications Manager에서 cisco.com의 Smart Software Manager로 직접 연결합니다. 이것이 기본 옵션입니다. 이 옵션을 사용하면 `tools.cisco.com` 해결할 수 있는 Unified Communications Manager에 DNS를 구축해야만 합니다.
- 전송 게이트웨이—Unified Communications Manager에서 온프레미스 Cisco Smart Software Manager 위성 또는 시스템 라이센싱에 대한 전송 게이트웨이로 연결합니다. URL 텍스트 상자에 Smart Software Manager 위성 또는 전송 게이트웨이의 주소 및 포트를 입력합니다. 예를 들어, `fqdn_of_smart_software_manager:port_number`입니다. HTTPS의 경우, 포트 443을 사용합니다.
- **HTTP/HTTPS** 프록시—Unified Communications Manager에서 프록시 서버로 연결합니다. 이 서버는 전송 게이트웨이 및 cisco.com의 위성과 함께 Cisco Smart Software Manager 서비스에 연결됩니다. 프록시 서버의 IP 주소 또는 호스트네임을 포트와 함께 입력합니다.

- HTTP 또는 HTTPS 프록시에서 인증 필요—인증 기반 프록시 서버를 사용하여 Cisco Smart Software Manager에 등록하려는 경우, 해당 확인란을 활성화합니다.
- 서버 IP 주소/호스트 네임
- 포트— HTTPS의 경우, 포트 443을 사용합니다.
- 사용자 이름
- 암호

단계 **4** Smart Licensing 등록 중에 내 호스트 네임 또는 **IP** 주소를 **Cisco**와 공유하지 않습니다 확인란에 체크 표시하여, Unified Communications Manager가 해당 IP 주소 및 호스트 네임을 공유하지 않도록 제한합니다.

단계 **5** 저장을 클릭합니다.

Cisco Smart Software Manager로 등록

이 절차를 사용하여 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 통해 제품을 등록합니다. 등록할 때까지 해당 제품은 계속해서 평가 모드로 유지됩니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 라이센싱 > 라이센스 관리를 선택합니다.
라이센스 관리 창이 나타납니다.

단계 **2** 스마트 소프트웨어 라이센싱 섹션에서 등록 버튼을 클릭합니다.
등록 창이 나타납니다.

단계 **3** 제품 인스턴스 등록 토큰 섹션에서 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 생성한 복사 또는 저장된 "등록 토큰 키"를 붙여 넣습니다.

단계 **4** 등록을 클릭하여 등록 프로세스를 완료합니다.

단계 **5** 닫기를 클릭합니다. 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **6** 라이센스 사용 보고서 섹션에서 사용 세부 정보 업데이트를 클릭하여 시스템 라이센스 사용 정보를 수동으로 업데이트합니다.

참고 사용 정보는 24시간 마다 자동으로 업데이트됩니다. 자세한 내용은 온라인 도움말을 참조하십시오.

Smart Software 라이센싱 추가 작업

다음 선택 작업은 Unified Communications Manager 및 Unified Communications Manager 라이센싱에 사용할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	인증 갱신, 15 페이지	이 작업을 완료하여 라이센스 유형에 나열된 모든 라이센스에 대한 라이센스 인증 상태를 수동으로 갱신합니다. 참고 라이센스 인증은 30일마다 자동으로 갱신됩니다. Cisco Smart Software Manager 또는 CCisco Smart Software Manager 위성에 연결되지 않은 경우, 인증 상태는 90일 후에 만료됩니다. Cisco Smart Software Manager 위성 옵션을 선택한 경우, 인증을 수행하려면 위성이 Cisco Smart Software Manager와 인터넷으로 연결되어 있어야 합니다. Cisco Smart Software Manager 위성은 두 가지 모드 즉, 연결 시간 구성이 가능한 연결 모드와 수동 동기화가 필요한 연결 중단 모드에서 작동할 수 있습니다.
단계 2	등록 갱신, 16 페이지	이 작업을 완료하여 등록 정보를 수동으로 갱신합니다. 참고 초기 등록은 1년 동안 유효합니다. 제품이 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 연결된 경우 6개월 마다 자동으로 등록 갱신이 수행됩니다.
단계 3	등록 해제, 17 페이지	이 작업을 완료하여 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 Unified Communications Manager 클러스터의 연결을 차단합니다. 평가 기간이 만료되지 않은 경우, 제품이 평가 모드로 되돌아갑

	명령 또는 동작	목적
		니다. 제품에 사용되는 모든 라이선스 자격이 가상 어카운트로 즉시 릴리스되어 다른 제품 인스턴스에서 사용할 수 있게 됩니다.
단계 **4**	Cisco Smart Software Manager로 라이센스 재등록, 18 페이지	이 작업을 완료하여 Cisco Smart Software Manager 또는 Cisco Smart Software Manager에서 Unified Communications Manager를 재등록합니다. 참고 새 가상 어카운트의 토큰을 사용하여 재등록하여 다른 가상 어카운트로 제품을 마이그레이션할 수 있습니다.

인증 갱신

이 절차를 사용하여 라이센스 유형에 나열된 모든 라이센스에 대한 라이센스 인증 상태를 수동으로 갱신합니다.

참고 라이센스 인증은 30일마다 자동으로 갱신됩니다. Cisco Smart Software Manager 또는 CCisco Smart Software Manager 위성에 연결되지 않은 경우, 인증 상태는 90일 후에 만료됩니다.

Cisco Smart Software Manager 위성 옵션을 선택한 경우, 인증을 수행하려면 위성이 Cisco Smart Software Manager와 인터넷으로 연결되어 있어야 합니다. Cisco Smart Software Manager 위성은 두 가지 모드 즉, 연결 시간 구성이 가능한 연결 모드와 수동 동기화가 필요한 연결 중단 모드에서 작동할 수 있습니다.

시작하기 전에

제품을 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성으로 등록해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 라이센싱 > 라이센스 관리를 선택합니다.
라이센스 관리 창이 나타납니다.

단계 **2** 스마트 소프트웨어 라이센싱 섹션에서 작업 드롭다운 목록을 클릭합니다.

단계 **3** 지금 인증 갱신을 선택합니다.
인증 갱신창이 나타납니다.

단계 **4** 확인을 클릭합니다.

Unified Communications Manager에서 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성으로 요청을 보내 "라이센스 인증 상태"를 확인하고, Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 Unified Communications Manager에 해당 상태를 다시 보고합니다. 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **5** 라이센스 사용 보고서 섹션에서 사용 세부 정보 업데이트를 클릭하여 시스템 라이센스 사용 정보를 수동으로 업데이트합니다.

참고 사용 정보는 24시간 마다 자동으로 업데이트됩니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

등록 갱신

Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 제품을 등록하는 동안, 제품 식별에 사용되며, 1년의 수명(즉, 등록 기간)을 갖는 등록 인증서에 의해 앵커링되는 보안 연결이 있습니다. 이것은 토큰 활성 상태에 대한 시간 제한이 있는 등록 토큰 ID 만료와는 다릅니다. 이 등록은 6개월마다 자동으로 갱신됩니다. 그러나 문제가 있는 경우, 이 등록 기간을 수동으로 갱신할 수 있습니다.

시작하기 전에

제품을 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성으로 등록해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 라이센싱 > 라이센스 관리를 선택합니다.
라이센스 관리 창이 나타납니다.

단계 **2** 스마트 소프트웨어 라이센싱 섹션에서 작업 드롭다운 목록을 클릭합니다.

단계 **3** 지금 등록 갱신을 선택합니다.
등록 창이 나타납니다.

단계 **4** 확인을 클릭합니다.

Unified Communications Manager에서 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성으로 요청을 보내 "등록 상태"를 확인하고, Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 Unified Communications Manager에 해당 상태를 다시 보고합니다.

단계 **5** 라이센스 사용 보고서 섹션에서 사용 세부 정보 업데이트를 클릭하여 시스템 라이센스 사용 정보를 수동으로 업데이트합니다.

참고 사용 정보는 24시간 마다 자동으로 업데이트됩니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

등록 해제

이 절차를 사용하여 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 등록을 해제하고 현재 가상 어카운트에서 모든 라이센스를 릴리스합니다. 이 절차는 또한 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 Unified Communications Manager 클러스터의 연결도 차단합니다. 제품에 사용되는 모든 라이센스 엔타이틀먼트가 가상 어카운트로 릴리스되어 다른 제품 인스턴스에서 사용할 수 있습니다.

참고 Unified Communications Manager에서 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 연결할 수 없고 제품이 계속해서 등록 해제 상태인 경우, 경고 메시지가 표시됩니다. 이 메시지는 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 제품을 수동으로 제거하여 라이센스를 확보하라는 알림을 제공 합니다.

시작하기 전에

제품을 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성으로 등록해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 라이센싱 > 라이센스 관리를 선택합니다.
라이센스 관리 창이 나타납니다.

단계 **2** 스마트 소프트웨어 라이센싱 섹션에서 작업 드롭다운 목록을 클릭합니다.

단계 **3** 등록 해제를 선택합니다.
등록 해제 창이 나타납니다.

단계 **4** 확인을 클릭합니다.

단계 **5** 라이센스 사용 보고서 섹션에서 사용 세부 정보 업데이트를 클릭하여 시스템 라이센스 사용 정보를 수동으로 업데이트합니다.

참고 사용 정보는 6시간 마다 자동으로 업데이트됩니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

참고

- Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 등록한 후에 데이터 플레인 암호화(혼합 모드의 Unified Communications Manager 클러스터)가 활성화되고 제품이 나중에 등록 해제된 경우에도, 혼합 모드는 계속해서 활성 상태가 유지됩니다.

  제품이 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에서 등록 해제될 경우, SmartLicenseExportControlNotAllowed라는 경고가 관리자에게 전송되어 클러스터를 비보안 모드로 설정합니다. 혼합 모드는 재부팅 후에도 계속해서 활성 상태로 유지됩니다.

- 등록 해제 이후의 동작은 제품의 향후 버전에서 변경 될 수 있습니다. CTL 클라이언트 설정에 대한 자세한 내용은 *Cisco Unified Communications Manager*에 대한 보안 설명서의 "Cisco CTL 클라이언트 설정" 장을 http://www.cisco.com/c/en/us/support/unified-communications/unified-presence/products-maintenance-guides-list.html에서 참조하십시오.

  Tokenless CTL을 사용하는 혼합 모드에 대한 자세한 내용은 "Tokenless CTL을 사용하는 CUCM 혼합 모드"를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-tech-notes-list.html에서 참조하십시오.

Cisco Smart Software Manager로 라이센스 재등록

이 절차를 사용하여 Cisco Unified Communications Manager에 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 등록합니다.

시작하기 전에

제품 인스턴스 등록 토큰 받기, 11 페이지.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 라이센싱 > 라이센스 관리를 선택합니다.
라이센스 관리 창이 나타납니다.

단계 **2** 스마트 소프트웨어 라이센싱 섹션에서 등록 버튼을 클릭합니다.
등록 창이 나타납니다.

단계 **3** 스마트 소프트웨어 라이센싱 섹션에서 작업 드롭다운 목록을 클릭합니다.

단계 **4** 등록을 선택합니다.
등록 창이 나타납니다.

단계 **5** 확인을 클릭합니다.

단계 **6** 제품 인스턴스 등록 토큰 섹션에서 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성을 사용하여 생성한 복사 또는 저장된 "등록 토큰 키"를 붙여 넣습니다.

단계 **7** 등록을 클릭하여 등록 프로세스를 완료합니다.

단계 **8** 닫기를 클릭합니다. 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **9** 라이센스 사용 보고서 섹션에서 사용 세부 정보 업데이트를 클릭하여 시스템 라이센스 사용 정보를 수동으로 업데이트합니다.

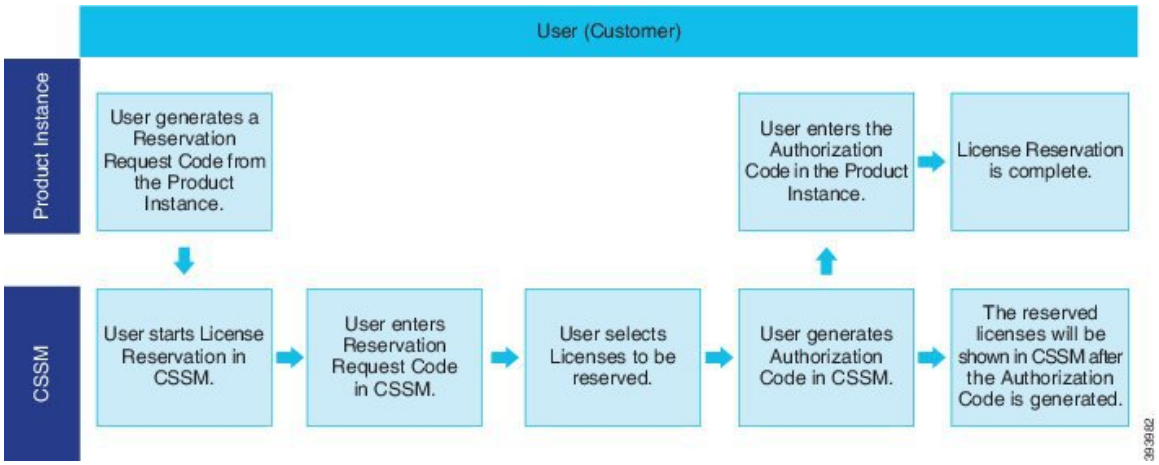
참고 사용 정보는 24시간 마다 자동으로 업데이트됩니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

특정 라이선스 예약

SLR(Specific License Reservation, 특정 라이선스 예약)은 매우 안전한 네트워크에서 사용되는 기능입니다. 사용 정보를 전달하지 않은 상태로 디바이스(제품 인스턴스 - Unified Communications Manager)에 소프트웨어 라이센스를 구축하는 방법을 고객에게 제공합니다.

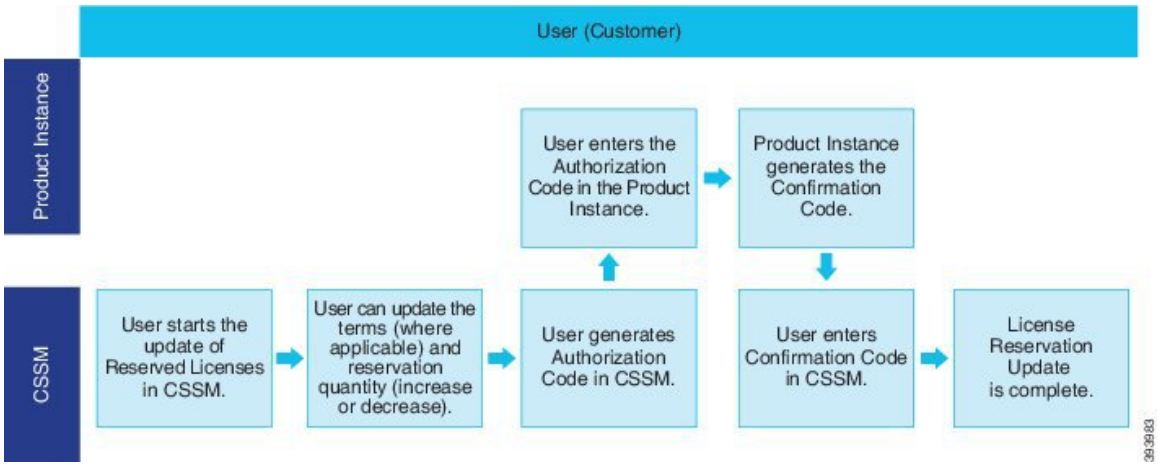
사용자는 Unified Communications Manager 제품에 대한 영구적이거나 기간 기반 라이센스를 지정 및 예약할 수 있습니다. 인증 코드를 교환한 후에는 예약 변경 시까지 정기적인 제품 동기화는 필요하지 않습니다. 예약된 라이센스는 반환 코드와 함께 제품에서 릴리스되지 않는 한 Cisco Smart Software Manager에서 차단 상태가 유지됩니다.

그림 ***1:*** 라이선스 예약



예약된 라이센스의 업데이트 또는 변경(증가 또는 감소)이 Cisco Smart Software Manager에서 이전에 예약된 라이센스에 대해 수행될 수 있습니다. 새 인증 코드를 제품에 설치할 수 있으며 확인 코드를 입수할 수 있습니다. 제품의 확인 코드가 Cisco Smart Software Manager에 설치되지 않은 경우, 새로운 변경 사항은 전송 상태로 그대로 유지됩니다.

그림 *2:* 라이선스 예약 업데이트

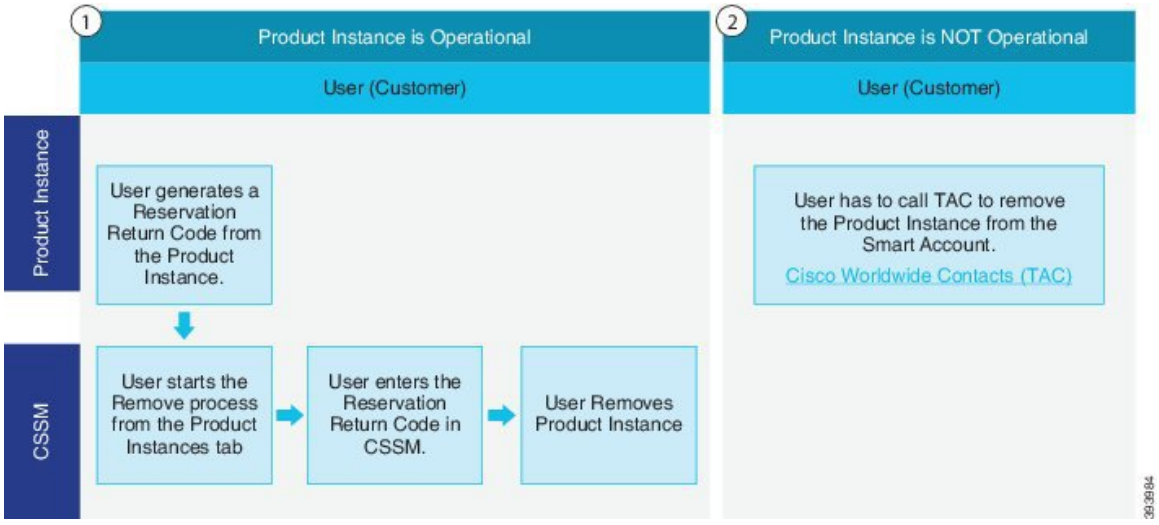


라이센스를 제품 인스턴스(Unified Communications Manager)에서 예약하는 경우, 스마트 어카운트에서 제품을 제거하고 해당 제품 인스턴스(Unified Communications Manager)에 대해 예약된 모든 라이센스를 릴리스하는 두 가지 방법이 있습니다.

제품 인스턴스 작동 중**(**정상 제거**):**사용자는 (인증 코드를 제거하는) 제품 인스턴스에 대한 예약 반환 코드를 생성하여 특정 라이센스 예약 인증을 반환한 다음, 예약 반환 코드를 Cisco Smart Software Manager에 입력할 수 있습니다.

제품 인스턴스가 작동하지 않은 상태**(**장애**/RMA** 또는 **VM**/컨테이너 파손**):** 사용자는 스마트 어카운트에서 제품 인스턴스를 제거할 수 있는 TAC에 문의해야 합니다.

그림 *3:* 제품 인스턴스 ***- Unified Communications Manager*** 제거



참고 사용자는 CLI 구성만을 사용하여 특정 라이센스 예약을 활성화할 수 있습니다.

참고 Unified Communications Manager에서 특정 라이센스 예약이 활성화되면, 클라우드 온본딩용 바우처 생성은 지원되지 않습니다.

스마트 어카운트에 대한 라이센스 예약 기능에 대한 권리가 있는 고객은 가상 어카운트에서 라이센스를 예약하고, 디바이스 UDI를 연결한 다음, 이러한 예약된 라이센스를 보유한 디바이스를 연결이 차단된 모드로 사용할 수 있습니다. 고객은 가상 어카운트에서 UDI에 대한 특정 라이센스와 카운트를 예약합니다. 다음 옵션은 특정 라이센스 예약에 대한 새로운 기능 및 설계 요소에 대해 설명합니다.

- 라이센스 스마트 예약 활성화
- 라이센스 스마트 예약 비활성화
- 라이센스 스마트 예약 요청
- 라이센스 스마트 예약 취소
- 라이선스 예약 업데이트
- 라이센스 스마트 예약 설치 "<authorization-code>"
- 라이센스 스마트 예약 설치 파일 <url>
- 라이센스 스마트 예약 반환
- 스마트 라이센스 예약 반환 승인 "<authorization-code>"

특정 라이선스 예약 작업 플로우

이러한 작업을 완료하여 Unified Communications Manager에 대한 특정 라이센스를 예약합니다.

라이센스 스마트 예약 활성화

이 절차를 사용하여 특정 라이센스 예약을 활성화합니다.

시작하기 전에

Unified Communications Manager는 Cisco Smart Software Manager 또는 위성을 통해 등록 취소됩니다.

프로시저

Cisco Unified CM 관리 콘솔에서 아래 CLI 명령을 실행합니다.

- 라이센스 스마트 예약 활성화

라이센스 스마트 예약 요청

이 절차를 사용하여 Unified Communications Manager 제품에서 예약 요청 코드 생성 요청 코드를 생성합니다.

시작하기 전에

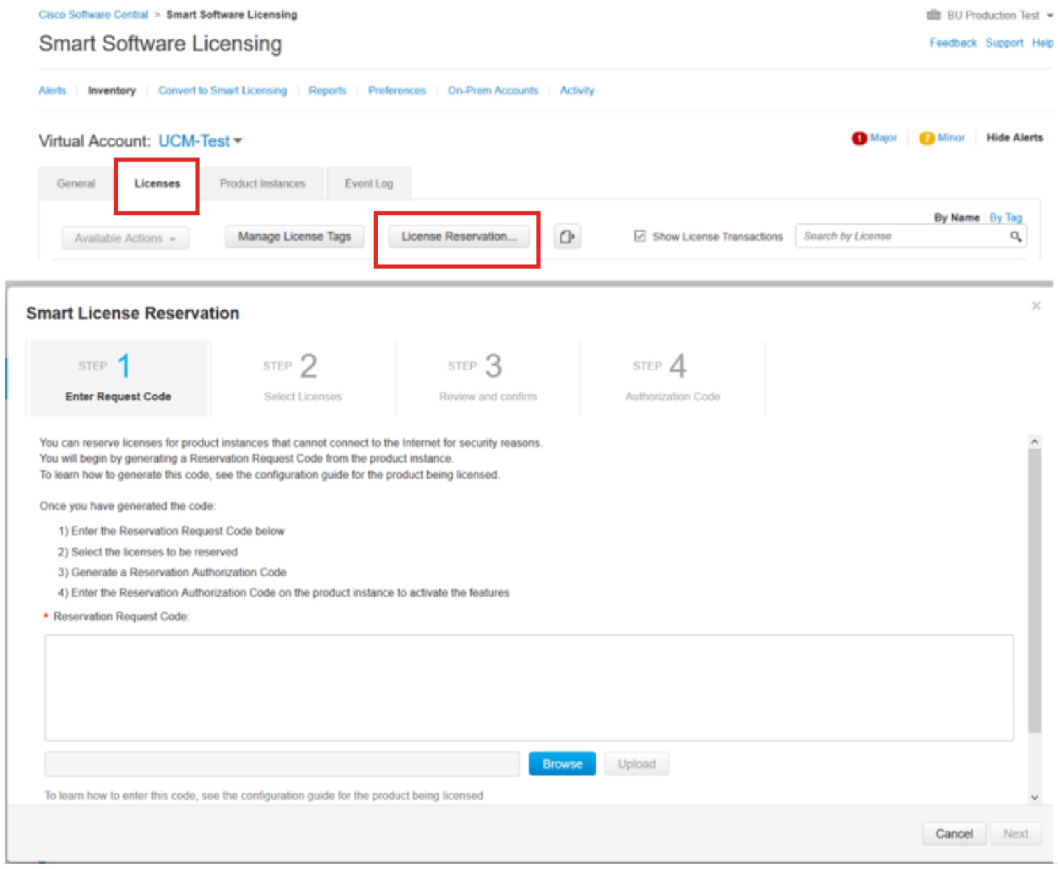
Unified Communications Manager 등록 상태가 예약 진행 중인지 라이센스 스마트 예약 활성화를 실행하여 확인하십시오.

command

프로시저

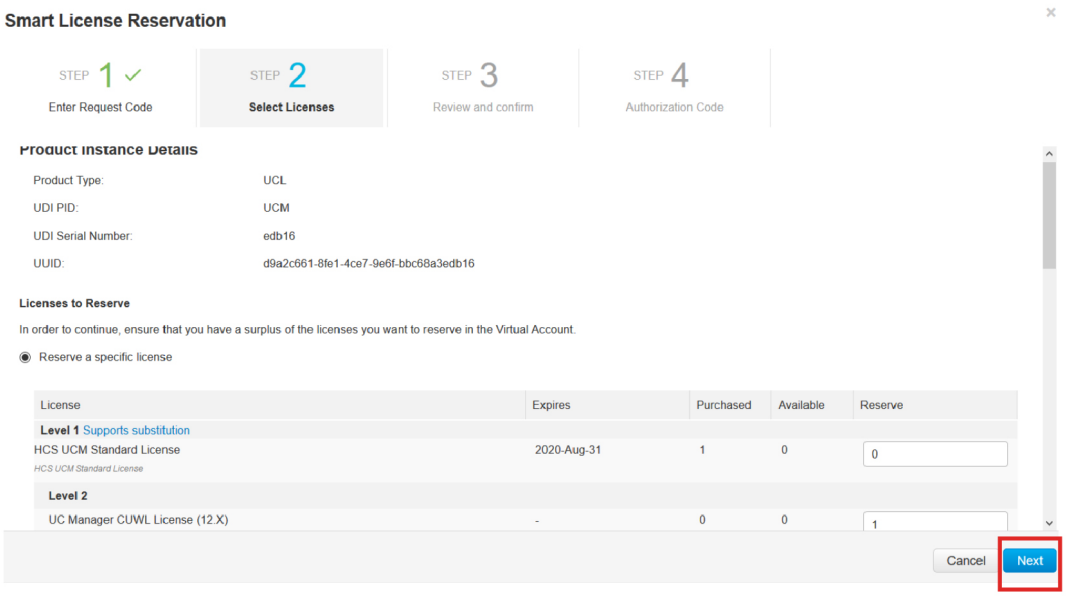
단계 **1** Cisco Unified CM 관리 콘솔에서 *license smart reservation request* 명령을 실행합니다.

단계 **2** CSSM[Cisco Smart Software 관리자]에 로그인하고 예약 요청 코드를 입력합니다.



450364

단계 **3** 이 디바이스에 대해 예약해야 하는 라이센스를 선택하고 인증 코드를 생성합니다.



450365

단계 **4** 인증 코드를 제품 인스턴스에 복사하고 라이센스 스마트 예약 설치 **"<authorization-code>"** 명령을 실행하여 설치합니다.

450366

라이센스 스마트 예약 설치 **"<authorization-code>"**

이 절차를 사용하여 Cisco Smart Software Manager에서 생성된 라이센스 예약 인증 코드를 설치합니다.

시작하기 전에

다음과 같은 순서대로 명령을 실행하여 Unified Communications Manager 등록 상태를 예약 진행 중으로 설정합니다.

- **license smart reservation enable**
- **license smart reservation request**

프로시저

Cisco Unified CM 관리 콘솔에서 아래 CLI 명령을 실행합니다.

- 라이센스 스마트 예약 설치 "<authorization-code>"

라이센스 스마트 예약 설치 파일 **<url>**

이 절차를 사용하여 Cisco Smart Software Manager에서 생성된 라이센스 예약 인증 코드 파일을 설치합니다.

시작하기 전에

아래 순서대로 명령을 실행하여 Unified Communications Manager 등록 상태가 [예약 진행 중]인지 확인하십시오.

- **license smart reservation enable**
- **license smart reservation request**

참고 URL은 다음 형식으로 SFTP 서버에 있는 인증 코드 파일의 필수 경로입니다.

sftp://<HostName/IP>:<port>/<Path to Authorization-Code file>

프로시저

Cisco Unified CM 관리 콘솔에서 아래 CLI 명령을 실행합니다.

- 라이센스 스마트 예약 설치 파일 <url>

특정 라이센스 예약을 포함한 추가 작업

다음 추가 작업은 특정 라이센스 예약을 위해 Unified Communications Manager에서 사용할 수 있습니다.

라이센스 스마트 예약 비활성화

이 절차를 사용하여 특정 라이센스 예약을 비활성화합니다.

시작하기 전에

특정 라이센스 예약이 Unified Communications Manager에서 활성화됩니다.

프로시저

Cisco Unified CM 관리 콘솔에서 아래 CLI 명령을 실행합니다.

- 라이센스 스마트 예약 비활성화

라이선스 예약 업데이트

이 절차를 사용하여 제품 인스턴스에 대한 라이센스 예약을 업데이트하고 새 인증 코드를 받습니다.

시작하기 전에

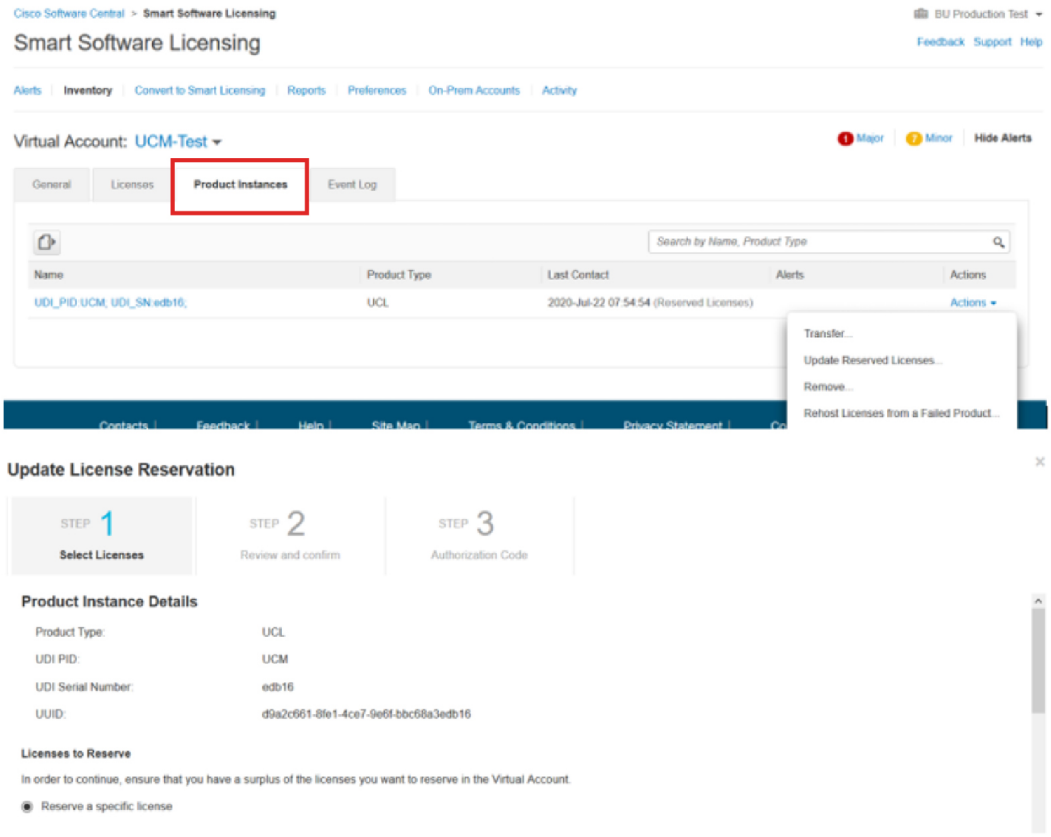
아래 순서대로 명령을 실행하여 Unified Communications Manager 등록 상태가 등록된 특정 라이센스 예약인지 확인하십시오.

- 라이센스 스마트 예약 활성화
- 라이센스 스마트 예약 요청
- 라이센스 스마트 예약 설치 "<authorization-code>"

참고 상위 계층에서 라이센스 임대는 Unified Communications Manager에서 특정 라이센스 예약이 활성화될 때 자동으로 수행되지 않습니다. 라이센스 예약은 Unified Communications Manager 라이센스 소비량/사용으로 수동으로 업데이트되어야 합니다.

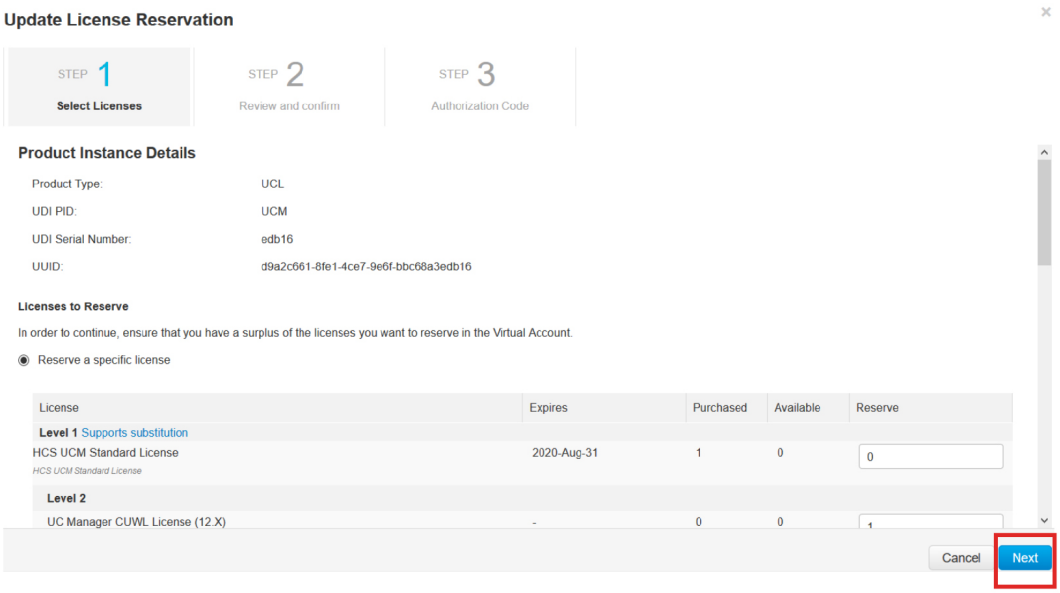
프로시저

단계 **1** CSSM에서 예약을 업데이트하려는 제품 인스턴스 옆의 작업 드롭다운 목록에서 예약된 라이센스 업데이트를 선택합니다.



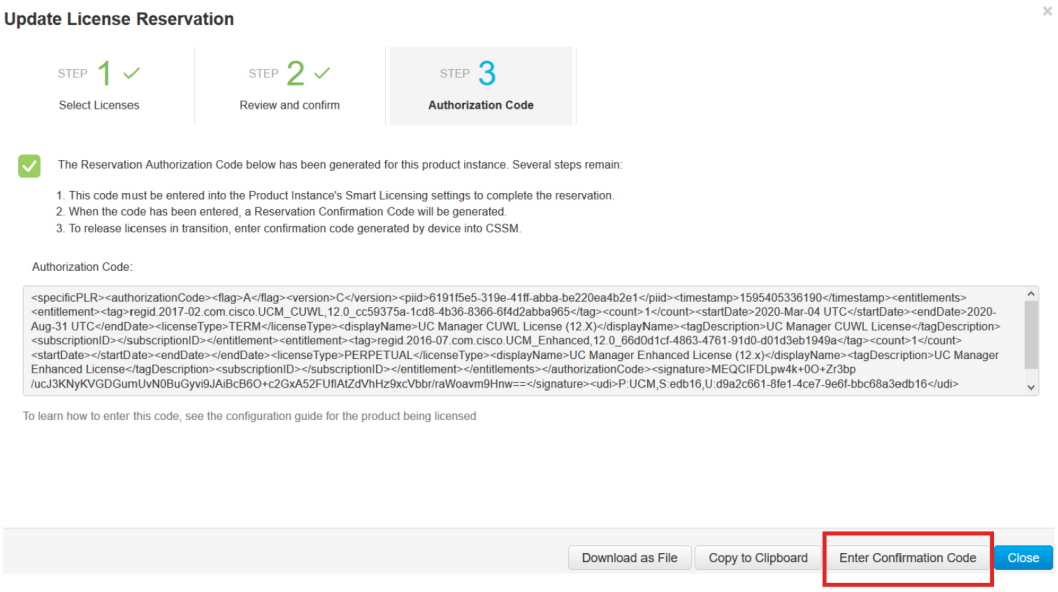
450363

단계 **2** 예약(이 제품 인스턴스에 대한 라이센스 추가/제거/업데이트)을 업데이트하고 인증 코드를 생성합니다.



450367

단계 **3** 인증 코드를 제품 인스턴스에 복사하고 라이센스 스마트 예약 설치 **"<authorization-code>"** 명령을 실행하여 설치합니다.

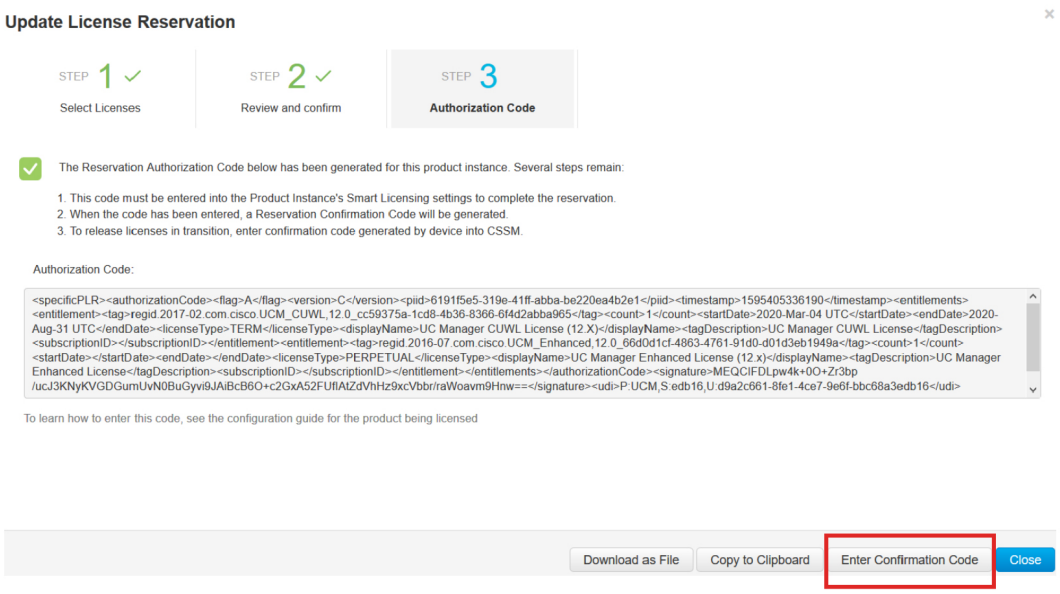


450362

단계 **4** 인증 코드가 성공적으로 설치되고 나면 제품에 대한 확인 코드가 생성됩니다.

450368

단계 **5** CSSM으로 확인 코드를 복사하고 입력하여 예약 업데이트를 완료합니다.



라이센스 스마트 예약 취소

이 절차를 사용하여 CUCM 요청 코드에 대한 Cisco Smart Software Manager의 인증 코드가 설치되기 전에 예약 프로세스를 취소합니다.

시작하기 전에

아래 순서대로 명령을 실행하여 Unified Communications Manager 등록 상태가 [예약 진행 중]인지 확인하십시오.

- **license smart reservation enable**
- **license smart reservation request**

프로시저

Cisco Unified CM 관리 콘솔에서 아래 CLI 명령을 실행합니다.

- 라이센스 스마트 예약 취소

라이센스 스마트 예약 반환

이 절차를 사용하여 가상 어카운트 풀로 라이센스를 반환하고 CSSM에서 제품 인스턴스를 제거하려면 Cisco Smart Software Manager에 입력해야 하는 반환 코드를 생성합니다.

시작하기 전에

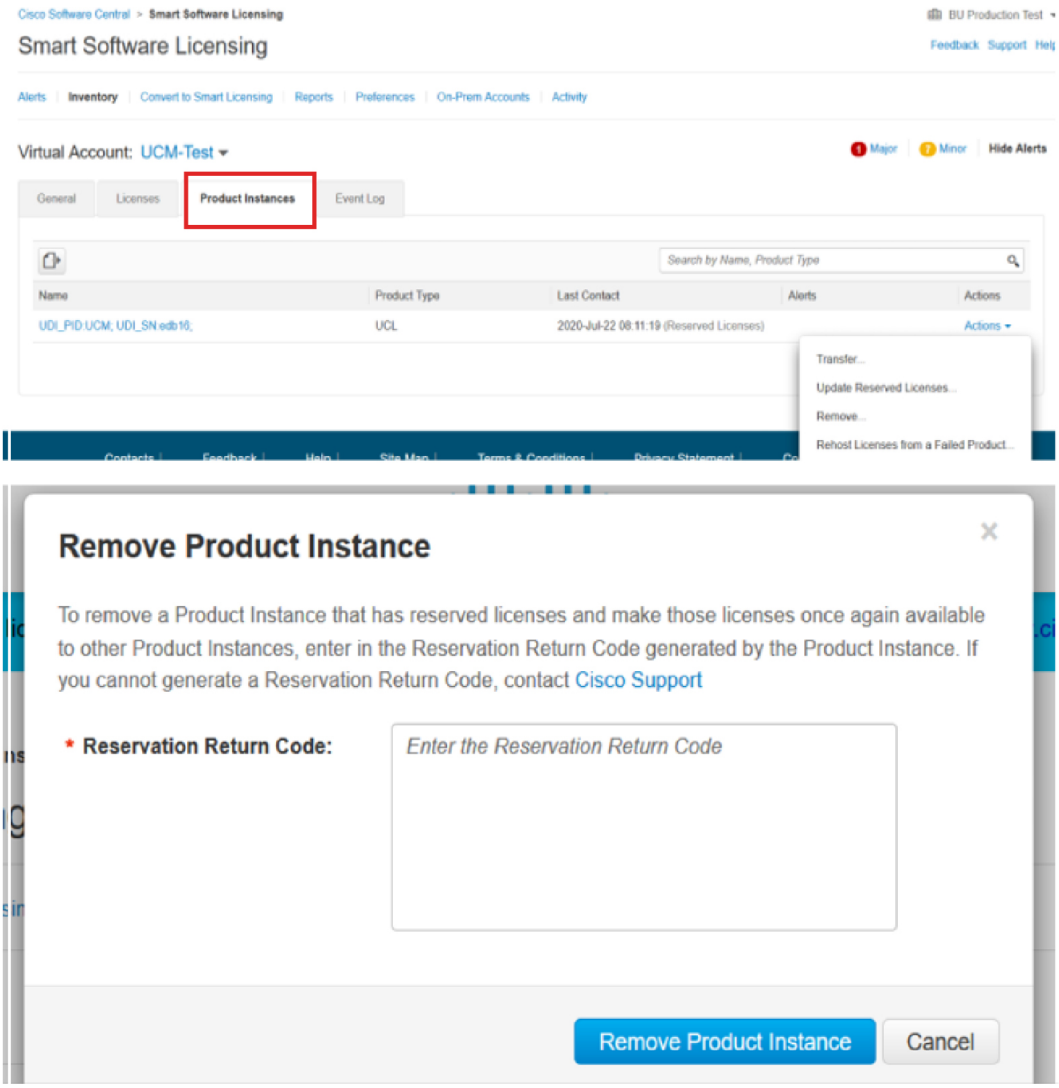
아래 순서대로 명령을 실행하여 Unified Communications Manager 등록 상태가 등록된 특정 라이센스 예약인지 확인하십시오.

- **license smart reservation enable**
- **license smart reservation request**
- 라이센스 스마트 예약 설치 **"<authorization-code>"**

프로시저

단계 **1** Cisco Unified CM 관리 콘솔에서 라이센스 스마트 예약 반환 명령을 실행합니다.

단계 **2** CSSM으로 예약 반환 코드를 복사한 다음 제품 인스턴스를 제거합니다.



450360

스마트 라이센스 예약 반환 승인 "<authorization-code>"

이 절차를 사용하여 아직 설치되지 않은 인증 코드에 대한 반환 코드를 생성합니다. 가상 어카운트 풀로 라이센스를 반환하고 CSSM에서 제품 인스턴스를 제거하려면 반환 코드를 Cisco Smart Software Manager에 입력해야 합니다.

시작하기 전에

아래 순서대로 명령을 실행하여 Unified Communcations Manager 등록 상태가 예약 진행 중인지 확인하십시오.

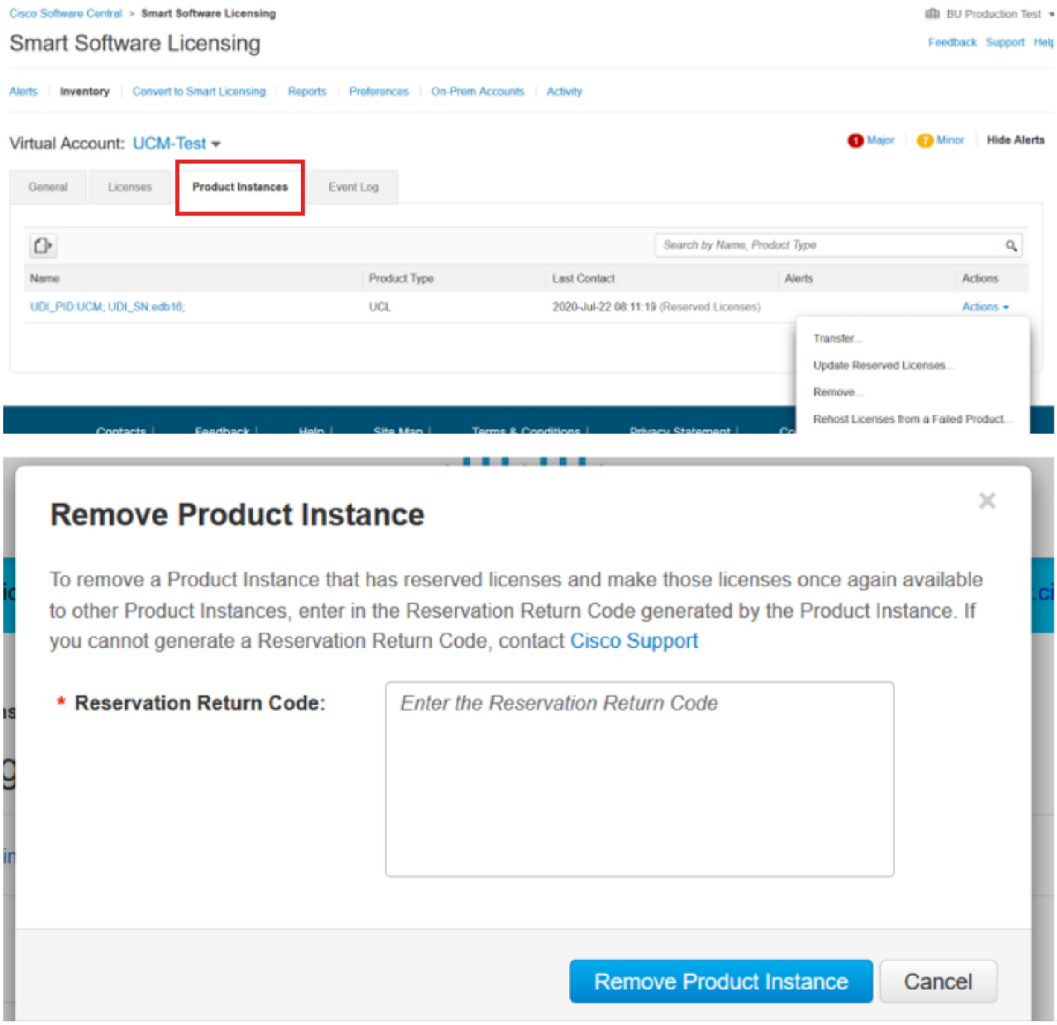
- **license smart reservation enable**

- **license smart reservation request**

프로시저

단계 **1** Cisco 통합 CM 관리 콘솔에서 라이센스 스마트 예약 반환 승인 "<authorization-code>" 명령을 실행합니다.

단계 **2** CSSM으로 예약 반환 코드를 복사한 다음 제품 인스턴스를 제거합니다.



특정 라이센스 예약 활성화 시스템을 버전 14로 업그레이드

라이센스 예약에 대해 활성화된 12.5 Unified Communications Manager 시스템을 버전 14로 업그레이드 중인 경우, 다음과 같은 시나리오를 고려해야 합니다.

1. 버전 14로 업그레이드하기 전에 "라이센스 스마트 예약 반환" 명령(권장)을 사용하여 12.x 라이센스를 반환합니다.

   또는

   버전 14로 업그레이드 한 이후 "라이센스 스마트 예약 반환" 명령을 사용하여 12.x 라이센스를 반환합니다.

2. "라이센스 스마트 예약 요청" 명령을 사용하여 요청 코드를 생성합니다. Cisco Smart Software Manager에서 낮은 버전의 라이센스로 인증 코드를 생성합니다.

3. Cisco Unified Communications Manager의 "라이센스 스마트 예약 설치 <auth-code>" 명령을 사용하여 인증 코드를 설치합니다.

영구 라이센스 예약 활성화 시스템을 버전 15로 업그레이드

영구 라이센스 예약(PLR)이 활성화된 14 SU2 이상 Unified Communications Manager 시스템을 버전 15로 업그레이드하는 경우 다음 시나리오를 고려하십시오.

1. 버전 15로 업그레이드하기 전에 "라이센스 스마트 예약 반환" 명령을 사용하여 라이센스를 반환합니다.

2. 업그레이드 후에 "라이센스 스마트 예약 요청" 명령을 사용하여 요청 코드를 생성합니다. Cisco Smart Software Manager에서 PLR 라이센스로 인증 코드를 생성합니다.

3. Unified Communications Manager의 "라이센스 스마트 예약 설치 <auth-code>" 명령을 사용하여 인증 코드를 설치합니다.

버전 독립적인 라이센싱

Unified Communications Manager는 버전 독립적인 사용자 라이센스를 지원합니다. 라이선스는 연금 스타일이며 구독 기간 동안 발급됩니다. Flex EA(엔터프라이즈 계약) 또는 Flex NU(명명된 사용자, Professional, Enhanced, Access)를 통해 이러한 V14 라이센스를 주문할 수 있습니다. 자세한 내용은 주문 가이드를 참조하십시오.

Unified Communications Manager는 계속해서 버전 12.X 라이센스를 사용합니다.

라이센스는 CSSM(Cisco Smart Software Manager)에서 관리됩니다. 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 'Smart Software 라이센싱' 장을 참조하십시오.

스마트 라이센싱 내보내기 컴플라이언스

스마트 라이센싱은 사용자가 내보내기 컨트롤 기능을 사용할 수 있도록 허용하는 방법을 제공합니다. 연결된 상태에서는 재등록 프로세스를 사용하여 내보내기 컨트롤 기능을 사용합니다. 연결이 차단된 상태에서는 스마트 라이센스 예약을 사용하여 내보내기 컨트롤 기능을 사용합니다.

이 내보내기 컨트롤 기능은 내보내기 제한이 적용되는 스마트 어카운트이 있는 고객들을 위한 솔루션입니다. 이 기능을 사용하여 사용자는 Cisco Smart Software Manager 또는 위성에서 승인된 규정 준수 내보내기 라이센스를 요청하고, Cisco Unified Communications Manager에서 내보내기 제한 기능을 활성화할 수 있습니다.

다음 옵션은 새로운 기능과 내보내기 컨트롤 기능을 위한 설계 요소를 설명합니다.

- 라이센스 스마트 내보내기 요청 로컬 <exportfeaturename>
- 라이센스 스마트 내보내기 반환 로컬 <exportfeaturename>
- 라이센스 스마트 내보내기 취소

수출 제어 작업 플로우

다음 작업을 완료하여 Cisco Unified Communications Manager에 대한 컨트롤 라이센스를 내보내십시오.

라이센스 스마트 내보내기 요청 로컬 **<exportfeaturename>**

이 명령을 사용하여 내보내기 제한이 적용되는 스마트 어카운트을 가진 사용자가 Cisco Smart Software Manager 또는 위성에서 내보내기 제한 라이센서를 요청할 수 있습니다.

이 명령은 Cisco Smart Software Manager 또는 위성에서 내보내기 제한 라이센스를 사용할 수 있고 해당 제품에 대한 내보내기 제한 기능을 활성화한 경우, 내보내기 인증 키를 반환합니다.

시작하기 전에

Cisco Unified Communications Manager가 Cisco Smart Software Manager 또는 위성에 등록됩니다. Cisco Smart Software Manager에서 <CUCM Export Restricted Authorization Key> 라이센스를 사용할 수 있는지 확인합니다.

프로시저

Cisco Unified CM 관리 콘솔에서 다음과 같은 CLI 명령을 실행합니다.

- 라이센스 스마트 내보내기 요청 로컬 <exportfeaturename>

라이센스 스마트 내보내기 반환 로컬 <exportfeaturename>

이 명령을 사용하면 이전에 요청된 내보내기가 제한된 라이센스를 Cisco Smart Software Manager 또는 위성으로 반환할 수 있습니다. 내보내기가 제한된 기능에 대한 내보내기 인증 키가 시스템에서 제거됩니다.

시작하기 전에

기능에 대한 내보내기 인증 키가 생성됩니다.

프로시저

Cisco Unified CM 관리 콘솔에서 다음과 같은 CLI 명령을 실행합니다.

- 라이센스 스마트 내보내기 반환 로컬 <exportfeaturename>

라이센스 스마트 내보내기 취소

이 명령을 사용하여 내보내기 제한이 적용되는 스마트 어카운트을 가진 사용자는 이전에 실패한 내보내기 요청의 자동 재시도를 취소 하거나 Cisco Smart Software Manager 또는 위성에서 복귀할 수 있습니다.

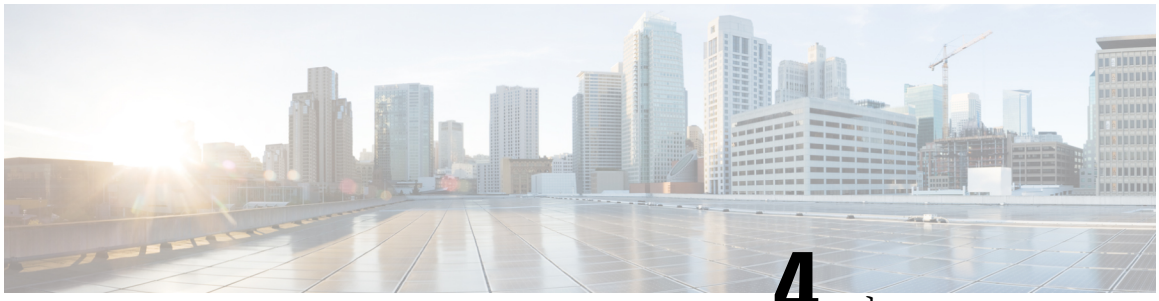
시작하기 전에

Cisco Unified Communications Manager가 Cisco Smart Software Manager 또는 위성에 등록됩니다.

프로시저

Cisco Unified CM 관리 콘솔에서 다음과 같은 CLI 명령을 실행합니다.

- 라이센스 스마트 내보내기 취소



4 장

엔터프라이즈 매개변수 및 서비스 구성

엔터프라이즈 매개변수 개요

엔터프라이즈 매개 변수는 동일한 클러스터의 모든 장치 및 서비스에 적용되는 기본 설정을 제공합니다. 클러스터는 동일한 데이터베이스를 공유하는 Cisco Unified Communications Manager 세트로 구성됩니다. 새 Cisco Unified Communications Manager를 설치하는 경우 이 Cisco Unified Communications Manager는 엔터프라이즈 매개 변수를 사용하여 관련 디바이스 기본값의 초기값을 설정합니다.

대부분의 엔터프라이즈 매개변수는 거의 변경할 필요가 없습니다. 변경하려는 기능을 완전히 이해했거나 Cisco TAC(기술 지원 센터)에서 변경을 지시한 경우가 아니면 엔터프라이즈 매개변수를 변경하지 마십시오.

대부분의 경우 권장된 기본 설정이 적용됩니다.

- IP 전화기에 대한 폴백 연결 모니터 지속 시간을 설정합니다.
- 모든 사용자에 대해 회사 디렉터리 검색을 허용합니다.
- 클러스터에 대해 FQDN(정규화된 디렉터리 번호)을 그리고 조직에 대해 최상위 도메인을 설정합니다.
- 비디오에 대한 Cisco Jabber 시작 조건을 설정합니다.
- (선택 사항) 네트워크에서 IPv6을 사용하는 경우, IPv6을 활성화합니다.
- (선택 사항) 원격 시스템 로그 서버 이름을 입력합니다.
- (선택 사항) 통화 추적 로그를 설정하여 구축 문제를 해결합니다.
- (선택 사항) 디펜던시 레코드를 활성화합니다.

서비스 매겨 변수 개요

서비스 매개변수를 사용하여 선택한 Unified Communications Manager 서버에서 다른 서비스들을 구성할 수 있습니다. 모든 서비스에 적용되는 엔터프라이즈 매개변수와 달리, 각 서비스는 별도의 서비스 매개변수 세트를 사용하여 구성됩니다.

서비스 매개변수를 사용하여 다음 두 가지 유형의 서비스 설정을 구성할 수 있습니다. 두 서비스 모두 Cisoc Unified Serviceability 내에서 활성화할 수 있습니다.

- 기능 서비스 - 이러한 서비스는 특정 시스템 기능을 실행하는 데 사용됩니다. 기능 서비스를 켜야만 시스템 기능을 사용할 수 있습니다.
- 네트워크 서비스 - 네트워크 서비스는 기본값으로 설정되어 있지만 문제 해결을 위해 네트워크 서비스를 중지 및 시작(또는 다시 시작)할 수 있습니다. 이러한 서비스에는 데이터베이스 및 플랫폼과 같은 시스템 구성 요소를 적절하게 작동할 수 있도록 허용해 주는 서비스가 포함됩니다.

서비스 매개변수 구성 창 내에서 ? 아이콘을 클릭하여 또는 매개변수 이름 중 하나를 클릭하여, 서비스 매개변수에 대한 서비스 매개변수 필드 설명을 볼 수 있습니다.

참고 서비스를 비활성화한 경우, Unified Communications Manager에서 업데이트된 서비슬 매개변수 값을 유지합니다. 서비스를 다시 시작할 경우, Unified Communications Manager에서 서비스 매개변수를 변경된 값으로 설정합니다.

시스템 매개변수 작업 플로우

시작하기 전에

Unified Communications Manager 노드 및 포트 설정을 설정합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	엔터프라이즈 매개변수 구성, 37 페이지.	Unified Communications Manager 노드의 초기 설정에 필요한 시스템 수준 매개변수를 구성합니다.
단계 **2**	필수 서비스 활성화, 42 페이지.	Cisoc Unified Serviceability을 사용하여 노드에서 서비스를 활성화할 수 있습니다.
단계 **3**	서비스 매개 변수 구성, 45 페이지.	클러스터의 퍼블리셔 및 가입자 노드에 대한 서비스 매개변수를 구성합니다.

엔터프라이즈 매개변수 구성

이 절차를 사용하여 구축을 위한 엔터프라이즈 수준 매개변수를 편집합니다. 이 기능을 사용하여 조직 최상위 도메인 또는 클러스터 FQDN(Fully Qualified Domain name)과 같은 엔터프라이즈 수준 설정을 설정할 수 있습니다.

참고 Cisco Unified CM 관리에서 매개변수를 편집할 경우, 새로운 설정은 Cisco Unified CM, IM and Presence 관리에서만 반영됩니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

엔터프라이즈 매개변수 창에 엔터프라이즈 매개변수 목록이 표시됩니다.

단계 **2** 매개변수 설정을 편집합니다.

매개변수 설명이 필요한 경우, GUI에서 매개변수 이름을 클릭합니다. 공통 엔터프라이즈 매개변수 목록에 대한 자세한 내용은 공통 엔터프라이즈 매개변수, 37 페이지를 참조하십시오.

단계 **3** 저장을 클릭합니다.

단계 **4** 재설정을 클릭한 다음 확인을 클릭하여 모든 디바이스를 재설정합니다.

참고 대부분의 매개변수는 설정을 저장한 이후 디바이스를 재설정해야 합니다. 디바이스를 등록한 경우, 모든 구성 변경을 완료한 다음 디바이스를 재설정하는 것이 좋습니다.

시스템의 모든 디바이스 풀을 재설정하여 모든 디바이스를 재설정할 수 있습니다.

공통 엔터프라이즈 매개변수

다음 표에는 조직 최상위 도메인 또는 클러스터 FQDN(Fully Qualified Domain Name)과 같은 엔터프라이즈 설정을 설정하는 데 사용 되는 일반 엔터프라이즈 매개변수가 나열되어 있습니다. 자세한 목록은 Cisco 통합 CM 관리의 시스템 > 엔터프라이즈 매개변수 메뉴를 사용하십시오.

표 ***2:*** 초기 설정에 대한 공통 엔터프라이즈 매개변수 ***Unified Communications Manager***

매개 변수명	설명
엔터프라이즈 매개변수	

매개 변수명	설명
연결 모니터 지속 시간	클러스터의 IP 전화기가 보조 노드에 등록되는 경우, 이 매개변수를 사용하여 기본 노드를 사용할 수 있게 된 후 IP 전화기가 기본 노드로 폴백되고 다시 등록되기 전에 대기하는 시간을 설정합니다. 이 매개변수는 특정 보안상 안전한 SRST(Survivable Remote Site Telephony) 라우터에 대한 보안상 안전한 모든 디바이스에 영향을 미칩니다. 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오. 기본값: 120초 모든 서비스를 다시 시작하여 변경 사항을 적용합니다.
CCMAdmin 매개변수	
디펜던시 레코드 활성화	이 매개변수는 문제 해결에 필요한 디펜던시 레코드를 표시하기 위해 사용합니다. 초기 시스템 설정 중에는 디펜던시 레코드 표시가 유용할 수 있습니다. 디펜던시 레코드를 표시하면 높은 CPU 사용량 스파이크가 발생하여 통화 처리에 영향을 줄 수 있습니다. 성능 문제를 방지하려면 시스템 설정이 완료된 후 이 매개변수를 비활성화해야 합니다. 사용량이 많지 않은 시간에 또는 유지 보수 기간 중에만 디펜던시 레코드를 표시하는 것이 좋습니다. 활성화된 경우, Unified Communications Manager를 통해 대부분의 설정창에서 액세스할 수 있는 관련 링크 드롭다운 목록에서 디펜던시 레코드를 선택할 수 있습니다. 기본값: 거짓
사용자 데이터 서비스 매개변수	
모든 사용자 검색 활성화	이 매개변수를 사용하면 성, 이름 또는 디렉터리 번호가 지정되지 않은 경우, 모든 사용자에 대한 회사 디렉터리를 검색할 수 있습니다. 이 매개변수는 **Cisco CallManager Self Care**(CCMUser) 창의 디렉터리 검색에도 적용됩니다. 기본값: 참
클러스터 수준 도메인 구성	
조직 최상위 도메인	이 매개변수는 조직의 최상위 도메인을 정의합니다. 예: cisco.com 최대 길이: 255자 허용되는 값: 대문자와 소문자, 숫자(0~9), 하이픈 및 점을 (도메인 레이블 구분 기호로) 사용하는 유효한 도메인입니다. 도메인 레이블은 하이픈으로 시작할 수 없습니다. 마지막 레이블은 숫자로 시작해서는 안 됩니다. 예를 들어, 이 도메인은 잘못된 cisco. 1om입니다.

매개 변수명	설명
클러스터 정규화된 도메인 이름	이 매개변수는 클러스터에 대해 하나 이상의 FQDN (정규화 된 도메인 이름)을 정의 합니다. 여러 FQDN은 공백으로 구분해야 합니다. 별표(*)를 사용하여 FQDN 내에 와일드카드를 지정합니다. 예: `cluster-1.cisco.com *. cisco.com .` 이 매개변수의 FQDN과 일치하는 호스트 부분이 있는 SIP 통화와 같은 URL을 포함하는 요청은 해당 클러스터와 연결된 디바이스로 라우팅됩니다. 최대 길이: 255자 허용되는 값: * 와일드카드를 사용하는 FQDN 또는 부분 FQDN입니다. 대문자와 소문자, 숫자(0~9), 하이픈 및 점(도메인 레이블 구분 기호) 도메인 레이블은 하이픈으로 시작할 수 없습니다. 마지막 레이블은 숫자로 시작해서는 안 됩니다. 예를 들어, 이 도메인은 잘못된 cisco. 1om입니다.
IPv6	
IPv6 사용	이 매개변수 Unified Communications Manager는 ipv6 (인터넷 프로토콜 버전 6)을 협상할 수 있는지 여부와 전화기가 ipv6 기능을 광고 하도록 허용되는지 여부를 결정 합니다. 모든 노드의 플랫폼을 포함하여 다른 모든 네트워크 구성 요소에서 IPv6을 활성화한 후에 이 매개변수를 활성화해야 합니다. 그렇지 않으면, 시스템이 계속해서 IPv4 전용 모드로 실행됩니다. 이것은 필수 필드입니다. 기본값: 거짓(IPv6가 비활성됨) IPv6 매개변수 변경 사항이 적용되로고 다음 서비스 및 IM and Presence 서비스 클러스터에서 해당 서비스를 다시 시작해야만 합니다. • Cisco CallManager • Cisco IP Voice Media Streaming App • Cisco CTIManager • Cisco Certificate Authority Proxy Function
Cisco Syslog Agent	

매개 변수명	설명
원격 Syslog 서버 이름 1	원격 Syslog 서버의 이름 또는 IP 주소를 입력합니다. 서버 이름을 지정하지 않은 경우, Cisco Unified Serviceability에서 Syslog 메시지를 전송하지 않습니다. 이 매개변수는 로그에 대한 Syslog 서버를 사용하는 경우에만 필요합니다. 최대 길이: 255자 허용되는 값: 대문자와 소문자, 숫자(0~9), 하이픈 및 점을 사용하는 유효한 원격 Sylog 서버 이름입니다. 다른 Unified Communications Manager 노드를 대상으로 지정하지 마십시오.
Cisco Jabber	
비디오로 통화 시작 절대 금지	이 매개변수는 화상 통화가 시작될 때 비디오를 보낼지 여부를 결정합니다. 비디오를 즉시 보내지 않고 화상 통화를 시작하려면 참을 선택합니다. 화상 통화 중에는 언제든지 비디오 전송을 시작하도록 선택할 수 있습니다. 이 매개변수는 모든 IM and Presence 서비스기본 설정을 재정의합니다. [거짓]으로 설정되어 있으면, IM and Presence 서비스에서의 기본 설정에 따라 화상 통화가 시작됩니다. 기본값: 거짓
SSO 및 **OAuth** 구성	
iOS에 대한 SSO 로그인 동작	이 매개변수는 Cisco Jabber에서 제어되는 모바일 디바이스 관리(MDM) 구축에서 IdP를 사용하여 인증서 기반 인증을 수행할 수 있도록 허용하기 위해 필요합니다. **iOS**에 대한 **SSO** 로그인 동작 매개 변수는 다음 옵션을 포함합니다. • 내장 브라우저 사용—이 옵션을 활성화한 경우, Cisco Jabber에서 SSO 인증을 위해 내장된 브라우저를 사용합니다. 이 옵션을 사용하여 기본 Apple Safari 브라우저로 교차 실행하지 않고 버전 9 이전의 iOS 기기에서 SSO를 사용할 수 있습니다. • 기본 브라우저 사용—이 옵션을 활성화하면 Cisco Jabber는 iOS 디바이스의 Apple Safari 프레임워크를 사용하여 MDM 구축에서 IdP(Identity Provider)를 사용하여 인증서 기반 인증을 수행합니다. 참고 기본 브라우저 사용은 내장된 브라우저 사용만큼 안전하지 않으므로 제어된 MDM 구축을 제외하고 이 옵션을 구성하지 않는 것이 좋습니다. 이것은 필수 필드입니다. 기본값: 내장 브라우저(WebView)를 사용합니다.

매개 변수명	설명
새로 고침 로그인 사용한 OAuth	이 매개변수는 Unified Communications Manager에 연결할 때 Cisco Jabber와 같은 클라이언트에서 사용하는 로그인 플로우를 제어합니다. • 활성화됨—이 옵션을 활성화하는 경우, 클라이언트는 OAuth 기반 고속 로그인 플로우를 사용하여 다시 로그인하기 위해 사용자 입력이 필요 없는 상태로 더 신속하고 간편한 로그인 환경을 제공할 수 있습니다(예: 네트워크 변경으로 인해 발생한 경우). 이 옵션을 사용하려면 Expressway 및 Unity Connection(새로 고침 로그인 플로우가 활성화되어 있는 호환 버전)과 같은 Unified Communications 솔루션의 기타 구성 요소의 지원이 필요합니다. • 비활성화됨—이 옵션을 활성화하는 경우, 기존 동작이 유지되고 이전 버전의 다른 시스템 구성 요소와 호환됩니다. 참고 Cisco Jabber를 사용한 모바일 및 원격 액세스 구축의 경우, OAuth를 지원하는 Expressway의 호환 버전만을 사용하여 이 매개변수를 활성화하는 것이 좋습니다. 비호환 버전은 Cisco Jabber 기능에 영향을 줄 수 있습니다. 지원되는 버전 및 구성 요구 사항에 대해서는 구체적인 제품 문서를 참조하십시오. 중요 이 기능은 릴리스 12.5(1)SU7 및 14SU3부터 적용할 수 있습니다. 또한 가입자 노드는 퍼블리셔와 함께 요청자 노드 데이터베이스에서 새로고침 토큰을 업데이트 할 수 있는 액세스 권한을 가지며 이는 클러스터 전체에 동일하게 복제됩니다. 이것은 필수 필드입니다. 기본값: 비활성화됨
새로 고침 토큰 자동 갱신	이 매개 변수를 사용하면 관리자는 새로 고침 토큰의 자동 갱신을 활성화하거나 비활성화할 수 있습니다. 기본적으로 이 매개 변수는 활성화되어 있습니다. 비활성화된 경우 Unified Communications Manager는 새로 고침 토큰을 자동 확장하지 않고 이전 동작을 유지합니다. 중요 이 기능은 릴리스 15 이후에 대해 적용할 수 있습니다. 이것은 필수 필드입니다. 기본값: 비활성화됨.

매개 변수명	설명
RTMT에 대해 SSO 사용	이 매개변수는 RTMT(실시간 모니터링 도구)에 대해 SAML SSO를 활성화하도록 구성되었습니다. **RTMT**에 대해 **SSO** 사용 매개변수는 다음과 같은 옵션을 포함합니다. • 참—이 옵션을 선택하는 경우, RTMT에서 SAML SSO 기반 IdP 로그인 창을 표시합니다. 참고 새로 설치를 수행할 때 **RTMT**에 대한 **SSO** 사용 매개변수의 기본값이 참으로 표시됩니다. • 거짓—이 옵션을 선택하는 경우, RTMT에서 기본 인증 로그인 창을 표시합니다. 참고 **RTMT**에 대해 **SSO** 사용 매개변수가 없는 Cisco Unified Communications Manager 버전에서 업그레이드를 수행하는 경우, 새 버전에서 이 매개변수의 기본 값은 거짓으로 표시됩니다. 이것은 필수 필드입니다. 기본값: 참

필수 서비스 활성화

이 절차를 사용하여 클러스터에서 서비스를 활성화합니다.

퍼블리셔 노드 및 가입자 노드에 대한 권장 서비스 목록은 다음 항목을 참조하십시오.

- 퍼블리셔 노드에 대한 권장 서비스, 43 페이지
- 가입자 노드를 위한 권장 서비스, 44 페이지

프로시저

단계 **1** Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.

단계 **2** 드롭다운 메뉴에서 서버를 선택하고 이동을 클릭합니다.

서비스 및 해당 서비스의 현재 상태가 표시됩니다.

단계 **3** 다음과 같이 원하는 서비스를 활성화하고 비활성화합니다.

- 서비스를 활성화하려면 활성화하려는 서비스 옆에 있는 확인란에 체크 표시합니다.
- 서비스를 비활성화하려면 비활성화하려는 서비스 옆에 있는 확인란을 선택 해제합니다.

단계 **4** 저장을 클릭합니다.

서비스 활성화를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 페이지를 새로 고쳐 상태 변경을 확인하십시오.

퍼블리셔 노드에 대한 권장 서비스

다음 표에는 비전용 TFTP 서버를 사용할 때 퍼블리셔Unified Communications Manager 노드에 대한 권장 서비스가 나와 있습니다.

표 ***3:*** 비전용 ***TFTP*** 서버 구축을 위한 권장 퍼블리셔 노드 서비스

유형	서비스 이름
CM 서비스	Cisco CallManager
	Cisco Unified Mobile Voice Access 서비스
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extended Functions
	Cisco 클러스터 간 조회 서비스
	Cisco 위치 대역폭 관리자
	Cisco TFTP
CTI 서비스	Cisco IP Manager Assistant
	Cisco WebDialer 웹 서비스
CDR 서비스	Cisco SOAP - CDROnDemand Service
	Cisco CAR Web Service
데이터베이스 및 관리 서비스	Cisco Bulk Provisioning Service
	AXL 웹 서비스
	Cisco URL Web 서비스
성능 및 모니터링 서비스	Cisco 서비스 가용성 리포터
	Cisco Certificate Authority Proxy Function
디렉터리 서비스	Cisco DirSync

팁 다음 서비스를 사용할 계획이 없는 경우, 이들 서비스를 안전하게 비활성화할 수 있습니다.

- Cisco Messaging Interface
- Cisco DHCP 모니터 서비스
- Cisco TAPS 서비스
- Cisco 디렉터리 번호 별칭 동기화
- Cisco 디렉터리 번호 별칭 SyncCisco Dialed Number Analyzer 서버
- Cisco Dialed Number Analyzer
- 셀프 프로비저닝 IVR

가입자 노드를 위한 권장 서비스

다음 표에는 비 전용 TFTP 서버를 사용할 때 Unified Communications Manager 가입자 노드를 위한 권장 서비스가 나열되어 있습니다.

팁 권장 서비스를 사용하지 않으려는 경우, 다른 서비스를 안전하게 비활성화할 수 있습니다.

표 *4:* 비 전용 ***TFTP*** 서버 구축을 위한 권장 가입자 노드 서비스

유형	서비스 이름
CM 서비스	Cisco CallManager
	Cisco IP Voice Media Streaming App
	Cisco CTIManager
	Cisco Extension Mobility
	Cisco Extended Functions
	Cisco TFTP

클러스터의 각 IM and Presence 서비스노드에서 다음 서비스를 활성화 해야만 합니다.

- Cisco SIP Proxy
- Cisco Presence 엔진
- Cisco XCP 연결 관리자
- Cisco XCP 인증 서비스

서비스 매개 변수 구성

Cisco 통합 커뮤니케이션 매니저 관리를 사용하여 노드에서 서비스 매개변수를 구성할 수 있습니다. 클러스터 수준으로 표시되는 서비스 매개변수는 클러스터의 모든 노드에 영향을 미칩니다.

주의 서비스 매개변수를 일부 변경하면 시스템 오류가 발생하는 경우가 있습니다. 변경하려는 기능에 대해 잘 아는 경우나 Cisco TAC(기술 지원 센터)에서 변경 내용을 지정한 경우 이외에는 서비스 매개변수를 변경하지 않는 것이 좋습니다.

시작하기 전에

- Unified Communications Manager 노드가 구성되어 있는지 확인하십시오.
- 서비스가 활성 상태인지 확인하십시오. 자세한 내용은 필수 서비스 활성화, 42 페이지를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 서비스를 선택합니다.

팁 서비스 매개변수 설정 창에서 **?** 아이콘을 클릭하여 서비스 매개변수 목록과 설명을 봅니다.

단계 **4** 고급을 클릭하여 숨겨진 매개변수 전체 목록을 봅니다.

단계 **5** 서비스 매개변수를 수정한 다음 저장을 클릭합니다.

창이 새로고침되고 서비스 매개변수 값이 업데이트됩니다.

기본값으로 설정 버튼을 클릭하여 모든 매개변수를 매개변수 값 필드 다음에 표시되는 제안 값으로 업데이트할 수 있습니다. 매개변수에 제안된 값이 없는 경우, 기본값으로 설정 버튼을 클릭해도 서비스 매개변수 값이 변경되지 않습니다.

클러스터 수준 서비스 매개변수 설정 보기

Cisco 통합 커뮤니케이션 매니저 Assistant와 Cisco Unified Serviceability를 사용하여 클러스터에서 노드의 서비스 상태를 볼 수 있습니다. 서비스 매개변수 설정 및 매개변수 설명을 보려면, Cisco 통합 커뮤니케이션 매니저 Assistant를 사용합니다.

프로시저

단계 **1** Cisco 통합 커뮤니케이션 매니저 Assistant를 사용하여 서비스를 표시하고 노드의 서비스 매개변수 설정을 보려면, 다음 단계를 수행합니다.

a) 시스템 > 서비스 매개변수를 선택합니다.
b) 서비스 매개변수 구성 창에서 서버 드롭다운 박스의 노드를 선택합니다.
c) 서비스 드롭다운 박스에서 서비스를 선택합니다.

선택된 노드에 적용되는 모든 매개변수가 나타납니다. 클러스터 수준 매개변수**(**일반**)** 섹션에서 나타나는 매개변수는 클러스터의 모든 노드에 적용됩니다.

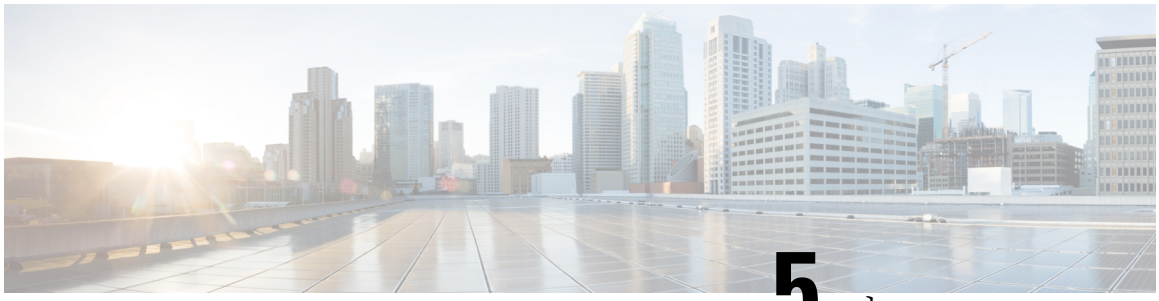
d) 서비스 매개변수 설정 창에서 **(?)** 아이콘을 클릭하여 서비스 매개변수 목록과 설명을 봅니다.

단계 **2** 클러스터의 모든 노드에 특정 서비스의 서비스 매개변수를 표시하려면, 서비스 매개변수 설정 창에서 관련 링크 드롭다운 박스의 모든 서버에 대한 매개변수를 선택한 다음, 이동을 클릭합니다.

모든 서버에 대한 매개변수 창이 표시됩니다. 목록에 나온 서버 이름이나 매개변수 값을 클릭하여 서비스 매개변수 구성 창을 열 수 있습니다.

단계 **3** 클러스터의 모든 노드에 특정 서비스의 동기화되지 않은 서비스 매개변수를 표시하려면, 모든 서버에 대한 매개변수 창에서 관련 링크 드롭다운 박스의 모든 서버에 대한 동기화되지 않은 매개변수를 선택한 다음, 이동을 클릭합니다.

모든 서버에 대한 동기화되지 않은 매개변수 창이 표시됩니다. 목록에 나온 서버 이름이나 매개변수 값을 클릭하여 서비스 매개변수 구성 창을 열 수 있습니다.



5 장

IPv6 스택 구성

IPv6 스택 개요

IPv6는 IPv4 주소가 사용하는 32 비트 대신 128 비트를 사용하는 IP 주소 지정 프로토콜입니다. IPv6는 IPv4에 비해 더 광범위한 범위의 IP 주소를 제공하여, IPv4 주소 지정과 관련된 주요 우려 사항 중의 하나인 IP 주소 소진의 위험을 크게 줄여 줍니다.

기본값으로 Cisco Unified Communications Manager는 IPv4 주소 지정을 사용하도록 구성되어 있습니다. 하지만 시스템을 구성하여 IPv6 stack을 지원하여 IPv6 전용 엔드포인트로 SIP 네트워크를 구축할 수도 있습니다. IP 주소 소진의 위험을 줄여 주는 것 이외에도 IPv6는 다음과 같은 몇 가지 혜택을 제공합니다.

- 무상태 주소 자동 설정
- 단순화된 멀티캐스팅 기능
- 단순화된 라우팅으로 라우팅 테이블에 대한 필요 최소화
- 서비스 최적화의 제공
- 더 나은 이동성 처리
- 더 우수한 프라이버시 및 보안

시스템 수준의 IPv6

IPv6 네트워크를 구축한 경우에도, 몇 가지 내부 통신을 위해 Cisco Unified Communications Manager 서버는 계속해서 IPv4를 사용합니다. 그 이유는 몇 가지 내부 시스템 부품과 애플리케이션이 IPv4만 지원하기 때문입니다. 따라서 모든 디바이스를 IPv6 전용 모드로 작동하고 있는 경우에도, 몇 가지 내부 통신을 위해 IPv4를 반드시 사용해야 하기 때문에 Cisco Unified Communications Manager 서버는 IPv6와 IPv4를 계속해서 사용합니다.

참고 SIP 디바이스를 IPv4 및 IPv6 네트워크에서 모두 작동해야 하는 경우, 두 개의 스택을 설정해야 합니다. 이 장에서 작업을 완료하여 Cisco Unified Communications Manager에서 IPv6 스택을 활성화한 다음에는 두 개의 스택에 대한 SIP 네트워크도 활성화해야 합니다. 두 개의 스택(IPv4 및 IPv6) 개요, 53 페이지를 참조하십시오.

IPv6 사전 요건

IPv6 지원을 통해 Cisco Unified Communications Manager를 구성하기 전에, IPv6을 지원하도록 다음 네트워크 서버 및 디바이스를 구성해야만 합니다. 자세한 내용은 디바이스 사용자 설명서를 참조하십시오.

- IPv6 지원을 통해 DHCP 및 DNS 서버를 프로비저닝합니다. Cisco Network Registrar 서버는 DHCP 및 DNS용 IPv6를 지원합니다.
- IPv6 지원을 통해 게이트웨이, 라우터 및 MTP와 같은 네트워크 디바이스에 대한 IOS를 구성합니다.
- IPv6을 실행하도록 TFTP 서버를 구성합니다.

IPv6 구성 작업 플로우

다음 작업을 완료하여 IPv6을 위해 시스템을 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	운영체제에서 IPv6 구성, 49 페이지	IPv6 주소를 지원하는 운영체제를 구성합니다.
단계 2	IPv6용 서버 구성, 50 페이지	IPv6 주소로 클러스터의 서버를 구성합니다.
단계 3	IPv6 사용, 50 페이지	IPv6을 위한 시스템을 활성화하는 엔터프라이즈 매개변수를 구성합니다.
단계 4	다음 중 하나를 수행합니다. • 클러스터에 대한 IP 주소 지정 기본 설정 구성, 51 페이지 • 디바이스의 IP 주소 지정 기본 설정 구성, 51 페이지	엔터프라이즈 매개변수를 구성하여 클러스터 수준 IP 주소 지정 기본 설정을 할당할 수 있습니다. 엔드포인트 그룹 마다 다른 기본 설정을 할당하려는 경우, 일반 디바이스 구성 내에서 주소 지정 기본 설정을 구성합니다.

	명령 또는 동작	목적
		IP 주소 지정 방법에서 권장하는 클러스터 설정을 구성합니다.
단계 5	서비스 다시 시작, 52 페이지	다음 네트워크 서비스를 다시 시작합니다. • Cisco CallManager • Cisco CTIManager • Cisco IP Voice Media Streaming App • Cisco Certificate Authority Proxy Function

다음에 수행할 작업

듀얼 스택 트렁크를 구성하려면 SIP 트렁크 구성에 대한 장을 참조하십시오.

SIP 디바이스에 대한 듀얼 스택을 구성하려면 구성하려는 SIP 디바이스에 대한 섹션을 참조하십시오.

운영체제에서 IPv6 구성

이 절차를 사용하여 Cisco Unified OS 관리에서 이더넷 IPv6을 설정합니다.

참고 Windows에서 [IPv6 DHCP 서버 구성]이 지원되지 않으므로 Cisco IOS IPv6 DHCP 서버를 사용합니다.

프로시저

단계 1 Cisco Unified OS 관리에서설정 > **IPv6** > 이더넷을 선택합니다.

단계 2 **IPv6** 활성화 확인란에 체크 표시합니다.

단계 3 주소 소스 드롭다운 목록 상자에서 시스템에서 IPv6 주소를 가져오는 방법을 다음과 같이 구성합니다.

- 라우터 알림—시스템에서 스테이트리스 자동 구성을 사용하여 IPv6 주소를 가져옵니다.
- **DHCP**—시스템에서 DHCP서버로부터 IPv6 주소를 가져옵니다.
- 수동 입력—IPv6 주소를 수동으로 입력하려는 경우, 이 옵션을 선택합니다.

단계 4 수동 항목을 IPv6 주소를 가져오는 방법으로 구성한 경우, 다음 필드를 완료합니다.

- **IPv6** 주소를 입력합니다. 예를 들어, **`fd62:6:96:21e:bff:fecc:2e3a`**입니다.
- **IPv6** 마스크(예:**`64`**)를 입력합니다.

단계 5 저장한 후에 시스템이 재부팅되도록 하려면 재부팅으로 업데이트 확인란에 체크 표시합니다.

단계 **6** 저장을 클릭합니다.

IPv6용 서버 구성

IPv6 주소로 클러스터의 서버를 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서버를 선택합니다.

단계 **2** **IPv6** 주소**(**듀얼 **IPv4/IPv6)** 필드에 다음 값 중 하나를 입력합니다.

- DNS가 구성되어 있고 DNS 서버에서 IPv6을 지원하는 경우, 서버 호스트네임을 입력합니다.
- 그렇지 않으면, 비링크 로컬 IPv6 주소를 입력합니다.

단계 **3** 저장을 클릭합니다.

단계 **4** 각 클러스터 노드에 대해 이들 단계를 반복합니다.

IPv6 사용

시스템에서 IPv6 지원을 설정하려면 시스템을 활성화하여 IPv6 디바이스를 지원해야만 합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** **IPv6** 활성화 엔터프라이즈 매개변수의 값을 참으로 설정합니다.

단계 **3** 저장을 클릭합니다.

다음에 수행할 작업

클러스터의 디바이스에 대한 IP 주소 지정 기본 설정을 구성합니다. 클러스터 수준 엔터프라이즈 매개변수를 통해 설정을 적용하거나, 일반 디바이스 구성을 사용하여 해당 구성을 사용하는 디바이스 그룹에 설정을 적용할 수 있습니다.

- 클러스터에 대한 IP 주소 지정 기본 설정 구성, 51 페이지
- 디바이스의 IP 주소 지정 기본 설정 구성, 51 페이지

클러스터에 대한 IP 주소 지정 기본 설정 구성

이 절차를 사용하여 엔터프라이즈 매개변수를 사용하여 IPv6에 대한 클러스터 수준 IP 주소 지정 기본 설정을 구성합니다. 재정의된 일반 디바이스 구성이 특정 트렁크 또는 디바이스에 적용되지만 않는다면, 시스템에서 이러한 설정을 모든 SIP 트렁크 및 디바이스에 적용합니다.

참고 일반 디바이스 구성의 IP 주소 기본 설정은 해당 일반 디바이스 구성을 사용하는 디바이스에 대한 클러스터 수준 엔터프라이즈 매개변수 설정을 재정의합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 미디어에 대한 **IP** 주소 지정 모드 기본 설정 값을 **IPv4** 또는 **IPv6**으로 설정합니다.

단계 **3** 신호 처리에 대한 **IP** 주소 지정 모드 기본 설정 값을 **IPv4** 또는 **IPv6**으로 설정합니다.

단계 **4** 저장을 클릭합니다.

디바이스의 IP 주소 지정 기본 설정 구성

기본 설정을 사용하여 일반 디바이스 구성을 설정하여 개별 디바이스의 IP 주소 지정 기본 설정을 구성할 수 있습니다. 트렁크, 전화기, 전화회의 브리지 및 트랜스코더와 같은 IPv6 주소 지정을 지원하는 SIP 및 SCCP 디바이스에 일반 디바이스 구성을 적용할 수 있습니다.

참고 일반 디바이스 구성의 IP 주소 기본 설정은 해당 일반 디바이스 구성을 사용하는 디바이스에 대한 클러스터 수준 엔터프라이즈 매개변수 설정을 재정의합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 디바이스 구성을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** SIP 트렁크, SIP 전화기 또는 SCCP 전화기의 경우, **IP** 주소 지정 모드 드롭다운 목록에 대한 값을 다음과 같이 선택합니다.

- **IPv4** 전용—디바이스에서 미디어 및 신호 처리에 IPv4 주소만 사용합니다.
- **IPv6** 전용—디바이스에서 미디어 및 신호 처리에 IPv6 주소만 사용합니다.
- **IPv4** 및 **IPv6(**기본값**)**—디바이스는 듀얼 스택 디바이스로 어떤 것이든 사용할 수 있는 IP 주소 유형을 사용합니다. 해당 디바이스에 두 IP 주소 유형이 모두 구성된 경우, 신호 처리를 위해 디

바이스에서 신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 설정을 사용하고 미디어를 위해 디바이스에서 미디어를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수를 사용합니다.

단계 **4** 이전 단계에서 IPv6을 구성한 경우, 신호 처리를 위한 **IP** 주소 지정 모드 드롭다운 목록에 대해 IP 주소 지정 기본 설정을 다음과 같이 구성합니다.

- **IPv4** —이중 스택 디바이스는 신호 처리를 위해 IPv4 주소를 선호합니다.
- **IPv6** —이중 스택 디바이스는 신호 처리를 위해 IPv6 주소를 선호합니다.
- 시스템 기본값 사용—신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수에 대한 설정을 사용합니다.

단계 **5** 일반 디바이스 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

IPv6 구성이 완료된 경우, 서비스 다시 시작, 52 페이지.

SIP 디바이스에서 IPv4 및 IPv6 네트워크를 동시에 모두 지원하도록 하려면 디바이스 수준에서 두 스택을 모두 지원하도록 시스템을 구성해야 합니다. 자세한 내용은 두 개의 스택(IPv4 및 IPv6) 개요, 53 페이지를 참조하십시오.

서비스 다시 시작

IPv6을 위한 시스템을 구성한 후 필수 서비스를 다시 시작합니다.

프로시저

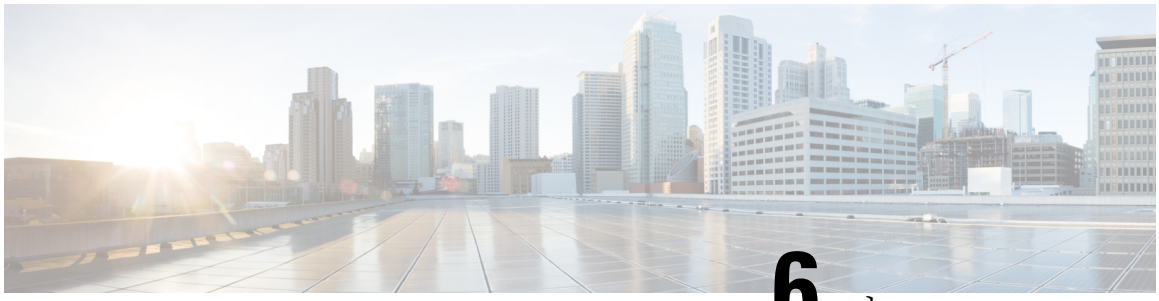
단계 **1** Cisco Unified Serviceability에 로그인하고 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 다음 각 서비스에 해당하는 확인란에 체크 표시 합니다.

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

단계 **3** 재시작을 클릭합니다.

단계 **4** 확인을 클릭합니다.



6 장

두 개의 스택 (IPv4 및 IPv6)을 구성합니다.

두 개의 스택(IPv4 및 IPv6) 개요

IPv4 및 IPv6 스택에 대해 모두 SIP 네트워크가 구성된 경우, SIP 디바이스는 다음과 같은 각 시나리오에 대한 통화를 처리할 수 있습니다.

- 통화의 모든 디바이스는 IPv4만 지원합니다.
- 통화의 모든 디바이스는 IPv6만 지원합니다.
- 통화의 모든 디바이스는 IPv4 및 IPv6 스택을 모두 지원합니다. 이 시나리오에서 시스템은 신호 처리 이벤트에 대한 신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 설정과 미디어 이벤트에 대한 미디어를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수를 위한 구성에 의해 IP 주소 유형을 판단합니다.
- 한 디바이스가 IPv4만 지원하고 다른 디바이스는 IPv6만 지원합니다. 이 시나리오에서 Unified Communications Manager는 통화 경로에 MTP를 삽입하여 두 주소 지정 유형 간의 신호 처리를 변환합니다.

SIP 디바이스 및 트렁크의 경우, AnaT(대체 네트워크 주소 유형)을 구성하여 두 스택 지원을 활성화할 수 있습니다. AnaT가 SIP 디바이스 또는 트렁크에 적용되는 경우, 디바이스 또는 트렁크에서 전송하는 SIP 신호 처리에는 IPv4 및 IPv6 주소가 모두 포함됩니다(둘 모두 사용 가능한 경우). AnaT를 통해 엔드포인트는 IPv4 전용 및 IPv6 전용 네트워크에서 원활하게 상호 운용할 수 있습니다.

두 개의 스택(IPv4 및 IPv6) 사전 요건

먼저 IPv6 스택을 지원하도록 Cisco Unified Communications Manager를 구성해야 합니다(기본값으로 IPv4가 활성화되어 있음). 이러한 작업에는 미디어 및 신호 처리를 위한 IP 주소 지정 기본 설정의 설정이 포함됩니다. 설정에 대한 자세한 내용은

두 개의 스택(IPv4 및 IPv6) 구성 작업 플로우

다음 작업을 완료하여 IPv4 및 IPv6 주소 지정을 동시에 지원하도록 SIP 디바이스 및 트렁크를 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	SIP 프로파일의 AnaT 구성, 54 페이지	IPv4 및 IPv6 스택을 동시에 지원하는 SIP 프로파일을 구성합니다.
단계 2	AnaT를 SIP 전화기에 적용, 55 페이지	AnaT 활성화 SIP 프로파일을 SIP 전화기에 적용합니다. 이렇게 하면 SIP 전화기에서 IPv4 및 IPv6 스택을 동시에 지원할 수 있습니다.
단계 3	SIP 트렁크에 AnaT 적용, 55 페이지	AnaT 활성화 SIP 프로파일을 SIP 트렁크에 적용합니다. 이렇게 하면 트렁크에서 IPv4 및 IPv6 스택을 동시에 지원할 수 있습니다.
단계 4	서비스 다시 시작, 56 페이지	IPv4 및 IPv6 스택을 동시에 지원하도록 시스템을 구성한 후, 필수 서비스를 재시작합니다.

SIP 프로파일의 AnaT 구성

이 절차를 사용하여 대체 네트워크 주소 유형(AnaT)을 지원하는 SIP 프로파일을 구성합니다. 이 프로파일을 사용하는 SIP 디바이스 및 트렁크는 IPv4 전용 및 IPv6 전용 네트워크 간에 원활하게 상호 운용될 수 있습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 다음 중 하나를 수행합니다.

a) 새로 추가를 클릭하여 새 SIP 프로파일을 만듭니다.

b) 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.

단계 3 **ANAT** 활성화 확인란을 선택합니다.

단계 4 **SIP** 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 5 저장을 클릭합니다.

이러한 디바이스가 IPv4 및 IPv6 스택을 동시에 지원하도록 하려면 SIP 프로파일을 SIP 전화기 또는 SIP 트렁크에 적용해야만 합니다.

AnaT를 SIP 전화기에 적용

이 절차를 사용하여 대체 네트워크 주소 유형(AnaT) 구성을 SIP 전화기에 적용합니다. AnaT가 활성화되면, 전화기에서 IPv4 전용 및 IPv6 전용 네트워크에서 동시에 통신할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 **2** 찾기를 클릭하고 기존 전화기를 선택합니다.

단계 **3** **SIP** 프로파일드롭다운 목록 상자에서 AnaT를 활성화한 SIP 프로파일을 선택합니다.

단계 **4** 전화기 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

SIP 트렁크에 AnaT 적용

이 절차를 사용하여 대체 네트워크 주소 유형 구성을 기존 SIP 트렁크에 적용합니다. 이렇게 하면 SIP 트렁크가 동시에 IPv4 및 IPv6 스택을 모두 지원할 수 있습니다.

참고 SIP 트렁크 구성 옵션에 대한 자세한 내용은 SIP 트렁크 구성, 94 페이지를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 **2** 찾기를 클릭하고 기존 SIP 트렁크를 선택합니다.

단계 **3** **SIP** 프로파일드롭다운 목록 상자에서 AnaT를 활성화한 SIP 프로파일을 선택합니다.

단계 **4** 트렁크 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

서비스 다시 시작

IPv4 및 IPv6 스택을 동시에 지원하도록 시스템을 구성한 후, 필수 서비스를 재시작합니다.

프로시저

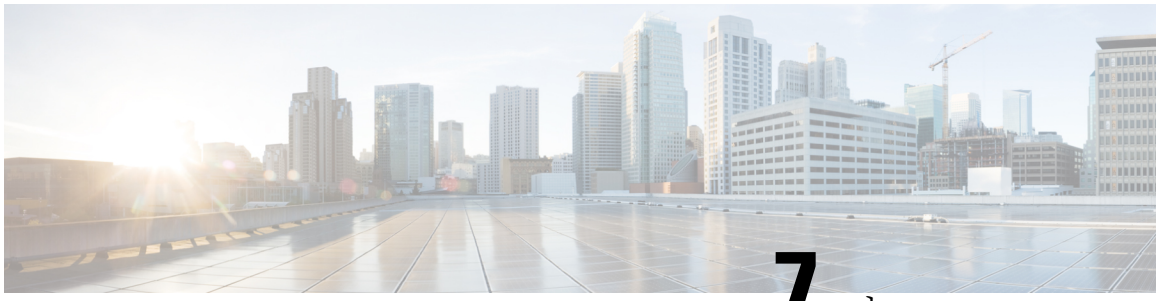
단계 **1** Cisco Unified Serviceability에 로그인하고 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 다음 각 서비스에 해당하는 확인란에 체크 표시 합니다.

- Cisco CallManager
- Cisco CTIManager
- Cisco Certificate Authority Proxy Function
- Cisco IP Voice Media Streaming App

단계 **3** 재시작을 클릭합니다.

단계 **4** 확인을 클릭합니다.



7 장

기본 보안 구성

보안 구성 정보

이 섹션에서는 Cisco Unified Communications Manager를 설정하기 위해 수행해야 하는 기본 보안 구성 작업에 대한 정보를 제공합니다.

보안 구성 작업

다음 작업을 수행하여 기본 보안 구성을 설정합니다.

클러스터에 대한 혼합 모드 활성화

이 절차를 사용하여 클러스터에서 혼합 모드를 활성화합니다.

프로시저

단계 **1** 퍼블리셔 노드의 CLI(Command Line Interface)에 로그인합니다.

단계 **2** **utils ctl set-cluster mixed-mode** CLI 명령을 실행합니다.

참고 Communications Manager가 Cisco Smart Software Manager 또는 Cisco Smart Software Manager 위성에 등록되어 있는지, 스마트 어카운트 또는 가상 어카운트에서 수신한 등록 토큰에 이 클러스터에 등록 중인 동안 내보내기 제어 기능 허용이 활성화되어 있는지 확인하십시오.

인증서 다운로드

인증서 다운로드 작업을 사용하여 인증서 사본을 가져오거나 CSR 요청을 제출할 때 인증서를 업로드할 수 있습니다.

프로시저

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

단계 **2** 검색 기준을 지정하고 찾기를 클릭합니다.

단계 **3** 필요한 파일 이름을 선택하고 다운로드를 클릭합니다.

인증서 서명 요청 생성

인증서 애플리케이션 정보, 공개 키, 조직 이름, 일반 이름, 지역 및 국가를 포함하는 암호화된 텍스트 블록인 인증서 서명 요청(CSR)을 생성합니다. 인증기관은 이 CSR을 사용하여 시스템에 대한 신뢰할 수 있는 인증서를 생성합니다.

참고 새 CSR을 생성하는 경우 기존 CSR을 덮어씁니다.

프로시저

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

단계 **2** **CSR** 생성을 클릭합니다.

단계 **3** 인증서 서명 요청 생성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 생성을 클릭합니다.

CSR(Certificate Signing Request) 다운로드

CSR을 생성 후 다운로드하고 인증기관에 제출할 준비를 합니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** **CSR** 다운로드를 클릭합니다.
단계 **3** 인증서 용도 드롭다운 목록에서 인증서 이름을 선택합니다.
단계 **4** **CSR** 다운로드를 클릭합니다.
단계 **5** (선택 사항) 프롬프트가 표시되면 저장을 클릭합니다.

타사 **CA** 루트 인증서 업로드

CA 루트 인증서를 CAPF-trust 저장소 및 Unified Communications Manager trust 저장소에 업로드하여 외부 CA를 사용하여 LSC 인증서에 서명합니다.

참고 타사 CA를 사용하여 LSC에 서명하지 않으려면 이 작업을 건너뜁니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서 용도 드롭다운 목록에서 **CAPF-trust**를 선택합니다.
단계 **4** 인증서에 대한 설명을 입력합니다. 예를 들어, 외부 **LSC** 서명 **CA**에 대한 인증서입니다.
단계 **5** 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.
단계 **6** 업로드를 클릭합니다.
단계 **7** 이 작업을 반복하여 인증서 용도에 대한 **callmanager-trust**에 인증서를 업로드합니다.

TLS 사전 요건:

최소 TLS 버전을 구성하기 전에, 네트워크 디바이스 및 애플리케이션에서 모두 TLS 버전을 지원하는지 확인하십시오. 또한 Unified Communications Manager 및 IM and Presence 서비스를 사용하여 구성하려는 TLS에 대해서도 활성화되어 있는지 확인하십시오. 다음 제품 중 하나가 구축된 경우, 최소 TLS 요구 사항을 충족하고 있는지 확인하십시오. 이러한 요구 사항을 충족되지 않은 경우, 다음과 같은 제품을 업그레이드해야 합니다.

- SCCP(Skinny Client Control Protocol) 전화회의 브리지
- 트랜스코더
- 하드웨어 MTP(미디어 터미네이션 포인트)
- SIP Gateway
- Cisco Prime Collaboration 보증
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment
- Cisco Unified Border Element(CUBE)
- Cisco Expressway
- Cisco TelePresence Conductor

전화회의 브리지, MTP(미디어 터미네이션 포인트), Xcoder, Prime Collaboration Assurance 및 Prime Collaboration Provisioning을 업그레이드할 수 없습니다.

참고 이전 버전의 Unified Communications Manager를 업그레이드하는 경우, 모든 디바이스 및 애플리케이션에서 더 높은 버전의 TLS를 지원하는지 확인하십시오. 예를 들어, Unified Communications Manager 및 IM and Presence 서비스, 릴리스 9.x는 TLS 1.0만 지원합니다.

최저 TLS 버전 설정

기본값으로 Unified Communications Manager에서는 1.0의 최소 TLS 버전을 지원합니다. 이 절차를 사용하여 Unified Communications Manager에 대해 지원되는 최소 TLS 버전을 재설정하고, IM and Presence 서비스를 1.1 또는 1.2와 같은 상위 버전으로 재설정합니다.

네트워크 디바이스 및 애플리케이션에서 구성하려는 TLS 버전을 지원하는지 확인하십시오. 자세한 내용은 TLS 사전 요건:, 60 페이지를 참조하십시오.

프로시저

단계 **1** **CLI(Command Line Interface)**에 로그인합니다.

단계 **2** 기존 TLS 버전을 확인하려면, **show tls min-version** CLI 명령을 실행합니다.

단계 **3** <*minimum*>가 TLS 버전을 나타내는 **set tls min-version**<*minimum*> CLI 명령어를 실행합니다.

예를 들어, **set tls min-version 1.2**을 실행하여 최소 TLS 버전을 1.2로 설정합니다.

단계 **4** 모든 Unified Communications Manager 및 IM and Presence 서비스 서비스 클러스터 노드에서 3단계를 수행합니다.

TLS 암호화 설정

SIP 인터페이스에 사용 가능한 가장 강력한 암호를 선택하여 더 약한 암호를 비활성화할 수 있습니다. 이 절차를 사용하여 Unified Communications Manager에서 TLS 연결 설정을 위해 지원하는 암호를 구성합니다.

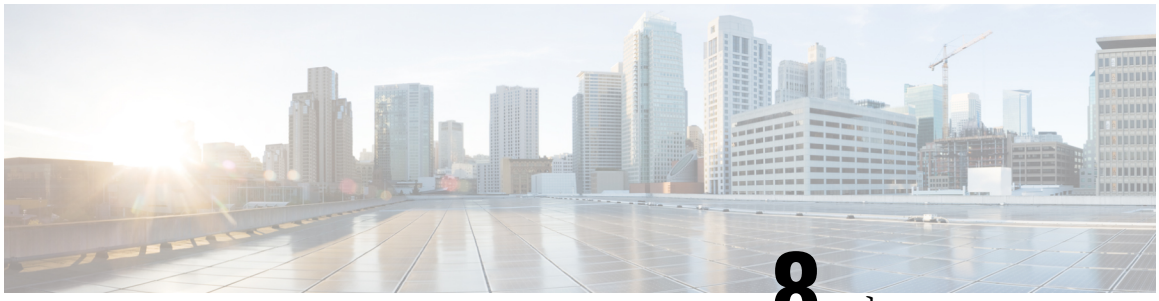
프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 보안 매개변수에서 **TLS** 암호화 엔터프라이즈 매개변수에 대한 값을 구성합니다. 사용 가능한 옵션에 대한 도움말은 엔터프라이즈 매개변수 온라인 도움말을 참조하십시오.

단계 **3** 저장을 클릭합니다.

참고 모든 TLS 암호는 클라이언트 암호화 기본 설정에 따라 조정됩니다.



8 장

SSO(Single Sign-On, 단일 인증) 구성

SAML SSO 솔루션 정보

중요 Cisco Jabber를 Cisco Webex Meeting 서버로 구축할 경우, Unified Communications Manager 및 Webex Meeting 서버는 같은 도메인에 있어야 합니다.

SAML은 관리자가 정의된 애플리케이션 중 하나에 로그인한 후에 해당 애플리케이션에 원활히 액세스하도록 해주는 XML 기반의 개방형 표준 데이터 형식입니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. 이것은 사용자를 인증하기 위해 서비스 제공자(예: Cisco Unified Communications Manager)가 사용하는 인증 프로토콜입니다. SAML은 IdP(Identity Provider)와 통신 사업자 간에 보안 인증 정보 교환을 가능하게 합니다.

SAML SSO는 SAML 2.0 프로토콜을 사용하여 Cisco 협업 솔루션에 대한 도메인 간 및 제품 간 SSO(Single Sign-On, 단일 인증)을 제공합니다. SAML 2.0을 사용하면 Cisco 애플리케이션에서 SSO를 활성화하고 Cisco 애플리케이션 및 IdP 간 페더레이션을 사용할 수 있습니다. SAML 2.0을 사용하면 Cisco 관리 사용자가 높은 보안 수준을 유지하면서 IdP 및 서비스 제공자 간에 보안 웹 도메인에 액세스하여 사용자 인증 및 인증 데이터를 교환할 수 있습니다. 기능은 다양한 애플리케이션 간에 일반 인증서 및 관련 정보를 사용하는 보안 메커니즘을 제공합니다.

SAML SSO 관리 액세스에 대한 인증은 Cisco 협업 애플리케이션에 로컬로 구성된 RBAC(역할 기반 액세스 제어)를 기반으로 합니다.

SAML SSO는 메타데이터 및 인증서를 프로비저닝 프로세스의 일부로 IdP와 서비스 제공업체 간에 교환하여 CoT(Circle of Trust)를 설정합니다. 서비스 제공자는 IdP의 사용자 정보를 신뢰하여 다양한 서비스 또는 애플리케이션에 대한 액세스를 제공합니다.

중요 서비스 제공자는 더 이상 인증과 관련되지 않습니다. SAML 2.0은 서비스 제공자와 IdP 사이의 인증을 대리합니다.

클라이언트가 IdP를 인증하고 IdP는 클라이언트에 어설션을 부여합니다. 클라이언트는 서비스 제공자에 어설션을 제공합니다. CoT가 설정되었으므로 서비스 제공자는 어설션을 신뢰하고 클라이언트에 대한 액세스를 부여합니다.

SAML SSO 구성 작업 플로우

이 작업을 완료하여 SAML SSO에 대한 Unified Communications Manager를 구성합니다.

시작하기 전에

SAML SSO 구성을 사용하려면 Unified Communications Manager를 구성하면서 동시에 ID 제공자(IdP)를 구성해야 합니다. IdP별 구성의 예는 다음을 참조하십시오.

- Active Directory Federation 서비스
- Okta
- Open Access Manager
- PingFederate

참고 위의 링크는 예로만 사용됩니다. 공식 설명서는 IdP 설명서를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 1	Cisco Unified Communications Manager에서 UC 메타데이터 내보내기, 65 페이지	신뢰 관계를 생성하려면 Unified Communications Manager와 IdP 간에 메타데이터 파일을 교환해야 합니다.
단계 2	ID 제공자(IdP)에 대한 SAML SSO 구성	다음 작업을 완료합니다. • CoT(Circle of Trust) 관계를 완료하기 위해 Unified Communications Manager에서 내보낸 UC 메타데이터 파일을 업로드합니다. • IdP에 대한 SAML SSO 구성 • IdP 메타데이터 파일을 내보냅니다. 이 파일을 Unified Communications Manager로 가져옵니다.

	명령 또는 동작	목적
단계 **3**	Cisco Unified Communications Manager에서 SAML SSO 활성화	IdP 메타데이터를 가져오고, Unified Communications Manager에서 SAML SSO를 활성화합니다.
단계 **4**	Cisco Tomcat 서비스 다시 시작, 68 페이지	SSO를 활성화하기 이전 및 이후에는 SSO가 활성화되어 있는 모든 클러스터 노드에서 Cisco Tomcat 서비스를 다시 시작해야 합니다.
단계 **5**	SAML SSO 구성 확인, 68 페이지	SAML SSO가 성공적으로 구성되었는지 확인하십시오.

Cisco Unified Communications Manager에서 UC 메타데이터 내보내기

이 절차를 사용하여 서비스 공급자(Unified Communications Manager)에서 UC 메타데이터 파일을 내보냅니다. CoT(Circle of Trust) 관계를 구축하기 위해 메타데이터 파일을 ID 제공자(IdP)로 가져옵니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **SAML SSO(Single Sign-On,** 단일 인증**)**을 선택합니다.

단계 **2** **SAML SSO(Single Sign-On,** 단일 인증**)** 창에서 **SSO** 모드 필드에 대한 옵션 중 하나를 선택합니다.

- 클러스터 수준—클러스터에 대한 단일 SAML 규약입니다.

  참고 이 옵션을 선택하는 경우 클러스터의 모든 노드에 대한 Tomcat 서버에 동일한 인증서(다중 서버 SAN 인증서)가 있는지 확인합니다.

- 노드 당—각 노드에는 별도의 SAML 계약이 있습니다.

단계 **3** **SAML SSO(Single Sign-On,** 단일 인증**)** 창에서 인증서 필드에 대한 옵션 중 하나를 선택합니다.

- 시스템에서 생성한 자체 서명 인증서 사용
- **Tomcat** 인증서 사용

단계 **4** 메타데이터 파일을 내보내려면 모든 메타데이터 내보내기를 클릭합니다.

참고 3단계에서 클러스터 수준 옵션을 선택하는 경우, 다운로드를 위해 클러스터에 대해 단일 메타데이터 XML 파일이 표시됩니다. 그러나 노드 당 옵션을 선택하는 경우, 다운로드를 위해 클러스터의 각 노드에 대해 하나의 메타데이터 XML 파일이 표시됩니다.

다음에 수행할 작업

IdP에 대한 다음 작업을 완료해야 합니다.

- Unified Communications Manager에서 내보낸 UC 메타데이터 파일 업로드
- IdP에 대한 SAML SSO 구성
- IdP 메타데이터 파일을 내보냅니다. 이 파일은 CoT(Circle of Trust) 관계를 완료하기 위해 Unified Communications Manager로 가져옵니다.

Cisco Unified Communications Manager에서 SAML SSO 활성화

이 절차를 사용하여 서비스 제공자(Unified Communications Manager)에서 SAML SSO를 활성화합니다. 이 프로세스에는 IdP 메타데이터를 Unified Communications Manager 서버로 가져오는 작업이 포함됩니다.

중요 SAML SSO를 활성화 또는 비활성화한 후에 Cisco Tomcat 서비스를 다시 시작하는 것이 좋습니다.

참고 SAML SSO를 활성화 또는 비활성화하면 Cisco CallManager 관리, Cisco Unified CM IM and Presence 관리, Cisco CallManager Serviceability 및 Unified IM and Presence Serviceability 서비스가 다시 시작됩니다.

시작하기 전에

이 절차를 완료하기 전에 다음을 확인하십시오.

- IdP에서 내보낸 메타데이터 파일이 필요합니다.
- 엔드 유저 데이터가 Cisco Unified Communications Manager 데이터베이스에 동기화되었는지 확인하십시오.
- Cisco Unified CM IM and Presence Cisco Sync Agent 서비스에서 데이터 동기화를 성공적으로 완료했는지 확인하십시오. 진단 > 시스템 문제해결 도구를 선택하여 **Cisco** 통합 **CM IM** 및 프레즌스 관리에서 이 테스트의 상태를 확인하십시오. "Sync Agent에서 관련 데이터(예: 디바이스, 사용자, 라이센싱 정보)를 동기화함" 테스트에서는 데이터 동기화가 성공적으로 완료된 경우 "테스트 통과" 결과를 표시합니다.
- 하나 이상의 LDAP 동기화된 사용자가 표준 CCM 수퍼 사용자 그룹에 추가되어 Cisco Unified 관리에 액세스할 수 있는지 확인합니다. 엔드 유저 데이터를 동기화하고 LDAP 동기화된 사용자를 그룹에 추가하는 것에 대한 자세한 내용은, Cisco Unified Communications Manager 관리 설명서의 "시스템 설정"과 "엔드 유저 설정" 섹션을 참조하십시오.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > **SAML Single Sign-On**을 선택합니다.

단계 **2** **SAML SSO** 활성화를 클릭한 다음 계속을 클릭합니다.

모든 서버 연결이 다시 시작된다는 경고 메시지가 통지됩니다.

단계 **3** 클러스터 수준 SSO 모드를 구성한 경우, 다중 서버 **tomcat** 인증서 테스트 버튼을 클릭합니다. 그렇지 않으면 이 단계를 생략할 수 있습니다.

단계 **4** 다음을 클릭합니다.

IdP 메타데이터를 가져올 수 있는 대화 상자가 표시됩니다. IdP와 서버 간 신뢰 관계를 구성하려면 먼저 IdP에서 신뢰 메타데이터 파일을 얻은 후 모든 서버로 가져와야 합니다.

단계 **5** IdP에서 내보낸 메타데이터 파일을 가져옵니다.

a) 브라우징을 통해 내보낸 IdP 메타데이터 파일을 찾아 선택합니다.
b) **IdP** 메타데이터 가져오기를 클릭합니다.
c) 다음을 클릭합니다.
d) 서버 메타데이터 다운로드 및 **IdP**에서 설치 화면에서 다음을 클릭합니다.

참고 클러스터의 노드 하나 이상에서 IdP 메타데이터 파일을 성공적으로 가져온 경우에만 다음 버튼이 활성화됩니다.

단계 **6** 다음과 같이 연결을 테스트하고 구성을 완료합니다.

a) 최종 사용자 설정 창에서 LDAP 동기화되었으며 권한 정보 목록 표에서 "표준 CCM 슈퍼 사용자"로서 권한을 갖는 사용자를 선택합니다.
b) 테스트 실행을 클릭합니다.

IdP 로그인 창이 표시됩니다.

참고 테스트가 성공하기 전까지는 SAML SSO를 활성화할 수 없습니다.

c) 유효한 사용자 이름과 암호를 입력합니다.

인증에 성공하면 다음 메시지가 표시됩니다:

`SSO 테스트가 성공했습니다.`

이 메시지가 표시되면 브라우저 창을 닫습니다.

인증이 실패하거나 인증에 60초 이상 걸리는 경우, [IdP 로그인] 창에 "로그인 실패" 메시지가 표시됩니다. [SAML Single Sign-On] 창에 다음 메시지가 표시됩니다.

`SSO 메타데이터 테스트 시간이 초과되었습니다.`

IdP에 다시 로그인을 시도하려면, 다른 사용자를 선택하고 다른 테스트를 실행합니다.

d) 마침을 클릭하여 SAML SSO 설정을 완료합니다.

SAML SSO가 활성화되고 SAML SSO에 참여하는 웹 애플리케이션이 모두 다시 시작됩니다. 웹 애플리케이션이 다시 시작되는 데 1~2분 걸릴 수 있습니다.

Cisco Tomcat 서비스 다시 시작

SAML 싱글 사인-온을 활성화 또는 비활성화하기 이전과 이후에, 싱글 사인-온을 실행 중인 모든 통합 CM 및 IM과 프레즌스 서비스 클러스터 노드에서 Cisco Tomcat 서비스를 다시 시작합니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** `utils service restart Cisco Tomcat` CLI 명령을 실행합니다.

단계 **3** SSO(Single Sign-On, 단일 인증)가 활성화된 모든 클러스터 노드에서 이 절차를 반복합니다.

SAML SSO 구성 확인

두 서비스 제공자(Unified Communications Manager) 및 IdP 모두에서 SAML SSO를 구성한 후에는 Unified Communications Manager에서 이 절차를 사용하여 구성이 작동하는지 확인합니다.

시작하기 전에

다음을 확인하십시오.

- Unified CM 관리의 **SAML Single Sign-on** 구성 창에 **IdP** 메타데이터 신뢰 파일을 성공적으로 가져왔다고 표시됩니다.
- 서비스 제공자 메타데이터 파일은 IdP에 설치됩니다.

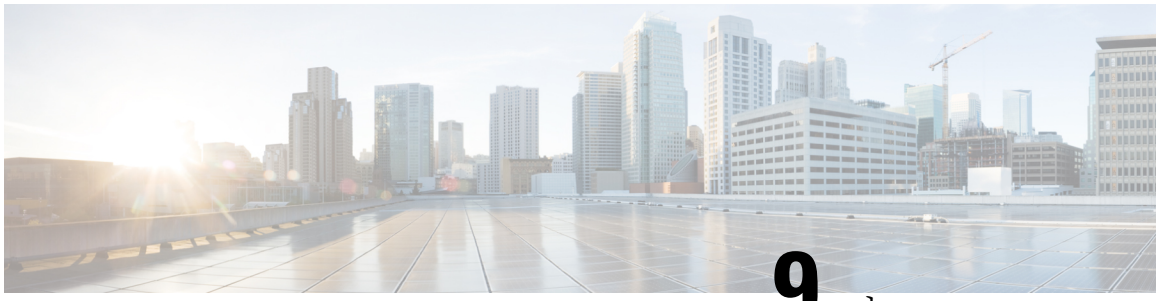
프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **SAML SSO(Single Sign-On,** 단일 인증**)**을 선택하고 **SAML Single Sign-on** 구성 창이 열리면 다음을 클릭합니다.

단계 **2** 유효한 관리자 사용자 이름 영역에서 관리 사용자를 선택하고 **SSO** 테스트 실행 **...** 버튼을 클릭합니다.

참고 테스트 사용자가 관리자 권한을 보유해야만 하며, IdP 서버에서 사용자로 추가되어 있어야만 합니다. [유효한 관리자 사용자 이름] 영역에 테스트를 실행하기 위해 가져올 수 있는 사용자 목록이 표시됩니다.

테스트에 성공하면 SAML SSO가 성공적으로 구성됩니다.



9 장

디바이스 풀에 대한 코어 설정 구성

디바이스 풀 개요

디바이스 풀은 디바이스 그룹에 대한 일반 구성 세트를 제공합니다. 디바이스 풀을 전화기, 게이트웨이, 트렁크 및 CTI 라우트 포인트와 같은 디바이스에 할당할 수 있습니다. 디바이스 풀을 생성한 후에는 각 디바이스를 개별적으로 구성하는 대신 디바이스 풀 설정을 상속하도록 디바이스를 연결할 수 있습니다.

디바이스 풀을 사용하면 날짜/시간 그룹, 지역 및 전화기 NTP 참조와 같은 위치 관련 정보를 할당하여 디바이스를 해당 위치에 따라 구성할 수 있습니다. 일반적으로 위치 당 하나씩 디바이스 풀을 필요한 만큼 생성할 수 있습니다. 그러나 디바이스 풀을 적용하여 작업 기능에 따라 구성을 적용할 수도 있습니다(예: 회사에 콜 센터가 있는 경우, 콜 센터 전화기를 하나의 디바이스 풀에 할당하고 관리 사무실 전화기를 다른 디바이스에 할당하려고 할 수 있습니다).

이 섹션에서는 다음과 같은 디바이스 풀에 대한 코어 설정을 설정하는 데 필요한 단계에 대해 설명합니다.

- NTP(Network Time Protocol)—전화기 NTP 참조를 구성하여 디바이스 풀의 SIP 디바이스에 NTP 지원을 제공합니다.
- 지역—특정 지역 통화에 대한 대역폭과 지원되는 오디오 코덱을 관리합니다.
- Cisco Unified Communications Manager 그룹—디바이스에 대한 통화 처리 리던던시 및 분산 통화 처리를 구성합니다.

NTP(Network Time Protocol) 개요

NTP를 사용하여 SIP 전화기와 같은 네트워크 디바이스에서 해당 시계를 네트워크 시간 서버 또는 네트워크 지원 시계에 동기화할 수 있습니다. NTP는 모든 네트워크 디바이스의 시간이 동일하고 감사

로그의 타임 스탬프가 네트워크 시간과 일치하도록 보장하는 데 매우 중요합니다. 청구 및 통화 세부 정보 레코드와 같은 기능은 네트워크 상에서 정확한 타임 스탬프에 의존합니다. 또한 시스템 관리자는 문제 해결을 위해 감사 로그에 정확한 타임 스탬프를 필요로 합니다. 이를 통해 서로 다른 시스템의 감사 로그를 비교할 수 있고 제기된 모든 문제에 대한 신뢰할 만한 타임라인과 이벤트 시퀀스를 생성할 수 있습니다.

설치 중에는 Unified Communications Manager 퍼블리셔 노드에 대한 NTP 서버를 설정해야 합니다. 그런 다음 가입자 노드는 퍼블리셔 노드의 시간을 동기화합니다.

최대 5대의 NTP 서버를 할당할 수 있습니다.

전화기 **NTP** 참조

- **SIP** 전화기의 경우: 전화기 NTP 참조를 구성하고 디바이스 풀을 통해 반드시 할당해야 합니다. 이러한 참조는 네트워크 시간을 제공할 수 있는 적절한 NTP 서버로 SIP 전화기를 바로 연결합니다. SIP 전화기가 프로비저닝된 "전화기 NTP 참조"에서 날짜/시간을 가져올 수 없는 경우, 전화기가 Unified Communications Manager에 등록 될 때 이 정보를 수신합니다.
- **SCCP** 전화기의 경우: SCCP 전화기에서 SCCP 신호 전달을 통해 Unified Communications Manager에서 네트워크 시간을 가져올 때 전화기 NTP 참조는 필요하지 않습니다.

인증된 **NTP**

네트워크의 NTP 부분에 추가적인 네트워크 보안을 제공하기 위해, 인증된 NTP를 구성할 수 있습니다. 인증된 NTP는 Cisco Unified Communications Manager 퍼블리셔 노드에서 구성됩니다. 가입자 노드 및 IM and Presence 노드에서 Unified CM 퍼블리셔 노드의 시간을 동기화합니다.

다음 인증 방법 중에서 선택할 수 있습니다.

- 대칭 키를 통한 인증: 이 옵션을 선택 하는 경우, 네트워크 디바이스에서 대칭 키를 사용하여 NTP 메시지를 암호화하고 인증합니다. 이 옵션은 RedHat과 같은 일부 공급업체에서 권장합니다.
- **Autokey** 키를 통한 인증**(PKI** 기반 인프라**)**: 이 옵션을 선택하는 경우, 네트워크 디바이스에서 Autokey 프로토콜을 사용하여 NTP 메시지를 암호화하고 인증합니다. 이 방법은 일반 기준 준수에 반드시 필요합니다.
- 인증 안 함: 대칭 키 또는 Autokey 방법을 통한 인증을 구성하지 않기로 선택한 경우, NTP 메시지가 인증되지 않습니다.

지역 개요

지역에서는 특정 통화에 대한 대역폭을 제한해야 할 수도 있는 다중 사이트Unified Communications Manager 구축을 위한 용량 제어 기능을 제공합니다. 예를 들어, 지역을 사용하여 WAN 링크를 통해 전송되는 통화에 대한 대역폭을 제한하면서, 내부 통화에 대해 더 높은 대역폭을 유지할 수 있습니다. 지역을 사용하여 지역내 또는 지역간 통화를 위한 최대 비트 전송률을 지역에서 제공할 수 있는 모든 대상으로 설정하여 오디오 및 화상 통화를 위한 대역폭을 제한할 수 있습니다.

또한, 시스템에서 지역을 사용하여 특정 코덱만을 지원하는 애플리케이션에 대한 오디오 코덱 우선 순위를 설정합니다. 지원되는 오디오 코덱의 우선순위 목록을 구성하고 이를 특정 지역에 대한 통화에 적용할 수 있습니다.

지역 구성 창에서 최대 오디오 비트 전송률 설정을 구성하는 경우(또는 서비스 매개변수 설정 창에서 서비스 매개변수를 사용하는 경우),이 설정이 필터의 역할을 합니다. 통화를 위해 오디오 코덱이 선택된 경우, Unified Communications Manager가 통화 레그의 양쪽에서 일치하는 코덱을 가져와 구성된 최대 오디오 비트 전송률을 초과하는 코덱을 필터링한 다음, 목록에 남아 있는 코덱 중에서 선호하는 코덱을 선택합니다.

Unified Communications Manager는 최대 2000 지역을 지원합니다.

지원 가능한 오디오 코덱

Unified Communications Manager 에서는 영상 스트림 암호화 및 다음과 같은 오디오 코덱을 지원합니다.

오디오 코덱	설명
G.711	가장 일반적으로 지원되는 코덱으로, 공중 전화망을 통해 사용됩니다.
G.722	화상 회의에 자주 사용되는 광대역 코덱입니다. G.722를 비활성화하지 않는 한 G.711을 통해 Unified Communications Manager에서 항상 기본값으로 설정됩니다.
G.722.1	24kb/s 및 32kb/s로 작동하는 낮은 복잡도의 광대역 코덱입니다. 사용하는 동안 오디오 품질은 G.722 품질과 유사하며 비트 레이트는 절반 이하입니다.
G.728	비디오 엔드포인트에서 지원하는 낮은 비트 레이트 코덱입니다.
G.729	Cisco IP Phone 7900에서 지원되며 일반적으로 WAN 링크를 통한 통화에 사용되는 8kb/s 압축의 낮은 비트 레이트 코덱입니다.
GSM	GSM(Global System for Mobile Communicaton)입니다. GSM은 GSM 무선 송수화기의 MNET 시스템이 Unified Communications Manager에서 작동할 수 있도록 활성화합니다.
L16	AAC-LD(Advanced Audio Coding-Low Delay)는 음성 및 음악을 우수한 음질로 제공하는 초광대역 오디오 코덱입니다. 이 코덱은 이전 코덱과 동등하거나 그 이상의 향상된 음질을 더 낮은 비트 레이트로 제공합니다.
AAC-LD(mpeg4-generic)	SIP 디바이스, 특히 Cisco TelePresence 시스템에 지원됩니다.
AAC-LD(MP4A-LATM)	LATM(Low-overhead MPEG-4 Audio Transport Multiplex)은 우수한 사운드를 제공하는 초광대역 오디오 코덱입니다. Tandberg 및 타사의 일부 엔드포인트를 포함하여 SIP 디바이스에 지원됩니다. 참고 AAC-LD(mpeg4-generic) 및 AAC-LD(MPA4-LATM)는 호환되지 않습니다.

오디오 코덱	설명
iSAC(Internet Speech Audio Codec)	특히 낮은 비트 레이트 및 중간 비트 레이트 애플리케이션 모두에서 광대역 음질을 낮은 지연으로 전달하기 위한 적응형 광대역 오디오 코덱입니다.
iLBC(Internet Low Bit Rate Codec)	독립적으로 인코딩된 음성 프레임으로 인해 손실이 있는 네트워크에서 정상적인 음성 품질이 저하되는 것을 감안하여 G.711과 G.729(비트 레이트 15.2kb/s 및 13.3kb/s)의 중간 정도의 오디오 품질을 제공합니다. .iLBC는 SIP, SCCP, H323, MGCP 디바이스에 지원됩니다. 참고 H.323 아웃바운드 고속 시작은 iLBC 코덱을 지원하지 않습니다.
AMR(Adaptive Multi-Rate)	GSM(WDMA, EDGE, GPRS) 기반 2.5G/3G 무선 네트워크에 필요한 표준 코덱입니다. 이 코덱은 4.75~12.2kb/s의 다양한 비트 레이트로 협대역(200-3400 Hz) 신호를 인코딩하며 유료 통화 품질은 7.4kb/s에서 시작합니다. AMR은 SIP 디바이스에만 지원됩니다.
AMR-WB(Adaptive Multi-Rate Wideband)	공식적으로 광대역으로 알려진 ITU-T 표준 음성 코덱 G.722.2로 체계화되었으며, 음성을 약 16kb/s로 코딩합니다. 이 코덱은 AMR 및 G.711과 같은 기타 협대역 음성 코덱보다 선호되는데, 이는 50~7000Hz의 더 넓은 음성 대역폭으로 더 우수한 음성 품질을 제공하기 때문입니다. AMR-WB는 SIP 디바이스에만 지원됩니다.
Opus	Opus 코덱은 대화형 음성 및 오디오 코덱으로, 특히 광범위한 대화형 오디오 애플리케이션(예: VoIP(Voice over IP), 비디오 회의, 게임 내 채팅, 실시간으로 분배되는 음악 공연)을 처리하기 위한 것입니다. 이 코덱은 협대역 낮은 비트 레이트에서 매우 높은 품질의 비트 레이트까지(6~510kb/s) 확장됩니다. 모든 SIP 디바이스에 기본값으로 Opus 코덱 지원이 활성화됩니다. **Opus Codec** 활성화됨 서비스 매개변수를 이용해 Opus 지원을 다시 구성할 수 있습니다(기본 설정은 모든 디바이스에 활성화입니다). 이 매개변수를 재구성하여 Opus 코덱 지원을 비활성화하거나 비 기록디바이스에서만 지원을 활성화할 수 있습니다. 참고 Opus는 g.722 코덱에 대한 종속성을 가집니다. 또한 SIP 디바이스에서 Opus 코덱을 사용하려면 **Advertise G.722 Codec** 엔터프라이즈 매개변수를 활성화됨으로 설정해야 합니다.

Cisco Unified CM 그룹 개요

Unified Communications Manager 그룹은 디바이스가 등록할 수 있는 최대 3개의 리던던시형 서버의 우선순위 목록입니다. 각 그룹에는 기본 노드와 최대 2개의 백업 노드가 있습니다. 노드 나열 순서에 따라 첫 번째 노드가 기본 노드, 두 번째 노드가 백업 노드, 세 번째 노드가 3차 노드가 되는 우선순서

가 결정 됩니다. 디바이스 풀 구성을 통해 Cisco Unified Communictions Manager 그룹에 디바이스를 할당할 수 있습니다.

Unified Communications Manager 그룹에서는 시스템을 위해 중요한 두 가지 기능을 제공합니다.

- 통화 처리 리던던시—디바이스를 등록하면 디바이스 풀에 할당된 그룹의 기본(첫 번째) Unified Communications Manager에 연결을 시도합니다. 기본 Unified Communications Manager를 사용할 수 없는 경우, 디바이스에서 첫 번째 백업 노드에 연결을 시도하고 해당 노드를 사용할 수 없는 경우 3차 노드에 연결을 시도합니다. 각 디바이스 풀에는 Unified Communications Manager 그룹이 하나씩 할당되어 있습니다.
- 분산 통화 처리 — 여러 디바이스 풀 및 Unified Communications Manager 그룹을 생성하여 복수의 Unified Communications Manager 전체에 걸쳐 디바이스 등록을 고르게 분산할 수 있습니다.

대부분의 시스템의 경우, 부하 분산 및 리던던시를 개선하기 위해 단일 Unified Communications Manager를 여러 그룹에 할당합니다.

통화 처리 리던던시

Unified Communications Manager 그룹에서 통화 처리 리던던시 및 복구를 다음과 같이 제공합니다.

- 페일오버—그룹의 기본 Unified Communications Manager가 실패하고 디바이스가 해당 그룹의 백업 Unified Communications Manager로 등록될 때 발생합니다.
- 폴백—실패한 기본 Unified Communications Manager가 서비스로 다시 들어올 때, 그리고 해당 그룹의 디바이스가 기본 Unified Communications Manager로 등록될 때 발생합니다.

정상 작동 중에는 그룹의 기본 Unified Communications Manager에서 해당 그룹과 연결된 등록된 모든 디바이스(예: 전화기 및 게이트웨이)에 대한 통화 처리를 제어합니다.

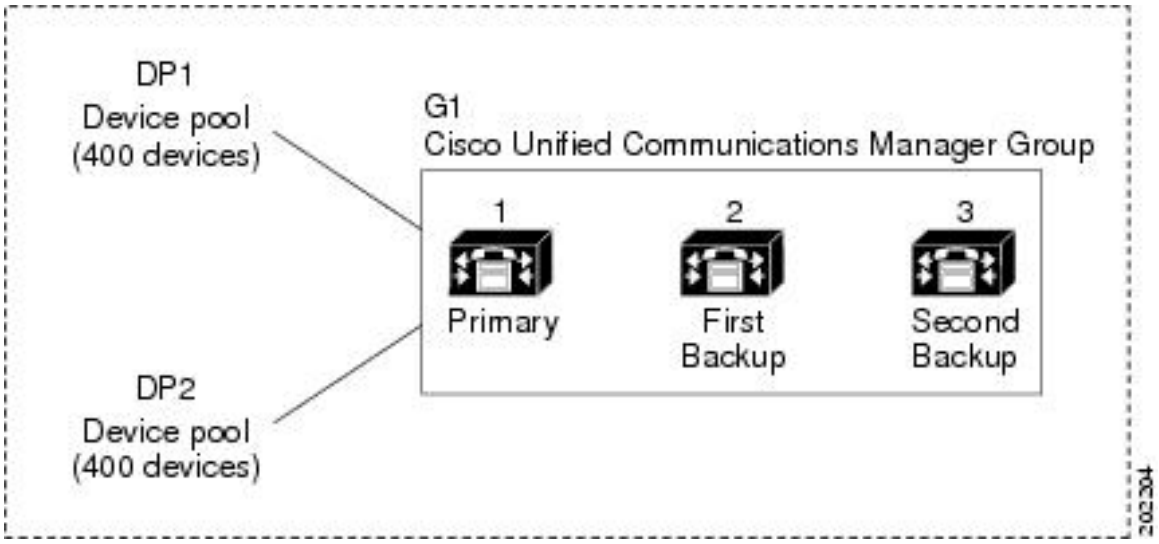
기본 Unified Communications Manager가 어떤 이유로든 실패할 경우, 그룹의 첫 번째 백업 Unified Communications Manager에서 기본 Unified Communications Manager로 등록된 디바이스를 제어합니다. 그룹에 대해 두 번째 백업 Unified Communications Manager를 지정한 경우, 기본 및 첫 번째 백업 Unified Communications Manager가 모두 실패할 경우, 해당 디바이스를 제어합니다.

실패한 기본 Unified Communications Manager가 다시 서비스로 돌아올 경우, 그룹을 다시 제어하고 해당 그룹의 디바이스가 기본 Unified Communications Manager로 자동으로 등록됩니다.

예제

예를 들어, 다음 그림에서는 800개의 디바이스를 제어하는 단일 그룹에서 세 가지 Unified Communications Manager가 포함된 간단한 시스템을 표시합니다.

그림 ***4: Unified Communications Manager*** 그룹



이 그림은 2개의 디바이스 풀, DP1 및 DP2에 할당된 Unified Communications Manager 그룹 G1을 나타냅니다. 그룹 G1의 기본 Unified Communications Manager로서 Unified Communications Manager 1은 정상 작동 시 DP1 및 DP2에서 모두 800개의 디바이스를 제어합니다. Unified Communications Manager 1이 실패하면 모든 800 장치에 대한 제어가 Unified Communications Manager 2로 전송됩니다. Unified Communications Manager 2도 실패하면 모든 800 장치에 대한 제어가 Unified Communications Manager 3으로 전송됩니다.

이 구성은 통화 처리 리던던시를 제공하지만, 예에서 나온 3개의 Unified Communications Manager 사이에서 통화 처리 부하를 효과적으로 구축하지 않습니다. Unified Communications Manager 그룹 및 디바이스 풀을 사용하여 클러스터 내에서 분산 통화 처리를 제공하는 방법에 대한 자세한 내용은, 다음 항목을 참조하십시오.

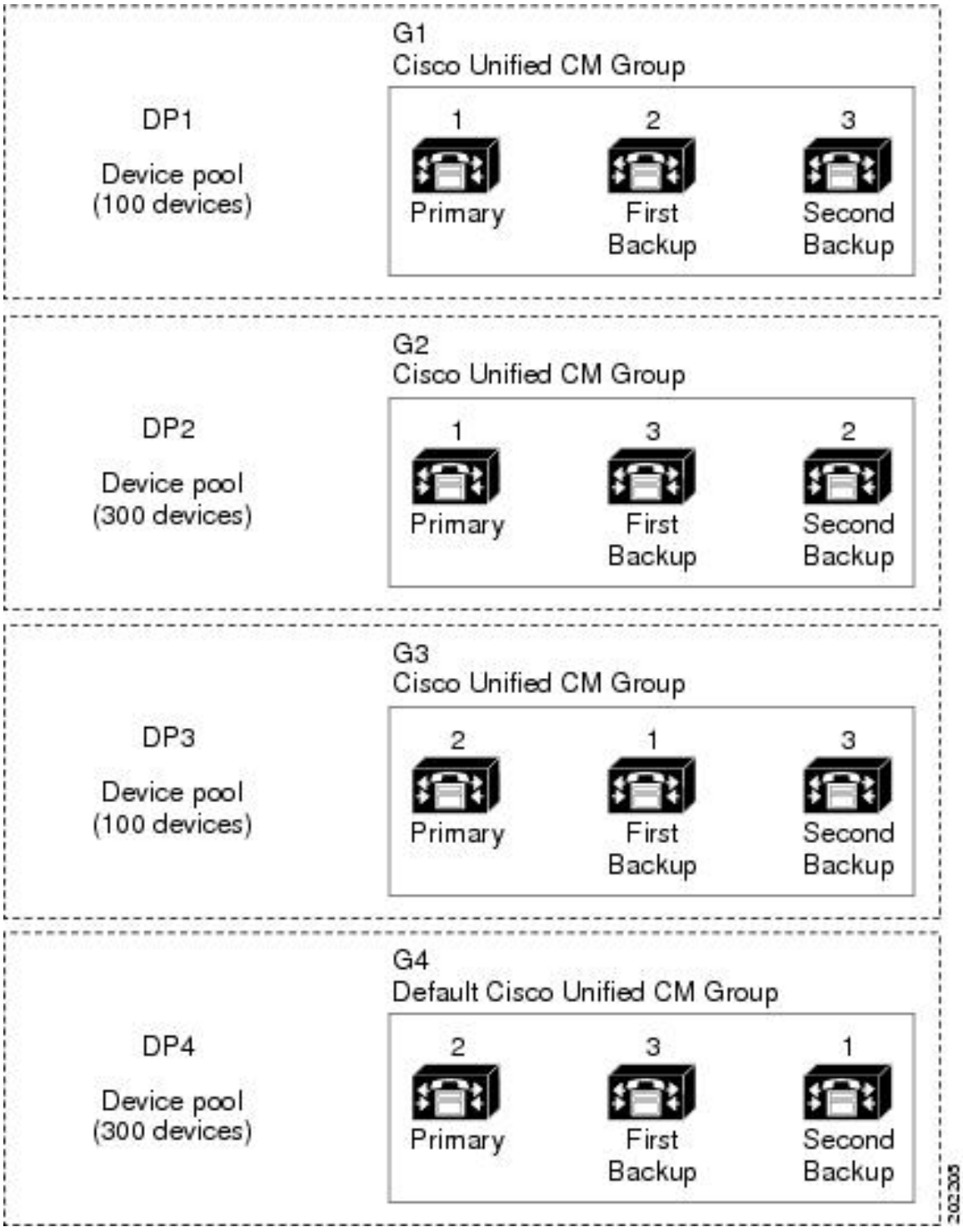
참고 빈 Unified Communications Manager그룹이 작동하지 않습니다.

분산 통화 처리

Unified Communications Manager 그룹에서 통화 처리 리던던시 및 분산 통화 처리를 모두 제공합니다. 그룹 간에 디바이스, 디바이스 풀 및 Unified Communications Manager를 분배하는 방법에 따라 시스템의 리던던시 및 로드 밸런싱 수준이 결정됩니다.

대부분의 경우, 그룹에서 하나의 Unified Communications Manager에 장애가 발생하는 경우 다른 Unified Communications Manager이 과부하되지 않도록 방지하는 방식으로 디바이스를 분산하려고 합니다. 다음 그림은 3개의 Unified Communications Manager 및 800대 디바이스의 시스템에 대한 분산 호처리 및 중복을 달성하기 위해 Unified Communications Manager 그룹과 디바이스풀을 설정하는 한 가지 가능한 방법을 보여줍니다.

그림 *5:* 분산 통화 처리와 결합된 리던던시



이전 그림은 구성되고 디바이스 풀에 할당된 Unified Communications Manager 그룹을 보여주므로, Unified Communications Manager 1은 두 개의 그룹 G1 및 G2에서 기본 컨트롤러로 사용됩니다. Unified

Communications Manager 1이 실패할 경우, 디바이스풀 DP1에서 100대의 디바이스가 Unified Communications Manager 2에 등록되고 DP2에서 300대의 디바이스가 Unified Communications Manager 3에 등록됩니다. 마찬가지로, Unified Communications Manager 2는 그룹 G3 및 G4의 기본 컨트롤러로 사용됩니다. Unified Communications Manager 2가 실패할 경우, 디바이스풀 DP3에서 100대의 디바이스가 Unified Communications Manager 1에 등록되고 DP4에서 300대의 디바이스가 Unified Communications Manager 3에 등록됩니다. Unified Communications Manager 1 및 Unified Communications Manager 2가 모두 실패할 경우, 모든 디바이스가 Unified Communications Manager 3에 등록됩니다.

디바이스 풀 사전 요건

디바이스 풀에 대해 적절히 계획을 세운 다음 디바이스 풀을 구성해야 합니다. 디바이스 풀 및 리던던트 Unified Communications Manager 그룹을 구성할 때는, 클러스터 전체에 걸쳐 등록을 고르게 분배하면서 전화기에 대한 서버 리던던시를 제공하려고 할 것입니다. 시스템 계획을 위해 사용할 수 있는 자세한 내용은 *Cisco Collaboration System Solution Reference Network Design*을 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-implementation-design-guides-list.html에서 참조하십시오.

Unified Communications Manager에 최신 표준 시간대 정보를 포함하기 위해, Unified Communications Manager를 설치한 후에 시간대 정보를 업데이트하는 COP(Cisco Options Package) 파일을 설치할 수 있습니다. 주요 시간대 변경 이벤트가 발생한 경우, https://software.cisco.com/download/navigator.html에서 최신 COP 파일을 다운로드할 수 있다는 사실에 대해 알려드립니다.

CMLocal에 대한 설정을 로컬 날짜 및 시간으로 변경합니다.

추가 디바이스 풀 구성

이 장에서는 Unified Communications Manager 그룹을 통한 전화기 NTP 참조, 지역 및 통화 처리 리던던시와 같은 코어 설정에 대해 중점적으로 설명합니다. 그러나 디바이스 풀 구성을 통해 이러한 선택적 기능 및 구성 요소를 디바이스에 적용할 수도 있습니다.

- 미디어 리소스—전화회의 브리지와 같은 미디어 리소스 및 음악 대기를 디바이스 풀의 디바이스에 할당합니다. 자세한 내용은 이 책의 미디어 리소스 구성 작업 플로우를 참조하십시오.
- SRST(Survivable Remote Site Telephony)—구축 시 AN 연결을 사용하는 경우, SRST를 구성하여 WAN이 중단되는 경우 IP 게이트웨이에서 제한된 통화 지원을 제공합니다. 자세한 내용은 이 책의 *SRST(Survivable Remote Site Telephony)* 구성 작업 플로우 섹션을 참조하십시오.
- 콜 라우팅 정보—인터클러스터 콜 라우팅 방법에 대한 자세한 내용은, 이 책의 콜 라우팅 구성 작업 플로우 섹션을 참조하십시오.
- 디바이스 모빌리티—디바이스 모빌리티 그룹을 구성하여 실제 위치에 따라 디바이스에서 설정을 가정할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서의 "디바이스 모빌리티 구성" 장을 참조하십시오.

디바이스 풀 구성 작업 플로우에 대한 코어 설정

디바이스 풀을 설정하고 이러한 디바이스 풀을 사용 하는 디바이스에 대한 지역, 전화기 NTP 참조 및 리던던시과 같은 설정을 적용 하려면 이러한 작업을 완료 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	NTP(Network Time Protocol) 구성, 77 페이지	이 작업 플로우의 작업을 완료하여 시스템에 NTP를 설정합니다. 전화기 NTP 참조를 구성하고 디바이스 풀에 할당할 수 있는 날짜/시간 그룹에 이를 적용합니다.
단계 **2**	지역 관계 구성, 83 페이지	이 작업을 완료하여 시스템에 대한 지역을 설정합니다. 최대 2000개 지역을 생성하고 지역이 제공할 수 있는 것에 따라 사용자 지정된 오디오 코덱 기본 설정 및 비트 전송률 제한과 같은 사용자 지정 설정을 구성할 수 있습니다.
단계 **3**	Cisco Unified CM 그룹 구성, 84 페이지	통화 처리 리던던시 및 로드 밸런싱에 대한 Unified Communications Manager 그룹을 구성합니다.
단계 **4**	디바이스 풀 구성, 85 페이지	시스템 디바이스에 대한 디바이스 풀을 설정합니다. 디바이스 풀에 구성한 기타 코어 설정을 적용하여 이 디바이스 풀을 사용하는 디바이스에 이러한 설정을 적용합니다.

NTP(Network Time Protocol) 구성

이러한 작업을 완료하여 시스템의 NTP(Network Time Protocol)을 구성합니다. 전화기 NTP 참조를 구성하고 디바이스 풀에 할당할 수 있는 날짜/시간 그룹에 적용합니다.

프로시저

	명령 또는 동작	목적
단계 1	NTP 서버 추가, 78 페이지	(선택 사항) NTP 서버를 추가해야 하는 겨우 이 절차를 사용합니다. NTP 서버를 최대 5개까지 추가할 수 있습니다. 참고 시스템 설치 도중에 Unified Communications Manager가 NTP 서버를 가리키도록해야 합니다. 추가 NTP 서버를 추가하려는 경우 이 절차를 사용할 수 있습니다. 그렇지 않은 경우 이 작업을 생략할 수 있습니다.
단계 2	다음 방법 중 하나를 선택하여 NTP 메시지를 인증합니다. • 대칭 키를 통해 NTP 인증 구성, 79 페이지 • Autokey를 통해 NTP 인증 구성, 79 페이지	(선택 사항) 추가 보안을 위해 인증된 NTP를 구성합니다. 대칭 키 또는 Autokey를 통해 인증을 구성할 수 있습니다. Autokey 방법은 CC(Common Criteria, 공통 평가 기준) 컴플라이언스를 위해 필요합니다.
단계 3	전화기 NTP 참조, 80 페이지	SIP 전화기의 경우, 전화기 NTP 참조를 구성하고 날짜/시간 그룹 및 디바이스 풀을 통해 적용해야 합니다.
단계 4	날짜/시간 그룹 추가, 81 페이지	시스템에 연결되어 있는 여러 디바이스의 시간대를 정의하고 해당 날짜/시간 그룹에 설정한 전화기 NTP 참조를 할당합니다.

참고 `utils ntp*` 명령 세트와 같은 NTP의 문제를 해결하고 구성하기 위해 사용할 수 있는 CLI 명령에 대한 자세한 내용은, *CLI(Command Line Interface)* 참조 가이드를 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html 에서 참조하십시오.

NTP 서버 추가

Unified Communications Manager에 NTP 서버를 추가합니다.

참고 Cisco Unified OS 관리 창의 NTP 서버 구성 창에서 NTP 서버를 설정 > **NTP** 서버에서 추가할 수도 있습니다.

프로시저

단계 **1** 명령줄 인터페이스에 로그인합니다.

단계 **2** 퍼블리셔 노드가 NTP 서버에 연결할 수 있는지 확인하려면, ip_address가 NTP 서버의 주소를 나타내는 **utils network ping <ip_address>**를 실행합니다.

단계 **3** 서버에 연결할 수 있는 경우, `utils ntp server add <ip_address>`를 실행하여 서버를 추가합니다.

단계 **4** `utils ntp restart` 명령을 사용하여 NTP 서비스를 재시작합니다.

대칭 키를 통해 **NTP** 인증 구성

대칭 키를 사용하여 네트워크에서 NTP 메시지를 인증하기 위해 이 절차를 사용합니다.

참고 SHA1 키 문자를 문자 단위로 입력해야 합니다. 현재 CLI framework는 붙여넣은 값을 읽어들이지 않습니다.

프로시저

단계 **1** Cisco Unified Communications Manager 퍼블리셔 노드에서 CLI(Command Line Interface)에 로그인합니다.

단계 **2** `utils ntp auth symmetric-key status`명령을 실행하여 현재 NTP 인증 설정 상태를 확인합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 대칭 키를 사용하여 NTP 인증을 활성화하려면 `utils ntp auth symmetric-key enable` CLI 명령을 실행합니다.
- 대칭 키를 사용하여 NTP 인증을 비활성화하려면 `utils ntp auth symmetric-key disable` CLI 명령을 실행합니다.

단계 **4** 프롬프트에 따라 NTP 서버의 키 ID 및 대칭 키를 입력합니다.

Autokey를 통해 **NTP** 인증 구성

PKI 기반 autokey를 통해 NTP 인증을 구성하려면 이 절차를 사용합니다.

참고 대칭 키를 사용하여 NTP 인증을 활성화한 경우, autokey를 사용하여 인증을 활성화하기 전에 먼저 이를 비활성화해야 합니다. 대칭 키를 사용하여 NTP 인증을 비활성화하려면 대칭 키를 통해 NTP 인증 구성, 79 페이지의 내용을 참조하십시오.

시작하기 전에

Autokey를 통해 NTP 인증을 활성화하려면 일반 기준 모드를 활성화해야 합니다. 일반 기준 모드 활성화 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서의 "FIPS 설정" 장을 참조하십시오.

프로시저

단계 **1** CLI(Command Line Interface)에 로그인합니다.

단계 **2** `Utils ntp autho auto-key status` 명령을 실행하여 현재 NTP 인증 설정을 확인하십시오.

단계 **3** 다음 중 하나를 수행합니다.

- NTP 인증을 활성화하려면 **utils ntp auth auto-key enable** CLI 명령을 실행합니다.
- NTP 인증을 비활성화 하려면 **utils ntp auth auto-key disable** CLI 명령을 실행합니다.

단계 **4** NTP 인증을 활성화 또는 비활성화하려는 NTP 서버의 번호를 입력합니다.

단계 **5** 인증을 활성화하는 경우, IFF 클라이언트 키를 입력합니다. NTP 서버에 대한 클라이언트 키를 붙여넣습니다.

전화기 **NTP** 참조

이 절차를 사용하여 SIP 전화기에 반드시 필요한 전화기 NTP 참조를 구성합니다. 날짜/시간 그룹을 통해 생성되는 NTP 참조를 디바이스 풀에 할당할 수 있습니다. 참조는 SIP 전화기에 네트워크 시간을 제공할 수 있는 해당 NTP 서버를 알려줍니다. SCCP 전화기의 경우, 이 구성이 필요하지 않습니다.

참고 Unified Communications Manager에서는 멀티캐스트 및 애니캐스트 모드를 지원하지 않습니다. 이러한 모드 중 하나를 선택할 경우, 시스템에서 기본값으로 다이렉트 브로드캐스트 모드를 사용합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 전화기 **NTP** 서버를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화기에서 사용하는 주소 지정 시스템에 따라 NTP 서버의 **IPv4** 주소 또는 **IPv6** 주소를 입력합니다.

참고 전화기 NTP 참조를 저장하려면 IPv4 주소 또는 IPv6 주소를 반드시 입력해야 합니다. IPv4 전화기와 IPv6 전화기를 모두 구축하는 경우, NTP 서버에 대한 IPv4 주소와 IPv6 주소를 모두 제공합니다.

단계 **4** 설명 필드에 템플릿에 대한 설명을 입력합니다.

단계 **5** 모드 드롭다운 목록에서, 전화기 NTP 참조에 대한 모드를 다음 옵션 목록에서 선택합니다.

- 유니캐스트—이 모드를 선택하는 경우, 전화기에서 NTP 쿼리 패킷을 해당 특정 NTP 서버로 보냅니다.
- 다이렉트 브로드캐스트—이 기본 NTP 모드를 선택하는 경우, 전화기는 NTP 서버의 날짜/시간 정보에 액세스하되 나열된 NTP 서버(첫 번째 = 기본, 두 번째 = 보조)에 우선 순위를 부여합니다.

참고 Cisco TelePresence 및 Cisco Spark 디바이스 유형은 유니캐스트 모드만 지원합니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

전화기 NTP 참조를 날짜/시간 그룹에 할당합니다. 자세한 내용은 날짜/시간 그룹 추가, 81 페이지을 참조하십시오.

날짜/시간 그룹 추가

날짜/시간 그룹을 구성하여 시스템의 표준 시간대를 정의합니다. 해당 그룹에 구성한 전화기 NTP 참조를 할당합니다. 데이터베이스에 새 날짜/시간 그룹을 추가한 이후 해당 그룹을 디바이스 풀에 할당하여 해당 디바이스 풀의 모든 디바이스에 대한 날짜 및 시간 정보를 구성할 수 있습니다.

변경 내용을 적용하려면 디바이스를 재설정해야 합니다.

팁 Cisco IP 전화기의 전 세계 분배의 경우, 각 시간대의 날짜/시간 그룹을 생성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 시간/날짜 그룹을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 이 그룹에 NTP 참조를 다음과 같이 할당합니다.

a) 전화기 **NTP** 참조 추가를 클릭합니다.
b) 전화기 **NTP** 참조 찾기 및 나열 팝업에서 찾기를 클릭하고 이전 작업에서 구성한 전화기 NTP 참조를 선택합니다.
c) 선택한 항목 추가를 클릭합니다.
d) 여러 개의 참조를 추가한 경우, 위쪽 및 아래쪽 화살표를 사용하여 우선순위를 변경합니다. 상단에 있는 참조의 우선순위가 더 높습니다.

단계 **4** 날짜/시간 그룹 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

지역 구성

다음 작업을 완료하여 시스템 풀에 대한 지역을 구성합니다. 지역간 관계를 구성하여 대역폭을 더 잘 관리합니다. 지역을 사용하여 특정 유형의 통화(예: 화상 통화)에 대한 최대 비트 전송률을 제어하고 특정 오디오 코덱의 우선순위를 지정할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	오디오 코덱 기본 설정 사용자 지정, 82 페이지	(선택 사항) 오디오 코덱에 대한 우선순위를 사용자 지정하려는 경우, 이 절차를 사용합니다. 다른 코덱에 앞서 특정 오디오 코덱의 우선순위를 지정하기 위해 이 작업을 진행하고자 할 수도 있습니다. 그렇지 않으면, 기본 오디오 코덱 목록 중 하나를 디바이스 풀에 할당할 수 있습니다.
단계 **2**	지역에 대한 클러스터 수준 기본값 구성, 83 페이지	지역에 대한 클러스터 수준 기본값을 구성합니다. 지역 구성 내에서 달리 구성하지 않는 한 모든 지역에서 이러한 기본 설정을 사용하게 됩니다.
단계 **3**	지역 관계 구성, 83 페이지	새 지역을 설정하거나 기존 지역에 대한 설정을 편집합니다. 지역 내 및 지역 간 통화 모두에 대한 관계를 구성합니다.

오디오 코덱 기본 설정 사용자 지정

이 절차를 사용하여 오디오 코덱에 대한 우선순위를 사용자 지정 합니다. 기존 목록에서 설정을 복사한 다음 새 목록 내에서 우선순위를 편집하여 새 오디오 코덱 기본 설정 목록을 생성합니다.

참고 오디오 코덱 우선순위를 사용자 지정할 필요가 없는 경우, 이 작업을 건너뛸 수 있습니다. 디바이스 풀을 구성할 때 기본 오디오 코덱 기본 설정 목록 중 하나를 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 지역 정보 > 오디오 코덱 기본 설정 목록을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 오디오 코덱 기본 설정 목록드롭다운 목록 상자에서 기존 오디오 코덱 기본 설정 목록 중 하나를 선택합니다.
선택한 목록에 대해 우선순위가 지정된 오디오 코덱의 목록이 표시됩니다.

단계 **4** 복사를 클릭합니다. 복사된 목록에서 우선순위가 지정된 코덱의 목록이 새로 생성된 목록에 적용됩니다.

단계 **5** 새 오디오 코덱 목록의 이름을 편집합니다. 예를 들면, `customizedCodecList`입니다.

단계 **6** 설명을 편집합니다.

단계 **7** 위쪽 및 아래쪽 화살표를 사용하여 코덱 목록 목록 상자에 표시되는 우선순위에 따라 코덱을 이동합니다.

단계 **8** 저장을 클릭합니다.

새 목록을 지역에 적용한 다음 해당 지역을 디바이스 풀에 적용해야만 합니다. 디바이스 풀의 모든 디바이스가 이 오디오 코덱 환경설 목록을 사용합니다.

지역에 대한 클러스터 수준 기본값 구성

이 절차를 사용하여 지역에 대한 클러스터 수준 기본값 설정을 구성합니다. 지역 구성 창 내에서 개별 지역에 대한 지역 관계를 구성하지 않는 한, 이들 설정은 모든 지역 간의 통화에 기본값으로 적용됩니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 Unified Communications Manager 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco CallManager** 서비스를 선택합니다.
서비스 매개변수 구성 창이 표시됩니다.

단계 **4** 클러스터 수준 매개변수**(**시스템 **-** 위치 및 지역**)**에서 원하는 새 서비스 매개변수 설정을 구성합니다. 서비스 매개변수 설명을 보려면, 매개변수 이름 중 하나를 클릭하 여 도움말 설명을 확인합니다.

단계 **5** 저장을 클릭합니다.

지역 관계 구성

이 절차를 사용하여 지역을 생성하고 특정 지역간 통화에 대한 사용자 지정 설정을 할당합니다. 기본 오디오 코넥과 최대 비트 전송률과 같은 설정을 편집할 수 있습니다. 예를 들어, 네트워크의 나머지 부분 보다 낮은 대역폭 용량을 갖는 지역이 있는 경우, 지역간 화상 통화에 대한 최대 세션 비트 전송률을 편집하기를 원할 수 있습니다. 이 값을 해당 지역에서 제공할 수 있는 것으로 재설정할 수 있습니다.

참고 확장성을 개선하고 시스템에서 리소스를 거의 사용하지 않도록 할 수 있도록, 가급적 서비스 매개변수 설정 창에서 기본값을 사용하는 것이 좋습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 지역 정보 > 지역을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기클릭하여 지역을 선택합니다.
- 새로 추가를 클릭하여 새 파티션을 생성합니다.
- 지역의 이름을 입력합니다. 예: 뉴욕.
- 저장을 클릭합니다.

읽기 전용 지역 관계 영역에 선택한 지역과 다른 지역 간에 설정한 모든 사용자 지정 설정이 표시됩니다.

단계 **3** 이 지역과 다른 지역(또는 지역 내 통화를 위한 동일한 지역) 간의 설정을 수정하려면 다른 지역으로의 관계 수정 영역에서 설정을 편집합니다.

a) 지역 영역에서 다른 지역(지역내 통화의 경우, 설정하려는 동일하 지역을 강조 표시합니다)을 강조 표시합니다.
b) 인접한 필드의 설정을 편집합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
c) 저장을 클릭합니다.
이제 새 설정이 지역 관계 영역에서 사용자 지정 규칙으로 표시됩니다.

참고 한 지역 내에서 지역 관계를 편집하는 경우, 다른 지역에서 설정이 자동으로 업데이트되므로 다른 지역에서 해당 설정을 반복할 필요가 없습니다. 예를 들면, 지역 설정 창에서 지역 1을 열고 사용자 정의 관계를 지역 2로 설정한다고 가정해봅시다. 그런 다음 지역 2를 열면 지역 관계 영역에 표시된 사용자 정의 관계를 볼 수 있을 것입니다.

Cisco Unified CM 그룹 구성

이 절차를 사용하여 디바이스 풀의 디바이스에 대한 통화 처리 리던던시, 로드 밸런싱 및 페일오버에 대한 Unified Communications Manager 그룹을 설정합니다.

팁 각 그룹에서 기본 서버가 서로 다른 여러 그룹 및 디바이스 풀을 설정하여 디바이스 등록이 클러스터 노드 간에 고르게 분산되는 분산 통화 처리를 제공합니다.

참고 기본 서버 그룹은 기술적인 설명이 포함되지 않아 혼동을 일으킬 수 있으므로 사용하지 마십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM** 그룹을 선택합니다.

단계 **2** 그룹에 대한 이름을 입력합니다.

참고 그룹을 다른 것들과 쉽게 구분할 수 있도록 이름에 노드의 순서를 식별하는 것에 대해 고려해야 합니다. 예를 들어, CUCM_PUB SUB입니다.

단계 **3** 자동 등록이 활성화되어 있을 때 이 Cisco Unified Communications Manager 그룹을 기본 Cisco Unified Communications Manager 그룹으로 삼으려면 **Cisco Unified Communications Manager** 그룹 자동 등록 확인란에 체크 표시합니다.

단계 **4** 사용 가능한 **Cisco Unified Communications Managers** 목록에서 이 그룹에 추가하려는 노드를 선택하고 아래쪽 화살표를 클릭하여 해당 노드를 선택합니다. 그룹에 서버를 최대 3대까지 추가할 수 있습니다.
이 그룹의 서버는 선택한 **Cisco Unified Communications Manager**] 목록 상자에 표시됩니다. 목록의 최상위 서버가 기본 서버입니다.

단계 **5** 선택한 **Cisco Unified Communications Manager** 목록 상자 옆의 화살표를 사용하여 기본 서버와 백업 서버를 변경합니다.

단계 **6** 저장을 클릭합니다.

디바이스 풀 구성

시스템 디바이스에 대한 디바이스 풀을 설정합니다. 디바이스 풀에 구성한 기타 코어 설정을 적용하여 이 디바이스 풀을 사용하는 디바이스에 이러한 설정을 적용합니다. 여러 디바이스 풀을 구성하여 구축 니즈를 충족할 수 있습니다.

시작하기 전에

SRST 구성을 할당하려면, SRST(Survivable Remote Site Telephony) 구성 작업 플로우, 118 페이지를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 디바이스 풀을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 디바이스 풀을 만듭니다.
- 찾기를 클릭하고 기존 디바이스풀을 선택합니다.

단계 **3** 디바이스 풀 이름 창에서 디바이스 풀의 이름을 입력합니다.

단계 **4** **Cisco Unified Communications Manager** 그룹 드롭다운에서, 설정한 그룹을 선택하여 통화 처리 리던던시와 로드 밸런싱을 처리합니다.

단계 **5** 날짜/시간 그룹 드롭다운에서, 설정한 그룹을 선택하여 이 디바이스 풀을 사용하는 디바이스의 날짜, 시간 및 전화기 NTP 참조를 처리합니다.

단계 **6** 지역 드롭다운 목록 박스에서 이 디바이스 풀에 적용하려는 지역을 선택합니다.

단계 **7** 미디어 리소스 그룹 목록 드롭다운에서, 이 디바이스 풀에 적용하려는 미디어 리소스가 포함된 목록을 선택합니다.

단계 **8** 이 디바이스 풀에 대한 SRST 설정을 다음과 같이 적용합니다.

a) **SRST** 참조 드롭다운에서 SRST 참조를 할당합니다.

b) 연결 모니터 지속 시간 필드의 값을 할당합니다. 이 설정은 전화기가 Unified Communications Manager에 대한 연결을 모니터링하는 시간을 정의하고 나서, SRST에서 등록 해제를 진행하고 Unified Communications Manager에 다시 등록합니다.

단계 **9** 디바이스 풀 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **10** 저장을 클릭합니다.

다음에 수행할 작업

여러 디바이스 풀을 구축 요건에 따라 구성합니다.

기본 디바이스 풀 구성 필드

표 ***5:*** 기본 디바이스 풀 구성 필드

필드	설명
디바이스 풀 이름	새 디바이스 풀의 이름을 입력합니다. 최대 50자까지 입력할 수 있으며, 영숫자, 마침표(.), 하이픈(-), 밑줄(_) 및 공백을 포함할 수 있습니다.
Cisco Unified Communications Manager 그룹	이 디바이스 풀의 디바이스에 할당할 Cisco Unified Communications Manager 그룹을 선택합니다. Cisco Unified Communications Manager 그룹에서는 최대 3개의 Unified Communications Manager 노드로 구성되는 우선 순위 목록을 지정합니다. 목록의 첫 번째 노드는 해당 그룹의 기본 노드의 역할을 하고, 그룹의 다른 구성원은 리던던시에 대한 백업 노드로 사용됩니다.
날짜/시간 그룹	이 디바이스 풀의 디바이스에 할당할 날짜/시간 그룹을 선택합니다. 날짜/시간 그룹은 표준 시간대와 날짜 및 시간의 표시 형식을 지정합니다.
지역	이 디바이스 풀에서 디바이스에 할당할 지역을 선택합니다. 지역 설정에서는 지역 내의 통신 및 다른 지역 간 통신에 사용될 수 있는 음성 및 비디오 코덱을 지정합니다.

통화 유지

Unified Communications Manager의 통화 유지 기능을 사용하면 Unified Communications Manager가 실패하거나 통화를 설정하는 디바이스와 Unified Communications Manager 간에 통신이 실패할 때에도 활성 통화가 중단되지 않도록 보장할 수 있습니다.

Unified Communications Manager에서는 확장된 Cisco Unified Communications 디바이스 세트에 대한 전체 통화 보존을 지원합니다. 이 지원에는 Cisco Unified IP Phone, FXO(Foreign Exchange Office)(비루프 시작 트렁크) 및 FXS(Foreign Exchange Station) 인터페이스를 지원하는 MGCP(Media Gateway Control Protocol) 게이트웨이, 이 보다 적게 전화회의 브리지, MTP 및 트랜스코딩 리소스 디바이스 간의 통화 보존이 포함됩니다.

고급 서비스 매개변수, Allow Peer to Perserve H.323 통화를 참으로 설정하여 H.323 통화 보존을 활성화합니다.

다음과 같은 디바이스 및 애플리케이션에서는 통화 보존을 지원합니다. 발신자와 착신자가 모두 다음 디바이스 중 하나를 통해 연결된 경우, Unified Communications Manager에서 다음과 같이 통화 보존을 유지합니다.

- Cisco Unified IP Phone
- SIP 트렁크
- 소프트웨어 전화회의 브리지
- 소프트웨어 MTP
- 하드웨어 전화회의 브리지(Cisco Catalyst 6000 8 Port Voice E1/T1 및 Services Module, Cisco Catalyst 4000 Access Gateway Module)
- 트랜스코더(Cisco Catalyst 6000 8 Port Voice E1/T1 및 Services Module, Cisco Catalyst 4000 Access Gateway Module)
- 비 IOS MGCP 게이트웨이(Catalyst 6000 24 Port FXS Analog Interface Module, Cisco DT24+, Cisco DE30+, Cisco VG200)
- Cisco IOS H.323 게이트웨이(예: Cisco 2800 series, Cisco 3800 series)
- Cisco IOS MGCP 게이트웨이(Cisco VG200, Catalyst 4000 Access Gateway Module, Cisco 2620, Cisco 3620, Cisco 3640, Cisco 3660, Cisco 3810)
- Cisco VG248 아날로그 전화기 게이트웨이

다음과 같은 디바이스 및 애플리케이션에서는 통화 보존을 지원하지 않습니다.

- 알림 디바이스
- H.323 엔드포인트(예: NetMeeting 또는 타사 H.323 엔드포인트)
- CTI 애플리케이션
- TAPI 애플리케이션

- JTAPI 애플리케이션

통화 유지 시나리오

다음 표에서는 여러 시나리오에서 통화 유지를 처리하는 방법에 대해 설명합니다.

표 *6:* 통화 유지 시나리오

시나리오	통화 유지 처리
Cisco Unified Communications Manager가 실패합니다.	Cisco Unified Communications Manager 장애로 인해 장애가 있는 Cisco Unified Communications Manager를 통해 설정된 모든 통화에 대한 통화 처리 기능이 소실됩니다. Cisco Unified Communications Manager에서는 엔드 유저가 전화를 끊을 때까지 또는 디바이스에서 미디어 연결이 해제되었음을 확인할 수 있을 때까지 해당 활성 통화를 유지합니다. 사용자는 이 장애로 인해 유지되는 통화에 대한 통화 처리 기능을 적용할 수 없습니다.
Cisco Unified Communications Manager와 디바이스 간에 통신 장애가 발생합니다.	디바이스 및 디바이스를 제어하는 Cisco Unified Communications Manager 간에 통신에 장애가 발생하는 경우, 디바이스에서 장애를 인식하고 활성 연결을 유지합니다. Cisco Unified Communications Manager에서는 통신 장애를 인식하고 통신이 두절된 디바이스의 통화와 연결된 통화 처리 엔티티를 소거합니다. Cisco Unified Communications Manager에서는 계속해서 해당 통화와 연결된 남아 있는 디바이스의 제어를 유지합니다. Cisco Unified Communications Manager에서는 엔드 유저가 전화를 끊을 때까지 또는 디바이스에서 미디어 연결이 해제되었음을 확인할 수 있을 때까지 해당 활성 통화를 유지합니다. 사용자는 이 장애로 인해 유지되는 통화에 대한 통화 처리 기능을 적용할 수 없습니다. 참고 • 페일오버의 경우, KeepAlive 타이머 내에서 Cisco Unified Communications Manager 노드를 가져오면 통화가 유지 모드인 경우에도 전화기가 현재 노드에 등록 된 상태가 유지됩니다. 이는 KeepAliver 시간이 활성 상태일 때 가능합니다. • 피어가 SIP 트렁크이고 IP 전화기와 SIP 트렁크 간에 통화가 설정되는 시나리오를 생각해 보십시오. 전화기가 Cisco Unified Communications Manager와의 통신이 끊어지면 트렁크 측에서 미디어를 변경하면 이유 헤더에 원인 값 38(네트워크 오류)이 포함된 488(허용되지 않는 미디어) 응답이 발생합니다.

시나리오	통화 유지 처리
디바이스 장애 (전화, 게이트웨이, 전화회의 브리지, 트랜스코더, MTP)	디바이스에 장애가 발생하면, 디바이스를 통해 존재하는 연결에서 스트리밍 미디어를 중지합니다. 활성 Cisco Unified Communications Manager에서 디바이스 장애를 인식하고 장애가 발생한 디바이스의 통화와 연결된 통화 처리 엔티티를 소거합니다. Cisco Unified Communications Manager에서는 해당 통화와 연결된 남아 있는 디바이스의 제어를 유지합니다. Cisco Unified Communications Manager에서는 남아 있는 엔드 유저가 전화를 끊을 때까지 또는 남아 있는 디바이스에서 미디어 연결이 해제되었음을 확인할 수 있을 때까지 남아 있는 디바이스와 연결된 활성 연결(통화)을 유지합니다.

10 장

트렁크 구성

SIP 트렁크 개요

통화 제어 신호 처리를 위해 SIP를 구축하는 경우, SIP 게이트웨이, SIP 프록시 서버, Unified Communications 애플리케이션, 전화회의 브리지, 원격 클러스터 또는 Session Management Edition과 같은 외부 디바이스에 Cisco Unified Communications Manager를 연결하는 SIP 트렁크를 구성합니다.

Cisco Unified CM 관리 내에서 **SIP** 트렁크 구성 창에 Cisco Unified Communications Manager에서 SIP 통화를 관리하기 위해 사용하는 SIP 신호 처리 구성이 포함됩니다.

IPv4 또는 IPv6 주소 지정, FQDN(Fully Qualified Domain name) 또는 단일 DNS SRV 레코드를 사용하여 SIP 트렁크에 대해 최대 16개의 서로 다른 대상 주소를 할당할 수 있습니다.

SIP 트렁크 사전 요건

SIP 트렁크를 구성하기 전에 다음을 수행합니다.

- 네트워크 토폴로지를 계획하여 트렁크 연결을 파악합니다.
- 트렁크 연결하려는 디바이스와 이러한 디바이스가 SIP를 구현하는 방법에 대해 확실하게 파악해야 합니다.
- 트렁크에 대한 디바이스 풀이 구성되었는지 확인합니다.
- 트렁크에 IPv6을 구축하는 경우, 클러스터 수준 엔터프라이즈 매개변수를 통해 또는 트렁크에 적용할 수 있는 일반 디바이스 구성을 통해 트렁크의 주소 지정 기본 설정을 구성해야 합니다.

- 트렁크를 사용하는 애플리케이션에 SIP 상호운용성 문제가 있는 경우. 기본 SIP 정규화 또는 투명성 스크립트 중 하나를 사용해야 할 수 있습니다. 기본 스크립트 중 어떤 것도 자신의 필요를 충족하지 않는 경우, 자체 스크립트를 만들 수 있습니다. 사용자 지정된 SIP 정규화 및 투명성 스크립트를 만드는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

SIP 트렁크 구성 작업 플로우

이러한 작업을 완료하여 SIP 트렁크를 설정합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	SIP 프로파일 구성, 92 페이지	SIP 트렁크에 적용되는 일반 SIP 설정을 구성합니다.
단계 **2**	SIP 트렁크 보안 프로파일 구성, 93 페이지	TLS 신호 처리 또는 다이제스트 인증과 같은 보안 설정을 사용하여 보안 프로파일을 구성합니다.
단계 **3**	SIP 트렁크 구성, 94 페이지	SIP 트렁크를 설정하고 SIP 프로파일 및 보안 프로파일을 트렁크에 적용합니다.

SIP 프로파일 구성

이 절차를 사용하여 이 프로파일을 사용하는 SIP 디바이스 및 트렁크에 할당할 수 있는 일반 SIP 설정으로 SIP 프로파일을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 프로파일을 편집할 SIP 프로파일을 선택합니다.
- 새로 추가를 클릭하여 새 프로파일을 생성합니다.

단계 **3** SIP 전화기 및 트렁크에서 IPv4 및 IPv6 스택을 지원하도록 하려면, **ANAT** 활성화 확인란을 선택합니다.

단계 **4** SDP 투명성 프로파일을 할당하여 **SDP** 투명성 프로파일 드롭다운 목록에서 SDP 상호운용성을 해결하려는 경우,

단계 **5** 정규화 또는 투명성 스크립트를 할당하여 정규화 스크립트 드롭다운 목록에서 SIP 상호운용성 문제를 해결하려는 경우, 스크립트를 선택합니다.

단계 **6** (선택 사항) Cisco Unified Border Element 내에서 통화를 라우팅하기 위해 필요할 수 있는 전역 다이얼 플랜 복제 구축에 대한 **ILS** 설정된 대상 경로 문자열 보내기 확인란에 체크 표시를 합니다.

단계 **7** **SIP** 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

SIP 트렁크 보안 프로파일 구성

다이제스트 인증 또는 TLS 신호 처리 암호화와 같은 보안 설정을 사용하여 SIP 트렁크 보안 프로파일을 구성합니다. 프로파일을 SIP 트렁크에 할당하면 트렁크는 보안 프로파일의 설정을 사용합니다.

참고 SIP 트렁크 보안 프로파일을 SIP 트렁크에 할당하지 않으면 Cisco Unified Communications Manager가 기본값으로 비보안 프로파일을 할당합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 보안 > **SIP** 트렁크 보안 프로파일을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** TLS를 사용하여 SIP 신호 처리 암호화를 활성화하려면 다음을 수행합니다.

a) 디바이스 보안 모드 드롭다운 목록에서 암호화를 선택합니다.
b) 수신 전송 유형 및 발신 전송 유형 드롭다운 목록에서 **TLS**를 선택합니다.
c) 디바이스 인증을 위해 **X.509** 제목 이름 필드에 X.509 인증서의 제목 이름을 입력합니다.
d) 수신 포트 필드에 TLS 요청을 수신하려는 포트를 입력합니다. TLS의 기본값은 5061입니다.

단계 **4** 다이제스트 인증을 활성화하려면 다음을 수행합니다.

a) 다이제스트 인증 활성화 확인란에 체크 표시합니다.
b) **Nonce** 유효 타이머 값을 입력하여 시스템에서 새 nonce를 생성하기 전에 경과해야 하는 시간(초)을 나타냅니다. 기본값은 600(10분)입니다.
c) 애플리케이션에 대한 다이제스트 인증을 활성화하려면 애플리케이션 수준 인증 활성화 확인란에 체크 표시합니다.

단계 **5** **SIP** 트렁크 보안 프로파일 설정 창에서 추가 필드를 완료합니다.필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

참고 트렁크가 설정을 사용할 수 있도록 트렁크 구성 창에서 프로파일을 트렁크에 할당해야 합니다.

SIP 트렁크 구성

이 절차를 사용하여 SIP 트렁크를 구성합니다. SIP 트렁크에 대해 최대 16개의 대상 주소를 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 트렁크 유형 드롭다운 목록에서 **SIP** 트렁크를 선택합니다.

단계 **4** 프로토콜 유형 드롭다운 목록에서 구축과 일치하는 SIP 트렁크 유형을 선택하고 다음을 클릭합니다.

- 없음**(**기본값**)**
- 통화 제어 탐색**(CCD)**
- 인터클러스터 내선 이동
- **Cisco Intercompany Media Engine**
- **IP Multimedia System Service Control**

단계 **5** (선택 사항) 일반 디바이스 구성을 이 트렁크에 적용하려는 경우, 드롭다운 목록에서 구성을 선택합니다.

단계 **6** 트렁크에서 암호화된 미디어를 허용하는 경우, **SRTP** 허용됨 확인란에 체크 표시합니다.

단계 **7** 모든 클러스터 노드에 트렁크를 활성화하려면 모든 활성 **Unified CM** 노드 확인란에 체크 표시합니다.

단계 **8** SIP 트렁크에 대한 대상 주소를 다음과 같이 구성합니다.

a) 대상 주소 텍스트 상자에 트렁크에 연결하려는 서버 또는 엔드포인트에 대한 IPv4 주소, FQDN(Fully Qualified Domain name) 또는 DNS SRV 레코드를 입력합니다.

b) 트렁크가 듀얼 스택 트렁크인 경우, 대상 주소 **IPv6** 텍스트 상자에 트렁크에 연결하려는 서버 또는 엔드포인트에 대한 IPv6 주소, FQDN(Fully Qualified Domain name) 또는 DNS SRV 레코드를 입력합니다.

c) 대상이 DNS SRV 레코드인 경우, 대상 주소가 **SRV**입니다 확인란에 체크 표시합니다.

d) 추가 대상을 추가하려면, **(+)**을 클릭합니다.

단계 **9** **SIP** 트렁크 보안 프로파일 드롭다운에서 보안 프로파일을 할당합니다. 이 옵션을 선택하지 않는 경우, 비보안 프로파일이 할당됩니다.

단계 **10** **SIP** 프로파일 드롭다운 목록에서 SIP 프로파일을 할당합니다.

단계 **11** (선택 사항) 이 SIP 트렁크에 정규화 스크립트를 할당하려면 정규화 스크립트 드롭다운 목록에서 할당하려는 스크립트를 선택합니다.

단계 **12** 트렁크 구성 창에서 모든 추가 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **13** 저장을 클릭합니다.

SIP 트렁크 상호 작용 및 제한 사항

기능	설명
동일한 대상의 여러 보안 SIP 트렁크	릴리스 12.5(1) 이후, Cisco Unified Communications Manager에서는 동일한 대상 IP 주소 및 목적지 포트 번호에 대한 여러 보안 SIP 트렁크 구성을 지원합니다. 이 기능은 다음과 같은 이점을 제공합니다. • 대역폭 최적화—무제한 대역폭이 있는 비상 통화용 라우트를 제공합니다. • 특정 지역 또는 CSS(발신 검색 공간) 구성에 기반한 선택적 라우팅
동일한 대상의 여러 비보안 SIP 트렁크	서로 다른 수신 포트가 있는 여러 비보안 SIP 트렁크가 동일한 대상 또는 포트를 가리키는 경우 통화 INVITE 중 해당 포트를 잘못 사용할 수 있습니다. 따라서 통화가 끊어집니다.
Unified Communications Manager에서 SIP 180 벨소리를 수신하면 SIP-UPDATE 메시지를 전송	SIP 트렁크는 "183 세션 진행" 후 "180 벨 울림"을 수신하면 "UPDATE" SIP 메시지를 전송하며, 제공된 "UPDATE" 값이 통화 흐름에서 지원됩니다.
BFCP를 사용한 프레젠테이션 공유	Cisco 엔드포인트에 대한 프레젠테이션 공유를 구축하는 경우, 모든 중간 SIP 트렁크의 SIP 프로파일에서 **BFCP**를 통한 프레젠테이션 공유 허용 확인란에 체크 표시가 되었는지 확인하십시오. 참고 타사 SIP 엔드포인트의 경우, 전화기 구성 창 내에서 동일한 확인란이 체크 표시되었는지도 확인하십시오.
iX 채널	iX 미디어 채널을 구축하는 경우, **iX** 애플리케이션 미디어 허용 확인란이 모든 중간 SIP 트렁크가 사용하는 SIP 프로파일에서 체크 표시되었는지 확인하십시오. 참고 암호화 iX 채널에 대한 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오.
90일 평가 라이센스	90일 평가 기간으로 실행 중에는 보안 SIP 트렁크를 구축할 수 없습니다. 보안 SIP 트렁크를 구축하려면, 시스템에서 내보내기 제어 기능 사용 제품 등록 토큰이 선택된 상태로 Smart Software Manager 계정에 등록되어 있어야만 합니다.

H.323 트렁크 개요

참고 릴리스 15부터 H.323 게이트키퍼 제어 옵션은 Unified Communications Manager에서 더 이상 사용할 수 없습니다. 따라서 위치 대역폭 관리자(LBM)와 함께 SIP 트렁크를 사용하는 것이 좋습니다.

H.323 구축을 가지고 있는 경우, H.323 트렁크는 원격 클러스터 및 게이트웨이와 같은 기타 H.323 디바이스에 대한 연결을 제공합니다. H.323 트렁크는 와이드 밴드 오디오 및 와이드 밴드 비디오를 제외하고 인터클러스터 통신을 위해 Unified Communications Manager에서 지원하는 대부분의 오디오 및 비디오 코덱을 지원합니다. H.323 트렁크는 통화 제어 신호 처리에는 H.225 프로토콜을, 미디어 신호 처리에는 H.245 프로토콜을 사용합니다.

Cisco Unified CM 관리 내에서 인터클러스터 트렁크(비 게이트키퍼에서 제어됨) 트렁크 유형 및 프로토콜 옵션을 사용하여 H.323 트렁크를 구성할 수 있습니다.

비 게이트키퍼 H.323 구축을 가지고 있는 경우, 로컬 Unified Communications Manager에서 IP WAN을 통해 통화할 수 있는 원격 클러스터의 각 디바이스 풀에 대해 별도의 인터클러스터 트렁크를 구성해야 합니다. 인터클러스터 트렁크는 원격 디바이스의 IPv4 주소 또는 호스트네임을 정적으로 지정합니다.

단일 트렁크에 대해 최대 16개의 대상 주소를 구성할 수 있습니다.

인터클러스터 트렁크

두 원격 인터클러스터에 인터클러스터 트렁크 연결을 구성하는 경우, 각 클러스터에서 인터클러스터 트렁크를 구성하고, 한 개의 트렁크에서 사용하는 대상 주소가 원격 클러스터의 트렁크에서 사용하는 통화 처리 노드와 일치하도록 트렁크 구성을 일치시켜야 합니다. 예:

- 원격 클러스터 트렁크는 모든 활성 노드에서 Run 사용—원격 클러스터 트렁크는 통화 처리 및 로드 밸런싱을 위해 모든 노드를 사용합니다. 로컬 클러스터에서 발생하는 로컬 인터클러스터 트렁크에서 원격 클러스터의 각 서버에 대한 IP 주소 또는 호스트네임을 추가합니다.
- 원격 클러스터가 모든 활성 노드에서 Run 미사용—원격 클러스터 트렁크는 통화 처리 및 로드 밸런싱ㅇ을 위해 트렁크의 디바이스 풀에 할당된 Unified Communications Manager 그룹의 서버를 사용합니다. 로컬 인터클러스터 트렁크 구성에서 원격 클러스터 트렁크의 디바이스 풀에 사용되는 Unified Communications Manager 그룹에서 각 노드의 IP 주소 또는 호스트네임을 추가해야 합니다.

보안 트렁크

H.323 트렁크에 대한 보안 신호 처리를 구성하려면 트렁크에 IPSec을 구성해야 합니다. 자세한 내용은 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오. 미디어 암호화를 허용하도록 트렁크를 구성하려면, 트렁크 구성 창에서 [SRTP 허용됨] 확인란에 체크 표시합니다.

H.323 트렁크 사전 요건

H.323 구축 토폴로지를 계획합니다. 인터클러스터 트렁크의 경우, 해당 원격 클러스터 트렁크에서 통화 처리 및 로드 밸런싱에 어떤 서버를 사용하고 있는지 확인하십시오. 원격 클러스터의 트렁크에서 사용하는 각 통화 처리 서버에 연결하도록 로컬 인터클러스터 트렁크를 구성해야 합니다.

트렁크에서 로드 밸런싱을 위한 트렁크 디바이스 풀에 할당된 Cisco Unified Communications Manager 그룹을 사용 중인 경우, 디바이스 풀 구성 작업 플로우에 대한 코어 설정, 77 페이지 섹션에서 구성을 완료합니다.

H.323 트렁크 구성

이 절차를 사용하여 H.323 구축을 위해 트렁크를 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 트렁크 유형 드롭다운 목록 상자에서 인터클러스터 트렁크**(**게이트 키퍼에서 제어하지 않음**)**를 선택합니다.

단계 **4** 프로토콜 드롭다운 목록 상자에서 인터클러스터 트렁크를 선택합니다.

단계 **5** **[**디바이스 이름**]** 텍스트 상자에 트렁크의 고유 ID를 입력합니다.

단계 **6** 디바이스 풀 드롭다운 목록 상자에서이 이 트렁크에 대해 구성한 디바이스 풀을 선택합니다.

단계 **7** 로컬 클러스터의 모든 노드를 사용하여 이 트렁크를 처리하려면 모든 활성 **Unified CM** 노드에서 실행 확인란에 체크 표시합니다.

단계 **8** 트렁크에서 암호화된 미디어를 허용하려면 **SRTP** 허용됨 확인란에 체크 표시합니다.

단계 **9** H. 235 통과를 구성하려면 **H.235** 통과 허용 확인란에 체크 표시합니다.

단계 **10** 원격 **Cisco Unified Communications Manager** 정보 섹션에서 이 트렁크가 연결된 각 원격 서버에 대한 IP 주소 또는 호스트네임을 입력합니다.

11 장

게이트웨이 구성

게이트웨이 개요

Cisco에서는 여러 음성 및 비디오 게이트웨이를 제공합니다. 게이트웨이는 Unified Communications 네트워크에서 외부 네트워크와 통신할 수 있도록 허용하는 인터페이스를 제공합니다. 일반적으로 게이트웨이는 IP 기반 Unified Communications 네트워크를 PSTN, PBX(Private Branch Exchange) 또는 아날로그 전화기 또는 팩스와 같은 레거시 디바이스와 같은 레거시 전화 인터페이스에 연결하기 위해 사용되고 있습니다. 가장 단순한 형태의 음성 게이트웨이는 IP 인터페이스와 레거시 전화 통신 인터페이스를 가지며, 게이트웨이는 두 네트워크가 통신할 수 있도록 두 네트워크 간에 메시지를 변환해 줍니다.

게이트웨이 프로토콜

대부분의 Cisco 게이트웨이에서는 여러 구축 옵션을 제공하며 여러 프로토콜 중 하나를 사용하여 구축할 수 있습니다. 구축하려는 게이트웨이에 따라 다음과 같은 통신 프로토콜을 사용하여 게이트웨이를 구성할 수 있습니다.

- MGCP(Media Gateway Control Protocol)
- SCCP(Skinny Call Control Policy)
- SIP(Session Initiation Protocol)
- H.323

VIC(벤더 인터페이스 카드)

외부 네트워크에 대한 연결 인터페이스를 제공하려면 VIC(벤더 인터페이스 카드)가 게이트웨이에 설치되어 있어야만 합니다. 대부분의 게이트웨이에서는 여러 VIC 옵션을 제공하며, 각 VIC에서는 아날로그 및 디지털 연결 모두에 대해 여러 다른 포트 및 연결 유형을 제공할 수 있습니다.

게이트웨이와 함께 제공되는 프로토콜, 카드 및 연결에 대해서는 게이트웨이 설명서를 참조하십시오.

게이트웨이 설정 사전 요건

하드웨어 설치

Cisco Unified Communications Manager에서 게이트웨이를 구성하기 전에 게이트웨이 하드웨어에 대한 다음 작업을 수행해야 합니다.

- 게이트웨이 설치 및 구성
- 게이트웨이에 VIC(벤더 인터페이스 카드)를 설치합니다.
- CLI를 사용하여 게이트웨이에서 IOS를 구성합니다.

자세한 내용은 게이트웨이와 함께 제공되는 하드웨어 및 소프트웨어 설명서를 참조하십시오.

참고 많은 게이트웨이 디바이스에 대한 기본 웹 페이지를 가져오기 위해, 해당 게이트웨이의 IP 주소를 사용할 수 있습니다. 하이퍼링크를 url = http://x.x.x.x/로 설정합니다. 여기서 x.x.x.x는 디바이스의 점형식 IP 주소입니다. 각 게이트웨이의 웹 페이지에는 디바이스 정보 및 게이트웨이의 실시간 상태가 포함되어 있습니다.

게이트웨이 구축 계획

Cisco Unified Communications Manager에서 게이트웨이를 구성하기 전에 게이트웨이에서 구성하려는 연결 유형을 적절하게 계획해야 합니다. MGCP, SIP, H.323 또는 SCCP 중 하나를 게이트웨이 프로토콜로 사용하여 많은 게이트웨이를 구성할 수 있습니다. 각 구축 유형에 대한 연결 유형은 선택하는 프로토콜과 게이트웨이에 설치되는 VIC에 따라 달라집니다. 다음 사항을 이해하고 있어야 합니다.

- 자신의 게이트웨이에서 지원하는 게이트웨이 프로토콜.
- 게이트웨이의 VIC가 지원하는 포트 연결 유형.
- 구성에 대해 계획 중인 연결 유형은 무엇입니까?
- 아날로그 연결의 경우, PSTN, 레거시 PBX 또는 레거시 디바이스에 연결하고 있습니까?
- 디지털 액세스 연결의 경우, T1 CAS 인터페이스 또는 PRI 인터페이스에 연결하고 있습니까?
- FXO 연결의 경우, 착신 통화를 어떻게 연결하시겠습니까? 착신 통화를 자동화된 IVR 또는 attendant로 연결 중입니까?

게이트웨이 구성 작업 플로우

다음 작업을 수행하여 네트워크 게이트웨이를 Unified Communications Manager에 추가해야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	구축하려는 프로토콜에 따라 다음 절차 중 하나를 수행합니다. • MGCP 게이트웨이 구성, 101 페이지 • SCCP 게이트웨이 구성, 109 페이지 • SIP 게이트웨이 구성, 112 페이지 • H.323 게이트웨이 구성, 114 페이지	Unified Communications Manager에서 게이트웨이를 구성합니다. 여러 Cisco 게이트웨이는 MGCP, SCCP, SIP 또는 H.323 중 하나를 사용하여 게이트웨이 프로토콜로 구축할 수 있습니다. 게이트웨이 설명서를 검토하여 게이트웨이가 지원하는 어떤 프로토콜이 구축에 가장 적합한지 결정합니다.
단계 **2**	게이트웨이에 대한 클러스터 수준 통화 분류 구성, 115 페이지	선택 사항. 네트워크의 게이트웨이 포트에서 수신되는 모든 통화를 내부(OnNet) 또는 외부(OffNet)으로 분류하도록 클러스터 수준 서비스 매개변수를 구성합니다.
단계 **3**	오프넷 차단 게이트웨이 전환, 116 페이지	선택 사항. Unified Communications Manager가 한 개의 외부(OffNet) 게이트웨이에서 다른 외부 게이트웨이로 통화를 전환하지 못하도록 차단하고, 오프넷간 호전환 차단 서비스 매개변수를 구성합니다.

MGCP 게이트웨이 구성

다음 작업을 수행하여 Cisco 게이트웨이를 구성하여 MGCP 구성을 사용합니다.

시작하기 전에

MGCP 게이트웨이에 대한 Unified CM 포트 연결을 확인합니다. Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM**으로 이동한 다음, 서버를 선택하고 구성된 MGCP Listen 포트 및 MGP Keep-alive 포트를 확인합니다. 대부분의 경우 기본 포트 설정을 변경할 필요가 없습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	MGCP (IOS) 게이트웨이 구성, 102 페이지	Cisco Unified CM 관리에 게이트웨이를 추가하고 게이트웨이 프로토콜로 **MGCP**를 선택합니다. 적절한 슬롯과 VIC(벤더 인터페이스 카드)를 사용하여 게이트웨이를 구성합니다.

	명령 또는 동작	목적
단계 2	게이트웨이 포트 인터페이스 구성, 103 페이지	게이트웨이에 설치된 VIC에 연결되는 디바이스의 게이트웨이 포트 인터페이스를 구성합니다. 대부분의 VIC에는 여러 포트 연결 및 옵션이 포함되어 있으므로 몇 가지 다른 포트 인터페이스 유형을 구성해야 할 수 있습니다. 팁 포트 인터페이스를 구성한 후, 관련 링크 드롭다운 목록에서 **MGCP** 구성으로 돌아가기 옵션을 선택하여 다른 포트 인터페이스를 선택하고 구성할 수 있는 게이트웨이 구성 창으로 복귀합니다.
단계 3	MGCP 게이트웨이의 디지털 액세스 T1 포트 추가, 107 페이지	선택 사항. 디지털 액세스 T1 CAS 포트 인터페이스를 구성한 경우, T1 CAS 포트를 게이트웨이에 추가합니다. 개별 방식으로 포트를 추가하거나 다양한 포트를 동시에 추가할 수 있습니다.
단계 4	게이트웨이 재설정, 108 페이지	게이트웨이를 재설정하고 나면 구성 변경 사항이 적용됩니다.

MGCP (IOS) 게이트웨이 구성

다음 절차에 따라 Unified Communications Manager에 MGCP (IOS) 게이트웨이를 추가 및 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 게이트웨이 유형 드롭다운 목록에서 게이트웨이를 선택하고 다음을 클릭합니다.

단계 4 프로토콜 드롭다운 목록에서 **MGCP**를 선택하고 다음을 선택합니다.

단계 5 구성된 슬롯, **VICs** 및 엔드포인트 영역에서 다음 단계를 수행합니다.

a) 각 모듈 드롭다운 목록에서 게이트웨이에 설치된 네트워크 인터페이스 모듈 하드웨어에 해당하는 슬롯을 선택합니다.

b) 각 하위 디바이스 드롭다운 목록에서 게이트웨이에 설치된 VIC를 선택합니다.

c) 저장을 클릭합니다.
포트 아이콘이 나타납니다. 각 포트 아이콘은 게이트웨이에서 사용 가능한 포트 인터페이스에 해당합니다. 해당 포트 아이콘을 클릭하여 포트 인터페이스를 구성할 수 있습니다.

단계 **6** 게이트웨이 구성 창에서 나머지 필드를 완료합니다. 필드에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

게이트웨이 포트 인터페이스 구성

게이트웨이에 설치된 VIC에 연결되는 디바이스의 포트 연결을 구성할 수 있습니다. 대부분의 VIC에는 여러 포트 연결 및 옵션이 포함되어 있으므로 몇 가지 다른 포트 인터페이스 유형을 구성해야 할 수 있습니다.

구성하려는 인터페이스 유형에 따라 다음 작업 중 하나를 선택합니다.

- 디지털 액세스 PRI 포트 구성, 103 페이지
- MGCP 게이트웨이의 디지털 액세스 T1 포트 구성, 104 페이지
- FXS 포트 구성, 104 페이지
- FXO 포트 구성, 105 페이지
- BRI 포트 구성, 106 페이지

디지털 액세스 **PRI** 포트 구성

MGCP (IOS) 게이트웨이의 PRI 포트 인터페이스를 구성합니다.

시작하기 전에

MGCP (IOS) 게이트웨이 구성, 102 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 찾기 를 클릭하고 PRI 포트를 구성하려는 게이트웨이를 선택합니다.

단계 **3** 구성된 슬롯**, VIC** 및 엔드포인트 영역에서 구성하려는 BRI 포트를 포함한 모듈 및 하위 디바이스를 찾고, 구성하려는 BRI 포트와 일치하는 포트 아이콘을 클릭합니다.
게이트웨이 구성 창에 BRI 포트 인터페이스가 표시됩니다.

단계 **4** 디바이스 풀 드롭다운 목록에서 디바이스 풀을 선택합니다.

단계 **5** 게이트웨이 구성 창에서 나머지 필드를 완료합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

단계 **7** (선택 사항) 게이트웨이에서 더 많은 포트 인터페이스를 구성하려면 관련 링크 드롭다운 목록에서 **MGCP** 구성으로 돌아가기를 선택하고 이동을 클릭합니다.

게이트웨이 구성 창에 게이트웨이용으로 사용할 수 있는 포트 인터페이스가 표시됩니다.

추가 포트 인터페이스 구성 작업을 완료하고 나면, 게이트웨이 재설정, 108 페이지의 내용을 참조하십시오.

MGCP 게이트웨이의 디지털 액세스 T1 포트 구성

MGCP (IOS) 게이트웨이의 디지털 액세스 T1 CAS 포트에 대한 포트 인터페이스를 구성합니다.

시작하기 전에

MGCP (IOS) 게이트웨이 구성, 102 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 찾기를 클릭하고 T1 포트를 구성하려는 게이트웨이를 선택합니다.

단계 **3** 구성된 슬롯, **VIC** 및 엔드포인트 영역에서 디지털 액세스 T1 (T1-CAS) 포트를 설정하려는 모듈과 하위 디바이스를 찾은 다음 해당 포트 아이콘을 클릭합니다.

단계 **4** 디바이스 프로토콜 드롭다운 목록에서 디지털 액세스 **T1**을 선택한 다음 다음을 클릭합니다.

단계 **5** 적절한 게이트웨이 구성 설정을 입력합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

디지털 액세스 T1 CAS 포트 인터페이스에 포트를 추가하는 방법에 대한 자세한 내용은 MGCP 게이트웨이의 디지털 액세스 T1 포트 추가, 107 페이지를 참조하십시오.

FXS 포트 구성

MGCP 게이트웨이에서 FXS(Foreign Exchange Station) 포트를 구성합니다. FXS 포트를 사용하여 게이트웨이를 POTS(기존 전화 서비스) 레거시 전화기 또는 팩스, 스피커폰, 레거시 음성 메시징 시스템 또는 IVR(대화형 음성 응답) 등의 다른 레거시 디바이스에 연결할 수 있습니다.

시작하기 전에

게이트웨이를 추가하고 나서 포트를 구성해야만 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 찾기 를 클릭하고 FXS 포트를 구성하려는 게이트웨이를 선택합니다.

단계 **3** 구성된 슬롯, **VIC** 및 엔드포인트 영역에서 구성하려는 포트에 대해 **FXS** 포트 아이콘을 클릭합니다.

포트 선택 영역이 표시됩니다.

단계 **4** 포트 유형 드롭다운 목록에서 구성하려는 연결 유형을 다음과 같이 선택합니다.

- **POTS** —이 포트를 레거시 전화기와 같은 POTS 디바이스에 연결하려면 이 옵션을 선택합니다.
- **Ground Start**—Ground Start 신호 처리를 사용하여 이 포트를 팩스, 레거시 음성 메시지 시스템 또는 IVR과 같은 무인 레거시 디바이스에 연결하려는 경우, 이 옵션을 선택합니다.
- **Loop Start**—Loop Start 신호 처리를 사용하여 이 포트를 팩스, 레거시 음성 메시지 시스템 또는 IVR과 같은 무인 레거시 디바이스에 연결하려는 경우, 이 옵션을 선택합니다.

단계 **5** 다음을 클릭합니다.
포트 구성 창에 디바이스 프로토콜로 아날로그 액세스를 사용하는 포트 인터페이스에 대한 구성이 표시됩니다.

단계 **6** 디바이스 풀 드롭다운 목록에서 디바이스 풀을 선택합니다.

단계 **7** 포트 구성 창에서 나머지 필드를 완료합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

단계 **9** (선택 사항) MGCP IOS 게이트웨이에서 더 많은 포트 인터페이스를 구성하려면, 관련 링크 드롭다운 목록에서 게이트웨이로 돌아가기를 선택하고 이동을 클릭합니다.

게이트웨이 구성 창에 게이트웨이에 대해 사용할 수 있는 포트가 표시됩니다.

추가 포트 인터페이스 구성 작업을 완료하고 나면, 게이트웨이 재설정, 108 페이지의 내용을 참조하십시오.

FXO 포트 구성

MGCP (IOS) 게이트웨이에서 FXO(이종 교환국) 포트를 구성합니다. FXO 포트를 사용하여 게이트웨이를 PSTN 또는 레거시 PBX에 연결할 수 있습니다.

참고 Unified Communications Manager 모든 loop-start 트렁크에 양성 연결 해제 감독이 없는 것으로 간주합니다. 양성 연결 해제 감독이 있는 트렁크는 ground start로 구성하므로, 서버 페일오버 중에 활성 통화를 유지할 수 있습니다.

시작하기 전에

MGCP (IOS) 게이트웨이 구성, 102 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 찾기를 클릭하고 FXO 포트를 구성하려는 게이트웨이를 선택합니다.

단계 **3** 구성된 슬롯, **VIC** 및 엔드포인트 영역에서 FXO 포트 인터페이스를 설정하고자 하는 FXO를 포함하고 있는 모듈 및 하위 디바이스를 찾고, 구성하려는 포트에 대한 포트 아이콘을 클릭합니다.

단계 **4** 포트 유형] 드롭다운 목록에서 **Ground-Start** 또는 **Loop-Start**를 선택합니다.

참고 VIC-2 FXO 포트를 구성 중인 경우, 하위 디바이스 모듈의 두 포트 모두에 대해 동일한 포트 유형을 선택해야만 합니다.

단계 **5** 디바이스 풀 드롭다운 목록에서 디바이스 풀을 선택합니다.

단계 **6** **ATTENDANT DN** 텍스트 상자에 이 포트 연결에서 모든 착신 통화를 라우팅할하려는 디렉터리 번호를 입력합니다. 예를 들어, attendant의 경우 0 또는 디렉터리 번호입니다.

단계 **7** 포트 구성 창에서 나머지 필드를 모두 완료합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

단계 **9** (선택 사항) MGCP IOS 게이트웨이에서 더 많은 포트 인터페이스를 구성하려면, 관련 링크 드롭다운 목록에서 게이트웨이로 돌아가기를 선택하고 이동을 클릭합니다.

게이트웨이 구성 창에 게이트웨이에 대해 사용할 수 있는 포트가 표시됩니다.

추가 포트 인터페이스 구성 작업을 완료하고 나면, 게이트웨이 재설정, 108 페이지의 내용을 참조하십시오.

BRI 포트 구성

MGCP (IOS) 게이트웨이에 대한 BRI 포트 인터페이스를 구성합니다.

시작하기 전에

MGCP (IOS) 게이트웨이 구성, 102 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 찾기 를 클릭하고 BRI 포트를 구성하려는 게이트웨이를 선택합니다.

단계 **3** 구성된 슬롯, **VIC** 및 엔드포인트 영역에서 BRI 포트를 사용하는 하위 디바이스를 찾고 구성하려는 포트에 대한 포트 아이콘을 클릭합니다.
게이트웨이 구성 창에 BRI 포트 인터페이스에 대한 정보가 표시됩니다.

단계 **4** 디바이스 풀 드롭다운 목록에서 디바이스 풀을 선택합니다.

단계 **5** 해당 [게이트웨이 정보] 및 [포트 정보] 설정을 입력합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

단계 **7** (선택 사항) 게이트웨이에서 더 많은 포트 인터페이스를 구성하려면 관련 링크 드롭다운 목록에서 **MGCP** 구성으로 돌아가기를 선택하고 이동을 클릭합니다.

게이트웨이 구성 창에 MGCP 게이트웨이에 사용할 수 있는 포트 인터페이스가 표시됩니다.

추가 포트 인터페이스 구성 작업을 완료하고 나면, 게이트웨이 재설정, 108 페이지의 내용을 참조하십시오.

MGCP 게이트웨이의 디지털 액세스 T1 포트 추가

MGCP 게이트웨이의 T1 디지털 액세스 포트 인터페이스에 T1 CAS 포트를 추가 및 구성합니다. 24개의 T1 CAS 포트를 추가 및 구성할 수 있습니다. 개별 방식으로 포트를 추가하거나 여러 개의 포트를 동시에 추가 및 구성할 수도 있습니다. 여러 포트를 입력하는 경우, Unified Communications Manager에서 구성을 전체 포트에 적용합니다.

시작하기 전에

MGCP 게이트웨이의 디지털 액세스 T1 포트 구성, 104 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 찾기를 클릭하고 T1 CAS 포트 인터페이스가 포함된 게이트웨이를 선택합니다.

단계 **3** 새 포트 추가를 클릭합니다.

단계 **4** 포트 유형 드롭다운 목록에서 추가하려는 포트 유형을 선택하고 다음을 클릭합니다.

단계 **5** 시작 포트 번호 및 종료 포트 번호 필드에 포트 번호를 입력하여 추가 및 구성하려는 포트 범위를 지정합니다.

예를 들어, **1**과 **10**을 입력하여 포트 1 ~ 10을 동시에 포트 인터페이스에 추가합니다.

단계 **6** 포트 방향] 드롭다운 목록에서 이 포트를 통과하는 통화의 방향을 다음과 같이 구성합니다.

- 양방향—포트에서 인바운드 및 아웃바운드 전화를 모두 허용하는 경우, 이 옵션을 선택합니다.
- 인바운드—포트에서 인바운드 통화만 허용하는 경우, 이 옵션을 선택합니다.
- 아웃바운드—포트에서 아웃바운드 통화만 허용하는 경우, 이 옵션을 선택합니다.

단계 **7** EANDM 포트의 경우, 발신자 선택 드롭다운 목록에서 발신 번호를 이 포트에 연결된 디바이스의 아웃바운드 통화에 대해 표시하려는 방법을 선택합니다.

- 발신자 - 발신 장치의 디렉토리 번호를 보냅니다.
- 첫 번째 재전송 번호—재전송 디바이스의 디렉터리 번호를 보냅니다.
- 마지막 재전송 번호 - 통화를 재전송할 마지막 장치의 디렉토리 번호를 보냅니다.
- 첫 번째 재전송 번호(외부)—외부 전화기 마스크가 적용된 상태로 첫 번째 재전송 디바이스의 디렉터리 번호를 보냅니다.
- 마지막 재전송 번호(외부)—외부 전화기 마스크가 적용된 상태로 마지막 재전송 디바이스의 디렉터리 번호를 보냅니다.

단계 **8** 저장을 클릭합니다.

단계 **9** MGCP 게이트웨이에서 더 많은 포트를 구성하려는 경우, 관련 링크에서 게이트웨이로 돌아가기를 선택하고 이동을 클릭합니다. 디지털 액세스 T1 포트 인터페이스가 나타나면 다음 단계 중 하나를 수행합니다.

- 이 포트 인터페이스에 추가 디지털 액세스 T1 CAS 포트를 추가하려는 경우, 이 절차의 3단계(새 포트 추가)로 돌아갑니다.
- 게이트웨이에서 더 많은 포트 인터페이스를 구성하려는 경우, 관련 링크에서 **MGCP** 구성으로 돌아가기를 선택하고 이동을 클릭합니다. 게이트웨이 구성 창에 게이트웨이 하위 디바이스 모듈에 대해 사용 가능한 포트가 표시됩니다.
- 추가 포트 인터페이스 구성 작업을 완료하고 나면, 게이트웨이 재설정, 108 페이지의 내용을 참조하십시오.

게이트웨이 재설정

구성 변경 사항을 적용하려면 대부분의 게이트웨이를 재설정해야 합니다. 필요한 모든 게이트웨이 구성을 완료한 다음 재설정을 수행하는 것이 좋습니다.

참고 H.323 게이트웨이를 재설정하면 Cisco Unified Communications Manager에서 로드한 구성만 다시 초기화될 뿐, 게이트웨이가 물리적으로 다시 시작되거나 재설정되지는 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 찾기를 클릭하고 게이트웨이를 선택합니다.

단계 **3** 재설정하려는 게이트웨이 옆의 확인란을 클릭하고 선택한 항목 재설정을 클릭합니다. 디바이스 추가 대화 상자가 나타납니다. 다음 작업 중 하나를 수행합니다.

단계 **4** 재설정을 클릭합니다.

MGCP 발신자-**ID** 제한

FROM 헤더에 수신 SIP 요청에 대한 특수 문자가 포함되어 있으면 SIP-MGCP/323 통화 흐름에 영향을 주고 시스템이 통화 연결을 끊거나 문제를 표시합니다. 따라서 요청이 Unified Communications Manager에 도달하는 네트워킹 노드를 수정합니다.

예를 들면 다음과 같습니다.

- "Per%cent"와 같은 알파벳과 함께 있는 특수 문자는 표시 이름에 영향을 미칩니다.
- "0%09%0A%01%05%0A%01%03%0A%01%04"와 같은 많은 특수 문자가 있는 경우, CRCX 같이 MGCP 측으로 전송되는 원격 이름에 문제가 발생할 수 있으므로 통화의 연결을 끊을 수 있습니다.

SCCP 게이트웨이 구성

다음 작업을 수행하여 Cisco 게이트웨이를 구성하여 SCCP 구성을 사용합니다.

프로시저

	명령 또는 동작	목적
단계 1	게이트웨이 프로토콜로 SCCP 구성, 109 페이지	게이트웨이를 구성하여 SCCP를 게이트웨이 프로토콜로 사용합니다.
단계 2	미구성 아날로그 FXS 포트의 자동 등록 활성화	미구성 아날로그 FXS 포트의 자동 등록을 활성화합니다.
단계 3	아날로그 전화기의 자동 등록 활성화, 110 페이지	지정된 포트에 대한 자동 등록을 활성화하여 자동 등록 DN 풀에서 DN을 페치합니다.

게이트웨이 프로토콜로 SCCP 구성

SCCP를 게이트웨이 프로토콜로 사용하도록 Cisco 게이트웨이를 구성할 수 있습니다. 이 구축 옵션을 사용하여 Unified Communications Manager를 FXS 또는 BRI 포트를 사용하는 아날로그 액세스 디바이스 또는 ISDN BRI 디바이스에 연결할 수 있습니다. SCCP 게이트웨이를 디지털 액세스 T1 또는 E1 트렁크에 연결할 수 없습니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 2 새로 추가를 클릭합니다.

단계 3 게이트웨이 유형 드롭다운 목록에서 SCCP를 사용하는 게이트웨이를 선택하고 다음을 클릭합니다.

단계 4 프로토콜 드롭다운 목록에서 **SCCP**를 선택합니다.

단계 5 구성 된 슬롯, **VIC** 및 하위 섹션에서 다음 단계를 수행합니다.

a) 각 모듈 드롭다운 목록에 대해 게이트웨이에 설치된 NIM(네트워크 인터페이스 모듈) 하드웨어에 해당하는 슬롯을 선택합니다.

b) 각 하위 디바이스 드롭다운 목록에서 게이트웨이에 설치된 VIC를 선택합니다.

단계 6 게이트웨이 구성 창에서 나머지 필드를 완료합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 7 저장을 클릭합니다.
포트 아이콘이 하위 디바이스 모듈과 함께 표시됩니다. 각 포트 아이콘은 게이트웨이에서 구성 가능한 포트 인터페이스에 해당합니다. 해당 포트 아이콘을 클릭하여 포트에서 아날로그 액세스 또는 ISDN BRI 전화기를 구성할 수 있습니다.

단계 8 업데이트를 완료하면 다음과 같이 게이트웨이에 변경 사항을 적용합니다.

a) 게이트웨이 재설정을 클릭합니다. 게이트웨이 다시 시작 팝업이 나타납니다.

b) 재설정을 클릭합니다.

아날로그 전화기의 자동 등록 활성화

지정된 포트에 대한 자동 등록을 활성화하여 자동 등록 DN 풀에서 디렉터리 번호를 페치합니다. 기본값으로 Unified Communications Manager는 아날로그 전화기의 자동 등록은 허용하지 않습니다. 관리자는 아날로그 전화기를 지원하도록 게이트웨이 모듈을 구성하여 SCCP 프로토콜을 사용하는 해당 게이트웨이를 통해 Unified CM에 자동 등록되도록 합니다.

참고 지원되는 게이트웨이 유형은 VG310, VG350, VG400, VG450 및 ISR4K 시리즈입니다.

시작하기 전에

- 자동 등록을 활성화하고 네트워크에 연결되어 있는 동안 새 엔드포인트에 할당되는 DN의 범위를 지정합니다. 자세한 내용은 자동 등록 활성화, 406 페이지 섹션을 참조하십시오.
- 게이트웨이에서 SCCP 프로토콜을 사용하여 자동 구성을 활성화합니다. 자세한 내용은 SCCP 게이트웨이의 CUCM 자동 구성을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다. 디바이스 > 게이트웨이

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 게이트웨이 유형 드롭다운 목록에서 SCCP를 사용하는 게이트웨이를 선택하고 다음을 클릭합니다.

단계 **4** 프로토콜 드롭다운 목록에서 **SCCP**를 선택합니다.

단계 **5** 게이트웨이 세부 정보 섹션에서 다음 단계를 수행합니다.

a) 텍스트 상자에 **MAC** 주소의 마지막 10자리를 입력합니다. 설명 필드 값은 MAC 주소를 입력하면 자동으로 채워집니다.

참고 게이트웨이의 MAC 주소는 이더넷 MAC 주소이거나, Unified Communications Manager와 통신하는 SCCP 게이트웨이의 인터페이스에 할당된 가상 MAC 주소일 수 있습니다.

MAC 주소를 제공할 때, 각 FXS 포트는 구성된 MAC 주소에서 포트 이름과 포트 번호를 가져옵니다. 해당 아날로그 전화기가 자동으로이 게이트웨이에 등록됩니다.

예를 들어, NM-4VWIC-MBRD가 슬롯 0 드롭다운 목록의 모듈에서 선택되고 하위 디바이스 **0** 드롭다운 목록에서 VIC3-4FXS/DID-SCCP가 선택된 경우, 4개의 FXS 포트 값이 **0/0/0, 0/0/1, 0/0/2, 0/0/3**으로 표시됩니다. 각 포트를 클릭하여 전화기 구성 창의 설명 필드에서 해당 포트 이름을 표시합니다. 표시된 포트 이름은 MAC 주소와 포트 값의 조합입니다.

게이트웨이는 가상 MAC 주소 또는 이더넷 MAC 주소를 사용하여 구성에 따라 Unified Communication Manager와 통신합니다. 손상된 게이트웨이를 교체할 때 조차도 가상 MAC 주소를 사용하면 Unified Communication Manager 애플리케이션에서 어떤 구성 변경도 수행할 필요가 없습니다.

b) 드롭다운 목록에서 필수 **Cisco Unified Communications Manager** 그룹을 선택하여 자동 등록을 활성화합니다.

단계 **6** 구성된 슬롯**, VIC** 및 엔드포인트 섹션에서 다음 단계를 수행합니다.

a) 각 모듈 드롭다운 목록에 대해 게이트웨이에 설치된 네트워크 인터페이스 모듈 하드웨어에 해당하는 슬롯을 선택하고, 저장을 클릭하여 각 하위 디바이스를 활성화합니다.

b) 복수의 하위 디바이스에 대해 게이트웨이에 설치된 해당 VIC를 선택하고 저장을 클릭합니다.

참고 슬롯 및 모듈에서는 어떤 슬롯과 모듈에 FXS 포트가 있는지 표시합니다. 또한 FXS 포트의 수도 표시합니다.

자동 등록할 때 포트 수준이 아닌 최대 하위 디바이스 수준까지만 게이트웨이를 구성하 자동 DN을 가져옵니다. 예를 들어, 하위 디바이스가 FXS로 선택되면 해당 FXS 포트는 자동 등록 DN 풀에서 사용할 수 있는 DN 중 하나를 선택하고 해당 DN을 선택한 포트에 할당합니다.

단계 **7** 구성 적용을 클릭합니다.

포트가 전화기에 연결되어 있는지 여부에 관계 없이, 게이트웨이는 모든 FXS 구성된 포트에 대한 등록 요청을 보냅니다.

미구성 아날로그 **FXS** 포트의 자동 등록 활성화

이 절차를 사용하여 미구성 아날로그 FXS 포트의 자동 재등록을 활성화합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.시스템 > 서비스 매개변수.

단계 **2** 서버 드롭다운 목록에서 실행 중인 필수 서버를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco Call Manager(**활성**)**를 선택합니다.

단계 **4** 클러스터 수준 매개변수**(**디바이스**-PRI** 및 **MGCP** 게이트웨이**)** 섹션에서 **FXS** 포트의 재등록 활성화 드롭다운 목록이 참으로 설정되어 있는지 확인하십시오.

참고 **FXS** 포트의 자동 등록 활성화의 값을 거짓으로 설정하여 미구성 아날로그 FXS 포트의 자동 재등록을 비활성화합니다.

단계 **5** 저장을 클릭합니다.

문제 해결 팁

Unified Communications Manager에서 다음을 수행하여 포트가 등록되었는지 확인하고 자동 DNS를 획득합니다.

1. 게이트웨이 유형으로 SCCP를 구성합니다.
2. 자동 등록 활성화
3. 디바이스 유형으로 아날로그 전화기를 선택합니다.
4. 풀에서 음성 포트 수를 수용할 수 있을 정도의 충분한 DNS를 사용할 수 있는지 확인합니다.

SIP 게이트웨이 구성

다음 작업을 수행하여 Unified Communications Manager에서 SIP 게이트웨이를 구성합니다. 많은 Cisco 게이트웨이와 타사 게이트웨이는 SIP를 사용할 수 있도록 구성할 수 있습니다. Unified Communications Manager에는 SIP 게이트웨이에 대한 게이트웨이 디바이스 유형이 포함되어 있지 않습니다.

시작하기 전에

Unified Communications Manager에 게이트웨이를 추가하기 전에 네트워크에 게이트웨이 하드웨어를 설치하고 게이트웨이에서 IOS 소프트웨어를 구성해야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	SIP 프로파일 구성, 113 페이지	SIP 설정을 구성하고 SIP 프로파일에 적용합니다. 트렁크는 이 설정을 사용하여 SIP 게이트웨이에 연결합니다.
단계 **2**	SIP 트렁크 보안 프로파일 구성., 113 페이지	트렁크에서 이를 사용하여 SIP 게이트웨이에 연결할 수 있도록 SIP 트렁크 보안 프로파일을 구성합니다. 디바이스 보안 모드, 다이제스트 인증 및 수신/발신 전송 유형 설정과 같은 보안 설정을 구성할 수 있습니다.

	명령 또는 동작	목적
단계 3	SIP 게이트웨이에 대한 SIP 트렁크 구성, 114 페이지	SIP 게이트웨이를 가리키는 SIP 트렁크를 구성합니다. SIP 프로파일과 SIP 트렁크 보안 프로파일을 SIP 트렁크에 적용합니다.

SIP 프로파일 구성

SIP 게이트웨이 연결을 위한 SIP 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 2 다음 단계 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 프로파일을 생성합니다.
- 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.

단계 3 **SIP** 프로파일 구성 창에서 나머지 필드를 완료합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

SIP 트렁크 보안 프로파일 구성.

SIP 게이트웨이에 연결되는 트렁크에 대한 보안 설정을 사용하여 SIP 트렁크 보안 프로파일을 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 보안 > **SIP** 트렁크 보안 프로파일을 선택합니다.

단계 2 다음 단계 중 하나를 수행합니다.

a) 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.
b) 새로 추가를 클릭하여 새 프로파일을 생성합니다.

단계 3 **SIP** 트렁크 보안 프로파일 구성 창에서 필드를 작성합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

SIP 게이트웨이에 대한 SIP 트렁크 구성

SIP 트렁크를 구성하여 Unified Communications Manager를 SIP를 사용하는 Cisco 또는 타사 게이트웨이에 연결합니다. 이 구성에서는 게이트웨이 구성 창에 게이트웨이를 디바이스로 입력하지 마십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 **2** 새로 추가를 클릭하여 새 SIP 트렁크를 설정합니다.

단계 **3** 트렁크 유형 드롭다운 목록에서 **SIP** 트렁크를 선택합니다.

단계 **4** 프로토콜 드롭다운 목록에서 없음을 선택합니다.

단계 **5** SIP 정보 창의 대상 주소 필드에 SIP 게이트웨이에 대한 IP 주소, FQDN(Fully Qualified Domain name) 또는 DNS SRV 레코드를 입력합니다.

단계 **6** **SIP** 트렁크 보안 프로파일 드롭다운 목록에서 이 게이트웨이에 대해 구성된 SIP 트렁크 보안 프로파일을 선택합니다.

단계 **7** **SIP** 프로파일 드롭다운 목록 상자에서 이 게이트웨이에 대해 구성된 SIP 프로파일을 선택합니다.

단계 **8** **SIP** 트렁크 구성 창에서 필드를 완료합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **9** 저장을 클릭합니다.

H.323 게이트웨이 구성

비 게이트키퍼 H.323 구축을 위해 Unified Communications Manager에서 H.323 게이트웨이를 구성합니다.

참고 구축에 H.323 게이트키퍼가 포함된 경우, 게이트키퍼 제어 H.225 트렁크를 설정하여 H.323 게이트웨이를 추가할 수도 있습니다. 이 시나리오는 게이트키퍼 사용이 최근 몇 년간 꾸준히 감소하고 있어 이 설명서에 기록되지 않았습니다. 게이트키퍼 및 H.225 게이트키퍼 제어 트렁크를 구성하려는 경우, *Cisco Unified Communications Manager* 관리 설명서, 릴리스 10.0(1)을 참조하십시오.

참고 게이트웨이를 Unified Communications Manager에 등록한 후에도 등록 상태가 Cisco Unified Communications Manager 관리에서 알 수 없음으로 표시될 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 게이트웨이를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 게이트웨이 유형 드롭다운 목록에서 **H.323** 게이트웨이를 선택합니다.

단계 **4** 디바이스 이름 필드에 게이트웨이의 IP 주소 또는 호스트네임을 입력합니다.

단계 **5** H.235를 사용하여 안전한 채널을 구성하려는 경우, **H.235** 데이터 통과 확인란에 체크 표시합니다

단계 **6** 게이트웨이 구성 창에서 필드를 구성합니다.

필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

단계 **8** 게이트웨이를 재설정하고 변경 사항을 적용하려면 재설정을 클릭합니다.

구성 변경 사항이 적용되도록 대부분의 게이트웨이를 재설정해야 합니다. 필요한 모든 게이트웨이 구성을 완료한 다음 재설정을 수행하는 것이 좋습니다.

게이트웨이에 대한 클러스터 수준 통화 분류 구성

네트워크 게이트웨이에 대한 통화 분류 설정을 구성합니다. 이 설정은 시스템에서 네트워크의 게이트웨이를 내부(온넷)로 또는 외부(오프넷)로 간주할 것인지 여부를 결정합니다.

통화 분류필드는 개별 게이트웨이 포트 인터페이스에 대한 [구성] 창에 표시되기도 합니다. 기본값으로 각 게이트웨이 포트 인터페이스는 클러스터 수준 서비스 매개변수의 설정을 사용하도록 구성 됩니다. 그러나 포트의 통화 분류가 클러스터 수준 서비스 매개변수와 다르게 구성된 경우, 해당 포트의 설정이 서비스 매개변수 설정을 재정의합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 Cisco CallManager 서비스가 실행 중인 서버를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 **4** 클러스터 수준 매개변수**(**디바이스 **-** 일반**)**에서 통화 분류 서비스 매개변수에 대해 다음 값 중 하나를 구성합니다.

- 온넷—이 게이트웨이의 통화는 회사 네트워크 내부에서 발신된 것으로 분류됩니다.
- 오프넷—이 게이트웨이의 통화는 회사 네트워크 외부에서 발신된 것으로 분류됩니다.

단계 **5** 저장을 클릭합니다.

오프넷 차단 게이트웨이 전환

하나의 외부 (OffNet) 게이트웨이에서 다른 외부 (OffNet) 게이트웨이로 전환된 통화를 차단하기 위해 시스템을 설정하려는 경우, 이 절차를 사용해야 합니다. 기본값으로 시스템은 하나의 외부 게이트웨이에서 다른 외부 게이트웨이로 전환할 수 있도록 설정되어 있습니다.

특정 게이트웨이가 외부 (OffNet) 또는 내부 (OnNet)인지 여부를 확인하는 설정은 통화 분류 설정에서 결정합니다. 클러스트 수준 서비스 매개변수를 사용하여 또는 다음과 같은 포트 인터페이스를 구성하여 설정됩니다.

- MGCP T1/E1 포트 인터페이스
- MGCP FXO 포트 인터페이스
- H.323 게이트웨이
- SIP 트렁크

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 Cisco CallManager 서비스가 실행 중인 서버를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

단계 **4** 오프넷 호전환에 대한 오프넷 차단 서비스 매개변수에 대한 설정을 다음과 같이 구성합니다.

- 참—이 옵션을 선택하여 두 개의 외부 (오프넷) 게이트웨이 간의 전환을 취소해야 합니다.
- 거짓—이 옵션을 선택하여 두 개의 외부 (오프넷) 게이트웨이 간의 전환을 허용해야 합니다. 이것이 기본 옵션입니다.

단계 **5** 저장을 클릭합니다.

참고 게이트웨이를 라우트 패턴에 연결하여 온넷 또는 오프넷으로 게이트웨이를 통해 통화를 분류할 수 있고, 통화 분류를 라우트 패턴 설정 창에서 구성할 수 있습니다.

12 장

SRST 구성

SRST(Survivable Remote Site Telephony) 개요

SRST(Survivable Remote Site Telephony)는 Unified Communications Manager 노드에 대한 WAN(광역 네트워크) 연결에 의존하는 사이트에 대한 선택적 기능입니다. Unified Communications Manager 관리 인터페이스에서 구성된 SRST 참조를 사용하면 WAN 장애가 발생하는 경우 IP 게이트웨이가 원격 사이트에서 IP 전화기로 제한된 전화 통신 서비스를 제공할 수 있습니다.

- 원격 사이트의 IP 전화기에서 서로 전화를 걸 수 있습니다.
- PSTN에서 걸려온 통화를 IP 전화기에 연결할 수 있습니다.
- IP 전화기의 통화는 PSTN을 통해 외부에 연결할 수 있습니다.

원격 사이트의 전화기에서 연결된 모든 Unified Communications Manager 노드에 대한 연결이 소실되는 경우, 전화기가 SRST 참조 IP 게이트웨이로 연결됩니다. IP 전화기의 상태 회선 표시에서 전화기가 백업 SRST 게이트웨이로 페일오버되었음을 나타냅니다. Unified Communications Manager에 대한 연결이 복원되면, IP 전화기에서 Unified Communications Manager에 등록하고 전체 전화 통신 서비스가 복원됩니다.

SRST는 PSTN 게이트웨이 액세스 이외에도 SCCP와 SIP 엔드포인트를 혼합하여 사용할 수 있는 원격 사이트를 지원합니다.

연결 모니터 지속 시간

WAN 링크를 통해 Unified Communications Manager와 연결을 설정할 수 있게 되는 즉시, WAN(광역 네트워크)을 통해 SRST 게이트웨이로 연결되는 IP 전화기가 자동으로 Unified Communications Manager에 재연결됩니다. 그러나 WAN 링크가 불안정한 경우, IP 전화기가 SRST 게이트웨이와 Unified Communications Manager 간에 전환됩니다. 이 상황으로 인해 전화 서비스가 일시적으로 소실될 수 있습니다 (발신음이 들리지 않음). WAN 링크 플랩핑 문제라고 하는 이러한 재연결 시도는 IP 전화기가 Unified Communications Manager로 자동으로 다시 연결될 때까지 계속됩니다.

Unified Communications Manager와 SRST 게이트웨이 간의 WAN 링크 플랩핑 문제를 해결하려면, IP 전화기가 SRST 게이트웨이에서 등록 해제된 다음 Unified Communications Manager로 다시 등록되기 전에 Unified Communications Manager에 대한 연결을 모니터링하는 시간(초)(연결 모니터 지속 시간)을 정의하면 됩니다. IP 전화기가 XML 구성 파일에서 연결 모니터 지속 시간 값을 수신합니다.

SRST(Survivable Remote Site Telephony) 구성 작업 플로우

시작하기 전에

다이얼 플랜을 검토합니다. 다이얼 플랜에 7자리 또는 8자리 숫자가 있는 경우 변환 규칙을 구성해야 할 수 있습니다. 변환 규칙에 대한 자세한 내용은 변환 패턴 구성, 196 페이지의 내용을 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	SRST 참조 구성, 118 페이지	다른 모든 Unified Communications Manager 노드에 연결할 수 없는 경우, 제한된 통화 제어 기능을 제공할 수 있는 게이트웨이를 구성합니다.
단계 **2**	디바이스 풀에 SRST 참조 할당, 119 페이지	각 디바이스 풀에 대해 Unified Communications Manager을(를) 사용할 수 없는 경우 통화를 완료하려고 시도할 때 발신 디바이스에서 검색한 게이트웨이를 할당합니다.
단계 **3**	다음 작업 중 하나를 수행합니다. • 클러스터에 대한 연결 모니터 지속 시간 구성, 119 페이지 • 디바이스 풀에 대한 연결 모니터 지속 시간 구성, 120 페이지	선택 사항: 연결 모니터 지속 시간을 구성합니다. 클러스터 수준 기본값을 적용하거나 디바이스 풀의 디바이스에 구성을 적용할 수 있습니다.
단계 **4**	SRST 게이트웨이에서 SRST 활성화, 120 페이지	게이트웨이에서 SRST 매개변수를 구성합니다.

SRST 참조 구성

SRST 참조는 특정 디바이스의 다른 모든 Cisco Unified Communications Manager 노드에 연결할 수 없는 경우 제한된 Cisco Unified Communications Manager 기능을 제공할 수 있는 게이트웨이를 설정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에 로그인하여 시스템 > **SRST**를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** **SRST** 참조 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

디바이스 풀에 **SRST** 참조 할당

전화기의 각 디바이스 풀에 대해 SRST를 구성할 수 있습니다. 디바이스 풀에 SRST 참조를 할당할 때, 디바이스 풀의 모든 전화기에서 Cisco Unified Communications Manager 노드에 연결할 수 없는 경우 할당된 SRST 게이트웨이에 연결을 시도합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 디바이스 풀을 선택합니다.

단계 **2** 찾기를 클릭하고 원격 IP 전화기가 등록된 디바이스 풀을 선택합니다.

단계 **3** 로밍 감도 설정 영역에서, **SRST** 참조 드롭다운 목록에서 SRST 참조를 선택합니다.

SRST 참조 드롭다운 목록에는 다음 옵션이 포함되어 있습니다.

- 비활성화—전화기가 Cisco Unified Communications Manager 노드에 연결할 수 없는 경우, SRST 게이트웨이에 연결을 시도하지 않습니다.
- 기본 게이트웨이 사용—전화기가 Cisco Unified Communications Manager 노드에 연결할 수 없는 경우, SRST 게이트웨이로 IP 게이트웨이에 연결을 시도합니다.
- 사용자 지정됨—전화기가 Cisco Unified Communications Manager 노드에 연결할 수 없는 경우, 이 SRST 게이트웨이에 연결을 시도합니다.

단계 **4** 저장을 클릭합니다.

클러스터에 대한 연결 모니터 지속 시간 구성

이 절차는 선택사항입니다. 연결 모니터 지속 시간에 대한 시스템 값(엔터프라이즈 매개변수)을 변경하려는 경우에만 이 절차를 완료해야 합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 시스템 > 엔터프라이즈 매개 변수를 선택합니다.

단계 **2** 연결 모니터 지속 시간 필드에 값을 입력합니다. 기본값은 120초입니다. 필드에 입력할 수 있는 최대 시간(초)은 2592000입니다.

단계 **3** 저장을 클릭합니다.

참고 변경 사항을 적용하려면 모든 서비스를 다시 시작해야 합니다.

엔터프라이즈 매개변수는 연결 모니터 지속 시간에 대한 클러스터 기본값을 형성합니다. 그러나 디바이스 풀 내에 재정의 구성이 존재하는 경우, 해당 설정이 디바이스 풀을 사용하는 디바이스에 대한 엔터프라이즈 매개변수 설정을 재정의합니다.

디바이스 풀에 대한 연결 모니터 지속 시간 구성

이 절차는 선택사항입니다. 다음 조건에 해당되는 경우에만 이 절차를 완료해야 합니다.

- 연결 모니터 지속 시간에 클러스터 수준의 값을 사용하지 않으려는 경우.
- 이 디바이스 풀에 대해 별도의 연결 모니터 지속 시간 값을 정의하려는 경우.

팁 디바이스 풀에 대한 연결 모니터 지속 시간의 값을 변경하는 경우, 이는 업데이트 중인 디바이스 풀에만 적용됩니다. 다른 모든 디바이스 풀은 자체적인 연결 모니터 지속 시간 필드의 값을 사용하거나 연결 모니터 지속 시간 엔터프라이즈 매개변수에 구성된 클러스터 수준 값을 사용합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 디바이스 풀을 선택합니다.

단계 **2** 찾기를 클릭하고 원격 IP 전화기가 등록된 디바이스 풀을 선택합니다.

단계 **3** 로밍 민감도 설정 영역에서 연결 모니터 지속 시간 필드에 값을 입력합니다. 필드에 입력할 수 있는 최대 시간(초)은 2592000입니다.

참고 이 설정은 연결 모니터 지속 시간에 대한 엔터프라이즈 매개변수 설정을 재정의합니다.

단계 **4** 저장을 클릭합니다.

SRST 게이트웨이에서 SRST 활성화

시작하기 전에

- 디바이스 풀에 SRST 참조 할당, 119 페이지
- (선택 사항) 다음 작업 중 하나를 수행합니다.
  - 클러스터에 대한 연결 모니터 지속 시간 구성, 119 페이지
  - 디바이스 풀에 대한 연결 모니터 지속 시간 구성, 120 페이지

프로시저

단계 **1** SRST 게이트웨이(라우터)에 로그인합니다.

단계 **2** **call-manager-fallback** 명령을 입력합니다.
이 명령은 라우터에서 SRST를 활성화합니다.

단계 **3** **max-ephones**max-phones 명령을 입력합니다. max-phones는(은) 지원되는 Cisco IP 전화의 최대 수입니다.

단계 **4** **max-dn**max-directory-numbers 명령을 입력합니다. max-directory-numbers는(은) 라우터를 통해 지원 가능한 디렉터리 번호(DN)와 가상 음성 포트의 최대 수입니다.

단계 **5** **ip source-address**ip-address 명령을 입력합니다. ip-address는 보통 라우터의 이더넷 포트 주소 중 하나인 기존 라우터 IP 주소입니다.
이 명령을 사용하면 SRST 라우터가 지정된 IP 주소를 통해 Cisco IP 전화기에서 메시지를 수신할 수 있습니다.

SRST 제한사항

제한 사항	설명
SRST 참조 삭제	디바이스 풀이나 다른 항목에서 사용 중인 SRST 참조를 삭제할 수 없습니다. SRST 참조를 사용 중인 디바이스풀을 알아내려면 **SRST** 참조 설정 창에서 디펜던시 레코드 링크를 클릭합니다. 디펜던시 레코드가 시스템에 대해 활성화되어 있지 않은 경우, [디펜던시 레코드 요약] 창에 메시지가 표시됩니다. 사용 중인 SRST 참조를 삭제하려고 하면 Unified Communications Manager에 오류 메시지가 표시됩니다. 현재 사용 중인 SRST 참조를 삭제하기 전에 다음 작업 중 하나 또는 둘 모두를 수행해야 합니다. • 삭제할 SRST 참조를 사용 중인 디바이스 풀에 다른 SRST 참조를 할당합니다. • 삭제할 SRST 참조를 사용 중인 디바이스 풀을 삭제합니다. 참고 SRST 참조를 삭제하기 전에 올바른 SRST 참조를 삭제하고 있는지 주의해서 확인하십시오. 삭제된 SRST 참조를 검색할 수 있습니다. SRST 참조를 실수로 삭제한 경우 다시 작성해야 합니다.

13 장

미디어 리소스 구성

미디어 리소스 정보

Cisco Unified Communications Manager 기능은 미디어 리소스를 사용해야 합니다. Cisco Unified Communications Manager에는 다음과 같은 미디어 리소스가 포함되어 있습니다.

- 음성 송출기
- IVR(Interactive Voice Response)
- MTP(미디어 터미네이션 포인트)
- 트랜스코더
- TRP(Trusted Relay Point)
- 전화회의 브리지
- 음악 대기/비디오 대기

미디어 리소스 그룹 목록에 미디어 리소스를 할당한 다음 해당 목록을 디바이스 풀 또는 개별 디바이스에 할당하여, 통화에 사용할 수 있는 미디어 리소스를 만들 수 있습니다. 개별 디바이스에 대한 기본 설정은 디바이스에서 사용 중인 디바이스 풀에 할당된 미디어 리소스를 사용해야 합니다.

참고 음악 대기 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

MTP(미디어 터미네이션 포인트)

MTP(미디어 터미네이션 포인트)는 두 개의 풀 듀플렉스(full-duplex) 미디어 스트림을 수락하여 스트림을 함께 브리징하고 독립적으로 설정되고 조각날 수 있도록 허용하는 엔티티입니다. Cisco Unified

Communications Manager에서는 미디어 경로에 MTP를 삽입하여 다음과 같은 여러 상황을 해결할 수 있습니다.

- TRP(Trusted Relay Point) 역할
- RTP 스트림을 위해 IPv4와 IPv6 간 변환 제공
- SIP 트렁크를 통해 SIP Early Offer 전달
- DTMF 전송 불일치 해결
- RSVP 에이전트 역할

H.323 통화를 위한 MTP

미디어 터미네이션 포인트를 H.323 통화를 위한 미디어 경로에 삽입하여, 통화 보류, 통화 전환, 통화 지정 보류 및 전화회의와 같은 보조 서비스를 확장할 수 있습니다. 이들 보조 서비스는 특정 통화가 H.323 엔트포인트로 라우트될 경우에는 통상 사용할 수 없습니다. H.323 보조 서비스의 경우, MTP는 ECS(EmptyCapability Set) 또는 FastStart를 지원하지 않는 엔드포인트에만 필요합니다. ECS 및 FastStart를 지원하는 모든 Cisco 및 기타 타사 엔드포인트에는 MTP가 필요하지 않습니다.

MTP 유형

Cisco Unified Communications Manager는 다음과 같은 MTP 유형을 지원합니다.

- IOS 게이트웨이의 소프트웨어 MTP
- IOS 게이트웨이의 하드웨어 MTP
- Cisco IP Voice Media Streaming 서비스에서 제공하는 소프트웨어 MTP

Cisco 미디어 터미네이션 포인트 Software MTP 유형은 네트워크의 속도와 NIC (네트워크 인터페이스 카드)에 따라 48개의 MTP(사용자 구성 가능) 리소스의 기본값을 제공합니다. 예를 들어, 100MB 네트워크/NIC 카드는 48개의 MTP 리소스를 지원할 수 있지만, 10MB NIC 카드는 지원하지 않습니다.

10MB 네트워크/NIC 카드의 경우, 약 24개의 MTP 리소스를 제공할 수 있습니다. 그러나 사용할 수 있는 MTP 리소스의 정확한 수는 해당 PC의 다른 애플리케이션에서 사용 중인 리소스, 프로세서 속도, 네트워크 로드 및 여러 기타 요인에 따라 달라 집니다.

MTP 등록

MTP 디바이스는 기본 Unified Communications Manager를 사용할 수 있는 경우 항상 해당 Unified Communications Manager로 등록하며, 이 디바이스가 지원하는 MTP 리소스의 수에 대해 Unified Communications Manager에 알려줍니다 동일한 Unified Communications Manager로 복수의 MTP를 등록할 수 있습니다. 여러 개의 MTP를 Unified Communications Manager를 통해 등록할 경우, 해당 Unified Communications Manager에서 각 MTP의 리소스 세트를 제어합니다.

예를 들어, MTP 서버 1은 48개의 MTP 리소스에 대해 구성된 것으로 MTP 서버 2는 24개의 리소스에 대해 구성된 것으로 간주해야 합니다. 두 MTP를 동일한 Unified Communications Manager로 모두 등

록하는 경우, Unified Communications Manager에서는 총 72개의 등록된 MTP 리소스에 대해서만 두 리소스 세트를 모두 유지관리합니다.

Unified Communications Manager에서 통화 엔드포인트에 MTP가 필요한 것으로 판단하는 경우, 최소 활성 스트림이 있는 MTP에서 MTP 리소스를 할당합니다. 해당 MTP 리소스가 엔드포인트를 대신하여 통화에 삽입됩니다. MTP 리소스 사용은 시스템 사용자와 대신 삽입된 엔드포인트에 모두 계속해서 표시되지 않습니다. 필요할 때 MTP 리소스를 사용할 수 없는 경우, 통화는 MTP 리소스를 사용하지 않는 상태로 연결되며 해당 통화에는 보조 서비스가 없습니다.

SRTP DTMF 상호 연동

중요 이 섹션은 14SU3 이후 릴리스부터 적용할 수 있습니다.

현재 Unified CM은 보안 통화와 비보안 통화 모두에서 DTMF 불일치의 경우 MTP를 삽입합니다. 그러나 보안 통화의 경우 DTMF 불일치로 인해 MTP가 삽입되지만 당사자 간의 미디어를 통과하기만 합니다. 따라서 DTMF 이벤트는 당사자 간에 전송되지 않습니다. Unified CM 릴리스 14SU3 이전에는 DTMF 불일치로 인해 MTP가 할당된 경우에만 비보안 통화에 대해 DTMF 변환이 수행되었습니다.

게이트웨이 IOS 버전 17.10.1부터 DTMF 변환을 위해 게이트웨이 측에서 보안 MTP가 지원됩니다. Unified Communications Manager에 등록된 보안 IOS 기반 MTP는 이제 SRTP DTMF 상호 연동을 지원합니다. 릴리스 14SU3부터 게이트웨이의 지원이 추가되어 Unified CM은 보안 엔드포인트 간의 DTMF 불일치에 대해 하드웨어 MTP(SRTP DTMF 상호 연동 지원)를 호출할 수 있습니다.

Unified Communications Manager은 이제 SCCP 메시지에서 MTP에 SRTP 키를 전송합니다. MTP는 키를 사용해 In-band DTMF 이벤트를 Out-of-band 이벤트로 해독하고 이를 다른 Call leg로 전송합니다. 마찬가지로 Out-of-band DTMF 이벤트도 Unified Communications Manager는 암호화된 In-band DTMF 이벤트를 다른 Call leg에 삽입합니다.

중요 고려 사항

- Unified Communications Manager는 14SU3 릴리스부터 Cisco IOS XE 17.10.1a 이후 버전과 함께 다음에 대해 이 기능을 지원합니다.
  - Cisco 4461 통합 서비스 라우터(ISR)
  - Cisco Catalyst 8200 시리즈 Edge 플랫폼
  - Cisco Catalyst 8300 시리즈 Edge 플랫폼
  - Cisco Catalyst 8000V Edge 소프트웨어

참고 이 기능에 필요한 게이트웨이 설정에 대한 자세한 정보는 Cisco IOS XE 17.10.1a 및 이후 플랫폼의 각 설정 가이드를 참조하십시오.

- Unified Communications Manager와 게이트웨이 간 성공적인 TLS 1.2 연결이 필수입니다. TLS 1.2 설정에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 보안 설명서을 참조하십시오.

- 이 기능은 통과 모드의 하드웨어 MTP에서만 지원되며, 이때 MTP는 통과 모드에서 DTMF-SRTP 상호 연동 지원이 있는 IOS 게이트웨이를 사용해 등록됩니다.
- 이 기능은 IPVMS 기반 MTP와 H.323 통화 흐름에서 지원되지 않습니다.

미디어 터미네이션 포인트 상호 작용 및 제한 사항

표 *7:* 미디어 터미네이션 포인트 상호 작용 및 제한 사항

제한 사항	설명
Cisco IP Voice Streaming 애플리케이션	서버당 하나의 Cisco IP Voice Streaming 애플리케이션만 활성화할 수 있습니다. 추가 MTP 리소스를 제공하기 위해 네트워크로 연결된 추가 서버에서 Cisco IP Voice Streaming 애플리케이션을 활성화할 수 있습니다. Cisco Unified Communications Manager의 성능이 저하될 수 있으므로 통화 처리 로드가 높은 Cisco Unified Communications Manager에서 Cisco IP Streaming Media 애플리케이션을 활성화하지 말 것을 강력 권장합니다.
Cisco Unified Communications Manager에 등록	각 MTP는 한 번에 하나의 Cisco Unified Communications Manager에만 등록될 수 있습니다. 시스템 구성 방법에 따라 시스템에 하나의 Cisco Unified Communications Manager에 각각 등록될 수 있는 여러 MTP가 존재할 수 있습니다.
페일오버 및 폴백	이 섹션에서는 등록된 Cisco Unified Communications Manager가 연결할 수 없게 되는 경우 MTP 디바이스 페일오버 및 폴백 방법에 대해 설명합니다. • 기본 Cisco Unified Communications Manager가 실패하는 경우, MTP가 속한 디바이스 풀에 대해 지정된 Cisco Unified Communications Manager 그룹에서 사용 가능한 다음 Cisco Unified Communications Manager에 등록을 시도합니다. • MTP 디바이스에서 장애 발생 후 이용 가능하고 현재 사용 중이 아니면 즉시 기본 Cisco Unified Communications Manager에 재등록합니다. • 시스템에서는 모든 상대방이 연결을 끊을 때까지 통화 유지 모드로 활성 상태의 통화 또는 전화회의를 유지합니다. 시스템에서 보조 서비스를 사용할 수 없도록 설정합니다. • MTP에서 새 Cisco Unified Communications Manager에 등록을 시도하고 등록 승인이 수신된 적이 없는 경우, MTP에서 다음 Cisco Unified Communications Manager에 등록합니다. 하드 또는 소프트 재설정 이후 MTP 디바이스에서 등록을 해제한 다음 연결을 끊습니다. 재설정이 완료되면 해당 디바이스에서 Cisco Unified Communications Manager에 등록합니다.

트랜스코더

트랜스코더는 한 코덱의 입력 스트림을 다른 코덱을 사용하는 출력 스트림으로 코덱 변환을 수행하는 디바이스입니다. 예를 들어, 트랜스코더는 G.711 스트림을 가져와서 G.729 스트림에 실시간으로 변환할 수 있습니다. 서로 다른 음성 코덱을 사용하는 엔드포인트에서 통화하는 경우, Cisco Unified Communications Manager에서 미디어 경로로 트랜스코더를 호출합니다. 트랜스코더는 호환되지 않는 두 코덱 간의 데이터 스트림을 변환하여 장치 간의 통신을 허용합니다. 트랜스코더는 통화에 관련된 사용자 또는 엔드포인트에 보이지 않습니다.

트랜스코더 리소스는 MRM(미디어 리소스 관리자)에서 관리합니다.

Opus 코덱 트랜스코더 지원

중요 이 섹션은 14SU1 이후 릴리스부터 적용할 수 있습니다.

이제 Cisco Unified Communications Manager에는 성공적인 미디어 협상에 필요한 트랜스코딩 Opus 오디오 코덱을 지원하는 SCCP(Skinny Client Control Protocol) 제어 iOS 기반 등록된 미디어 리소스가 포함됩니다.

대부분의 Cisco 엔드포인트는 Opus 코덱을 지원합니다. Opus 코덱은 낮은 대역폭 환경에서 G711/G729보다 우수한 품질을 제공합니다. Opus 코덱 트랜스코더 지원을 사용하면 Unified CM이 Opus 코덱 불일치에 대한 트랜스코더를 호출하 여 Opus 코덱 측에서 낮은 비트 전송률을, 원격 측에서는 더 높은 비트 전송률을 허용합니다. 그러나 Unified CM에서 Opus 코덱을 지원하는 트랜스코더가 성공적으로 등록되어야 합니다.

지원되는 버전

Opus 트랜스코딩 기능은 다음 Unified Communications Manager 및 게이트웨이 버전에서 작동합니다.

- Unified CM 버전 14 SU1 이상
- 게이트웨이 IOS 버전 IOS XE 17.6.1
- DSP 펌웨어 버전 58.2.0 이상

구성

1. Opus 코덱 트랜스코딩을 지원하는 ISR(통합 서비스 라우터) 게이트웨이를 사용하여 트랜스코더를 구성합니다. 트랜스코더 프로파일에 Opus 코덱을 추가해야 합니다.
2. Cisco Unified Communications Manager DSPFARM 프로파일에서 Opus 코덱을 지원하는 트랜스코더를 등록합니다.
3. 트랜스코딩을 요청하는 엔드포인트 또는 트렁크의 미디어 리소스 그룹 목록(MRGL)에 트랜스코더를 연결하고 두 발신자 간의 지역 설정을 최대 7kbps로 구성합니다.

참고 트랜스코더로 구성된 MRGL를 두 발신자의 디바이스풀로 연결하면, Unified CM은 미디어 협상을 위해 적절한 트랜스코더를 호출합니다. 자세한 내용은 트랜스코더 구성을 참조하십시오.

MTP 기능을 사용하는 트랜스코더

코덱 변환 이외에도 트랜스코더는 MTP(미디어 터미네이션 포인트)와 동일한 기능을 제공할 수 있습니다. 트랜스코더 기능 및 MTP 기능이 모두 필요한 경우, 트랜스코더에서 두 기능 세트를 동시에 제공할 수 있다는 사실 때문에 시스템에서 트랜스코더를 할당합니다. MTP 기능만 필요한 경우, 시스템이 리소스 풀에서 트랜스코더 또는 MTP를 할당합니다. 리소스 선택은 미디어 리소스 그룹에서 결정합니다.

필요한 때 소프트웨어 MTP 리소스를 사용할 수 없는 경우, 신뢰할 수 있는 릴레이 지점 할당 실패 시 호출 실패 및 **MTP** 할당 실패 시 호출 실패 필드가 **Cisco Unified CM** 관리 > 시스템 > 서비스 매개 변수 > 서비스 매개 변수 구성창에서 '거짓'으로 설정되어 있으면 통화는 MTP 리소스 및 MTP/TRP 서비스를 사용하지 않고 연결을 시도합니다. (하나의 코덱을 다른 코덱으로 변환하기 위해) 하드웨어 트랜스코더 기능이 필요하지만 트랜스코더를 사용할 수 없는 경우, 해당 통화는 실패합니다.

트랜스코더 유형

Cisco Unified Communications Manager 관리의 트랜스코더 유형은 다음 표에 나열 되어 있습니다.

참고 트랜스코더는 트랜스코더로 작동하고 MTP/TRP 기능을 제공할 때 G.711과 G.711을 포함한 모든 코덱 간의 트랜스 코딩을 지원합니다.

표 *8:* 트랜스코더 유형

트랜스코더 유형	설명
Cisco 미디어 터미네이션 포인트 하드웨어	Cisco Catalyst 4000 WS-X4604-GWY 및 Cisco Catalyst 6000 WS-6608-T1 또는 WS-6608-E1을 지원하는 이 유형에서는 다음과 같은 수의 트랜스 코딩 세션을 제공합니다. Cisco Catalyst 4000 WS-X4604-GWY의 경우 • G.711으로 트랜스코딩의 경우 - 16 MTP 트랜스코딩 세션 Cisco Catalyst 6000 WS-6608-T1 또는 WS-6608-E1의 경우 • G.723에서 G.711으로 트랜스코딩/G.729에서 G.711로 트랜스코딩의 경우, 물리적 포트 당 24 MTP 트랜스코딩 세션, 모듈 당 192 세션

트랜스코더 유형	설명
Cisco 미디어 터미네이션 포인트(하드웨어)	Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745, Cisco 3660, Cisco 3640, Cisco 3620, Cisco 2600 및 Cisco VG200 게이트웨이를 지원하는 이 유형에서는 다음과 같은 수의 트랜스코딩 세션을 제공합니다. NM-HDV 당 • G.711에서 G. 729-60으로 트랜스코딩 • G.711에서 GSM FR/GSM EFR-45로 트랜스코딩
Cisco IOS Enhanced 미디어 터미네이션 포인트(하드웨어)	**NM-HD** 당 Cisco 2600XM, Cisco 2691, Cisco 3660, Cisco 3725, Cisco 3745 및 Cisco 3660 Access Routers를 지원하는 이 유형에서는 다음과 같은 수의 트랜스코딩 세션을 제공합니다. • G.711에서 G.729a/G.729ab/GSMFR-24로 트랜스코딩 • G.711에서 G.729/G.729b/GSM EFR-18로 트랜스코딩 **NM-HDV2** 당 Cisco 2600XM, Cisco 2691, Cisco 3725, Cisco 3745 및 Cisco 3660 Access Routers를 지원하는 이 유형에서는 다음과 같은 수의 트랜스코딩 세션을 제공합니다. • G.711에서 G.729a/G.729ab/GSMFR-128로 트랜스코딩 • G.711에서 G.729/G.729b/GSM EFR-96으로 트랜스코딩 **PVDM4** • 온보드 PVDM4 모듈(PVDM4-32, PVDM4-64, PVDM4-128, PVDM4-256) • T1/E1 모듈의 DSP 모듈(PVDM4-32, PVDM4-64, PVDM4-128, PVDM4-256) • DSP NIM(NIM-PVDM4-32, NIM-PVDM4-64, NIM-PVDM4-128, NIM-PVDM4-256) 이러한 유형은 ISR4K(ISR44xx, ISR43xx), C83xx 및 C82xx 플랫폼에서 다음과 같은 수의 트랜스코딩 세션을 제공합니다. • G.711에서 G.729a/G.729ab/GSMFR-24로 트랜스코딩 • G.711에서 G.729/G.729b/GSM EFR-18로 트랜스코딩 • G.711에서 G.729a/G.729ab/GSMFR-128로 트랜스코딩 • G.711에서 G.729/G.729b/GSM EFR-96으로 트랜스코딩 • G.711/G.729/G.729ab/G.729a/G.729b에서 Opus로 트랜스코딩

트랜스코더 유형	설명
Cisco 미디어 터미네이션 포인트 (WS-SVC-CMM)	이 유형에서는 도터 카드당 64 트랜스코딩 세션을 제공합니다. 즉, 한 개의 도터 카드에 64 트랜스코딩 세션, 두 개의 도터 카드에 128 트랜스코딩 세션, 세 개의 도터 카드에 192 트랜스코딩 세션 그리고 네 개의 도터 카드(최대)에 256 트랜스코딩 세션이 제공됩니다. 이 형식은 다음과 같은 코덱 조합 간의 트랜스코딩을 제공합니다. • G.711 a-law 및 G.711 mu-law • G.729 부록 A 및 부록 B • G.723.1 • GSM(FR) • GSM(EFR)

트랜스코더 상호 작용 및 제한 사항

트랜스코더 상호 작용 및 제한 사항

상호 작용 및 제한 사항	설명
트랜스코더 삭제	미디어 리소스 그룹에 할당된 트랜스코더는 삭제할 수 없습니다. 트랜스코더를 사용 중인 미디어 리소스 그룹을 알아내려면 트랜스코더 설정 창의 관련 링크 드롭다운 목록 표에서 디펜던시 레코드를 클릭한 다음 이동을 클릭합니다. [종속성 레코드 요약] 창에 트랜스코더를 사용하고 있는 미디어 리소스 그룹에 대한 정보가 표시됩니다. 미디어 리소스 그룹에 대한 추가 정보를 알아내려면 미디어 리소스 그룹을 클릭하십시오. 그러면 [디펜던시 레코드 세부 정보] 창이 표시됩니다. 디펜던시 레코드가 시스템에 대해 활성화되어 있지 않은 경우, [디펜던시 레코드 요약] 창에 메시지가 표시됩니다. 사용 중인 트랜스코더를 삭제하려고 시도하는 경우, Cisco Unified Communications Manager에 메시지가 표시됩니다. 현재 사용 중인 트랜스코더를 삭제하기 전에 할당된 미디어 리소스 그룹에서 트랜스코더를 제거해야 합니다.

상호 작용 및 제한 사항	설명
페일오버 및 폴백	트랜스코더 페일오버 및 폴백은 다음과 같이 작동합니다. • 기본 Unified Communications Manager 노드가 실패하는 경우 트랜스코더는 트랜스코더가 속한 디바이스풀에 대해 지정된 Unified Communications Manager 그룹에서 사용 가능한 다음 노드에 등록하려고 시도합니다. • 트랜스코더 디바이스는 사용할 수 있게 되면 즉시 기본 Cisco Unified Communications Manager노드에 재등록합니다. • 트랜스코더 디바이스는 연결할 수 없게 되는 Unified Communications Manager 노드에서 등록이 취소됩니다. 트랜스코딩에 이 트랜스코딩 프로파일을 사용하던 통화는 보존 상태로 이동하고 트랜스코더는 사용 가능한 다음 노드에 등록하려고 시도합니다. 게이트웨이는 RTP/RTCP 시간 초과를 사용하여 등록된 Unified Communications Manager에 리소스 릴리스 정보를 제공합니다. • 트랜스코더가 새 Unified Communications Manager 노드에 등록을 시도하고 레지스터 승인이 수신되지 않는 경우, 트랜스코더는 목록의 다음 노드에 등록됩니다. 트랜스코더 디바이스는 하드 또는 소프트 재설정 이후 등록 취소되고 연결이 차단됩니다. 재설정이 완료되고 나면, 디바이스가 기본 Cisco Unified Communications Manager 노드에 다시 등록됩니다.
Opus 코덱 트랜스코더 지원	트랜스코더 프로파일이 Unified Communications Manager에 등록된 경우 사용자에게 다음과 같은 시나리오가 있습니다. • ISR 게이트웨이가 Opus 트랜스코딩을 지원하고 Unified CM이 Opus 트랜스코딩을 지원하지 않는 경우 시스템은 코덱 불일치에 대해 트랜스코더를 할당합니다. 그러나 필요한 매개 변수가 SCCP 메시지에 없으므로 ISR 게이트웨이는 ORC(OpenReceiveChannel) 및 SMT(StartMediaTransmission) SCCP 메시지를 거부합니다. • ISR 게이트웨이가 Opus 트랜스코딩을 지원하지 않고 Unified CM이 Opus 코덱 트랜스코딩을 지원하는 경우 Opus에 대한 트랜스코더 할당 요청이 실패합니다. • 엔드포인트가 파일 멀티캐스트 전송 프로토콜(FMTP) "sprop-stereo" 매개변수 값 중 하나가 해당 SDP에서 1로 설정된 Opus 코덱을 지원하는 경우 시스템은 OLC/SMT를 거부하는 게이트웨이로 "sprop-stereo" 값이 1인 ORC/SMT 메시지를 전송합니다. 그러면 결국 통화가 끊어집니다.

TRP(Trusted Relay Point) 개요

TRP(Trusted Relay Point)는 Cisco Unified Communications Manager에서 통화 미디어의 제어 지점으로 작용하도록 미디어 스트림에 삽입할 수 있는 MTP 또는 트랜스코더입니다. TRP는 스트림에서의 추가 처리를 제공할 수 있으며 스트림이 특정 경로를 따르도록 보장할 수 있습니다.

특정 통화가 TRP(Trusted Relay Point)를 요구할 경우, Cisco Unified Communications Manager가 TRP 기능을 통해 활성화될 수 있는 MTP 또는 트랜스코더를 할당합니다.

구성

MTP와 트랜스코더는 미디어 터미네이션 포인트 설정 또는 트랜스코더 설정 창에서 **TRP(Trusted Relay Point)** 확인란을 체크하여 TRP 기능을 제공하도록 설정할 수 있습니다.

TRP(Trusted Relay Point) 사용 필드를 다음 구성 창에 대해 **ON**으로 구성하여 개별 통화에 대한 TRP 요구 사항을 구성할 수 있습니다.

- 전화기 구성
- 게이트웨이 구성
- 음성 메일 포트 구성
- 트렁크 구성
- CTI 라우트 포인트 구성
- 일반 디바이스 구성
- 범용 디비이스 템플릿 구성
- 여러 미디어 리소스 구성(음성 송출기, IVR, MTP, 트랜스코더, 전화회의 브리지, 음악 대기)

TRP(Trusted Realay Point) 상호 작용 및 제한 사항

기능	상호 작용 및 제한 사항
RSVP(Resource Reservation Protocol)	통화에 대해 RSVP가 활성화된 경우 Cisco Unified Communications Manager에서 TRP로 표시되는 RSVPAgent를 할당하려고 시도합니다. 그렇지 않으면 다른 TRP 디바이스가 RSVPAgent와 엔드포인트 사이에 삽입됩니다.
통화용 트랜스코더	통화용 트랜스코더가 필요하고 TRP가 필요한 엔드포인트와 동일한 측면에서 트랜스코더를 할당해야 하는 경우, Cisco Unified Communications Manager에서 TRP로 표시된 트랜스코더를 먼저 할당하려고 시도합니다. 그렇지 않으면 다른 TRP 디바이스가 트랜스코더와 엔드포인트 사이에 삽입됩니다.
엔드포인트용 MTP 할당	엔드포인트를 위해 미디어 터미네이션 포인트 필수 확인란과 **Trusted Relay Point** 사용 확인란에 체크 표시하는 경우, Cisco Unified Communications Manager에서 TRP이기도 한 MTP를 할당해야 합니다. 관리자가 이러한 MTP 또는 TRP를 할당하는 데 실패하면 통화 상태가 표시됩니다.

기능	상호 작용 및 제한 사항
TRP 할당	대부분의 경우 사용자가 통화에 응답한 후에 TRP가 할당됩니다. 따라서 TRP 할당 실패로 인해 통화에 실패한 경우, 사용자는 통화에 응답한 이후 빠른 신호음을 들을 수 있습니다 (MTP가 필요한 SIP 아웃바운드 레그 또는 h.323 아웃바운드 faststart는 예외입니다).
엔드포인트용 TRP 삽입	Cisco Unified Communications Manager에서는 디바이스와 연관된 엔드포인트 또는 디바이스 풀을 위해 **Trusted Relay Point** 사용 확인란에 체크 표시한 경우 엔드포인트용 TRP를 반드시 삽입해야 합니다. Cisco Unified Communications Manager에서 TRP 할당에 실패할 경우 통화에 실패할 수 있습니다. 이 때 **TRP** 할당 실패 시 통화 실패 서비스 매개변수는 **True**로 설정되어 있습니다.
TRP 및 원격 사용자	TRP는 홈 원격 사용자의 작업을 위한 보안 솔루션 제공에 권장되지 않으며 Expressway의 모바일 및 원격 접속을 권장합니다.

TRP 리소스가 부족한 통화 동작

다음 섹션에서는 MTP 리소스가 부족하게 할당된 경우 Cisco Unified Communications Manager에서 해당 통화를 처리하는 방법에 대한 예를 제공합니다. 이러한 엔드포인트에 대해 MTP 및 TRP가 필요한지 여부와 MTP 또는 TRP 할당이 실패할 경우 시스템이 자동으로 통화를 실패하도록 구성되었는지 여부에 따라, 결과적인 통화 동작은 달라집니다.

MTP 및 TRP가 모두 필요합니다.

다음 표에서는 엔드포인트에 대해 미디어 터미네이션 포인트 필수 및 **Trusted Relay Point** 사용 옵션이 모두 선택된 경우, 통화가 실패하는지 그리고 MTP 및 TRP 리소스가 부족한지 여부를 보여줍니다.

Trusted Relay Point 할당이 실패할 경우 통화 실패 및 **MTP** 할당이 실패할 경우 통화 실패 서비스 매개변수가 자동으로 통화 실패로 설정되었는지 여부에 따라, 최종 통화 상태는 달라집니다.

TRP 할당이 실패할 경우 통화 실패 서비스 매개변수	**MTP** 할당이 실패할 경우 통화 실패 서비스 매개변수	**Unified CM**에서
True	True	예
True	False	예
False	True	예, MTP가 H.323 오, MTP가 SIP 인
False	False	아니요

MTP/TRP 리소스 부족에 대한 자동 통화 실패 활성화되지 않음

다음 표에서는 MTP/TRP 리소스가 부족하고 **TRP** 할당 실패 시 통화 실패 및 **MTP** 할당 실패 시 통화 실패 서비스 매개변수가 거짓으로 설정되어 있을 때의 통화 동작을 보여줍니다.

MTP 필요 = 예	**TRP** 사용 = 예	리소스 할당 상태	통화 동작
Y	Y	TRP 할당됨	오디오 통화는 패스스루 지원이 없는 경우에만 해당.
Y	Y 또는 N	MTP만 해당	오디오 통화만 해당. TRP 지원 없음.
Y	Y 또는 N	할당되지 않음	MTP 필요가 H.323 엔드포인트에 대해 체크 표시된 경우, 보조 서비스가 비활성화됩니다.
N	Y	TRP 할당됨	오디오 또는 화상 통화는 엔드포인트 기능 및 CAC(Call Admission Control)에 따라 달라집니다. 보조 서비스가 작동합니다.
N	Y	할당되지 않음	오디오 또는 화상 통화 보조 서비스가 계속해서 작동하지만 TRP 지원은 없습니다.

음성 송출기 개요

음성 송출기는 Cisco Unified Communications Manager에서 실행되고 Cisco IP 전화기 및 게이트웨이에 미리 녹음된 메시지와 신호음을 보낼 수 있도록 해주는 SCCP 소프트웨어 디바이스입니다. 음성 송출기는 해당 노드에서 Cisco IP Voice Media Streaming 서비스를 켜면 클러스터 노드에서 활성화됩니다. MLPP, SIP 트렁크, IOS 게이트웨이 및 소프트웨어 전화회의 브리지와 같은 기능은 음성 송출기에 의존하여 단방향 미디어 스트림을 통해 미리 정의된 메시지를 전화기 또는 게이트웨이로 전송합니다. 그 외에도,

- IPv4 및 IPV6이 모두 지원됩니다. 시스템의 플랫폼이 IPv6용으로 구성되고 IPv6 엔터프라이즈 매개변수가 활성화되었다면 음성 송출기는 자동으로 듀얼 모드로 구성됩니다.
- SRTP 지원됨

음성 송출기 확장성

기본값으로 음성 송출기는 48개의 동시 미디어 스트림을 지원합니다. 추가 노드에서 음성 송출기를 활성화하거나 통화 카운트 서비스 매개변수를 통해 기본값으로 설정된 음성 송출기 미디어 스트림의 수를 변경하여 용량을 추가할 수 있습니다. 그러나 **Cisco CallManager** 서비스가 해당 노드에서 비활성화된 경우가 아니라면 노드에서 이 값을 늘리지 않는 것이 좋습니다.

음성 송출기가 **Cisco CallManager** 서비스가 실행되지 않는 전용 가입자 노드에서 실행되는 경우, 음성 송출기에서 최대 255개의 동시 알림 스트림을 지원할 수 있습니다. 전용 가입자 노드가 사용자 1만 명에 대한 OVA 가상 머신 구성을 충족하는 경우, 음성 송출기는 최대 400개의 동시 알림 스트림을 지원할 수 있습니다.

주의 통화 처리 로드가 높은 Unified Communications Manager 노드에서 음성 송출기를 활성화하지 마십시오.

전화회의 브리지가 있는 음성 송출기

음성 송출기는 다음과 같은 조건에서 전화회의 브리지에 사용할 수 있습니다.

- 음성 송출기가 포함된 미디어 리소스 그룹 목록이 전화회의 브리지가 존재하는 디바이스 풀에 할당된 경우.
- 음성 송출기가 기본 미디어 리소스로 구성된 경우.

미디어 리소스 그룹 목록이 전화회의를 제어하는 디바이스에 직접 할당된 경우에는 음성 송출기를 전화회의 브리지에 사용할 수 없습니다.

각 전화회의는 하나의 알림만 지원합니다. 현재 알림이 재생되는 동안 시스템에서 다른 알림을 요청하는 경우, 새로운 알림이 재생 중인 알림을 대체합니다.

기본 음성 송출기 알림 및 신호음

Cisco Unified Communications Manager에서는 Cisco IP Media Streaming Application 서비스를 활성화하면 사전에 녹음된 음성 송출기 알림을 자동으로 제공합니다. 다음과 같은 조건에 대한 알림이나 신호음이 재생됩니다.

- 알림 — Cisco MLPP(Multilevel Precedence 및 Preemption)에 대해 구성된 디바이스를 위해 재생됩니다.
- 참여 신호음 — 참가자가 애드-혹 전화회의에 참여하기 전에 들립니다.
- 다시 울림 신호음 — IOS 게이트웨이를 통해 PSTN에서 통화를 전환할 때, 통화가 활성 상태이면 게이트웨이에서 신호음을 재생할 수 없기 때문에 음성 송출기에서 신호음을 재생합니다.
- 다시 울림 신호음 — H.323 인터클러스터 트렁크에서 통화를 전환할 때 신호음이 재생됩니다.
- 다시 울림 신호음 — SCCP를 실행 중인 전화에서 SIP 클라이언트로 통화를 전환할 때, 신호음이 재생됩니다.

사전에 녹음된 기본 음성 송출기 알림을 변경하거나 추가 알림을 추가할 수 없습니다. Cisco Unified Communications Manager 로캘 설치 관리자가 설치되어 있고 Cisco Unified IP Phone 또는 디바이스 풀에 대해 로캘 설정이 구성되어 있는 경우, 알림 현지화가 지원됩니다. 사용자와 (결합된) 네트워크 로캘을 위한 로캘 설치 관리자와 파일에 대한 자세한 내용은, *Cisco Unified Communications Manager* 설치를 참조하십시오. 로캘 설치 관리자를 다운로드하려면, www.cisco.com.에서 지원 페이지를 참조하십시오.

표 *9:* 사전에 녹음된 음성 송출기 알림

조건	알림
동등하거나 그 이상의 우선 순위 통화가 진행 중입니다.	우선 순위 액세스 제한으로 인해 통화를 완료할 수 없습니다. 통화를 끊고 다시 시도해야 합니다. 이 내용은 녹음본입니다.
우선 순위 액세스 제한이 존재합니다.	우선 순위 액세스 제한으로 인해 통화를 완료할 수 없습니다. 통화를 끊고 다시 시도해야 합니다. 이 내용은 녹음본입니다.
누군가가 인증되지 않은 우선 순위 수준을 시도하였습니다.	사용된 우선순위가 회선에 대해 인증되지 않았습니다. 인증된 우선순위를 사용하거나 운영자에 게 도움을 요청해야 합니다. 이 내용은 녹음본입니다.
통화가 통화 중으로 나타나거나, 관리자가 통화 대기 또는 선점에 대한 디렉터리 번호를 구성하지 않았습니다.	전화를 건 번호가 통화 중이며, 통화대기 또는 선점 상태가 아닙니다. 통화를 끊고 다시 시도해야 합니다. 이 내용은 녹음본입니다.
시스템에서 통화를 완료할 수 없습니다.	전화를 건 대로 통화를 완료할 수 없습니다. 디렉터리와 통화를 다시 찾아보거나 운영자에 게 도움을 요청해야 합니다. 이 내용은 녹음본입니다.
서비스 중단이 발생했습니다.	서비스 중단으로 인해 통화를 완료할 수 없습니다. 비상 통화의 경우, 운영자에게 문의해야 합니다. 이 내용은 녹음본입니다.

다음 표에는 음성 송출기에서 지원하는 신호음이 나와 있습니다.

표 *10:* 신호음 설명

유형	설명
통화 중 신호음	착신 번호가 통화 중일 때 통화 중 신호음이 들립니다.
참여 신호음	참가자가 애드-혹 전화회의에 참가하기 전에 전화회의 참여 신호음이 들립니다.
다시 울림 신호음	다음과 같은 시나리오의 경우, 경고음이 들립니다. • IOS 게이트웨이를 통해 PSTN에서 통화를 전환하는 경우. • H.323 인터클러스터 트렁크에서 통화를 전환하는 경우. • SCCP 전화기에서 SIP 클라이언트로 통화를 전환하는 경우.

IVR(대화형 음성 응답) 개요

IVR(대화형 음성 응답) 디바이스에서는 Cisco 통합 커뮤니케이션 매니저를 활성화하여 사전에 기록된 기능 알림(.wav 파일)을 디바이스(예: Cisco 통합 IP 전화 및 게이트웨이)에 재생합니다. 이러한 알림은 지금 전화회의와 같은 IVR 알림이 필요한 기능을 사용하는 디바이스에서 재생됩니다.

노드를 추가하면 이 노드에 IVR 디바이스가 자동으로 추가됩니다. 해당 노드에서 Cisco IP Voice Media Streaming Application 서비스가 활성화될 때까지 IVR 디바이스가 비활성 상태로 유지됩니다.

기본값으로 IVR은 48명의 동시 발신자를 지원합니다. IVR 발신자 수는 Cisco IP Voice Media Streaming Application 서비스 매개변수를 사용하여 변경할 수 있습니다. 단, 노드당 IVR 발신자가 48명을 초과하지 않는 것이 좋습니다. IVR에 예상되는 동시 통화 수에 따라 지금 전화회의 참가에 대해 IVR 발신자 수를 구성할 수 있습니다.

⚠

주의 통화 처리 로드가 높은 Cisco 통합 커뮤니케이션 매니저 노드에서 IVR 디바이스를 활성화하지 마십시오.

기본 IVR 알림 및 신호음

Cisco Unified Communications Manager 에서는 Cisco IP Media Streaming Application 서비스를 활성화할 때 미리 녹음된 IVR(대화식 음성 응답) 알림을 자동으로 제공합니다. 기본값인 미리 녹음된 IVR 알림을 대체할 수 있습니다. 다음 조건에 대한 알림이 재생됩니다.

표 *11:* 미리 녹음된 *IVR* 알림

알림	조건
ConferenceNowAccessCodeFailed 알림	참가자가 최대 시도 횟수를 초과하여 [지금 전화회의]에 참가하기 위해 잘못된 액세스 코드를 입력하면 재생됩합니다.
ConferenceNowAccessCodeInvalid 알림	참가자가 잘못된 액세스 코드를 입력하면 재생됩니다.
ConferenceNowCFBFailed 알림	[지금 전화회의]를 시작하는 동안 전화회의 브리지 용량 한도가 초과되면 재생됩니다.
ConferenceNowEnterAccessCode 알림	참가자가 [지금 전화회의]에 참가하고 호스트가 참가자 액세스 코드를 설정하면 재생됩니다.
ConferenceNowEnterPIN 알림	호스트 또는 참가자가 미팅에 참가하려고 시도하면 재생됩니다.
ConferenceNowFailedPIN 알림	호스트가 올바른 PIN을 입력하는 최대 시도 횟수를 초과하면 재생됩니다.
ConferenceNowGreeting 알림	[지금 전화회의]에 대한 인사말 메시지를 재생합니다.
ConferenceNowInvalidPIN 알림	호스트가 잘못된 PIN을 입력하면 재생됩니다.

알림	조건
ConferenceNowNumberFailed 알림	호스트 또는 참가자가 최대 시도 횟수를 초과하여 잘못된 미팅 번호를 입력하면 재생됩니다.
ConferenceNowNumberInvalid 알림	호스트나 참가자가 잘못된 미팅 번호를 입력하면 재생됩니다.

IVR(대화형 음성 응답) 제한 사항

기능	제한 사항
로드 밸런싱	IVR(대화형 음성 응답)은 일반 미디어 디바이스 드라이버를 통해 RTP(Real-Time Protocol) 스트림을 사용합니다. 이 디바이스 드라이버는 또한 음악 대기(MOH), 소프트웨어 미디어 터미네이션 포인트(MTP), 소프트웨어 전화회의 브리지(CFP) 및 음성 송출기와 같은 Cisco IP Voice Media Streaming 애플리케이션 서비스에서 제공하는 기타 소프트웨어 미디어 디바이스에서도 사용합니다. 더 큰 통화 볼륨을 구성하면 시스템 성능이 영향을 받습니다. 이는 또한 Call Manager 서비스가 동일한 서버 노드에서 활성 상태인 경우 통화 처리에도 영향을 줍니다.
DTMF 숫자	IVR에서는 OOB(Out of Band) DTMF 숫자 수집 방법만 지원합니다. 발신 디바이스와 IVR 간에 DTMF 기능이 일치하지 않는 경우, MTP가 할당됩니다.
코덱	IVR에서는 G.711(a-law and mu-law), G.729 및 Wide Band 256K를 지원합니다. 발신 디바이스와 IVR 간에 코덱이 일치하지 않는 경우, 트랜스코더가 할당됩니다.

알림 개요

Cisco Unified Communications Manager 관리에서 메뉴 리소스 > 알림 메뉴 경로를 사용하여 알림을 구성합니다. 다음 2가지 분류의 알림이 있습니다.

- 시스템 알림—일반적인 통화 처리에 사용되거나 샘플 기능 알림으로 제공되는 미리 정의된 알림입니다.
- 기능 알림—음악 대기(MOH), 통화 대기가 있는 헌트 파일럿 또는 외부 통화 제어와 같은 기능에 의해 사용됩니다. Cisco에서 제공하는 오디오 파일을 업로드하거나 사용자 지정 `.wav` 파일을 업로드하여 자체 기능 알림을 사용자 지정할 수 있습니다. 모든 사용자 지정 알림 `.wav` 파일은 클러스터의 모든 서버에 업로드합니다.

참고 트렁크 또는 게이트웨이를 통해 연결되어 있는 경우, 경고 또는 재정렬 신호음과 같은 사용자 지정 알림을 들을 수 있습니다. 그러나 두 IP 전화기 또는 IP 전화기와 Jabber 클라이언트 간의 통화에 대한 사용자 지정 알림은 들을 수 없습니다.

형식

알림의 권장 형식은 다음과 같은 사양을 포함합니다.

- 16비트 PCM wav 파일
- 스테레오 또는 모노
- 샘플 레이트 48kHz, 44.1kHz, 32kHz, 16kHz, 8kHz

기본 알림

사용자 지정 알림 wav 파일을 업로드하거나 시스템 알림을 위해 Cisco에서 제공하는 파일을 변경할 있습니다. 그러나 알림 ID를 변경할 수는 없습니다. 예를 들어 발신자가 잘못된 번호로 전화를 거는 경우 시스템 알림(VCA_00121)이 재생됩니다. 이를 일반적으로 빈 통화 알림이라고 합니다.

표 ***12:*** 알림 찾기 및 나열 창의 알림

알림 **ID**	설명
Gone_00126	시스템: 없음
MLPP-BNEA_00123	시스템: MLPP 통화 중 기능 없음
MLPP-BPA_00122	시스템: MLPP 높은 우선 순위
MLPP-ICA_00120	시스템: MLPP 서비스 중단
MLPP-PALA_00119	시스템: MLPP 우선 순위 액세스 제한
MLPP-UPA_00124	시스템: MLPP 인증되지 않은 우선 순위
Mobility_VMA	연결하려면 1을 누르십시오.
MonitoringWarning_00055	시스템: 모니터링 또는 녹음
RecordingWarning_00038	시스템: 녹음
TemporaryUnavailable_00125	시스템: 일시적 사용 불가
VCA_00121	시스템: 빈 번호/잘못된 번호로 전화 검
Wait_In_Queue_Sample	기본 제공: 샘플 대기열 발신자 주기적 알림
Welcome_Greeting_Sample	기본 제공: 샘플 발신자 인사말

미디어 리소스 구성 작업 플로우

이들 작업을 완료하여 시스템에 대한 미디어 리소스를 구성합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	소프트웨어 미디어 리소스 활성화, 140 페이지	IPVMS 서비스를 켜면 서버의 소프트웨어 미디어 리소스가 활성화됩니다.
단계 **2**	MTP(미디어 터미네이션 포인트) 구성, 141 페이지	시스템에 대한 미디어 터미네이션 포인트(MTP)를 구성합니다.
단계 **3**	트랜스코더 구성, 142 페이지	트랜스코더 리소스를 시스템에 추가합니다.
단계 **4**	IVR(대화형 음성 응답) 구성, 142 페이지	시스템 IVR에 대한 기본 설정을 구성합니다.
단계 **5**	음성 송출기 구성, 143 페이지	음성 송출기에 대한 시스템 설정을 구성합니다.
단계 **6**	미디어 리소스 그룹 구성, 143 페이지	미디어 리소스를 미디어 리소스 그룹에 추가합니다. 다양 한 리소스 조합을 사용하여 여러 그룹을 설정합니다.
단계 **7**	미디어 리소스 그룹 목록 구성, 144 페이지	엔드포인트 또는 엔드포인트 클래스에 할당할 수 있는 미디어 리소스 그룹 목록을 만듭니다.
단계 **8**	디바이스 또는 디바이스 풀에 미디어 리소스 할당, 144 페이지	디바이스 또는 디바이스 풀에 미디어 리소스를 할당하여 엔드포인트에서 사용할 수 있도록 만듭니다.
단계 **9**	알림 구성, 145 페이지	선택 사항. 특정 알림에 대한 설정을 구성합니다. 알림은 일반 처리 또는 음악 대기 또는 IVR과 같은 기능에 사용됩니다.
단계 **10**	사용자 지정된 알림 업로드, 145 페이지	선택 사항. 사전에 녹음된 알림를 업로드합니다. 파일을 새로운 알림 또는 기존 알림에 할당합니다.

소프트웨어 미디어 리소스 활성화

CISCO IP Voice Media Streaming 서비스를 활성화하여 다음 소프트웨어 미디어 리소스를 활성화합니다.

- 알림 디바이스

- IVR(Interactive Voice Response)
- MTP(미디어 터미네이션 포인트)
- 소프트웨어 전화회의 브리지
- 대기 중 음악

프로시저

단계 **1** Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.
단계 **2** 서버 드롭다운 목록에서 Unified Communications Manager 노드를 선택합니다.
단계 **3** **CISCO IP Voice Media Streaming** 서비스를 선택하고 저장을 클릭합니다.

MTP(미디어 터미네이션 포인트) 구성

이 절차를 사용하여 소프트웨어 MTP(미디어 터미네이션 포인트)를 구성합니다.

시작하기 전에

소프트웨어 MTP(미디어 터미네이션 포인트)가 활성화되도록 하려면 Cisco IP Voice Media Streaming 서비를 실행해야만 합니다.

필요한 MTP 리소스의 수와 필요한 MTP 디바이스의 수를 결정하여 이러한 리소스를 제공합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > 미디어 터미네이션 포인트를 선택합니다.
단계 **2** 다음 중 하나를 수행합니다.
- 찾기를 클릭하고 기존 MTP를 선택합니다.
- 새로 추가를 클릭하여 새 MTP를 생성합니다.

단계 **3** **MTP(**미디어 터미네이션 포인트**)**를 할당합니다.
단계 **4** 디바이스 풀을 할당합니다.
단계 **5** 이 MTP를 TRP(Trusted Relay Point)로 지정하려는 경우 **TRP(Trusted Relay Point)** 확인란에 체크 표시합니다.
단계 **6** 저장을 클릭합니다.

트랜스코더 구성

트랜스코더는 한 코덱의 입력 스트림을 다른 코덱을 사용하는 출력 스트림으로 변환하는 디바이스입니다.

시작하기 전에

IVR이 활성화되도록 Cisco IP Voice Media Streaming 서비스가 실행되고 있어야만 합니다.

필요한 트랜스코더 리소스의 수 및 이러한 리소스를 제공하는 데 필요한 트랜스코더 디바이스의 수를 결정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에 로그인하고 미디어 리소스 > 트랜스코더를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 트렁크를 선택합니다.
- 새로 추가를 클릭합니다.

단계 **3** 트랜스코더 유형을 선택합니다.

단계 **4** 트랜스코더의 **MAC** 주소를 입력합니다.

단계 **5** 드롭다운 메뉴에서 디바이스 풀을 할당합니다.

단계 **6** 이 트랜스코더를 TRP(Trusted Relay Point)로 사용할 수 있게 만들려는 경우, **TRP(Trusted Relay Point)** 확인란에 체크 표시합니다.

단계 **7** 저장을 클릭합니다.

IVR(대화형 음성 응답) 구성

이 절차를 사용하여 IVR에 대한 설정을 구성합니다.

시작하기 전에

IVR(대화형 음성 응답)을 활성화하려면 Cisco IP Voice Media Streaming 서비스를 실행해야만 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > **IVR(**대화형 음성 응답**)**을 선택합니다.

단계 **2** 찾기를 클릭하고 IVR을 선택합니다.

단계 **3** 이름과 설명을 입력합니다.

단계 **4** IVR 통화에서 TRP(Trusted Relay Point)를 사용하려면, **TRP** 사용 드롭다운을 **ON**으로 설정합니다.

단계 **5** **IVR(**대화형 음성 응답**)** 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

음성 송출기 구성

음성 송출기에 대한 시스템 설정을 구성합니다.

시작하기 전에

알림 디바이스를 활성화 하려면 Cisco IP Voice Media Streaming service가 실행 되 고 있어야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > 음성 송출기를 선택합니다.

단계 **2** 찾기를 클릭하고 음성 송출기를 선택합니다.

단계 **3** 이름과 설명을 입력합니다.

단계 **4** 디바이스 풀을 선택합니다.

단계 **5** 음성 송출기에서 신뢰할 수 있는 릴레이 포인트를 사용하도록 하려는 경우, 신뢰할 수 있는 릴레이 포인트 사용 드롭다운을 **ON**으로 설정합니다.

단계 **6** 저장을 클릭합니다.

미디어 리소스 그룹 구성

미디어 리소스 그룹에는 엔드포인트 또는 엔드포인트 그룹에 할당하려는 미디어 리소스 목록이 포함되어 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > 미디어 리소스 그룹을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 미디어 리소스 그룹을 선택합니다.
- 새로 추가를 클릭하여 새 미디어 리소스 그룹을 만듭니다.

단계 **3** 미디어 리소스 그룹 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 그룹의 이름과 설명을 입력합니다.

단계 **5** 사용 가능한 미디어 리소스에서 이 그룹에 추가하려는 리소스를 선택하고 화살표를 사용하여 선택한 미디어 리소스로 리소스를 이동합니다.

단계 **6** (선택 사항) 음악 대기 오디오에 대한 멀티캐스트를 사용하려면, **MOH** 오디오에 대한 멀티캐스트 사용 확인란에 체크 표시합니다.

단계 **7** 저장을 클릭합니다.

미디어 리소스 그룹 목록 구성

미디어 리소스 그룹의 우선순위 목록을 생성합니다. 이 목록을 개별 디바이스 또는 디바이스 풀에 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > 미디어 리소스 그룹 목록을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 목록을 선택합니다.
- 새로 추가클릭하고 새 목록을 생성합니다.

단계 **3** 미디어 리소스 그룹 목록의 이름을 입력합니다.

단계 **4** 사용 가능한 미디어 리소스 그룹에서 추가하려는 그룹을 선택하고 화살표를 사용하여 선택한 미디어 리소스 그룹으로 이동합니다.

단계 **5** 저장을 클릭합니다.

참고 엔드포인트에서 이러한 미디어 리소스를 사용하려면, 목록을 디바이스 풀, 게이트웨이 포트 또는 특정 디바이스에 할당해야만 합니다.

디바이스 또는 디바이스 풀에 미디어 리소스 할당

우선순위가 지정된 미디어 리소스 그룹 목록을 디바이스 풀 또는 개별 디바이스에 연결하여 엔드포인트에 미디어 리소스를 할당합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

- 디바이스 풀에 미디어 리소스를 추가 하려면 시스템 > 디바이스 풀을 선택합니다.
- 엔드포인트에 직접 미디어 리소스를 추가하려면 디바이스 > 전화기를 선택합니다.

단계 **2** 찾기를 클릭하고 이러한 미디어 리소스를 할당하려는 디바이스 풀 또는 디바이스를 선택합니다.

단계 **3** 미디어 리소스 그룹 목록 드롭다운에서 목록을 선택합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 선택한 항목에 구성 적용을 클릭합니다.
디바이스 이름과 적용 가능한 구성 변경 내용을 보여주는 구성 적용 창이 표시됩니다.

알림 구성

시스템 알림 또는 기능 알림으로 사용할 수 있는 알림을 구성할 수 있습니다. 시스템 알림은 통화 처리 또는 샘플 기능 알림의 사용에 사용되는 반면, 기능 알림은 헌트 파일럿 통화 대기 또는 외부 통화 제어와 관련하여 MOH(음악 대기)와 같은 특정 기능에 사용됩니다.

Cisco Unified Communications Manager에서 기존 알림을 수정하거나 새로운 알림을 구성할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > 공지사항을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 편집할 기존 알림을 선택합니다.
- 새로 추가를 클릭하여 새 알림을 추가합니다.

단계 **3** 알림 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

사용자 지정된 알림 업로드

다른 알림을 사용하여 업로드된 사용자 지정된 .wav 파일을 사용하여 기본 알림을 수정할 수 있습니다. 오디오 소스 파일을 가져오면 Unified Communications Manager가 파일을 처리하여 음악 대기 서버에서 사용할 수 있는 올바른 형식으로 변환합니다.

참고 알림은 로캘(언어)별로 고유합니다. 설치에서 여러 언어 로캘을 사용하는 경우, 각 사용자 지정된 알림을 개별 언어로 별도의 wav 파일에 기록해야하고 적절한 로캘을 할당하여 업로드해야 합니다. 또한 이 작업을 위해 미국 영어 이외의 다른 언어로 사용자 지정된 알림 wav 파일을 업로드하려면 먼저 각 서버에 적절한 로캘 패키지도 설치해야 합니다.

MOH 오디오 소스 파일과 유사한 알림의 권장 형식에는 다음 사양이 포함됩니다.

- 16비트 PCM .wav 파일
- 스테레오 또는 모노
- 샘플 레이트 48kHz, 44.1kHz, 32kHz, 16kHz, 8kHz

Unified Communications Manager의 알림 찾기 및 나열 창에서 하이퍼링크되지 않은 알림은 업데이트할 수 없습니다. 이 창의 하이퍼링크를 사용하여 밑줄이 표시된 Cisco에서 제공하는 알림에 대해 사용자 지정된 알림을 추가할 수 있습니다. 예를 들면, MLPP-ICA_00120 및 MonitoringWarning_00055입니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > 알림을 선택합니다.

단계 **2** 알림 찾기 및 나열 창에서 검색 기준을 입력하고, 찾기를 클릭한 다음 결과 목록에서 해당 알림에 대한 하이퍼링크를 클릭합니다.

단계 **3** 알림 구성 창에서 파일 업로드를 클릭합니다.

단계 **4** 파일 업로드 팝업 창에서 로캘을 선택하고 파일 이름을 입력하고 .wav 파일을 탐색하여 선택한 다음 파일 업로드를 클릭합니다.

업로드 프로세스가 시작되고, 처리가 완료되면 해당 상태가 업데이트됩니다. 닫기를 선택하여 파일 업로드 창을 닫습니다.

단계 **5** (선택 사항) Unified Communications Manager에서 Cisco에서 제공하는 알림을 재생하는 대신 사용자 정의된 알림을 재생하려는 경우, 알림 설정 창의 로케일별 알림 창에 활성화 확인란이 표시되는지 확인하십시오.

활성화 확인란이 체크 표시되어 있지 않은 경우, Unified Communications Manager에서 Cisco에서 제공한 알림을 재생합니다.

단계 **6** 저장을 클릭합니다.

다음에 수행할 작업

알림 파일이 클러스터 내의 서버 간에 전파되지 않으므로 클러스터의 각 노드에서 알림을 업로드합니다. 클러스터 내 각 서버에서 Cisco Unified Communications Manager 관리를 탐색하고 업로드 프로세스를 반복합니다.

14 장

전화회의 브리지 구성

전화회의 브리지 개요

Cisco Unified Communications Manager의 컨퍼런스 브리지는 애드-혹 및 Meet-Me 음성 전화회의를 모두 허용하도록 설계된 소프트웨어 또는 하드웨어 애플리케이션입니다. 추가 전화회의 브리지 유형은 화상 전화회의를 포함한 다른 유형의 전화회의를 지원합니다. 각 컨퍼런스 브리지는 여러 개의 동시 다자간 전화회의를 호스팅할 수 있습니다. 하드웨어 전화회의 브리지와 소프트웨어 전화회의 브리지를 동시에 활성화할 수 있습니다. 소프트웨어 및 하드웨어 전화회의 브리지는 스트림 수와 지원되는 코덱 유형이 다릅니다. 새 서버를 추가하면 시스템에서 소프트웨어 전화회의 브리지를 자동으로 추가합니다.

참고 Cisco Unified Communications Manager 서버가 생성되면 전화회의 브리지 소프트웨어도 자동으로 생성되며, 이는 삭제할 수 없습니다. 전화회의 브리지 소프트웨어를 Cisco Unified Communications Manager 관리에 추가할 수 없습니다.

전화회의 브리지 유형

다음 전화회의 브리지 유형은 Cisco Unified Communications Manager 관리에서 사용할 수 있습니다.

표 **13:** 전화회의 브리지 유형

컨퍼런스 브리지 유형	설명
Cisco Conference Bridge Hardware	이 유형은 Cisco Catalyst 4000 및 6000 음성 게이트웨이 모듈과 다음 수의 전화회의 세션을 지원합니다. **Cisco Catalyst 6000** • G.711 또는 G.729432 전화회의 - 포트당 32명의 참가자, 전화회의당 6명의 참가자, 모듈당 총 256명의 참가자, 3명의 참가자에 10개의 브리지. • GSM - 포트당 24명의 참가자, 전화회의당 최대 6 명의 참가자, 모듈 당 총 192명의 참가자. **Cisco Catalyst 4000** G.711 전화회의만 해당 - 24명의 전화회의 참가자, 6명의 참가자 각각이 포함된 최대 4개의 전화회의.
Cisco Conference Bridge 소프트웨어	소프트웨어 전화회의 디바이스는 기본값으로 G.711 코덱을 지원합니다. 이 유형의 최대 발신자 수는 256입니다. 256으로 설정된 경우, 소프트웨어 컨퍼런스 브리지는 각각 4명의 발신자로 설정된 64건의 컨퍼런스 세션을 지원할 수 있습니다. 전화회의 세션의 최대 발신자 수는 최대 애드-혹 전화회의 및 최대 **MeetMe** 전화회의 유니캐스트 서비스 매개변수를 통해 지정됩니다. 주의 이 유형의 전화회의 브리지(SW 전화회의 브리지)는 구현하기에 간단합니다. 무음 상태의 대상자를 식별하지 않으며 단순한 서밍 알고리즘을 사용합니다. 이 알고리즘은 참가자의 수가 많을 때 전화회의의 오디오 품질과 낮은 볼륨 레벨 문제를 야기할 수 있습니다.
Cisco IOS Conference Bridge	• NM-HDV 또는 NM-HDV 네트워크 모듈을 사용합니다. • G.711 a/mu-law, G.729, G.729a, G.729b, G.297ab 참가자는 단일 전화회의 통화에 참가할 수 있습니다. • 최대 6명의 대상자가 단일 전화회의 통화에 참가할 수 있습니다. Cisco Unified Communications Manager에서 동적 기준에 따라 전화회의 리소스를 통화에 할당합니다. 음성 게이트웨이 라우터에 대한 Cisco IOS 컨퍼런싱 및 트랜스코딩에 대한 자세한 내용은, 이 제품과 함께 수령한 Cisco IOS 설명서를 참조하십시오.

컨퍼런스 브리지 유형	설명
Cisco IOS 인해스드 브리지	• Cisco 2800 및 3800 시리즈 음성 게이트웨이 라우터에서 온보드 Cisco Packet Voice/Fax Digital Signal Processor Modules(PVDM2)을 사용하거나 NM-HD 또는 NM-HDV2 네트워크 모듈을 사용합니다. • G.711 a-law/mu-law, G.729, G.729a, G.729b, G.729ab, GSM FR 및 GSM EFR 참가자는 단일 전화회의에 참가할 수 있습니다 • 최대 8명의 대상자가 단일 통화에 참가할 수 있습니다. 참고 ISR4000 라우터 및 SM-X-PVDM-3000/ SM-X-PVDM-2000/ SM-X-PVDM-1000/ SM-X-PVDM-500을 사용하는 경우, 각 전화회의 브리지 프로파일에서는 Unified Communications Manager 4096 최대 스트림 제한으로 인해 최대 512건의 세션까지 등록할 수 있습니다. Cisco Unified Communications Manager에서 동적 기준에 따라 전화회의 리소스를 통화에 할당합니다. 음성 게이트웨이 라우터에 대한 Cisco IOS 컨퍼런싱 및 트랜스코딩에 대한 자세한 내용은, 이 제품과 함께 수령한 Cisco IOS 설명서를 참조하십시오. 이 전화회의 브리지 유형은 ISR 4000 시리즈 게이트웨이가 구축되어 있는 지원되는 SIP 전화기에 대해 AES_CM_128_HMAC_SHA1_80로 SRTP 미디어 암호화를 지원합니다. SCCP 전화기 및 지원되지 않는 SIP 전화기는 AES_CM_128_HMAC_SHA1_32 암호화로 폴백됩니다. 참고 게이트웨이 로드가 해당 암호를 지원하는지 확인합니다. 지원에 대한 상세 정보는 게이트웨이 설명서를 참조하십시오.
Cisco 전화회의 브리지 (WS-SVC-CMM)	이 전화회의 브리지 유형은 Cisco Catalyst 6500 시리즈 및 Cisco 7600 시리즈 communications Media Module(CMM)을 지원합니다. 전화회의 당 최대 8명의 대상자와 포트 어댑터 당 최대 64건의 전화회의를 지원합니다. 이 전화회의 브리지 유형은 다음 코덱을 지원합니다. 이 전화회의 브리지 유형은 애드-혹 전화회의를 지원합니다. • G.711 a-law/mu-law • G.729 부록 A 및 부록 B • G.723.1
Cisco 비디오 전화회의 브리지(IPVC-35xx)	Cisco 비디오 전화회의 브리지는 Cisco IP 비디오 전화기, H.323 엔드포인트 및 오디오 전용 Cisco Unified IP Phone에 오디오 및 비디오 전화회의 기능을 제공합니다. Cisco 비디오 전화회의 브리지는 비디오용 H.261, H.263 및 H.264 코덱을 지원합니다.

컨퍼런스 브리지 유형	설명
Cisco IOS 이종 비디오 전화회의 브리지	Cisco ISR G2(Integrated Services Routers Generation 2)는 즉석 및 MeetMe 비디오 전화회의를 지원하는 IOS 기반 전화회의 브리지 역할을 할 수 있습니다. 라우터를 전화회의 브리지로 사용하려면 DSP 모듈을 라우터에 설치해야 합니다. 이종 비디오 전화회의에서 모든 전화회의 참가자는 서로 다른 비디오 형식 특성을 사용하는 전화기를 통해 전화회의 브리지에 연결됩니다. 이종 회의에서 다양한 형식 간에 신호를 변환하려면 트랜스코딩 및 Transsizing 기능이 필요합니다. 이종 비디오 회의에서 발신자는 다음 조건에 따라 전화회의에 오디오 참가자로 연결됩니다. • DSP 리소스가 불충분한 경우 • 전화기의 비디오 기능을 지원하지 않도록 전화회의 브리지가 구성된 경우 ISR G2 라우터를 사용하는 비디오 전화회의에 대한 자세한 내용은, 비디오 전화회의 구성 및 비디오 트랜스코딩을 참조하십시오.
Cisco 보증 오디오 비디오 전화회의 브리지	Cisco Integrated Services Routers 2세대(ISR G2)는 Routers Generation 2)는 애드-혹 및 MeetMe 음성 및 비디오 전화회의를 지원하는 IOS 기반 전화회의 브리지로 작동할 수 있습니다. 라우터를 전화회의 브리지로 사용하려면 DSP 모듈을 라우터에 설치해야 합니다. DSP 리소스는 전화회의의 오디오 부분을 위해 예약되어 있으며 비디오 서비스는 보장되지 않습니다. 전화회의 시작 시 DSP 리소스를 사용할 수 있는 경우, 비디오 전화기의 발신자는 비디오 서비스를 받을 수 있습니다. 그렇지 않으면, 발신자는 오디오 참가자로 전화회의에 연결됩니다. ISR G2 라우터를 사용하는 비디오 전화회의에 대한 자세한 내용은, 비디오 전화회의 구성 및 비디오 트랜스코딩을 참조하십시오.

컨퍼런스 브리지 유형	설명
Cisco IOS 동종 화상 회의 브리지	Cisco ISR G2(Integrated Services Routers Generation 2)는 즉석 및 MeetMe 비디오 전화회의를 지원하는 IOS 기반 전화회의 브리지 역할을 할 수 있습니다. 라우터를 전화회의 브리지로 사용하려면 DSP 모듈을 라우터에 설치해야 합니다. Cisco IOS 동종 비디오 전화회의 브리지는 동종 비디오 전화회의를 지원하는 IOS 기반 전화회의 브리지 유형입니다. 동종 비디오 전화회의는 모든 참가자가 동일한 비디오 형식 특성을 사용하여 연결되는 비디오 전화회의입니다. 모든 비디오 전화기가 동일한 비디오 형식을 지원하고 전화회의 브리지에서 모든 비디오 참가자에게 동일한 데이터 스트림 형식을 전송합니다. 전화회의 브리지가 전화기의 비디오 형식을 지원하도록 미구성 경우, 해당 전화기의 발신자는 오디오 전용 참가자로 전화회의에 연결됩니다. ISR G2 라우터를 사용하는 비디오 전화회의에 대한 자세한 내용은, 비디오 전화회의 구성 및 비디오 트랜스코딩을 참조하십시오.

컨퍼런스 브리지 유형	설명
Cisco TelePresence MCU	Cisco TelePresence MCU는 Cisco Unified Communications Manager의 하드웨어 전화회의 브리지 세트입니다. Cisco TelePresence MCU는 HD(High-Definition) 멀티포인트 비디오 컨퍼런스 브리지입니다. 초당 30프레임, 모든 전화회의에 대한 완벽한 연속 프레즌스, 전체 트랜스코딩으로 최대 1080p를 제공하며, 혼합 HD 엔드포인트 환경에 가장 적합합니다. Cisco TelePresence MCU에는 신호 처리 통화 제어 프로토콜로 SIP가 지원됩니다. 시스템 및 전화회의의 전체 구성, 제어 및 모니터링을 수행할 수 있는 내장 웹 서버에 있습니다. Cisco TelePresence MCU는 HTTP를 통한 XML 관리 API를 제공합니다. Cisco TelePresence MCU에서는 즉석 및 회의개설 음성/비디오 전화회의를 모두 수행할 수 있습니다. 각 컨퍼런스 브리지는 여러 개의 동시 다자간 전화회의를 호스팅할 수 있습니다. Cisco Unified Communications Manager에서는 Unified Communications Manager와 Cisco TelePresence MCU 사이에서 Binary Floor Control Protocol(BFCP)과의 프레젠테이션 공유를 지원합니다. Cisco TelePresence MCU는 포트 예약 모드로 구성해야만 합니다. 자세한 내용은 *Cisco TelePresence MCU* 구성 설명서를 참조하십시오. 참고 Cisco TelePresence MCU는 일반적인 Out-of-band DRMF 방법을 지원하지 않습니다. 기본 설정에서 Cisco Unified Communications Manager에서는 미디어 터미네이션 포인트(MTP)가 필요하지 않습니다. 하지만 미디어 터미네이션 포인트 필수 확인란이 체크 표시된 경우, Cisco Unified Communications Manager에서 MTP를 할당하고 SIP 트렁크가 RFC2833에 따라 DTMF에 대해 협상합니다.
Cisco TelePresence Conductor	Cisco TelePresence Conductor는 인텔리전트 전화회의 관리 제어 기능을 제공하며 확장 가능하므로 여러 MCU 간 로드 밸런싱 및 복수 디바이스 가용성을 위한 디바이스 클러스터링을 지원할 수 있습니다. 관리자는 Cisco UCS(Cisco Unified Computing System) 플랫폼 또는 타사 기반 플랫폼을 지원하는 VMware에 Cisco TelePresence Conductor를 어플라이언스 또는 가상화된 애플리케이션으로 구현할 수 있습니다. Cisco TelePresence Conductor는 각각의 새로운 전화회의에 가장 적합한 Cisco TelePresence 리소스를 동적으로 선택합니다. 애드-혹, “MeetMe” 및 예약된 음성 및 비디오 전화회의가 역동적으로 성장하여 개별 MCU의 용량을 초과할 수 있습니다. Cisco TelePresence Conductor 어플라이언스 또는 가상화된 애플리케이션은 탁월한 복원력을 제공하도록 최대 3개까지 클러스터링할 수 있습니다. One Cisco TelePresence Conductor 어플라이언스 또는 Cisco TelePresence Conductor 클러스터의 시스템 용량은 30 MCU 또는 2400 MCU 포트에 달합니다.

컨퍼런스 브리지 유형	설명
Cisco Meeting Server	이 전화회의 브리지 솔루션을 사용하면 임시, 지금 미팅, Conference Now 및 랑데부 전화회의가 가능합니다. 이 전화회의 브리지는 프레미스 기반 오디오, 비디오 및 웹 컨퍼런싱 기능을 제공하며 타사 온프레미스 인프라에서도 작동합니다. 소규모 또는 대규모 구축에 맞추어 크기가 조정됩니다. 필요에 따라 용량을 점증적으로 추가하여 조직의 현재 및 향후 요구를 지원할 수 있도록 보장할 수 있습니다. 이 전화회의 브리지는 고급 상호운용성을 제공합니다. 참가자 수에 상관 없이 다음에서 미팅을 생성하고 참여할 수 있습니다. • Cisco 또는 타사 회의실 또는 데스크톱 비디오 시스템 • Cisco Jabber Cilent • Cisco Meeting App(기본 사용 또는 WebRTC 호환 브라우저 사용 가능) • Skype for Business Cisco Meeting Server 2.0의 최소 릴리스에서는 Cisco Meeting Server 전화회의 브리지를 사용해야 합니다. Cisco Meeting Server는 신호 처리 통화 제어 프로토콜로 SIP를 지원합니다. 시스템 및 전화회의의 전체 구성, 제어 및 모니터링을 수행할 수 있는 내장 웹 서버에 있습니다. Cisco Meeting Server는 HTTP를 통한 XML 관리 API를 제공합니다. 참고 Cisco Meeting Server는 H.265 비디오 코덱 및 종단 카메라 제어를 지원하지 않습니다.

전화회의 브리지 구성 작업 플로우

프로시저

	명령 또는 동작	목적
단계 **1**	전화회의 브리지 구성, 154 페이지	하드웨어 또는 소프트웨어 전화회의 브리지를 구성하여 애드-혹 및 Meet-me 음성 전화회의를 모두 허용합니다.
단계 **2**	전화회의 브리지에 대한 서비스 매개변수 구성, 154 페이지	네트워크에 Cisco IOS Conference Bridge 및 Cisco IOS Enhanced Conference Bridge가 모두 포함된 경우, 이 절차를 수행합니다.
단계 **3**	전화회의 브리지에 SIP 트렁크 연결 구성, 154 페이지	이 절차를 수행하여 전화회의 브리지에 대한 SIP 트렁크 연결을 구성합니다.

전화회의 브리지 구성

하드웨어 또는 소프트웨어 전화회의 브리지를 구성하여 애드-혹 및 Meet-me 음성 전화회의를 모두 허용해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 미디어 리소스 > 전화회의 브리지를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화회의 브리지 구성 창에서 필드를 구성합니다. 필드에 대한 상세 설명은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

네트워크에 Cisco IOS Conference Bridge 및 Cisco IOS Enhanced Conference Bridge가 모두 포함된 경우, 전화회의 브리지에 대한 서비스 매개변수 구성, 154 페이지.

전화회의 브리지에 대한 서비스 매개변수 구성

네트워크에 Cisco IOS Conference Bridge 및 Cisco IOS Enhanced Conference Bridge가 모두 포함된 경우, 이 절차를 수행합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서비스 매개변수 구성 창에서 서버를 선택하고 Cisco CallManager 서비스를 선택합니다.

단계 **3** 클러스터 수준 매개변수(기능 - 전화회의) 섹션에서 다음 매개변수를 6으로 설정합니다.

- Maximum Ad Hoc Conference
- Maximum MeetMe Conference Unicast

단계 **4** 저장을 클릭합니다.

전화회의 브리지에 **SIP** 트렁크 연결 구성

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 **2** 다음 단계 중 하나를 완료해야 합니다.

- 새 SIP 트렁크를 추가하려면 새로 추가를 클릭합니다.
- 기존 트렁크에 대한 연결을 추가하려는 경우, 찾기를 클릭하고 해당 트렁크를 선택합니다.

단계 **3** 디바이스 프로토콜을 **SIP**로 선택합니다.

단계 **4** 트렁크 서비스 유형을 없음으로 선택합니다.

단계 **5** 전화회의 브리지에 대한 IP 주소 또는 호스트네임을 추가하여 대상 영역에서 전화회의 브리지에 대한 항목을 만듭니다. 새 회선이 필요한 경우, **(+)**를 클릭하여 추가할 수 있습니다.

단계 **6** 정규화 스크립트 드롭다운 목록 상자에서 정규화 스크립트를 선택합니다. 예를 들어, 다음과 같은 스크립트는 필수입니다.

- **cisco-telepresence-conductor-interop** – 이 트렁크를 Cisco TelePresence Conductor에 연결 중인 경우, 이 스크립트를 선택합니다.
- **cisco-telepresence-mcu-ts-direct-interop** – 이 트렁크를 Cisco TelePresence MCU에 연결 중인 경우, 이 스크립트를 선택합니다.
- **cisco-meeting-server-interop** – 이 트렁크를 Cisco Meeting Server에 연결 중인 경우, 이 스크립트를 선택합니다.

단계 **7** 트렁크 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

15 장

고급 위치 기반 콜수락 제어(CAC) 구성

고급 위치 기반 콜수락 제어(CAC)

고급 위치 기반 콜수락 제어(CAC)를 사용하면 복잡한 WAN 토폴로지 및 인터클러스터 네트워크를 통해 오디오 품질 및 비디오 가용성을 제어할 수 있습니다. 여기에는 멀티 티어 및 멀티 홉 네트워크가 포함됩니다.

전체 네트워크 토폴로지 모델을 생성하여, 해당 위치를 연결하는 다른 위치(LAN) 및 WAN 링크를 나타낼 수 있습니다. 각 위치 및 WAN 링크의 경우, 해당 링크에서의 모든 통화에 대해 한 번에 사용할 수 있는 총 대역폭을 나타내는 대역폭 한도를 할당합니다. 특정 통화에 대한 대역폭을 사용할 수 없는 경우, 통화 중 신호를 통해 통화가 거부됩니다. 이렇게 하면 WAN 링크가 초과 가입된 결과로 인한 오디오 및 비디오 품질의 저하가 방지됩니다.

LBM(Location Bandwidth Manger) 복제 그룹의 인터클러스터 복제 기능을 사용하면 인터클러스터 네트워크에서 위치 구성을 복제하여, 대규모 클러스터 네트워크에서 더 쉽게 관리할 수 있습니다.

고급 위치 기반 콜수락 제어(CAC) 구성 요소

이 기능은 다음 구성 요소를 사용합니다.

- 위치—위치는 LAN을 나타냅니다. 위치는 엔드포인트를 포함하거나, 단순히 WAN 네트워크 모델링을 위한 링크 간 통과 위치의 역할을 합니다. Cisco Unified Communications Manager에서는 최대 2000개의 위치를 지원합니다.
- 링크—두 위치 간의 연결입니다. 이 기능을 구성하면 각 링크에 대한 대역폭 할당과 가중치를 할당합니다.
- 가중치—위치 쌍 사이의 유효 경로를 형성할 때 링크의 상대적 우선 순위입니다. 가중치는 두 위치 간에 여러 경로가 존재하는 경우에만 사용됩니다. 가중치는 유효한 경로(최소 누적 가중치를 갖는 경로)를 계산하기 위해 사용됩니다.

- 대역폭 할당—특정 링크에서 특정 트래픽 유형(오디오, 데스크톱 비디오, 몰입형 비디오)에 할당된 총 대역폭입니다. 대역폭은 내부 위치 통화에 대해 할당될 수도 있습니다(기본 설정은 제한 없음).
- LBM(Location Bandwidth Manager)—고급 위치 기반 콜수락 제어(CAC)가 작동하려면 Cisoc Unified Serviceability에서 반드시 활성화되어야 하는 기능 서비스입니다. 이 서비스는 네트워크 모델을 조합하고, 소스와 대상 사이의 모든 링크와 위치의 가중치를 추가하여 그리고 최소 누적 가중치를 갖는 경로를 선택하여 위치 간 유효한 경로를 계산합니다.

지역에 대한 위치 관계

고급 위치 기반 콜수락 제어(CAC)의 위치 구성은 지역을 통해 적용되어 통화에 대한 대역폭을 관리합니다.

- 지역 구성 내의 대역폭 할당은 두 지역 간 통화의 엔드포인트가 사용할 수 있는 총 대역폭을 할당합니다.
- 위치 구성 내의 대역폭 할당은 이들 위치 간의 모든 통화에서 사용할 수 있는 총 대역폭을 할당합니다. 개별 통화의 경우, 지역 구성 내의 대역폭은 위치 구성에서 사용할 수 있는 대역폭에서 차감됩니다. 예를 들어, 위치 구성에서 특정 링크를 통해 160 kb/s의 대역폭을 사용할 수 있다고 지정할 경우, 해당 링크는 80 kb/s에서 두 개의 G.711 통화를 각각 동시에 지원할 수 있습니다.

참고 서버의 CPU 사용률을 불필요하게 급증 시킬 수 있기 때문에 제조 중에는 Location Bandwidth Manager 대역폭 또는 링크 구성을 변경하지 마십시오.

Cisco Unified Communications Manager에서는 클러스터당 최대 2,000개의 위치와 2,000개의 지역을 지원합니다.

인터클러스터 LBM 복제

위치 대역폭 관리자 허브 그룹의 인터클러스터 복제 기능을 사용하여 대규모 인터클러스터 네트워크에서 위치 및 링크 할당을 복제할 수 있습니다. LBM을 LBM 허브에 할당하여, 인터클러스터 메시형 네트워크에서 위치와 링크 정보를 적극적으로 복제할 수 있습니다. LBM 허브는 공통된 연결을 통해 서로를 검색하고 완전한 망형 복제 네트워크를 형성합니다. 스포크 역할을 할당받은 LBM은 해당 클러스터의 LBM 허브를 통해 인터클러스터 복제에 간접적으로 참가합니다.

인터클러스터 토폴로지 관리

인터클러스터 네트워크를 구성하고 관리하기 위한 여러 방법이 있습니다. 다음 표는 인터클러스터 토폴로지를 구성하고 관리하는 두 가지 접근 방법을 요약하고 있습니다.

설계 접근 방식	설명
위치 및 링크 관리	단일 클러스터를 사용하여 인터클러스터 네트워크의 모든 링크에 대한 대역폭 할당을 구성하고 관리합니다. 이 방식은 특히 많은 공통 위치를 사용하여 구축 시 구성 오버헤드를 단순화합니다. 인터클러스터 구성 방식은 다음과 같습니다. 관리 클러스터에서 전체 토폴로지에 대한 모든 위치 및 링크(대역폭 할당 및 가중치 포함)를 구성합니다. 이 정보는 인터클러스터 네트워크로 복제됩니다. 토폴로지의 다른 클러스터의 경우: • 로컬 클러스터에 대한 위치만 구성합니다. 이렇게하면 디바이스를 위치에 연결될 뿐입니다. • 링크 정보를 구성하지 마십시오. • 로컬 클러스터에서 모든 대역폭 할당을 무제한으로 유지합니다. 관리 클러스터에서 로컬 클러스터 보다 낮은 대역폭 할당을 복제하는 경우, 더 제한적인 구성이 적용됩니다.
인터클러스터 고급 위치 기반 콜수락 제어(CAC)	이 접근 방식을 이용할 경우: • 각 클러스터 내에서 로컬 위치와 링크 정보를 인접한 클러스터에만 구성합니다. • 가중치 및 대역폭을 포함한 링크 정보를 인접한 클러스터에만 할당합니다. 나머지 토폴로지도 복제됩니다 • Hub_None 위치는 클러스터마다 고유한 이름으로 변경해야 합니다. 그렇지 않을 경우, 클러스터에서 공통 위치가 됩니다. • 각 클러스터마다 고유의 클러스터 ID가 필요합니다. 참고 모든 클러스터 내에서 일관된 방식으로 클러스터의 이름을 지정하는 것이 복제를 위해 중요합니다.

고급 위치 기반 콜수락 제어(CAC) 사전 요건

이 기능을 구성하기 전에 먼저 LAN 및 WAN 네트워크 토폴로지를 이해하고 있어야 합니다. 위치 및 링크에 대한 대역폭을 할당하기 위해 필요하기 때문입니다.

고급 위치 기반 콜수락 제어(CAC) 작업 플로우

이러한 작업을 완료하여 시스템에서 고급 위치 기반 콜수락 제어(CAC)를 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	위치 대역폭 관리자 활성화, 160 페이지	Cisco Location Bandwidth Manager 기능 서비스가 하나 이상의 클러스터 노드에서 실행되고 있어야만 합니다.
단계 2	LBM 그룹 설정, 161 페이지	기본값으로 Cisco Callmanager 서비스는 로컬 LBM 서비스와 통신합니다. 그러나 LBM 그룹을 사용하여 이 통신을 관리하여, 리던던시에 대한 활성 및 대기 LBM 상태를 제공할 수 있습니다.
단계 3	위치 및 링크 구성, 161 페이지	네트워크에 대한 위치(LAN)를 생성하고 해당 위치를 연결하는 WAN 링크에 대한 대역폭 할당을 할당합니다.
단계 4	LBM 인터클러스터 복제 그룹 구성, 162 페이지	구성된 CAC 정보를 다른 클러스터에 복제하는 인터클러스터 복제 그룹을 생성합니다.
단계 5	SIP 인터클러스터 트렁크 구성, 162 페이지	네트워크의 SIP 인터클러스터 트렁크에 그림자 위치를 할당합니다.
단계 6	콜수락 제어(CAC) 서비스 매개변수 구성, 163 페이지	(선택 사항) 콜수락 제어(CAC)에 대한 서비스 매개변수 설정을 구성합니다. 대부분의 구축에서는 기본 설정 만으로도 충분합니다.

위치 대역폭 관리자 활성화

고급 위치 콜수락 제어(CAC)의 경우, 클러스터에 있는 하나 이상의 노드에서 Cisco Location 대역폭 관리자 기능 서비스를 활성화해야 합니다. 이 서비스는 기본값으로 꺼져 있습니다.

프로시저

단계 1 Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.

단계 2 서버 드롭다운에서 서비스를 실행하려는 클러스터 노드를 선택하고 이동을 클릭합니다.

단계 3 **CM** 서비스에서 **Cisco Location** 대역폭 관리자 서비스에 체크 표시합니다.

단계 4 저장을 클릭합니다.

단계 5 추가 노드에서 서비스를 시작하려는 경우, 이 작업을 반복합니다.

참고 Cisco에서는 Cisco CallManager 서비스를 실행하는 클러스터의 각 가입자 노드에서 Cisco Location 대역폭 관리자 서비스를 실행할 것을 권장합니다.

LBM 그룹 설정

이 절차를 사용하여 LBM 그룹을 구성합니다. 기본값으로 Cisco Callmanager 서비스는 로컬 LBM 서비스와 통신합니다. 그러나 LBM 그룹을 사용하여 이 통신을 관리하여, 리던던시에 대한 활성 및 대기 LBM 상태를 제공할 수 있습니다.

참고 Cisco CallManager 서비스에서 LBM을 사용하는 순서는 다음과 같습니다.

- LBM 그룹 지정
- 로컬 LBM(공존)

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 위치 > 위치 대역폭 관리자 그룹을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 그룹에 이름을 할당합니다.

단계 **4** 활성 구성원 드롭다운에서 이 그룹의 활성 구성원을 선택합니다.

단계 **5** 대기 구성원 드롭다운에서 활성 구성원을 사용할 수 없을 때 사용할 원하는 대기 구성원을 선택합니다.

단계 **6** 저장을 클릭합니다.

위치 및 링크 구성

이 절차를 사용하여 네트워크에서 위치(LAN)를 생성합니다. 이들 위치 간에 WAN 링크를 사용하는 통화에 대한 총 대역폭과 가중치를 할당합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 위치 정보 > 위치를 선택합니다.

단계 **2** 새로 추가를 클릭하여 새 위치를 생성합니다.

단계 **3** 위치에 대한 이름을 할당합니다.

단계 **4** 이 위치와 인접 위치 간의 링크 - 대역폭 영역에서 다른 위치로의 WAN 링크에 대한 설정을 다음과 같이 구성합니다.

a) 위치 목록 상자에서 두 번째 위치를 선택합니다.
b) 유효 경로를 구성할 때 이 링크의 상대적 우선 순위를 반영하는 가중치를 구성합니다.
c) 오디오, 비디오 및 몰입 형 비디오(TelePresence) 통화에 대한 총 대역폭을 구성합니다.

d) 이러한 하위 단계를 반복하여 추가 위치에 대한 링크를 구성합니다.

단계 **5** (선택 사항) 이 위치 내의 디바이스에 대한 위치 내 대역폭 영역을 확장하고 새로 만든 위치의 위치 내 통화에 대한 총 대역폭 할당을 구성합니다. 이러한 통화에 대한 모든 미디어 유형의 기본 설정은 무제한입니다.

단계 **6** 기타 위치에 대한 설정 수정 영역에서 다른 위치에 대한 RSVP 설정을 다음과 같이 구성합니다.

a) 위치 열에서 다른 위치를 선택합니다.

b) 러한 위치 간 통화에 대한 **RSVP** 설정을 선택합니다.

c) 이러한 하위 단계를 반복하여 추가 위치가 있는 통화에 대한 RSVP 설정을 추가합니다.

단계 **7** 저장을 클릭합니다.

단계 **8** 이 절차를 반복하여 추가 위치를 생성하고 이러한 새 위치에 대한 링크를 구성합니다.

LBM 인터클러스터 복제 그룹 구성

이 절차를 사용하여 LBM 인터클러스터 복제 그룹을 구성합니다. 이는 인터클러스터 네트워크 상에서 고급 위치 기반 콜수락 제어(CAC) 대역폭 정보를 복제하는 데 필요합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 위치 정보 > **LBM(**위치 대역폭 관리자 인터클러스터 복제 그룹을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 그룹에 대한 이름을 입력합니다.

단계 **4** 부트스트랩 서버 영역에서 연결 정보를 다른 허브로 복제하는 일을 담당하는 하나 이상의 LBM 서버를 할당합니다.

단계 **5** 역할 할당 영역에서 위쪽 및 아래쪽 화살표를 사용하여 허브로 작동할 로컬 LBM 서버와 스포크로 남아 있을 LBM 서버를 선택합니다.

단계 **6** 저장을 클릭합니다.

SIP 인터클러스터 트렁크 구성

고급 위치 기반 콜수락 제어(CAC)를 사용하여 인터클러스터 네트워크의 SIP 인터클러스터 트렁크에 그림자 위치를 할당해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 **2** 찾기를 클릭하고 적절한 인터클러스터 트렁크를 선택합니다.

단계 **3** 위치 드롭다운에서 그림자를 선택합니다.

단계 **4** 트렁크 구성 창에서 원하는 다른 필드를 모두 입력합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

단계 **6** 고급 위치 콜수락 제어(CAC)에 대한 정보를 복제하는 다른 인터클러스터 트렁크 대해 이 작업을 반복합니다.

콜수락 제어(CAC) 서비스 매개변수 구성

이 절차를 사용하여 고급 위치 기반 콜수락 제어(CAC)에 대한 선택적 서비스 매개변수 구성

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 클러스터 노드를 선택합니다.

단계 **3** **Cisco CallManager** 서비스에 대한 서비스 매개변수를 다음과 같이 구성합니다.

a) 서비스 드롭다운 목록에서 **Cisco CallManager**를 선택합니다.

b) 클러스터 수준 매개변수**(**콜수락 제어**(CAC))** 영역에서 서비스 매개변수를 구성합니다. 매개변수 도움말 설명을 보려면 GUI에서 매개변수 이름을 클릭하십시오.

c) 저장을 클릭합니다.

단계 **4** **Cisco** 위치 대역폭 관리자 서비스에 대한 설정을 구성합니다.

a) 서비스 드롭다운에서 **Cisco** 위치 대역폭 관리자를 선택합니다.

b) 원하는 모든 서비스 매개변수를 구성합니다. 매개변수 도움말 설명을 보려면 GUI에서 매개변수 이름을 클릭하십시오.

c) 저장을 클릭합니다.

고급 위치 기반 콜수락 제어(CAC) 상호 작용 제한 사항

다음 표에는 고급 위치 기반 콜수락 제어(CAC)에 대한 기능 상호 작용 및 제한 사항이 표시되어 있습니다.

기능	상호 작용 및 제한 사항
LBM 보안 모드	기본값으로 LBM 보안 모드는 Insecure입니다. **LBM** 보안 모드 엔터프라이즈 매개변수로 이 설정을 다시 구성할 수 있습니다. 이 매개변수는 **Secure**, **Insecure**또는 **Mixed**로 설정 가능합니다. **Mixed** 설정은 임시로 사용하여 모든 클러스터를 보호하면서 커뮤니케이션을 유지할 수 있습니다. 그 이후에는 **Secure**로 설정을 변경할 수 있습니다. 이 매개변수를 변경한 후에는 변경의 효과가 발생할 수 있도록 클러스터에서 모든 Cisco LBM 서비스 허브를 재설정해야 합니다.
화상 통화의 오디오 대역폭 도출	기본값으로 화상 통화의 오디오 부분에 대한 대역폭은 비디오 풀에서 도출됩니다. **Deduct Audio Portion from Audio Pool for Video Calls** 서비스 매개변수를 **True**로 설정하여(기본 설정= **False**) 화상 통화의 오디오 부분이 오디오 풀에서 도출될 수 있도록 시스템을 구성할 수 있습니다.
화상 통화 분류	Cisco TelePresence 엔드포인트는 **Immersive**의 구성이 가능하지 않은 화상 통화 분류를 가지고 있습니다. 다른 엔드포인트는 **Desktop**의 구성이 가능하지 않은 화상 통화 분류를 가지고 있습니다. SIP 트렁크의 경우, 연결된 SIP 프로파일 내에서 **Video Call Traffic Class**를 구성하여 비디오 분류(Desktop, Immersive 또는 Mixed)를 설정할 수 있습니다.
미디어 리소스	미디어 리소스의 대역폭은 콜수락 제어(CAC)를 통해 할당되지 않습니다.
위치 서비스 가용성	Cisoc Unified Serviceability 인터페이스에는 위치 토폴로지 관리 및 모니터링을 위한 추가 도구가 포함되어 있습니다. 자세한 내용은 *Cisoc Unified Serviceability* 관리 설명서의 "위치" 주제를 참조하십시오.
세션 대역폭 한정자	SIP 프로파일 구성 창 내에서 SIP 엔드포인트에서 어떤 세션 대역폭 한정자를 사용할 것인지 할당할 수 있습니다.
대역폭 할당 충돌	공통 링크 또는 위치에서 대역폭 용량이나 가중치 할당이 충돌하는 경우, 로컬 클러스터는 할당된 최소값을 사용합니다.
디바이스 지원	시스템 및 LBM에서는 IP 폰, 게이트웨이 및 H.323을 포함한 모든 종류의 디바이스와 SIP 트렁크 대상에 대한 대역폭을 관리합니다. 하지만 인터클러스터 고급 위치 기반 콜수락 제어(CAC)는 시스템 그림자 위치에 SIP ICT를 할당하도록 요구합니다. 일반(고정) 위치로 할당된 경우에만 다른 모든 종류의 디바이스가 지원됩니다.
네트워크 오류	네트워크 오류 상태에서는 Unified Communications Manager 의해 계산된 대역폭 예약 라우트에 네트워크 상태가 정확히 반영되지 않을 수 있습니다. 이 모델에는 이 시나리오를 고려한 만족스러운 방법이 없습니다.

기능	상호 작용 및 제한 사항
동기화 문제	시스템에서 생성된 모델이 항상 완벽하게 동기화되지는 않습니다. 보수적 대역폭 할당을 사용하여 이 제한 사항을 수용합니다.
WAN을 통한 클러스터링	WAN을 통한 클러스터링과 로컬 페일오버를 포함하는 구축의 경우, 인터클러스터 LBM 트래픽은 WAN 대역폭 계산으로 이미 계산되었습니다.
유연한 DSCP 표시	추가 QoS의 경우 DSCP 표시를 사용하여 다른 통화에 비해 특정 유형의 통화 플로우에 우선순위를 부여할할 수 있습니다. 예를 들어, 비디오에 비해 오디오에 우선순위를 부여하여 네트워크가 혼잡하여 영상 미디어가 차단된 상태에서도 오디오를 통해 기본 커뮤니케이션을 계속할 수 있습니다. 다음 두 가지 방법으로 DSCP 표시를 구성할 수 있습니다. • 서비스 매개변수—서비스 매개변수 구성 창의 클러스터 수준 매개변수(시스템 - **QoS)** 섹션 내에서 클러스터 수준 DSCP 기본값을 설정합니다. • SIP 프로파일—SIP 프로파일에서 사용자 지정된 DSCP 설정을 구성하고 이를 특정 SIP 디바이스 그룹에 적용합니다. 이 설정은 클러스터 수준 기본값을 재정의합니다.
APIC-EM 컨트롤러	APIC_EM 컨트롤러를 사용하여 외부 QoS 관리를 위한 SIP 미디어 플로우를 관리할 수 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

16 장

리소스 예약 프로토콜 구성

RSP 콜수락 제어(CAC) 개요

RSVP(리소스 예약 프로토콜)는 IP 네트워크에서 리소스를 예약하기 위한 리소스 예약, 전송 수준 프로토콜입니다. 고급 위치 기반 콜수락 제어(CAC) 대신 RSVP를 사용할 수 있습니다. RSVP는 특정 세션에 대한 리소스를 예약합니다. 세션은 특정 대상 주소, 목적지 포트 및 프로토콜 식별자(TCP 또는 UDP)가 있는 플로우입니다.

RSVP 콜수락 제어(CAC) 사전 요건

IPv4 주소 지정을 사용해야 합니다. RSVP는 IPv6 주소 지정을 지원하지 않습니다.

RSVP 구성 작업 플로우

프로시저

	명령 또는 동작	목적
단계 **1**	클러스터 수준 기본 RSVP 정책 설정, 168 페이지	클러스터의 모든 노드에 대한 RSVP 정책을 구성합니다.
단계 **2**	위치-쌍 RSVP 정책 구성, 169 페이지	(선택 사항) 위치 쌍이 클러스터의 나머지 부분과 다른 정책을 사용하도록 하려는 경우, 특정 위치 쌍에 대한 RSVP 정책을 구성할 수 있습니다.
단계 **3**	RSVP 재시도 구성, 170 페이지	RSVP 재시도의 빈도 및 횟수를 구성합니다.

	명령 또는 동작	목적
단계 4	통화 중 RSVP 오류 처리 구성, 170 페이지	통화 중에 RSVP가 실패할 때 시스템에서 응답하는 방법을 구성합니다.
단계 5	MLPP 대 RSVP 우선순위 매핑 구성, 171 페이지	(선택 사항) MLPP(Multilevel Precedence and Preemption)를 사용하는 경우, 발신자 MLPP 우선순위 수준을 RSVP 우선순위로 매핑합니다.
단계 6	RSVP 에이전트를 구성합니다.	게이트웨이 디바이스에서 이 IOS 절차를 수행합니다. RSVP 에이전트 구성 방법에 대한 자세한 내용은 디바이스 설명서를 참조하십시오.
단계 7	애플리케이션 ID 구성, 172 페이지	RSVP 애플리케이션 ID를 구성하면, 시스템에서 음성 및 비디오 트래픽에 모두 식별자를 추가하여 Cisco RSVP 에이전트에서 수신하는 식별자에 기반하여 두 트래픽 유형에 대한 별도의 대역폭 제한을 설정할 수 있게 됩니다.
단계 8	DSCP 표시 구성, 173 페이지	DSCP 표시를 구성하여, RSVP 예약이 실패할 경우 시스템에서 RSVP 에이전트 또는 엔드포인트 디바이스에 최상의 노력을 다하여 미디어 DSCP(Differentiated Services Control Point) 표시를 변경하도록 지시할 수 있습니다. 그렇지 않은 경우, EF로 표시된 미디어 패킷이 과도하게 많아지면서 예약된 플로우에 대해서도 QoS(서비스 품질)가 저하될 수 있습니다.

클러스터 수준 기본 RSVP 정책 설정

클러스터의 모든 노드에 대한 RSVP 정책을 구성합니다.

프로시저

단계 1 Cisco Unified Communications Manager 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 서비스 매개변수 구성 창에서 서버를 선택하고 Cisco CallManager 서비스를 선택합니다.

단계 3 클러스터 수준 매개변수(시스템 - RSVP) 섹션에서 기본 위치 간 RSVP 정책 서비스 매개변수를 구성합니다.

이 서비스 매개변수를 다음 값으로 설정할 수 있습니다.

- 예약 없음 - 두 위치 간에 어떤 RSVP 예약도 수행할 수 없습니다.

- 옵션(비디오 필수) - 오디오 및 비디오 스트림 모두에 대한 예약을 가져오는 데 실패하는 경우, 최선의 노력을 다하는 오디오 전용 통화로 통화를 진행할 수 있습니다. RSVP 에이전트에서 오디오에 대한 RSVP 예약을 계속해서 시도하며, 예약에 성공할 경우, Cisco Unified Communications Manager에 알립니다.
- 필수 - 오디오 스트림(통화가 화상 통화인 경우 비디오 스트림 포함)에 대한 RSVP 예약이 성공하는 경우에만 Cisco Unified Communications Manager에서 착신 디바이스의 벨을 울립니다.
- 원하는 비디오 -오디오 스트림에 대한 예약이 성공하지만 비디오 스트림에 대한 예약이 성공하지 않을 경우, 화상 통화를 오디오 전용 통화로 진행할 수 있습니다.

다음에 수행할 작업

다음 옵션 중 하나를 선택합니다.

- 위치 쌍이 클러스터의 나머지 부분과 다른 정책을 사용하도록 하려는 경우, 위치-쌍 RSVP 정책 구성, 169 페이지을 참조하십시오.
- 클러스터의 모든 노드에 대해 동일한 RSVP 정책을 사용 중인 경우 RSVP 재시도 구성, 170 페이지를 참조하십시오.

위치-쌍 RSVP 정책 구성

위치 쌍이 클러스터의 나머지 부분과 다른 정책을 사용하도록 하려는 경우, 특정 위치 쌍에 대한 RSVP 정책을 구성할 수 있습니다. 이 절차를 사용하면 위치 쌍에 대해 구성하는 RSVP 정책이 클러스터에 대해 구성된 정책에 우선합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 위치를 선택합니다.

단계 **2** 위치 쌍의 한 위치를 찾아 이 위치를 선택합니다.

단계 **3** 선택한 위치와 다른 위치 간에 RSVP 정책을 수정하려면 위치 쌍에서 다른 위치를 선택합니다.

단계 **4** **RSVP** 설정 드롭다운 목록에서이 위치 쌍에 대한 RSVP 정책을 선택합니다.

이 필드를 다음 값으로 설정할 수 있습니다.

- 시스템 기본값 사용–위치 쌍에 대한 RSVP 정책이 클러스터 수준 RSVP 정책과 일치합니다.
- 예약 없음–두 위치 간에 어떤 RSVP 예약도 수행할 수 없습니다.
- 원하는 비디오(선택 사항)–오디오 및 비디오 스트림 모두에 대한 예약을 가져오는 데 실패할 경우, 가장 효율적인 오디오 전용 통화로 통화를 진행할 수 있습니다. RSVP 에이전트에서 오디오에 대한 RSVP 예약을 계속해서 시도하며, 예약에 성공할 경우, Cisco Unified Communications Manager에 알립니다. 오디오 스트림(통화가 화상 통화인 경우 비디오 스트림 포함)에 대한 RSVP 예약이 성공하는 경우에만 시스템에서 착신 디바이스의 벨을 울립니다.

- 원하는 비디오 –오디오 스트림에 대한 예약이 성공하지만 비디오 스트림에 대한 예약이 성공하지 않을 경우, 화상 통화를 오디오 전용 통화로 진행할 수 있습니다.

다음에 수행할 작업

RSVP 재시도 구성, 170 페이지

RSVP 재시도 구성

이 절차를 사용하여 RSVP 재시도 빈도 및 횟수를 구성합니다.

시작하기 전에

- 클러스터 수준 기본 RSVP 정책 설정, 168 페이지
- (선택 사항) 위치-쌍 RSVP 정책 구성, 169 페이지

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서비스 매개변수 구성 창에서 서버를 선택하고 Cisco CallManager 서비스를 선택합니다.

단계 **3** 클러스터 수준 매개변수(시스템 - RSVP) 섹션에서 지정된 서비스 매개변수를 구성합니다.

이러한 서비스 매개변수를 다음 값으로 설정할 수 있습니다.

- RSVP 재시도 타이머-RSVP 재시도 타이머 값을 초로 지정합니다. 이 매개변수를 0으로 설정하면 시스템에서 RSVP 재시도가 비활성화됩니다.
- 필수 RSVP 통화 중 재시도 카운터 - RSVP 정책이 필수로 지정되어 있고 통화 중 오류 처리 옵션이 "재시도 카운터가 초과된 이후 통화 실패"로 설정된 경우, 통화 중 RSVP 재시도 카운터를 지정합니다. 기본값이 1 시간을 지정합니다. 서비스 매개변수를 -1로 설정한 경우, 예약이 성공하거나 통화가 중단될 때까지 재시도가 무한정 계속됩니다.

다음에 수행할 작업

통화 중 RSVP 오류 처리 구성, 170 페이지

통화 중 RSVP 오류 처리 구성

이 절차를 사용하여 통화 중 RSVP 오류 처리를 구성합니다.

시작하기 전에

RSVP 재시도 구성, 170 페이지

프로시저

단계 1 Cisco Unified Communications Manager Administration에서 시스템 > 서비스 매개 변수를 선택합니다.

단계 2 서비스 매개변수 구성 창에서 서버를 선택하고 Cisco CallManager 서비스를 선택합니다.

단계 3 클러스터 수준 매개변수(시스템-RSVP) 섹션에서 지정된 서비스 매개변수를 구성합니다.

필수 RSVP mid 통화 오류 처리 옵션 서비스 매개변수를 다음 값으로 설정할 수 있습니다.

- 통화가 best-effort(최선 노력) 통화가 됨-통화 중에 RSVP가 실패하면 통화가 best-effort 통화가 됩니다. 재시도가 활성화되면, 동시에 RSVP 재시도 시도가 시작됩니다.
- 재시도 카운터가 초과된 이후 통화 실패- 통화 중에 RSVP가 실패하는 경우, RSVP의 N번째 재시도 이후 통화가 실패합니다. 이때 RSVP Mid 통화 재시도 카운터 서비스 매개변수가 N을 지정합니다.

다음에 수행할 작업

게이트웨이 디바이스에서 RSVP 에이전트를 구성합니다. RSVP 에이전트 구성 방법에 대한 자세한 내용은 디바이스 설명서를 참조하십시오. 게이트웨이에서 RSVP 에이전트를 구성한 후에 Cisco Unified Communications Manager 관리로 돌아가 다음 옵션 중 하나를 선택합니다.

- 선택 사항. 네트워크에서 다단계 우선순위와 선점을 사용하는 경우, MLPP 대 RSVP 우선순위 매핑 구성, 171 페이지.
- 애플리케이션 ID 구성, 172 페이지

MLPP 대 RSVP 우선순위 매핑 구성

(선택 사항) 다음 클러스터 수준(시스템 - RSVP) 서비스 매개변수를 사용하여 발신자 MLPP 우선순위 수준에서 RSVP 우선순위로의 매핑을 구성합니다.

- RSVP 우선순위 매핑에 대한 MLPP 이그제큐티브 오버라이드
- RSVP 우선순위 매핑에 대한 MLPP 플래시 오버라이드
- RSVP 우선순위 매핑에 대한 MLPP 플래시
- RSVP 우선순위 매핑에 대한 MLPP 즉시
- RSVP 우선순위 매핑에 대한 MLPP PL 우선순위
- RSVP 우선순위 매핑에 대한 MLPP PL 루틴

이러한 서비스 매개변수를 찾아 구성하려면 다음 단계를 수행합니다.

프로시저

단계 1 Cisco Unified Communications Manager 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 서비스 매개변수 구성 창에서 서버를 선택하고 Cisco CallManager 서비스를 선택합니다.

단계 3 클러스터 수준 매개변수(시스템 - RSVP) 섹션에서 지정된 서비스 매개변수를 구성합니다.

이러한 서비스 매개변수는 다음과 같이 작동합니다.

- Cisco Unified Communications Manager에서는 다음과 같은 구성에 따라 RSVP 예약을 시작할 때 발신자 우선순위 수준을 RSVP 우선순위로 매핑합니다. 즉, 서비스 매개변수 값이 높을수록 우선순위가 높습니다.
- IOS 라우터가 RSVP 우선순위를 기반으로 통화를 선점합니다.
- RSVP 에이전트는 선점에 대한 원인을 포함하여 RSVP 예약 실패의 원인에 대해 Cisco Unified Communications Manager에 알려야 합니다.
- Cisco Unified Communications Manager에서는 기존 MLPP 메커니즘을 사용하여 선점에 대해 선점된 발신자 및 착신자에 게 알립니다.

다음에 수행할 작업

게이트웨이 디바이스에서 RSVP 에이전트를 구성합니다. RSVP 에이전트 구성 방법에 대한 자세한 내용은 디바이스 설명서를 참조하십시오. 게이트웨이에서 RSVP 에이전트를 구성한 후에 Cisco Unified Communications Manager 및 애플리케이션 ID 구성, 172 페이지로 돌아갑니다.

애플리케이션 ID 구성

RSVP 애플리케이션 ID를 구성하면, 시스템에서 음성 및 비디오 트래픽에 모두 식별자를 추가하여 Cisco RSVP 에이전트에서 수신하는 식별자에 기반하여 두 트래픽 유형에 대한 별도의 대역폭 제한을 설정할 수 있게 됩니다.

이 절차를 시작하기 전에 게이트웨이 디바이스에서 RSVP 에이전트를 구성합니다. RSVP 에이전트 구성 방법에 대한 자세한 내용은 디바이스 설명서를 참조하십시오.

시작하기 전에

네트워크에 RSVP 애플리케이션 ID를 구축하려면 Cisco RSVP 에이전트 라우터에서 최소 버전의 Cisco IOS 릴리스 12.4(6)T 이상을 사용해야 합니다.

프로시저

단계 1 Cisco Unified Communications Manager 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 서비스 매개변수 구성 창에서 서버를 선택하고 Cisco CallManager 서비스를 선택합니다.

단계 **3** 클러스터 수준 매개변수(시스템 - **RSVP)** 섹션에서 RSVP 오디오 애플리케이션 ID 서비스 매개변수를 구성합니다.

(기본값 = 오디오 스트림)

단계 **4** 클러스터 수준 매개변수(시스템 - **RSVP)** 섹션에서 RSVP 비디오 애플리케이션 ID를 구성합니다.

(기본값 = 비디오 스트림)

다음에 수행할 작업

DSCP 표시 구성, 173 페이지

DSCP 표시 구성

RSVP 예약이 실패하는 경우, (RSVP 에이전트를 할당하지 못하는 상황이 발생할 경우) 시스템에서 RSVP 에이전트 또는 엔드포인트 디바이스에 최상의 노력으로 미디어의 DSCP(차별화 서비스 제어 지점) 표시를 변경하도록 지시합니다. 그렇지 않은 경우, EF로 표시된 미디어 패킷이 과도하게 많아지면서 예약된 플로우에 대해서도 QoS(서비스 품질)가 저하될 수 있습니다.

시작하기 전에

애플리케이션 ID 구성, 172 페이지

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서비스 매개변수 구성 창에서 서버를 선택하고 Cisco CallManager 서비스를 선택합니다.

단계 **3** 클러스터 수준 매개변수(시스템 - **QoS)** 섹션에서 **RSVP** 실패 시 오디오 통화용 **DSCP** 서비스 매개변수를 구성합니다.

단계 **4** 클러스터 수준 매개변수(시스템 - **QoS)** 섹션에서 **RSVP** 실패 시 비디오 통화용 **DSCP** 서비스 매개변수를 구성합니다.

17 장

푸시 알림 구성

푸시 알림 개요

클러스터에서 푸시 알림이 활성화되면 Unified Communications Manager와 IM and Presence 서비스는 Google 및 Apple의 클라우드 기반 푸시 알림 서비스를 사용하여 음성 및 화상 통화, 인스턴트 메시지 알림을 일시 중지 모드(백그라운드 모드라고도 함)에서 실행 중인 Android 및 iOS 클라이언트의 Cisco Jabber 또는 Cisco Webex에 푸시합니다. 푸시 알림을 사용하면 시스템이 Cisco Jabber 또는 Cisco Webex와 지속적인 통신을 유지할 수 있습니다. 푸시 알림은 엔터프라이즈 네트워크 내에서 연결되는 Android 및 iOS 클라이언트의 Cisco Jabber 및 Cisco Webex 및 Expressway의 모바일 및 원격 액세스 기능을 통해 온프레미스 배포에 등록하는 클라이언트 모두에 필요합니다.

푸시 알림 작동 방식

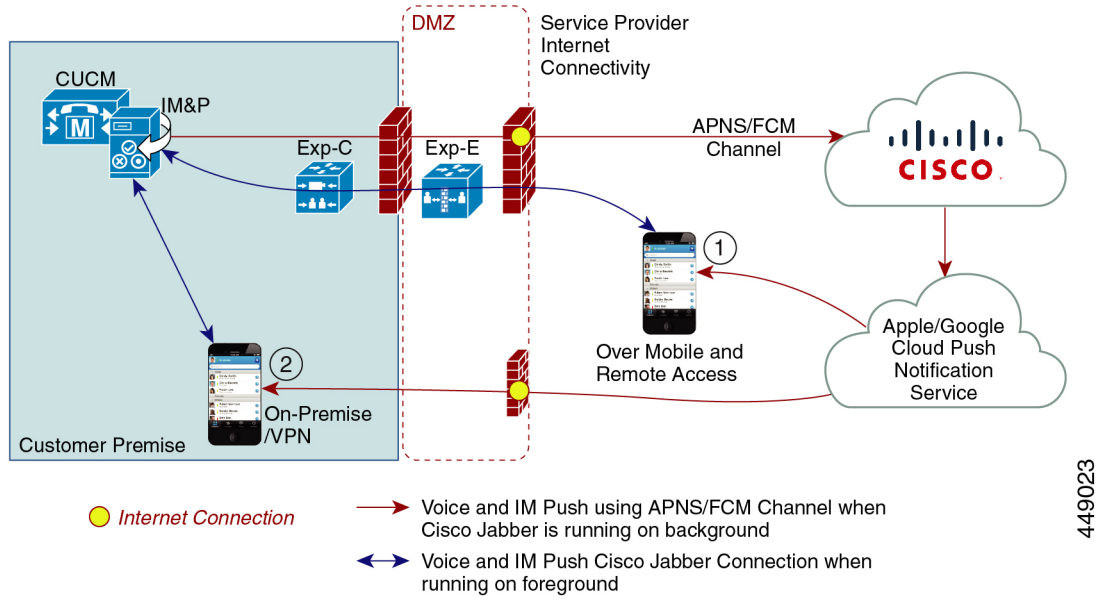
시작 시, Android 및 iOS 플랫폼 디바이스에 설치된 클라이언트는 Unified Communications Manager, IM and Presence 서비스 및 Google과 Apple 클라우드에 등록됩니다. 모바일 및 원격 액세스 구축을 사용하는 경우 클라이언트는 Expressway를 통해 온-프레미스 서버에 등록됩니다. Cisco Jabber 및 Cisco Webex 클라이언트가 포그라운드 모드로 유지되는 한 Unified Communications Manager와 IM and Presence 서비스는 클라이언트에 직접 전화 및 인스턴트 메시지를 보낼 수 있습니다.

그러나 Cisco Jabber 또는 Cisco Webex 클라이언트가 일시 중지 모드(예: 배터리 수명 유지를 위해)로 전환되면 표준 통신 채널을 사용할 수 없으므로 Unified Communications Manager와 IM and Presence 서비스는 클라이언트와 직접 통신할 수 없습니다. 푸시 알림은 파트너 클라우드를 통해 클라이언트에 연결할 수 있는 또 다른 채널을 제공합니다.

참고 다음 조건 중 하나라도 해당되면 Cisco Jabber 및 Cisco Webex는 일시 중단 모드로 실행되고 있는 것으로 간주됩니다.

- Cisco Jabber 또는 Cisco Webex 애플리케이션이 화면 밖(즉, 백그라운드에서)에서 실행 중임
- Android 또는 iOS 기기가 잠겨 있음
- Android 또는 iOS 디바이스 화면이 꺼져 있음

그림 *6:* 푸시 알림 아키텍처



위의 다이어그램은 Android and iOS용 Cisco Jabber 또는 Cisco Webex 클라이언트가 백그라운드에서 실행되거나 중 될 때 수행되는 작업을 표시합니다. 이 그림은 (1) Expressway를 통해 온프레미스 Cisco Unified Communications Manager 및 IM and Presence 서비스 구축과 연결되는 모바일 및 원격 액세스 구축, (2) 엔터프라이즈 네트워크 내에서 온프레미스 구축에 직접 연결하는 Android 및 iOS용 Cisco Jabber 또는 Cisco Webex 클라이언트를 보여줍니다.

참고 Apple 클라이언트 및 지원되는 Android 클라이언트에 대한 iOS13의 경우 음성 통화 및 메시지는 별도의 푸시 알림 채널 (' VoIP ' 및 ' Message ')을 사용하여 백그라운드 모드에서 실행 중인 클라이언트에 연결 합니다. 그러나, 두 채널에 대한 일반 흐름은 동일 합니다. IOS 12에서는 음성 통화와 메시지가 동일한 채널을 사용하여 전달 됩니다.

Cisco Jabber 및 **Cisco Webex**에 대한 푸시 알림 동작

다음 표에서는 Cisco Jabber 또는 IM and 현재 서비스에 등록 된 Cisco Webex iOS 클라이언트에 대한 iOS 12 및 iOS 13의 동작에 대해 설명 합니다Unified Communications Manager.

Cisco Jabber 또는 **Cisco Webex** 클라이언트가 실행되고 있습니다.	**Cisco Jabber**가 **iOS12** 디바이스에서 실행되고 있습니다.	**Cisco Jabber**가 **iOS13** 디바이스 또는 **Android** 디바이스에서 실행되고 있습니다.
포그라운드 모드	음성 및 영상 통화 Unified Communications Manager 표준 SIP communications 채널을 사용하여 Cisco Jabber 또는 Cisco Webex 클라이언트에 음성 및 영상 통화를 직접 전송 합니다. 통화의 경우에 Unified Communications Manager도 푸시 알림은 포그라운드 모드에 있는 Cisco Jabber 또는 Cisco Webex 클라이언트로 전송 됩니다. 그러나 표준 SIP 채널은 푸시 알림 채널이 아닌 통화를 설정 하는 데 사용 됩니다. 메시지 IM and 현재 서비스는 표준 SIP 통신 채널을 사용하여 메시지를 클라이언트에 직접 전송 합니다. 메시지의 경우 푸시 알림은 포그라운드 모드에 있는 클라이언트로 전송되지 않습니다.	동작은 iOS12와 동일합니다.

Cisco Jabber 또는 **Cisco Webex** 클라이언트가 실행되고 있습니다.	**Cisco Jabber**가 **iOS12** 디바이스에서 실행되고 있습니다.	**Cisco Jabber**가 **iOS13** 디바이스 또는 **Android** 디바이스에서 실행되고 있습니다.
일시 중지 모드(백그라운드 모드)	음성 또는 영상 통화 표준 통신 채널을 사용할 수 없습니다. 통합 CM은 푸시 알림 채널을 사용합니다. 알림을 받으면 Cisco Jabber 또는 Cisco Webex 클라이언트는 자동으로 포그라운드 모드로 다시 들어가고 클라이언트의 전화벨이 울립니다. 메시징 표준 통신 채널을 사용할 수 없습니다. IM and Presence 서비스는 푸시 알림 채널을 사용하여 다음과 같이 IM 알림을 보냅니다. **1.** IM and Presence 서비스는 Cisco 클라우드의 Push REST 서비스로 IM 알림을 보내고, 알림은 Apple 클라우드로 전달됩니다. **2.** Apple 클라우드는 IM 알림을 Cisco Jabber 또는 Cisco Webex 클라이언트에 푸시하고 Cisco Jabber 또는 Cisco Webex 클라이언트에 알림이 나타납니다. **3.** 사용자가 알림을 클릭하면 Cisco Jabber 또는 Cisco Webex 클라이언트가 포그라운드로 돌아갑니다. Cisco Jabber 또는 Cisco Webex 클라이언트는 IM and Presence 서비스로 세션을 재개하고 인스턴트 메시지를 다운로드합니다. 참고 Cisco Jabber 또는 Cisco Webex 클라이언트가 일시 중지 모드에 있는 동안 사용자의 프레즌스 상태가 자리 비움으로 표시됩니다.	IOS13를 사용 하는 경우 통화 트래픽 및 메시지 트래픽은 별도의 푸시 알림 채널로 분할 됩니다. 통화에 대한 ' VoIP ' 채널 및 메시징의 "메시지" 채널이 구분 됩니다. 음성 또는 영상 통화 표준 통신 채널을 사용할 수 없습니다. 통합 CM은 푸시 알림 ' VoIP ' 채널을 사용합니다. Jabber는 VoIP 알림을 수신 하면 발신자 ID를 사용하여 CallKit를 실행합니다. 이 동작은 Cisco Jabber 또는 Cisco Webex iOS 클라이언트의 경우 보류됩니다. 메시징 표준 통신 채널을 사용할 수 없습니다. IM and 현재 서비스에서 푸시 알림 ' 메시지 ' 채널을 사용합니다. **1.** IM and Presence 서비스는 Cisco 클라우드의 Push REST 서비스로 IM 알림을 보내고, 알림은 Apple 클라우드로 전달됩니다. **2.** Apple 클라우드는 IM 알림을 Cisco Jabber 또는 Cisco Webex 클라이언트로 푸시합니다. **3.** 사용자가 알림을 클릭하면 Cisco Jabber 또는 Cisco Webex 클라이언트가 포그라운드로 돌아갑니다. Cisco Jabber 또는 Cisco Webex 클라이언트는 IM and Presence 서비스로 세션을 재개하고 메시지를 다운로드합니다. 참고 Cisco Jabber 또는 Cisco Webex 클라이언트가 일시 중지 모드에 있는 동안 사용자의 프레즌스 상태가 자리 비움으로 표시됩니다.

푸시 알림에 대해 지원되는 클라이언트

클라이언트	**OS**	플랫폼 클라우드	클라우드 서비스
iPhone 및 iPad의 Cisco Jabber	iOS	Apple	Apple 푸시 알림 서비스 APN)
Android의 Cisco Jabber	Android	Google	Android PNS 서비스
iOS의 Webex	iOS	Apple	Apple 푸시 알림 서비스 APN)
Android의 Webex	Android	Google	Android PNS 서비스

푸시 알림 구성

푸시 알림을 구성하고 구축하는 방법에 대한 자세한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *iPhone* 및 *iPad*에서 *Cisco Jabber*에 대한 푸시 알림을 참조하십시오.

II 부

다이얼 플랜

18 장

파티션 구성

파티션 개요

파티션은 다음 중 하나에 대한 논리적 그룹입니다.

- 라우트 패턴
- 디렉터리 번호(DN)
- 변환 패턴
- 변환 패턴
- 범용 리소스 표시기(URI)
- 헌트 파일럿

파티션은 유사한 접근성 요구사 사항, 조직, 위치 및 통화 유형에 따라 라우트 플랜을 논리적 하위 집합으로 나눔으로써 콜 라우팅을 지원합니다.

CSS(발신 검색 공간) 개요

CSS(발신 검색 공간)은 파티션의 우선순위 목록입니다. CSS(발신 검색 공간)에서는 발신자가 통화하기 위해 이용할 수 있는 통화 대상을 결정합니다. 통화 대상은 발신자의 CSS(발신 검색 공간)에서 사용할 수 있는 파티션에 있어야만 합니다. 아니면 발신자는 해당 대상에 통화를 할 수 없습니다. CSS(발신 검색 공간)을 디렉터리 번호 및 전화기 및 게이트웨이와 같은 디바이스에 할당할 수 있습니다.

CSS(발신 검색 공간)이 발신자의 전화기와 발신자의 디렉터리 번호에 모두 할당된 경우, 시스템에서 둘 모두에 연결하여 발신자에게 CSS를 제공합니다.

파티션과 CSS(발신 검색 공간)을 사용하여 통화 권한에 따라 시스템을 조직할 수 있습니다. 예를 들면, 다음을 진행할 수 있습니다.

- 일부 직원의 장거리 통화를 제한합니다
- 로비 전화가 CEO 직통으로 연결되지 않도록 제한합니다

CoS(서비스 종별)

파티션 및 CSS(발신 검색 공간)를 사용하여 서비스 종별를 구성할 수 있습니다. 아래 표에는 다음에 PSTN 액세스를 제공하는 서비스 종별에 대해 생성할 수 있는 파티션 및 발신 검색 공간의 예가 나와 있습니다.

- 비상 통화
- 로컬 통화
- 국내 통화
- 국제 전화걸기

표 ***14:*** 파티션 및 발신 검색 공간의 예

발신 검색 공간	라우트 파티션 **1**	라우트 파티션 **2**	라우트 파티션 **3**	기능
Base_CSS	Base_PT	—	—	• 긴급 • 온넷
LocalPSTN_CSS	PSTN_Local_PT	—	—	• 긴급 • 온넷 • 로컬
nationalPSTN_CSS	PSTN_Local_PT	PSTN_national_PT	—	• 긴급 • 온넷 • 로컬 • 국내

발신 검색 공간	라우트 파티션 1	라우트 파티션 2	라우트 파티션 3	기능
InternationalPSTN_CSS	PSTN_Local_PT	PSTN_national_PT	PSTN_Intl_PT	• 긴급 • 온넷 • 로컬 • 국내 • 국제

디바이스는 Base_CSS와 같은 발신 검색 공간에 자동으로 등록됩니다. 이렇게 하면 모든 디바이스에서 온넷 및 비상 오프넷 번호로 모두 전화를 걸 수 있습니다. 로컬 7자리 또는 로컬 10자리, 국내 및 국제 전화걸기 기능을 제공하려면 사용자 디바이스 프로파일의 디렉터리 번호에 나머지 발신 검색 공간을 할당해야만 합니다.

파티션 구성 작업 플로우

프로시저

	명령 또는 동작	목적
단계 1	파티션 구성, 185 페이지	유사한 연결성 특성이 포함된 시스템 리소스의 논리적 그룹을 생성하는 파티션을 구성합니다.
단계 2	발신 검색 공간 구성, 187 페이지	통화를 완료하려고 시도할 때 발신 디바이스에서 검색하는 파티션을 구성합니다.

파티션 구성

유사한 연결성 특성을 갖는 시스템 리소스의 논리적 그룹을 생성하는 파티션을 구성합니다. 다음 중 하나에 대한 파티션을 만들 수 있습니다.

- 라우트 패턴
- 디렉터리 번호(DN)
- 변환 패턴
- 변환 패턴
- 범용 리소스 표시기(URI)
- 헌트 파일럿

파티션은 조직, 위치 및 통화 유형에 따라 라우트 플랜을 논리적 하위 집합으로 나눔으로써 콜 라우팅을 지원합니다. 여러 파티션을 구성할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스 > 파티션.

단계 **2** 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 **3** 파티션 이름**,** 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 **4** 파티션 이름 뒤에 쉼표(,)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([ ])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 **5** 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 **6** 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 **7** 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대 를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 **8** 저장을 클릭합니다.

파티션 이름 지침

발신 검색 공간의 파티션 목록에서 최대 문자 수는 1024자로 제한됩니다. 즉, CSS의 최대 파티션 수는 파티션 이름의 길이에 따라 달라집니다. 다음 표를 사용하여 파티션 이름이 고정 길이인 경우 발신 검색 공간에 추가할 수 있는 최대 파티션 수를 결정합니다.

표 ***15:*** 파티션 이름 지침

파티션 이름 길이	최대 파티션 수
2자	340
3자	256

파티션 이름 길이	최대 파티션 수
4자	204
5자	172
...	...
10자	92
15자	64

발신 검색 공간 구성

발신 검색 공간은 일반적으로 디바이스에 할당되어 있는 정렬된 경로 파티션 목록입니다. 발신 검색 공간은 통화를 완료하려고 시도할 때 발신 디바이스에서 검색할 수 있는 파티션을 결정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 **4** 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 **5** 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤**(CTRL)** 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 **6** 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 **7** (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 **8** 저장을 클릭합니다.

파티션 상호 작용 및 제한 사항

표 ***16:*** 파티션 제한 사항

기능 또는 작업	제한 사항
파티션 삭제	파티션을 삭제하기 전에 다음 작업 중 하나를 완료했는지 확인하십시오. • 삭제하려는 파티션을 사용 중인 CSS(발신 검색 공간), 디바이스 또는 기타 항목에 다른 파티션을 할당합니다. • 삭제할 파티션을 사용 중인 발신 검색 공간, 디바이스 또는 기타 항목을 삭제합니다. 삭제된 파티션을 검색할 수 없으므로 정확한 파티션을 삭제하고 있는지 신중하게 확인하십시오. 파티션을 실수로 삭제한 경우 다시 작성해야 합니다.
변환 패턴	변환 패턴은 숫자 조작을 포함하며 파티션에 할당됩니다. 통화가 변환 패턴과 일치하면, Unified CM에서 변환을 수행한 다음 변환 패턴이 지정하는 CSS(발신 검색 공간)을 사용하여 통화를 다시 라우팅합니다. 변환 패턴에 대한 자세한 내용은 콜 라우팅 구성 장을 참조하십시오.
시간 라우팅	착신 통화 수락에 파티션을 언제 사용할 수 있는 지에 대한 일정을 구성합니다. 시간 라우팅 구성에 대한 자세한 내용은 콜 라우팅 구성 장을 참조하십시오.
논리적 파티션	선택 사항: 외부 네트워크에서 게이트웨이 및 트렁크 액세스를 사용하여 내부 VoIP 네트워크를 분할할 수 있습니다. 논리적 파티션은 대부분의 구축에 대해 선택 사항이지만, 내부 네트워크를 떠나는 모든 통화가 로컬 PSTN 게이트웨이로 이동할 것을 의무적으로 규정하고 있는 인도와 같은 국가에서는 필수 사항입니다. 논리적 파티션 설정에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 설정 가이드의 "논리적 파티셔닝 설정" 장을 참조하십시오.

19 장

국가 번호 지정 플랜 설치

국가 번호 지정 플랜 개요

Cisco Unified Communications Manager에서는 기본값으로 naNP(북아메리카 번호 지정 플랜)를 제공합니다. 다른 다이얼 플랜 요구 사항을 갖는 국가의 경우, Cisco 국제 다이얼 플랜을 설치하고 이를 사용하여 요구 사항에 따른 고유한 번호 지정 플랜을 생성할 수 있습니다.

번호 지정 플랜에는 해당 번호 지정 플랜에 따른 DDI(폐기 숫자 지침)와 태그가 포함되어 있습니다. 콜 라우팅을 구성할 때 이러한 항목을 사용하여 번호 지정 플랜에 적용할 수 있는 라우팅 규칙을 만들 수 있습니다.

이 장에서는 국가 번호 지정 플랜을 설치하는 방법에 대해 설명합니다. 국가 번호 지정 플랜 사용에 대한 자세한 내용은 *Unified Communications Manager* 다이얼 플랜 구축 설명서를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 참조하십시오.

국가 번호 지정 플랜 사전 요건

북미 이외의 국가에 대한 국가 번호 지정 플랜을 설치하는 경우, 현재 릴리스에 대한 국제 다이얼 플랜이 포함된 COP(Cisco Option Package) 파일을 다운로드하십시오. COP 파일은 명명 규칙 IDP v.*x* 를 사용하며 Cisco 웹사이트에서 사용할 수 있습니다.

- https://software.cisco.com/download/navigator.html

Unified Communications Manager에서 액세스할 수 있는 외부 FTP 또는 SFTP 서버에 해당 파일을 배치합니다.

국가 번호 지정 플랜 설치 작업 플로우

프로시저

	명령 또는 동작	목적
단계 **1**	COP 파일 설치, 190 페이지	선택 사항. 북미 이외 국가의 경우 번호 지정 플랜을 설치하려면 현재 릴리스에 대한 국제 다이얼 플랜이 포함된 COP(Cisco Option Package) 파일을 다운로드합니다.
단계 **2**	국가 번호 지정 플랜 설치, 191 페이지	클러스터의 각 Unified Communications Manager 노드에 국가 번호 지정 플랜을 설치합니다. 북미 이외 국가의 국가 번호 지정 플랜을 설치하는 경우에만 이 절차를 수행해야 합니다.
단계 **3**	CallManager 서비스 다시 시작, 192 페이지	변경 사항은 서비스를 다시 시작한 후에 적용됩니다.

COP 파일 설치

이 절차를 사용하여 국제 다이얼 플랜이 포함된 COP(Cisco Option Package) 파일을 설치합니다.

프로시저

단계 **1** Unified Communications Manager 퍼블리셔 노드를 이 절차를 시작합니다. Cisco Unified Communications OS 관리에서 소프트웨어 업그레이드 > 설치를 선택합니다.
소프트웨어 설치/업그레이드창이 나타납니다.

단계 **2** 소스 필드에서 원격 파일 시스템을 선택합니다.

단계 **3** 소프트웨어 설치/업그레이드 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 관련 항목을 참조하십시오.

단계 **4** 다음을 클릭합니다.
창이 새로 고쳐지면서 사용 가능한 소프트웨어 옵션 및 업그레이드 목록이 표시됩니다.

단계 **5** 옵션/업그레이드 드롭다운 목록에서 **DP COP** 파일을 선택하고 다음을 클릭합니다.
설치 파일 창이 열리고 FTP 서버에서 파일이 다운로드됩니다. 창에 다운로드 진행 상황이 표시됩니다.

단계 **6** 체크섬 창이 나타나면 다운로드한 파일의 체크섬에 대한 체크섬 값을 확인하십시오.

단계 **7** 다음을 클릭하여 소프트웨어 업그레이드를 진행합니다.
경고 메시지에 설치하려고 선택한 DP COP 파일이 표시됩니다.

단계 **8** 설치를 클릭합니다.

설치 상태 창이 나타납니다.

단계 **9** 마침을 클릭합니다.

단계 **10** Unified Communications Manager 가입자 노드에서 이 절차를 반복합니다. 클러스터의 모든 노드에 COP 파일을 설치해야 합니다.

관련 항목

COP 파일 설치 필드, 191 페이지

COP 파일 설치 필드

필드	설명
디렉터리	COP 파일이 위치한 디렉터리를 입력합니다.
원격 서버	COP 파일이 위치한 서버의 호스트 네임 또는 IP 주소를 입력합니다.
원격 사용자	원격 서버에 대한 사용자 이름을 입력합니다.
원격 암호	원격 서버의 암호를 입력합니다.
전송 프로토콜	프로토콜을 선택하여 원격 서버와 연결할 때 사용합니다.

국가 번호 지정 플랜 설치

북미 이외 국가의 국가 번호 지정 플랜을 설치하는 경우에만 이 절차를 수행해야 합니다.

클러스터의 각 Unified Communications Manager 노드에 국가 번호 지정 플랜을 설치합니다. Unified Communications Manager 퍼블리셔 노드를 시작합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 다이얼 플랜 설치 관리자를 선택합니다.

단계 **2** 검색 기준을 입력하고 찾기를 클릭합니다.

단계 **3** 사용 가능한 버전 드롭다운 목록 상자에서 설치할 다이얼 플랜 버전을 선택합니다.

단계 **4** 설치를 클릭합니다.
[상태]에 다이얼 플랜이 설치되었다는 내용이 표시됩니다.

단계 **5** 클러스터의 모든 가입자 노드에 대해 이 절차를 반복합니다.

CallManager 서비스 다시 시작

프로시저

단계 **1** Cisco Unified Serviceability 인터페이스에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 Unified Communications Manager 서버를 선택합니다.
CM 서비스 영역에서 Cisco CallManager가 서비스 이름 열에 표시됩니다.

단계 **3** Cisco CallManager 서비스에 해당하는 라디오 버튼을 클릭합니다.

단계 **4** 재시작을 클릭합니다.
서비스가 다시 시작되고 서비스가 다시 시작되었습니다라는 메시지가 표시됩니다.

20 장

콜 라우팅 구성

콜 라우팅 개요

시스템에서 라우트 플랜을 사용하여 인터클러스터에 통화를 라우팅하는 방법을 결정하고 외부 통화를 프라이빗 네트워크 또는 PSTN(Public Switched Telephone Network)으로 라우팅하는 방법을 결정합니다. 구성하는 라우트 플랜에서 각 통화 유형을 라우팅하기 위해 시스템에서 사용하는 경로를 지정합니다. 예를 들어, On-Net 통화에 대해 IP 네트워크를 사용하거나 로컬 PSTN 통화에 대해 하나의 캐리어를 사용하고 국제 전화에 대해 또 다른 캐리어를 사용하는 라우트 플랜을 만들 수 있습니다.

변환 패턴

변환 패턴을 구성하여 모든 통화 유형에 대한 숫자를 조작할 수 있습니다. 변환 패턴은 경로 패턴과 동일한 일반 규칙을 따르며 동일한 와일드카드를 사용합니다. 라우트 패턴과 마찬가지로, 변환 패턴을 파티션에 할당합니다. 하지만 착신 번호가 변환 패턴과 일치하는 경우, Unified CM에서 통화를 게이트웨이 같은 외부 엔티티로 라우팅하지 않습니다. 대신, 먼저 변환을 수행한 다음 통화를 다시 라우팅합니다. 이 때 변환 패턴 내에서 구성된 CSS(발신 검색 공간)을 사용합니다.

참고 생성하는 각 변환 패턴의 경우, 파티션, 경로 필터 및 번호 지정 플랜의 조합이 고유해야 합니다. 중복 항목을 나타내는 오류 메시지를 수신하는 경우, 경로 패턴 또는 헌트 파일럿, 변환 패턴, 디렉터리 번호, 통화 지정 보류 번호, Meet-Me 번호 구성 창을 확인하십시오.

변환 패턴

변환 패턴을 사용하여 숫자를 삭제하고, 앞자리 숫자를 추가하고, 발신자 변환 마스크를 추가하고, 발신자 번호의 표시를 제어한 다음, 시스템에서 전화기 또는 PSTN으로 통화를 전송할 수 있습니다.

변환 패턴을 구성하고 이를 라우트 파티션에 연결하여, 파티션을 포함하는 CSS(발신 검색 공간)에 패턴을 할당합니다. 구성 창의 [발신자 변환 CSS] 또는 [착신자 변환 CSS] 필드를 통해 특정 디바이스, 디바이스 풀, 게이트웨이 또는 트렁크에 대한 통화 설정에 패턴을 할당할 수 있습니다.

다음과 같은 변환 패턴을 구성할 수 있습니다.

- 발신자 변환 패턴 — 시스템에서 발신자 번호의 전역 형태를 게이트웨이나 트렁크 같은 라우트 그룹 디바이스에 연결된 오프클러스터 네트워크에 필요한 로컬 형태로 변환할 수 있습니다.

  착신자 변환 패턴 — 시스템에서 착신자 번호의 전역 형태를 라우트 그룹 디바이스에 연결된 오프클러스터 네트워크에 필요한 로컬 형태로 변환할 수 있습니다.

라우트 패턴

시스템에는 다음 구성 요소를 사용하는 라우트 계획에 대한 3계층 접근 방법이 있습니다.

- 라우트 패턴 — 시스템에서 외부 다이얼 문자열과 일치하는 구성된 라우트 패턴을 검색하고 이를 사용하여 통화를 게이트웨이 또는 라우트 목록으로 보냅니다. 라우트 패턴을 게이트웨이, 트렁크 또는 하나 이상의 라우트 그룹을 포함하는 라우트 목록에 할당할 수 있습니다.
- 라우트 목록 — 통화에 사용할 수 있는 경로에 대한 우선순위 목록입니다.
- 라우트 그룹 — 사용 가능한 경로입니다. 라우트 그룹에서 통화를 게이트웨이 및 트렁크에 분배합니다.

추가 콜 라우팅

라우트 플랜에는 다음과 같은 선택적 구성 요소도 포함될 수 있습니다.

- 로컬 라우트 그룹 — 여러 사이트가 있는 경우, 로컬 라우트 그룹을 사용하여 라우트 패턴 구성에 의해서가 아니라 디바이스 풀에 지정된 대로 Off-Net 통화를 게이트웨이로 라우팅할 수 있습니다. 이렇게 하면 여러 위치에 단일 라우트 패턴 세트를 사용할 수 있습니다.
- 라우트 필터 — 라우트 필터를 생성하고 이를 라우트 패턴 또는 헌트 파일럿에 추가하여 사용자가 패턴을 사용하지 못하도록 합니다. 다이얼 플랜 설치 관리자 파일을 사용 중인 경우, 라우트 필터는 필수이지만, 수동 다이얼 플랜 구성의 경우 선택 사항입니다. 수동 구성의 경우, 패턴에서 @ 와일드카드를 사용하는 경우에만 라우트 필터가 적용됩니다.
- **AAR(**자동 대체 라우팅**)** —대역폭 부족으로 시스템에서 통화를 차단할 때 PSTN 또는 다른 네트워크를 통해 통화를 자동으로 다시 라우팅합니다.
- **TOD(Time of Day)** 라우팅 — 착신 통화를 받기 위해 제공된 파티션이 언제 사용 가능한지를 지정한 일정을 생성합니다.

콜 라우팅 사전 요건

- 파티션 구성 작업 플로우, 185 페이지에서 작업을 완료하십시오.
- 다음 정보가 있는지 확인하십시오.
  - 내부 번호 내선 번호
  - 각 게이트웨이로 라우팅되는 통화를 나열하는 플랜

호라우팅에 대한 자세한 내용은 *Cisco* 협업 시스템 솔루션 참조 네트워크 설계에서 통화 제어 및 라우팅 항목을 참조하십시오.

콜 라우팅 구성 작업 플로우

프로시저

	명령 또는 동작	목적
단계 **1**	변환 패턴 구성, 196 페이지	변환 패턴을 구성하여 특정 파티션의 통화에 대한 숫자 변환을 완료하는 방법을 지정합니다.
단계 **2**	착신자 변환 패턴 구성, 197 페이지	이 절차를 사용하여 발신 번호를 변환합니다. 예를 들어, PSTN을 호출할 때 발신자의 내선 번호를 사무실의 기본 번호로 대체하는 변환 패턴을 구성할 수 있습니다.
단계 **3**	착신자 변환 패턴 구성, 197 페이지	이 절차를 사용하여 착신 번호를 변환합니다. 예를 들어, 10자리 발신 번호의 마지막 5자리만 유지하는 변환 패턴을 구성할 수 있습니다.
단계 **4**	로컬 라우트 그룹 구성, 198 페이지	선택 사항. 로컬 라우트 그룹을 사용하면 여러 위치에 단일 라우트 패턴 세트를 사용할 수 있습니다. Unified CM에서는 라우트 패턴보다는 발신 디바이스 위치를 기반으로 게이트웨이를 할당합니다.
단계 **5**	라우트 그룹 구성, 200 페이지	선택 사항. 라우트 그룹을 구성하여 게이트웨이 디바이스의 선택 순서를 설정합니다. 라우트 그룹에는 하나 이상의 디바이스가 포함됩니다.

	명령 또는 동작	목적
단계 **6**	라우트 목록 구성, 200 페이지	선택 사항. 라우트 목록에는 이상의 라우트 그룹이 포함됩니다. 라우트 목록을 구성 하여 라우트 그룹의 선택 순서를 제어 합니다.
단계 **7**	라우트 필터 구성, 201 페이지	선택 사항. 라우트 필터를 사용하여 라우트 패턴에서 달리 허용되는 특정 번호를 제한합니다.
단계 **8**	라우트 패턴 구성, 205 페이지	라우트 패턴을 구성하여 특정 디바이스에 대한 통화를 보내고 특정 숫자 패턴을 포함 또는 제외합니다.
단계 **9**	클러스터 수준 자동 대체 라우팅 활성화, 209 페이지	선택 사항. AAR(자동 대체 라우팅)을 활성화하여 대역폭 부족으로 인해 통화가 차단될 때 시스템에서 PSTN 또는 다른 네트워크로 통화를 재라우팅합니다.
단계 **10**	AAR 그룹 구성, 210 페이지	선택 사항. 숫자 변환을 사용하여 AAR 그룹을 구성하여 AAR(자동 대체 라우팅)에 적용합니다.
단계 **11**	시간 라우팅 구성, 210 페이지	선택 사항. 착신 통화를 받기 위해 제공된 파티션이 언제 사용 가능한지를 지정한 일정을 생성합니다.

변환 패턴 구성

변환 패턴을 구성하여 다이얼 문자열이 패턴과 일치하는 경우, 발신 및 착신 번호에 숫자 조작을 적용합니다. 시스템에서 숫자 변환을 완료한 다음 해당 통화를 다시 라우팅합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 변환 패턴을 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가를 클릭하여 새 변환 패턴을 추가합니다.
- 찾기를 클릭하고 기존 변환 패턴을 선택합니다.

단계 **3** 변환 패턴 필드에 시스템에서 이 패턴을 사용하는 다이얼 문자열에 일치시키려는 패턴을 입력합니다.

단계 **4** 파티션 드롭다운 목록에서 이 패턴을 할당하려는 파티션을 선택합니다.

단계 **5** 변환 패턴 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

착신자 변환 패턴 구성

이 절차를 사용하여 발신 번호를 변환합니다. 예를 들어, PSTN을 호출할 때 발신자의 내선 번호를 사무실의 기본 번호로 대체하는 변환 패턴을 구성할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.콜 라우팅 > 변환 > 변환 패턴 > 발신자 변환 패턴

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가를 클릭하여 새 착신자 변환 패턴 추가합니다.
- 찾기를 클릭하고 기존 패턴을 선택합니다.

단계 **3** 패턴 필드에서 발신자 번호와 일치시키려는 패턴을 입력합니다.

참고 아웃바운드 통화의 경우**:**

발신자 변환 마스크는 사전 변환 발신자 번호에 따라 선택됩니다. (IP 전화기에 할당된 내선).

SIP 트렁크에서 발신자 변환 마스크를 선택하는 동안 발신자 번호가 라우트 패턴/그룹의 다른 번호로 변환 되는 경우, 발신자 변환 마스크를 선택하려면 항상 사전 변환 발신 번호가 사용됩니다.

Dna(전화 건 번호 분석기)에 따라 변환된 번호가 발신자 변환 마스크를 선택하기 위해 사용됩니다. 그러나 이는 Dna의 잘못된 동작입니다.

단계 **4** 발신자 변환 패턴 구성 창에서 나머지 필드를 완료합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

착신자 변환 패턴 구성

이 절차를 사용하여 착신 번호를 변환합니다. 예를 들어, 10자리 숫자로 전화를 건 통화의 마지막 5자리만 유지하는 변환 패턴을 구성할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 변환 > 변환 패턴 > 착신자 변환 패턴을 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가를 클릭하여, 새 착신자 변환 패턴 추가합니다.
- 찾기를 클릭하고 기존 패턴을 선택합니다.

단계 **3** 패턴 필드에서 착신 번호와 일치시키고자 하는 패턴을 입력합니다.

단계 **4** 착신자 변환 패턴 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

로컬 라우트 그룹 구성

선택 사항. 로컬 라우트 그룹을 구성하여 필요한 라우트 목록의 수를 줄일 수 있습니다. 라우트 목록은 PSTN 게이트웨이의 위치를 기준으로 시스템에서 통화를 라우팅하기 위해 사용하는 PSTN 게이트웨이를 가리킵니다. 다른 방법으로 로컬 라우트 그룹을 사용하여 게이트웨이에 액세스하기 위해 사용되는 라우트 패턴에서 PSTN 게이트웨이의 위치를 분리할 수 있습니다. 이 구성을 통해 다른 위치의 전화기 및 기타 디바이스가 단일 라우트 패턴 세트를 사용할 수 있으며, Unified Communications Manager에서 통화를 라우팅하기 위해 올바른 게이트웨이를 선택합니다.

예를 들어, 로컬 라우트 그룹을 사용하면 국가의 모든 도시에 대한 별도의 다이얼 플랜이 아니라 국가 전체의 단일 다이얼 플랜을 가질 수 있습니다. 이 방법은 중앙 집중식 통화 구축 시나리오에만 적용됩니다.

프로시저

	명령 또는 동작	목적
단계 **1**	로컬 라우트 그룹 이름 구성, 199 페이지	선택 사항. 시스템에서는 기본 로컬 라우트 그룹으로 불리는 기본 로컬 라우트 그룹을 제공하지만, 추가 로컬 라우트 그룹을 구성할 수 있습니다. 이 절차를 사용하여 추가 로컬 라우트 그룹의 이름을 지정합니다.
단계 **2**	로컬 라우트 그룹을 디바이스 풀과 연결, 199 페이지	시스템의 각 디바이스가 로컬 라우트 그룹을 알 수 있도록 프로비저닝되어 있도록, 로컬 라우트 그룹을 디바이스 풀과 연결합니다.
단계 **3**	라우트 목록에 로컬 라우트 그룹 추가, 199 페이지	선택 사항. 라우트 목록에 추가할 수 있는 로컬 라우트 그룹을 구성합니다. 로컬 라우트 그룹을 만들 때 시스템은 발신 통화를 디바이스 풀 수준에서 사용자에 대해 정의된 게이트웨이로 라우팅합니다.

로컬 라우트 그룹 이름 구성

선택 사항. 시스템에서는 기본 로컬 라우트 그룹으로 불리는 기본 로컬 라우트 그룹을 제공하지만, 추가 로컬 라우트 그룹을 구성할 수 있습니다. 이 절차를 사용하여 추가 로컬 라우트 그룹의 이름을 지정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트/헌트 > 로컬 라우트 그룹 이름을 선택합니다.

단계 **2** 행 추가를 클릭합니다.

단계 **3** 새로운 로컬 라우트 그룹의 이름과 설명을 입력합니다.

단계 **4** 저장을 클릭합니다.

로컬 라우트 그룹을 디바이스 풀과 연결

로컬 라우트 그룹을 할당하여 시작 디바이스의 디바이스 풀 설정을 기반으로 기존 라우트 그룹을 사용할 수 있습니다. 이 설정을 통해 다른 위치의 전화기 및 기타 디바이스에서 단일 라우트 패턴 세트를 사용할 수 있으며, 동시에 Unified Communications Manager에서 올바른 게이트웨이를 선택하여 통화를 라우팅합니다.

시스템의 각 디바이스가 로컬 라우트 그룹을 알 수 있도록 프로비저닝되어 있도록, 로컬 라우트 그룹을 디바이스 풀과 연결합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 디바이스 풀을 선택합니다.

단계 **2** 검색 조건을 입력하고 찾기를 클릭한 다음, 결과 목록에서 디바이스 풀을 선택합니다.

단계 **3** 로컬 라우트 그룹 설정 영역의 기본 로컬 라우트 그룹 드롭다운 목록에서 라우트 그룹을 선택합니다.

단계 **4** 저장을 클릭합니다.

라우트 목록에 로컬 라우트 그룹 추가

라우트 목록에 추가할 수 있는 로컬 라우트 그룹을 구성합니다. 로컬 라우트 그룹을 만들 때 시스템은 발신 통화를 디바이스 풀 수준에서 사용자에 대해 정의된 게이트웨이로 라우팅합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트/헌트라우트 목록을 > 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가를 클릭하여 새 라우트 목록을 추가합니다.
- 찾기를 클릭하고 결과 목록에서 라우트 목록을 선택하여 기존 라우트 포인트에 대한 설정을 수정합니다.

라우트 목록 구성 창이 나타납니다.

단계 **3** 라우트 목록에 로컬 라우트 그룹을 추가하려면 라우트 그룹 추가 버튼을 클릭합니다.

단계 **4** 라우트 그룹 드롭다운 목록에서 로컬 라우트 그룹을 선택하여 경로 목록에 추가합니다. 기본 로컬 라우트 그룹을 추가하거나 생성한 사용자 지정 로컬 라우트 그룹을 추가할 수 있습니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 구성 적용을 클릭합니다.

라우트 그룹 구성

시스템에서 발신 통화에 대한 게이트웨이를 선택하는 순서에 우선순위를 지정하도록 라우트 그룹을 구성합니다. 이 절차를 사용하여 유사한 특성을 갖는 게이트웨이를 그룹화하여 그룹의 모든 게이트웨이에서 해당 통화에 전화를 걸 수 있도록 합니다. 시스템에서 라우트 그룹을 구성할 때 지정하는 순서에 따라 사용할 게이트웨이를 선택합니다.

디바이스를 여러 라우트 그룹에 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트/헌트 > 라우트 그룹을 선택합니다.

라우트 그룹 구성 창이 나타납니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가를 클릭하여 새 라우트 그룹을 추가합니다.
- 찾기를 클릭하고 결과 목록에서 라우트 그룹을 선택하여, 기존 라우트 그룹에 대한 설정을 수정합니다.

라우트 그룹 구성 창이 나타납니다.

단계 **3** 라우트 그룹록 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

라우트 목록 구성

라우트 목록을 구성하여 라우트 그룹을 식별하고 우선순위에 따라 배치합니다. Unified Communications Manager는 라우트 목록에 있는 순서를 사용하여 발신 통화에 사용할 수 있는 디바이스를 검색합니다.

라우트 목록을 구성하는 경우, 하나 이상의 라우트 그룹을 구성해야 합니다. 라우트 목록에는 라우트 그룹과 로컬 라우트 그룹만 포함될 수 있습니다.

참고 라우트 목록을 통해 발신 통화가 전송되면, 라우트 목록 프로세스에서 발신 디바이스를 잠가 통화가 완료되기 전에 경고 메시지가 전송되지 않도록 방지합니다. 발신 디바이스가 잠긴 후에는 헌트 목록에서 착신 통화를 더 이상 헌팅하지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트/헌트라우트 목록을 > 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가를 클릭하여 새 라우트 목록을 추가합니다.
- 찾기를 클릭하고 결과 목록에서 라우트 목록을 선택하여 기존 라우트 포인트에 대한 설정을 수정합니다.

단계 **3** 라우트 그룹록 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **4** 라우트 목록에 라우트 그룹을 추가하려면 라우트 그룹 추가 버튼을 클릭합니다.

단계 **5** 라우트 그룹 드롭다운 목록에서 라우트 목록에 추가할 라우트 그룹을 선택합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** 구성 적용을 클릭합니다.

라우트 필터 구성

라우트 필터는 전화 건 번호 문자열을 사용하여 통화가 처리되는 방식을 결정합니다. 라우트 필터는 at(@) 와일드카드를 포함하는 라우트 패턴을 구성할 때만 적용됩니다. 라우트 패턴에 @ 와일드카드가 포함되어 있는 경우, Unified Communications Manager에서 이 절차에서 지정한 번호 지정 플랜에 따라 통화를 라우팅합니다.

다이얼 플랜 설치 관리자를 사용하는 경우 라우트 필터가 필수입니다. 즉, 다이얼 플랜 파일을 설치한 다음 해당 번호 지정 플랜에 따라 라우트 패턴을 구성하는 경우가 이에 해당합니다. 다이얼 플랜을 수동으로 구성하는 경우 라우트 플랜은 선택 사항입니다.

다이얼 플랜을 수동으로 구성하는 경우, @ 와일드카드를 포함하는 라우트 패턴이 있을 때마다 라우트 필터를 구성해야 합니다. 라우트 패턴에 @ 와일드카드가 포함된 경우, 시스템에서 라우트 필터를 사용하여 지정한 번호 지정 플랜에 따라 통화를 라우팅합니다.

참고 콜 라우팅을 구성할 때 많은 라우트 패턴에 단일 라우트 필터를 할당하지 않도록 주의해야 합니다. 수백 개의 연결된 라우트 패턴이 있는 라우트 필터를 편집하려는 경우, 시스템 코어가 발생할 수 있습니다. 이는 라우트 필터를 사용하는 모든 라우트 패턴에 대한 콜 라우팅을 업데이트하는 데 필요한 추가 시스템 처리때문입니다. 중복 라우트 필터를 만들고 단일 라우트 필터를 250개 이하의 라우트 패턴과 연결합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트 필터를 선택합니다.

단계 **2** 번호 지정 플랜 드롭다운 목록에서 다이얼 플랜을 선택하고 다음을 클릭합니다.

단계 **3** 라우트 필터 이름 필드에 이름을 입력합니다.

각 라우트 필터 이름이 라우트 플랜에 고유한지 확인하십시오.

단계 **4** 라우트 필터 태그 및 연산자를 선택하고 데이터를 입력하여 이 라우트 필터에 대한 절을 생성합니다.

사용 가능한 라우트 필터 태그에 대한 자세한 내용은를 라우트 필터 태그, 203 페이지의 내용을 참조하십시오.

참고 EXISTS, DOES-NOT-EXIST 또는 NOT-SELECTED 연산자를 사용하는 태그에 대한 라우트 필터 태그 값을 입력하지 마십시오.

단계 **5** 라우트 필터 연산자를 선택하고 해당하는 데이터를 입력하여 이 라우트 필터에 대한 절을 생성합니다.

사용 가능한 라우트 필터 연산자에 대한 자세한 내용은 라우트 필터 연산자, 204 페이지의 내용을 참조하십시오.

단계 **6** 저장을 클릭합니다.

단계 **7** 구성 적용을 클릭합니다.

라우트 필터 설정

라우트 필터링은 특정 라우트가 로컬 라우트 데이터베이스에 포함되는 것으로 간주되지 않는 프로세스입니다. 라우트 패턴이 구성된 경우에만 적용됩니다.

다음 항목은 라우트 필터 기본 설정에 대한 정보를 나열합니다.

- 라우트 필터 태그, 203 페이지
- 라우트 필터 연산자, 204 페이지
- 라우트 필터 예 , 205 페이지

라우트 필터 태그

태그는 라우트 필터의 핵심 구성 요소로 사용됩니다. 태그는 전화 건 번호 문자열 하위 집합에 이름을 적용합니다. 예를 들어 naNP 번호 972-555-1234는 LOCAL-AREA-CODE(972), OFFICE-CODE(555) 및 SUBSCRIBER(1234) 라우트 필터 태그로 구성됩니다.

라우트 필터 태그에는 연산자가 필요하며 통화가 필터링될지 결정하기 위해 추가 값이 필요할 수 있습니다.

라우트 필터 태그 필드의 값에는 와일드카드 문자 X, *, #, [,], -, ^와 0-9까지의 숫자가 포함될 수 있습니다. 다음 표의 설명에는 실제 숫자를 나타내기 위해 [2-9] 및 XXXX 표기법이 사용되고 있습니다. 이 표기법에서 [2-9]는 범위 2에서 9 까지의 단일 숫자를 나타내며 X는 0~9 범위의 단일 숫자를 나타냅니다. 따라서 [2-9]XX 형식의 세 자리 지역 번호의 경우, 실제 번호 200~999나 모든 와일드카드 또는 실제 번호와 해당 범위의 패턴을 나타내는 와일드카드를 조합하여 입력할 수 있습니다.

라우트 필터 태그는 [라우트 필터 구성] 창의 [번호 지정 플랜] 드롭다운 목록 상자에서 선택한 번호 지정 플랜에 따라 달라집니다. 다음 표에서는 북미 번호 지정 플랜에 대한 라우트 필터 태그에 대해 설명합니다.

표 ***17:*** 라우트 필터 태그

태그	설명
AREA-CODE	[2-9]XX 형식의 이 세 자리 지역 번호는 장거리 통화를 위한 지역 번호를 식별합니다.
COUNTRY CODE	이 1자리, 2자리 또는 3자리 코드는 국제 전화 대상 국가를 지정합니다.
END-OF-DIALING	이 단일 문자는 전화 건 번호 문자열의 끝자리를 식별합니다. # 문자는 naNP 내에서 전화 거는 국제 번호에 대한 전화걸기 끝 신호로 사용됩니다.
국제 접속	이 2자리 액세스 코드는 국제 다이얼을 지정합니다. 이 코드의 경우 미국에서 걸리는 통화는 01을 사용합니다.
국제 직통 전화	이 한 자리 코드는 직접 건 국제 전화를 식별합니다. 이 코드의 경우 미국에서 걸리는 통화는 1을 사용합니다.
국제 오퍼레이터	이 한 자리 코드는 오퍼레이터가 지원하는 국제 전화를 식별합니다. 이 코드는 미국에서 걸리는 통화에 0을 지정합니다.
지역 번호	[2-9]XX 형식의 이 세 자리 지역 번호는 10자리 로컬 통화에 대한 지역 번호를 식별합니다.
지역 직통 전화	이 한 자리 코드는 직접 건 로컬 통화를 식별합니다. 이 코드의 경우 naNP 통화는 1을 사용합니다.
지역 오퍼레이터	이 한 자리 코드는 오퍼레이터가 지원하는 로컬 통화를 식별합니다. 이 코드의 경우 naNP 통화는 0을 사용합니다.
장거리 직통 전화	이 한 자리 코드는 직접 건 장거리 통화를 식별합니다. 이 코드의 경우 naNP 통화는 1을 사용합니다.

태그	설명
장거리 오퍼레이터	이 1자리 또는 2자리 코드는 naNP 내에서 오퍼레이터가 지원하는 장거리 통화를 식별합니다. 이 코드의 경우 오퍼레이터가 지원하는 통화는 0을 사용하고 오퍼레이터 액세스는 00을 사용합니다.
국내 번호	이 태그는 국제 전화용 번호 문자열의 국가 관련 부분을 지정합니다.
사무실 코드	이 태그는 7자리 디렉터리 번호의 처음 세 자리를 [2-9]XX 형식으로 지정합니다.
위성 서비스	이 한 자리 코드는 국제 전화용 위성 연결에 대한 액세스를 제공합니다.
SERVICE	이 세 자리 코드는 911(긴급), 611(복구), 411(정보) 등의 서비스를 지정합니다.
가입자	이 태그는 7자리 디렉터리 번호의 마지막 네 자리를 XXXX 형식으로 지정합니다.
트랜짓 네트워크	이 4자리 값은 장거리 캐리어를 식별합니다. TRANSIT-NETWORK 값에 선행 101 캐리어 액세스 코드 접두사를 포함하지 마십시오. 자세한 내용은 TRANSIT-NETWORK-ESCAPE를 참조하십시오.
트랜짓 네트워크 이스케이프	이 세 자리 값은 장거리 캐리어 식별자 앞에 옵니다. 이 필드의 값은 101입니다. TRANSIT-NETWORK-ESCAPE 값에 4자리 캐리어 식별 코드를 포함하지 마십시오. 자세한 내용은 TRANSIT-NETWORK를 참조하십시오.

라우트 필터 연산자

라우트 필터 태그 연산자는 해당 태그와 연결된 전화를 건 번호 문자열에 따라 통화가 필터링되는지 여부를 결정합니다. EXISTS 및 DOES-NOT-EXIST 연산자는 전화 건 번호 문자열 부분이 있는지 확인합니다. == 연산자는 실제 전화 건 번호와 지정된 값 또는 패턴을 비교합니다. 다음 표에서는 라우트 필터 태그와 함께 사용할 수 있는 연산자에 대해 설명합니다.

표 ***18:*** 라우트 필터 연산자

연산자	설명
NOT-SELECTED	이 태그와 연결된 전화 건 번호 문자열에 따라 통화를 필터링하지 않도록 지정합니다. 참고 연산자가 연결된 태그의 존재 여부로는 Cisco Unified Communications Manager의 통화 전송이 차단되지 않습니다.
EXISTS	이 태그와 연결된 전화 건 번호 문자열이 발견되면 통화를 필터링하도록 지정합니다. 참고 Cisco Unified Communications Manager는 전화 건 번호 문자열에 태그와 연결된 일련의 번호가 있는 경우에만 통화를 전송하거나 차단합니다.

연산자	설명
DOES-NOT-EXIST	이 태그와 연결된 전화 건 번호 문자열이 발견되지 않으면 통화를 필터링하도록 지정합니다. 참고 Cisco Unified Communications Manager는 전화 건 번호 문자열에 태그와 연결된 일련의 번호가 없는 경우에만 통화를 전송하거나 차단합니다.
==	이 태그와 연결된 전화 건 번호 문자열이 지정된 값과 일치하면 통화를 필터링하도록 지정합니다. 참고 Cisco Unified Communications Manager는 전화 건 번호 문자열이 태그와 연결된 일련의 번호를 포함하며 연결된 필드에 지정된 숫자 범위 내에 있는 경우에만 통화를 전송하거나 차단합니다.

라우트 필터 예

예 1: AREA-CODE 및 DOES-NOT-EXIST 연산자를 사용하는 라우트 필터는 지역 번호를 포함하지 않는 모든 전화 건 문자열을 선택합니다.

예 2: AREA-CODE, 연산자 == 및 항목 515를 사용하는 라우트 필터는 지역 번호 515를 포함하지 않는 모든 전화 건 문자열을 선택합니다.

예 3: AREA-CODE, 연산자 == 및 항목 5[2-9]X를 사용하는 라우트 필터는 지역 번호 520 - 599를 포함하지 않는 모든 전화 건 문자열을 선택합니다.

예 4: TRANSIT-NETWORK, 연산자 == 및 항목 0288을 사용하는 경로 필터는 통신업체 액세스 코드 1010288을 포함하는 모든 전화 건 문자열을 선택합니다.

라우트 패턴 구성

Cisco Unified Communications Manager는 라우트 패턴을 사용하여 내부 및 외부 통화를 모두 라우팅하거나 차단합니다. 라우트 패턴을 게이트웨이, 트렁크 또는 하나 이상의 라우트 그룹을 포함하는 라우트 목록에 할당할 수 있습니다.

참고 라우트 패턴이 게이트웨이를 바로 가리킬 수 있음에도, 라우트 목록과 라우트 그룹을 구성하는 것이 좋습니다. 이 방법을 사용하면 콜 라우팅 및 확장성에 대한 최고의 유연성을 제공받을 수 있습니다.

경로 패턴이 게이트웨이 또는 트렁크에 직접 할당된 경우 게이트웨이 또는 트렁크를 경로 그룹에 연결할 수 없습니다. 마찬가지로 이미 경로 목록의 구성원인 게이트웨이나 트렁크는 경로 패턴에 연결할 수 없습니다.

프로시저

단계 **1** Cisco 통합 CM 관리에서 콜 라우팅 > 라우트/헌트 > 라우트 패턴을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 라우트 패턴을 생성합니다.
- 찾기를 클릭하고 기존 라우트 패턴을 선택합니다.

라우트 목록 구성 창이 나타납니다.

단계 **3** 라우트 패턴 필드에 다이얼 문자열이 반드시 일치해야 하는 번호 패턴을 입력합니다.

단계 **4** 게이트웨이/라우트 드롭다운 목록에서 이 라우트 패턴과 일치하는 통화를 보내려는 대상을 선택합니다.

단계 **5** 라우트 패턴 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

라우트 패턴 설정

Unified CM을 활성화하기 위해 번호 문자열(주소) 및 연결된 번호 세트로 구성된 다른 라우트 패턴을 생성하여 라우트 목록이나 게이트웨이로 통화를 라우팅할 수 있도록 조작할 수 있습니다.

다음은 구성하려는 라우트 패턴 유형의 예입니다.

- 라우트 패턴의 와일드카드 및 특수 문자, 206 페이지
- Pre-dot 숫자 제거 예, 208 페이지
- 접두 번호 지정의 예, 209 페이지
- 온넷 및 오프넷 패턴의 예, 209 페이지
- 블록 및 라우트 패턴의 예, 209 페이지

라우트 패턴의 와일드카드 및 특수 문자

라우트 패턴에서 와일드카드 및 특수 문자를 통해 다양한 번호(주소)와 일치하는 단일 라우트 패턴을 사용할 수 있습니다. 이러한 와일드카드 및 특수 문자를 사용하여 Unified Communications Manager에서 번호를 조작한 다음 인접 시스템에 전송할 수 있는 지침을 작성할 수도 있습니다.

다음 표에서는 Cisco Unified Communications Manager에서 지원하는 와일드카드 및 특수 문자에 대해 설명합니다.

표 ***19:*** 와일드카드 및 특수 문자

문자	설명	예
@	at 특수문자(@) 와일드카드는 모든 국가 번호 지정 플랜 번호와 일치합니다. 각 라우트 패턴에는 @ 와일드카드가 하나만 있을 수 있습니다.	라우트 패턴 9.@은 국가 번호 지정 플랜에서 인식하는 모든 숫자를 라우트 또는 차단합니다. 다음 라우트 패턴의 예는 @ 와일드카드가 포함된 국가 번호 지정 플랜 번호를 표시합니다. • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X 와일드카드는 범위 0에서 9까지의 모든 단일 숫자와 일치합니다.	라우트 패턴 9XXX는 9000 ~ 9999 범위의 모든 숫자를 라우트 또는 차단합니다.
!	느낌표 (!) 와일드카드는 0 ~ 9 범위에 있는 하나 이상의 숫자와 일치합니다.	라우트 패턴 91!는 910 ~ 91999999999999999999999 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
?	물음표 표시 (?) 와일드카드는 선행 숫자 또는 와일드카드 값이 0회 이상 발생에 일치합니다. 참고 물음표 표시(??) 와일드 카드를 사용하는 경우 두 번째 물음표가 빈 입력과 일치하지 않습니다. 라우터 패턴 예: *33X?*X?*X?#	라우트 패턴 91X?는 91 ~ 91999999999999999999999 범위에 있는 모든 숫자를 라우트 또는 차단 합니다.
+	더하기 기호 (+) 와일드카드는 선행 숫자 또는 와일드카드 값이 1회 이상 발생에 일치 합니다.	라우트 패턴 91X+는 910 ~ 91999999999999999999999 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
[ ]	대괄호 ([ ]) 문자는 여러 값을 포함합니다.	라우트 패턴 813510 [012345]은 8135100~8135105 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
-	대괄호와 함께 사용되는 하이픈 (-) 문자는 여러 값을 나타냅니다.	라우트 패턴 813510[0-5]은 8135100~8135105 범위에 있는 모든 숫자를 라우트 또는 차단합니다.

문자	설명	예
^	대괄호와 함께 사용되는 circumflex (^) 문자는 여러 값을 무효화합니다. 여는 괄호 ([) 뒤에 나오는 첫 번째 문자인지 확인합니다. 각 라우트 패턴에는 하나의 ^ 문자만 사용될 수 있습니다.	라우트 패턴 813510[^0-5]은 8135106 ~ 8135109 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
.	구분 기호로 사용되는 점 (.) 문자는 디렉터리 번호와 Cisco Unified Communications Manager 액세스 코드를 구분합니다. 이 특수 문자를 폐기 숫자 지침과 함께 사용하여 Cisco Unified Communications Manager 액세스 코드를 제거한 다음 해당 번호를 인접 시스템으로 전송합니다. 각 라우트 패턴에는 점 (.) 문자가 하나만 있을 수 있습니다.	라우트 패턴 9.@은 국가 번호 지정 플랜 통화의 Cisco Unified Communications Manager 액세스 코드로 초기 9를 식별합니다.
*	별표 (*) 문자는 전화 건 특수 번호에 추가 숫자를 제공할 수 있습니다.	디렉터리 지원을 위해 내부 운영자에게 액세스를 제공하도록 라우트 패턴 *411을 구성할 수 있습니다.
#	번호 기호 (#) 문자는 다이얼링 시퀀스의 종료를 식별합니다. # 문자가 패턴의 마지막 문자인지 확인합니다.	라우트 패턴 901181910555#는 국가 번호 지정 플랜 내에서 발신된 국제 번호를 라우트 또는 차단합니다. 마지막 5 이후 나오는 # 문자는이 숫자를 시퀀스의 마지막 숫자로 식별합니다.
\+	백슬래시 앞에 나오는 더하기 기호(\+)는 국제 이스케이프 문자 +를 구성하려고 함을 나타냅니다.	\+를 사용하는 것은 국제 이스케이프 문자 +가 와일드카드가 아니라 전화 번호에 있는 기호로 사용됨을 의미합니다.

Pre-dot 숫자 제거 예

라우트 패턴에서 pre-dot 숫자 제거를 사용하는 한 가지 예는 전화기 사용자가 외부 회선에 연결하기 위해 액세스 코드를 연결하기를 원하는 경우입니다. 북미에서는 일반적으로 사용자가 외부 회선에 액세스하기 위해 9를 누릅니다. 다음 라우트 패턴을 사용하여 지정할 수 있습니다.

- 로컬 통화: **`9.@`** or **`9.[2-9]XXXXXX`**
- 국내 통화: **`9.1[2-9]XX`**

- 국제 통화: **9.011!#**

이러한 패턴에서 9는 외부 회선에 대한 액세스 코드이고, 점(.)은 네트워크 내부에 있는 숫자와 외부 숫자가 무엇인지를 표시하여 라우트 패턴의 형식 지정을 지원하는 구분 기호입니다. 시스템에서 PSTN으로 전화를 거는 번호를 전송할 때, [자릿수 삭제] 옵션을 사용하여 PSTN에서 해당 통화를 라우팅할 수 있도록 전화를 건 문자열에서 pre-dot 숫자를 제거할 수 있습니다.

접두 번호 지정의 예

라우트 패턴에서 접두 번호 지정을 사용하는 한 가지 예는 사이트 간에 온넷 다이얼링 구성할 때입니다. 조직 내 사용자가 8 + XXX-XXXX로 전화를 걸어 사이트 간에 통화할 수 있도록 라우트 패턴을 만들 수 있습니다. 오프넷 통화의 경우 앞자리 숫자(8)를 제거하고 새 앞자리 숫자 1 <area code>을 추가하여 E.164 형식으로 통화를 PSTN으로 라우팅할 수 있습니다.

온넷 및 오프넷 패턴의 예

통화 분류 필드를 사용하여 라우트 패턴을 온넷 또는 오프넷으로 구성할 수 있습니다. 사용자가 보조 발신음을 사용하여 자신의 통화가 조직 외부에서 진행되고 있음을 알릴 수 있도록 할 경우에는 통화를 오프넷으로 분류할 수 있습니다. 예를 들어, 사용자가 외부 회선에 액세스하기 위해 9로 전화를 걸어야 하는 라우트 패턴을 생성하였고 이를오프넷 패턴으로 분류한 경우, 시스템에서 다음과 같은 신호음을 제공합니다.

- 전화기가 오프 훅 상태일 때 9로 전화를 걸기 전에 신호음이 울립니다.
- 9로 전화를 건 후 들리는 보조 신호음은 시스템에서 PSTN(Public Switched Telephone Network) 번호로 전화를 걸 준비가 되었음을 나타냅니다.

이 옵션을 사용할 때 디바이스 재정의 허용 확인란의 체크 표시를 해제했는지 확인하십시오.

블록 및 라우트 패턴의 예

차단 및 라우트 패턴을 사용하여 라우팅하지 않으려는 발신 또는 착신 통화를 방지합니다. 블록 패턴을 사용하여 다음을 수행합니다.

- 특정 패턴을 차단 합니다. 예를 들어, 패턴 91900XXXXXXX를 차단하면 사용자가 900개의 서비스에 전화를 걸 수 없습니다.
- 특정 지역 번호 및 위치로 통화를 차단하여 유료 사기를 방지합니다.

클러스터 수준 자동 대체 라우팅 활성화

클러스터에 대한 AAR (자동 대체 라우팅)를 활성화합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 Cisco CallManager를 선택합니다.

단계 **4** 클러스터 수준 매개변수(시스템 - CCM ARR) 영역에서 **ARR(**자동 대체 라우팅**)** 활성화 매개변수를 참으로 설정합니다.

AAR 그룹 구성

불충분한 위치 대역폭으로 인해 시스템에서 통화를 차단할 때 PSTN 또는 다른 네트워크를 통해 통화를 자동으로 재라우팅하도록 AAR(자동 대체 라우팅)를 구성합니다. AAR을 사용하면 발신자가 전화를 끊고 착신자에게 재다이얼할 필요가 없습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > **AAR** 그룹을 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가를 클릭하여 새 AAR 그룹을 추가합니다.
- 찾기를 클릭하고 결과 목록에서 AAR 그룹을 선택하여 기존 AAR 그룹에 대한 설정을 수정합니다.

AAR 그룹 구성 창이 나타납니다.

단계 **3** 이름에서 새 AAR 그룹에 할당하려는 이름을 입력합니다.

이 이름은 최대 20자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

창이 새로고침되고 추가 필드가 표시됩니다.

단계 **4** **AAR** 그룹 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **5** 저장을 클릭합니다.

참고 선택 사항. 헌트 파일럿을 사용하여 AAR를 활성화하려면, 헌트 파일럿 구성 작업 플로우, 223 페이지를 참조하십시오.

시간 라우팅 구성

(선택 사항) 착신 통화를 받기 위해 제공된 파티션이 언제 사용 가능한지를 지정한 일정을 생성합니다.

참고 MWI(메시지 대기 표시) 차단에 대해 시간 라우팅이 구현되지 않았습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	기간 구성, 211 페이지	이 절차를 사용하여 기간을 정의합니다. 시작 시간과 종료 시간을 정의할 수 있고, 또한 반복 간격을 연간 달력에 요일이나 지정된 날짜로 지정할 수도 있습니다.
단계 **2**	일정 구성, 211 페이지	이 절차를 사용하여 일정을 만듭니다. 이전 절차에서 구성한 기간은 이 일정에 대한 빌딩 블록입니다. 여러 일정에 기간을 할당할 수 있습니다.
단계 **3**	시간 일정을 파티션에 연결, 212 페이지	일정을 파티션과 연결하여 발신 디바이스에서 특정 시간 동안 통화를 완료하려고 시도할 때 어디를 검색하는지 확인합니다.

기간 구성

이 절차를 사용하여 기간을 정의합니다. 시작 시간과 종료 시간을 정의할 수 있고, 또한 반복 간격을 연간 달력에 요일이나 지정된 날짜로 지정할 수도 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 제어 클래스 > 기간을 선택합니다.

단계 **2** 기간기 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **3** 저장을 클릭합니다.

일정 구성

이 절차를 사용하여 일정을 만듭니다. 이전 절차에서 구성한 기간은 이 일정에 대한 빌딩 블록입니다. 여러 일정에 기간을 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 제어 클래스 > 일정을 선택합니다.

단계 **2** 시간 일정 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **3** 저장을 클릭합니다.

시간 일정을 파티션에 연결

일정을 파티션과 연결하여 발신 디바이스에서 특정 시간 동안 통화를 완료하려고 시도할 때 어디를 검색하는지 확인합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 제어 클래스 > 파티션을 선택합니다.

단계 **2** 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.
시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 **3** 저장을 클릭합니다.

콜 라우팅 제한

기능	제한 사항
라우트 필터 연결	콜 라우팅을 구성할 때 너무 많은 라우트 패턴에 단일 라우트 필터를 할당하지 않도록 주의해야 합니다. 수백 개의 연결된 라우트 패턴이 있는 라우트 필터를 편집하려는 경우, 시스템 코어 crash가 발생할 수 있습니다. 이는 라우트 필터를 사용하는 모든 라우트 패턴에 대한 콜 라우팅을 업데이트하는 데 필요한 추가 시스템 처리때문입니다. 이런 일이 발생하지 않도록 중복 라우트 필터를 생성합니다.
외부 전화 제어	외부 통화 제어에서 Cisco Unified Routing Rules Interface를 사용하여 보조 라우트 서버가 Cisco Unified Communications Manager를 위한 콜 라우팅 결정을 내리도록 합니다. 외부 통화 제어를 구성할 때 Cisco Unified Communications Manager에서는 발신자 및 착신자 정보가 포함된 라우트 요청을 보조 라우트 서버에 대해 발행합니다. 해당 서버가 요청을 수신하고, 적절한 비즈니스 논리를 적용하고, 적용할 추가 콜 라우팅 방법에 대한 시스템 지침인 라우트 응답을 반환합니다. 자세한 내용은 외부 통화 제어 장을 *Cisco Unified Communications Manager* 기능 구성 설명서에서 참조합니다.

기능	제한 사항
통화 제어 탐색(CCD)	통화 제어 탐색(CCD)을 통해 Unified Communications Manager 클러스터는 SAF(Service Advertisement Framework)로 불리는 Cisco IOS 서비스 라우팅 프로토콜에 가입하여 호스트 중인 DN 범위를 자동으로 변경할 수 있습니다. 이 기능을 사용하여 클러스터는 자체 호스트 DN 범위를 네트워크로 알릴 뿐만 아니라 네트워크의 다른 통화 에이전트에 의해 생성된 광고에 가입할 수 있습니다. SAF CCD 사용의 주요 혜택은 다음과 같습니다. • SAF CCD 네트워크에 참여한 통화 에이전트 간에 콜 라우팅 정보의 자동 분배, 그 결과 새로운 통화 에이전트가 추가될 때 또는 DN 범위가 특정 통화 에이전트에 추가될 때 점진적 구성 작업을 피할 수 있음. • 중앙 집중식 다이얼 플랜 해상도 제어 지점에 의지하지 않음. • 복수의 Unified CM 클러스터가 결합될 때를 포함한 라우팅 변경 발생 시, 통화 간 에이전트 콜 라우팅 정보의 자동 복구. 통화 제어 탐색(CCD)을 구성하려며면, 통화 제어 탐색*(CCD)* 구성 장을 *Cisco Unified Communications Manager* 기능 구성 설명서에서 참조하십시오.
경로 플랜 보고서	Cisco Unified CM 관리의 라우트 계획 보고서 창 내에서 상세한 라우트 계획을 볼 수 있습니다(콜 라우팅 > 라우트 계획 보고서). 라우트 계획 보고서를 통해 라우트 계획의 일부 또는 전체 목록을 볼 수 있으며, 보고서의 패턴/디렉터리 번호, 파티션 또는 라우트 열에서 항목을 클릭하여 연결된 설정창으로 바로 이동할 수 있습니다. 또한 라우트 계획 보고서를 사용하여 보고서 데이터를 .csv 파일로 저장하여 다른 애플리케이션으로 가져올 수 있습니다. .csv 파일에는 전화기의 디렉터리 번호, 라우트 패턴, 패턴 사용, 디바이스 이름 및 디바이스 설명을 비롯하여 웹페이지보다 더 자세한 정보가 포함되어 있습니다.

착신 번호 분석기로 문제 해결하기

착신 번호 분석기가 Cisco Unified Communications Manager와 함께 기능 서비스로 설치됩니다. 이 도구를 사용하면 구축하기 전에 Cisco Unified Communications Manager 다이얼 플랜 구성을 테스트할 수 있습니다. 다이얼 플랜이 구축된 이후에도 이 도구를 사용하여 다이얼 플랜을 분석할 수도 있습니다.

다이얼 플랜은 여러 디바이스, 변환 패턴, 라우트 패턴, 라우트 목록, 라우트 그룹, 발신자 및 착신자 변환, 디바이스 수준 변환을 포함하여 복잡할 수 있으므로 다이얼 플랜에 오류가 포함될 수 있습니다. 착신 전화 분석기를 사용하여 착신 번호를 입력으로 제공하여 다이얼 플랜을 테스트할 수 있습니다. 이 도구는 착신 번호를 분석하고 통화 세부 정보를 보여줍니다. 이러한 결과를 사용하여 다이얼 플랜을 진단하고, 문제가 있는지 확인하고, 구축하기 전에 다이얼 플랜을 조정할 수 있습니다.

착신 번호 분석기 설정 및 사용 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 착신 번호 분석기를 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 참조하십시오.

회선 그룹 설정

이 장에서는 회선 그룹을 추가 또는 삭제하거나, 디렉터리 번호를 추가하거나, 회선 그룹에서 디렉터리 번호를 제거하기 위한 정보를 제공합니다.

추가적인 정보는 *Cisco Unified Communications Manager* 시스템 설명서에서 라우트 플랜의 이해와 관련된 항목을 참조하십시오.

회선 그룹 설정 정보

Cisco 통합 커뮤니케이션 매니저 관리에서 콜 라우팅 > 라우트/헌트 > 회선 그룹 메뉴 라우트를 사용하여 회선 그룹을 구성합니다.

회선 그룹을 사용하면 디렉토리 번호가 선택되는 순서를 지정할 수 있습니다. Cisco 통합 커뮤니케이션 매니저에서는 통화 분배 알고리즘과 RnaR(응답 없음 벨소리 복귀) 시간 제한 설정에 따라 회선 그룹의 유휴 또는 사용 가능 구성원에게 통화를 분배합니다.

참고 사용자는 회선 그룹에 속하는 DN에 대한 통화를 직접 통화 당겨받기 기능을 사용하여 당겨받을 수 없습니다.

팁 구성원(디렉토리 번호)이 없는 빈 회선 그룹을 구성할 수는 있지만, Cisco 통합 커뮤니케이션 매니저에서는 통화 전송에 대해 이 구성을 지원하지 않습니다. 회선 그룹에 구성원이 없으면 통화가 빈 회선 그룹으로 전송될 때 헌트 목록에서 헌팅이 중지됩니다. 이러한 상황을 방지하려면 회선 그룹에 하나 이상의 구성원을 구성해야 합니다.

회선 그룹 구성 팁

회선 그룹을 구성하기 전에 하나 이상의 디렉토리 번호를 정의해야 합니다.

회선 그룹을 구성하거나 업데이트한 후에는 해당 회선 그룹에서 구성원을 추가하거나 제거할 수 있습니다.

회선 그룹 삭제

하나 이상의 경로/헌트 목록에서 참조하는 회선 그룹은 삭제할 수 있습니다. 사용 중인 회선 그룹을 삭제하려고 하면 Cisco Unified Communications Manager에 오류 메시지가 표시됩니다.

팁 회선 그룹에는 디펜던시 레코드가 지원되지 않습니다. 항상 구성을 먼저 확인하고 회선 그룹을 삭제하는 것이 좋습니다.

회선 그룹 설정

필드	설명
회선 그룹 정보	
회선 그룹 이름	이 회선 그룹의 이름을 입력합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다. 각 회선 그룹 이름은 라우트 플랜에 따라 고유한지 확인하십시오. 간편한 방법 회선 그룹에 대해 설명이 포함된 간단한 이름을 사용합니다. CompanynameLocationGroup 형식은 일반적으로 충분한 수준의 상세정보를 제공하며 회선 그룹을 빠르고 쉽게 식별할 수 있을 정도로 길이가 짧습니다. 예를 들어 CiscoDallasAA1는 달라스 Cisco 사무실의 Cisco Access Analog 회선 그룹을 식별합니다.
Rna 복귀 시간 초과	통화에 응답하지 않을 경우 그리고 첫 번째 헌트 옵션, [다음 구성원 시도 후 헌트 목록에서 다음 그룹 시도]가 선택된 경우, Unified Communications Manager에서 이 회선 그룹의 사용 가능한 다음 구성원 또는 유휴 구성원으로 통화를 분배하거나 다음 회선 그룹으로 통화를 분배하기까지 걸리는 시간(초)을 입력합니다. Rna 복귀 시간 초과는 회선 그룹 수준에서 모든 구성원에 적용됩니다.

필드	설명
분배 알고리즘	드롭다운 목록표의 다음 옵션 중에서 회선 그룹 수준에서 적용되는 분배 알고리즘을 선택합니다. • 위에서 아래로 - 이 분배 알고리즘을 선택하는 경우 Unified Communications Manager는 회선 그룹의 첫 번째 유휴 또는 사용 가능한 구성원부터 시작하여 마지막 유휴 또는 사용 가능한 구성원까지 유휴 또는 사용 가능한 구성원으로 통화를 분배합니다. • 순환 - 이 분배 알고리즘을 선택하는 경우 Unified Communications Manager는 라우트 그룹의 (n+1)번째 구성원부터 시작하여 유휴 또는 사용 가능한 구성원을 대상으로 통화를 분배합니다. 여기서 n번째 구성원은 목록에서 유휴 또는 통화 중 상태이되 "작동 중단"되지 않은 다음 순서의 구성원입니다. n번째 구성원이 라우트 그룹의 마지막 구성원인 경우 Unified Communications Manager는 라우트 그룹의 맨 위부터 시작하여 통화를 분배합니다. • 최장 유휴 시간 - 이 분배 알고리즘을 선택하는 경우 Unified Communications Manager는 회선 그룹의 최장 유휴 구성원부터 시작하여 최단 유휴 구성원까지 유휴 구성원만 대상으로 통화를 분배합니다. • 브로드캐스트 - 이 분배 알고리즘을 선택하는 경우 Unified Communications Manager는 회선 그룹의 모든 유휴 또는 사용 가능한 구성원을 대상으로 동시에 통화를 분배합니다. 브로드캐스트 분배 알고리즘을 사용하는 경우 적용되는 추가 제한 사항에 대해서는 [선택한 DN/라우트 파티션] 필드에 대한 설명에 있는 참고 사항을 참조하십시오. 기본값은 [최장 유휴 시간]입니다.
헌트 옵션	

필드	설명
응답 없음	지정된 분배 알고리즘에 대해 응답하지 않는 회선 그룹의 구성원으로 통화가 배분되는 경우 Unified Communications Manager에 사용할 헌트 옵션을 선택합니다. 이 옵션은 구성원 수준에서 적용됩니다. 드롭다운 목록표의 다음 옵션 중에서 선택합니다. • 다음 구성원 시도 후 헌트 목록에서 다음 그룹 시도 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 회선 그룹의 첫 번째 유휴 또는 사용 가능한 구성원부터 시작하여 마지막 유휴 또는 사용 가능한 구성원까지 유휴 또는 사용 가능한 구성원을 대상으로 통화를 분배합니다. 실패할 경우 Unified Communications Manager는 헌트 목록의 다음 회선 그룹을 시도합니다. • 다음 구성원을 시도하지만 다음 그룹으로는 이동하지 마십시오 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 회선 그룹의 첫 번째 유휴 또는 사용 가능한 구성원부터 시작하여 마지막 유휴 또는 사용 가능한 구성원까지 유휴 또는 사용 가능한 구성원을 대상으로 통화를 분배합니다. 현재 회선 그룹의 마지막 구성원에 도달하면 Unified Communications Manager에서 시도를 중단합니다. • 나머지 구성원을 생략하고 다음 그룹으로 바로 이동해야 합니다 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 첫 번째 구성원에 대한 Rna 복귀 시간 초과 값이 경과할 경우 이 회선 그룹의 나머지 구성원을 건너뜁니다. Unified Communications Manager에서 헌트 목록의 다음 회선 그룹으로 바로 진행합니다. • 헌팅 중지 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 이 회선 그룹의 첫 번째 구성원으로 통화를 분배하려고 시도한 후 구성원이 통화에 응답하지 않으면 헌팅을 중단합니다.
응답이 없는 경우 헌트 구성원 자동 로그아웃	이 확인란에 체크 표시하면 회선 구성원이 자동으로 헌트 목록에서 로그오프됩니다. 회선 구성원은 "헌트로그" 소프트키 또는 PLK를 사용하여 다시 로그인할 수 있습니다.

필드	설명
통화 중	지정된 분배 알고리즘에 대해 통화 중인 회선 그룹의 구성원으로 통화가 분배되는 경우 Unified Communications Manager에 사용할 헌트 옵션을 선택합니다. 드롭다운 목록표의 다음 옵션 중에서 선택합니다. • 다음 구성원 시도 후 헌트 목록에서 다음 그룹 시도 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 회선 그룹의 첫 번째 유휴 또는 사용 가능한 구성원부터 시작하여 마지막 유휴 또는 사용 가능한 구성원까지 유휴 또는 사용 가능한 구성원을 대상으로 통화를 분배합니다. 실패할 경우 Unified Communications Manager는 헌트 목록의 다음 회선 그룹을 시도합니다. • 다음 구성원을 시도하지만 다음 그룹으로는 이동하지 마십시오 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 회선 그룹의 첫 번째 유휴 또는 사용 가능한 구성원부터 시작하여 마지막 유휴 또는 사용 가능한 구성원까지 유휴 또는 사용 가능한 구성원을 대상으로 통화를 분배합니다. 현재 회선 그룹의 마지막 구성원에 도달하면 Unified Communications Manager에서 시도를 중단합니다. • 나머지 구성원을 생략하고 다음 그룹으로 바로 이동해야 합니다 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 통화 중인 구성원이 발견되면 이 회선 그룹의 나머지 구성원을 건너뜁니다. Unified Communications Manager에서 헌트 목록의 다음 회선 그룹으로 바로 진행합니다. • 헌팅 중지 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 이 회선 그룹의 통화 중인 첫 번째 구성원으로 통화를 분배하려고 시도한 후 헌팅을 중단합니다.

필드	설명
해당 없음	지정된 분배 알고리즘에 대해 사용할 수 없는 회선 그룹의 구성원으로 통화가 분배되는 경우 Unified Communications Manager에 사용할 헌트 옵션을 선택합니다. 해당 DN과 연결된 전화기 중 등록된 전화기가 없는 경우에 [사용할 수 없음] 상태가 발생합니다. [사용할 수 없음]은 내선 이동이 사용 중이며 DN/사용자가 로그인되지 않은 경우에도 발생합니다. 드롭다운 목록표의 다음 옵션 중에서 선택합니다. • 다음 구성원 시도 후 헌트 목록에서 다음 그룹 시도 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 회선 그룹의 첫 번째 유휴 또는 사용 가능한 구성원부터 시작하여 마지막 유휴 또는 사용 가능한 구성원까지 유휴 또는 사용 가능한 구성원을 대상으로 통화를 분배합니다. 실패할 경우 Unified Communications Manager는 헌트 목록의 다음 회선 그룹을 시도합니다. • 다음 구성원을 시도하지만 다음 그룹으로는 이동하지 마십시오 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 회선 그룹의 첫 번째 유휴 또는 사용 가능한 구성원부터 시작하여 마지막 유휴 또는 사용 가능한 구성원까지 유휴 또는 사용 가능한 구성원을 대상으로 통화를 분배합니다. 현재 회선 그룹의 마지막 구성원에 도달하면 Unified Communications Manager에서 시도를 중단합니다. • 나머지 구성원을 생략하고 다음 그룹으로 바로 이동해야 합니다 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 사용할 수 없는 구성원이 발견되면 이 회선 그룹의 나머지 구성원을 건너뜁니다. Unified Communications Manager에서 헌트 목록의 다음 회선 그룹으로 바로 진행합니다. • 헌팅 중지 - 이 헌트 옵션을 선택하면 Unified Communications Manager에서 이 회선 그룹의 사용할 수 없는 첫 번째 구성원으로 통화를 분배하려고 시도한 후 헌팅을 중단합니다.
회선 그룹 구성원 정보	
회선 그룹에 추가할 디렉토리 번호 찾기	
파티션	드롭다운 목록표에서 이 회선 그룹의 라우트 파티션을 선택합니다. 기본값은 <None>입니다. [찾기]를 클릭하면 [사용 가능한 DN/라우트 파티션] 목록 상자에 선택한 파티션에 속하는 모든 DN이 표시됩니다.
디렉토리 번호 포함	원하는 디렉토리 번호에 있는 문자를 입력하고 [찾기] 버튼을 클릭합니다. 입력한 문자와 일치하는 디렉토리 번호가 [사용 가능한 DN/라우트 파티션] 상자에 표시됩니다.

필드	설명
사용 가능한 DN/라우트 파티션	[사용 가능한 DN/라우트 파티션] 목록 상자에서 디렉토리 번호를 선택하고 [회선 그룹에 추가]를 클릭하여 [선택한 DN/라우트 파티션] 목록 상자에 추가합니다.
현재 회선 그룹 구성원	
공유 회선 DN을 사용하는 브로드캐스트 알고리즘	디렉토리 번호의 우선순위를 변경하려면 [선택한 DN/라우트 파티션] 목록 상자에서 디렉토리 번호를 선택합니다. 목록 상자 오른쪽의 화살표를 클릭하여 디렉토리 번호를 목록에서 위 또는 아래로 이동합니다. [선택한 DN/라우트 파티션] 목록 상자에서 디렉토리 번호의 우선순위를 역순으로 바꾸려면 [선택한 DNs/라우트 파티션 역순]을 클릭합니다. 참고 회선 그룹에 DN과 라우트 파티션을 추가할 때 공유 회선에 해당하는 DN을 브로드캐스트 분배 알고리즘을 사용하는 회선 그룹에 포함시키지 마십시오. DN이 브로드캐스트 분배 알고리즘을 사용하는 회선 그룹의 구성원인 경우 Unified Communications Manager에서 DN이 공유 회선으로 구성된 디바이스의 공유 회선에 해당하는 DN을 모두 표시하지 못합니다.
제거된 DN/라우트 파티션	[선택한 DN/라우트 파티션] 목록 상자에서 디렉토리 번호를 선택하고 두 목록 상자 사이에 있는 아래쪽 화살표를 클릭하여 [제거된 DN/라우트 파티션] 목록 상자에 추가합니다.
디렉토리 번호	
(현재 이 회선 그룹에 속하는 DN 목록)	지정된 디렉토리 번호의 [디렉토리 번호 구성] 창으로 이동하려면 이 목록에서 디렉토리 번호를 클릭합니다. 참고 새 회선 그룹을 추가하는 경우 회선 그룹을 저장할 때까지 이 목록이 표시되지 않습니다.

회선 그룹에 구성원 추가

새 회선 그룹 또는 기존 회선 그룹에 구성원을 추가할 수 있습니다. 다음 절차에서는 기존 회선 그룹에 구성원을 추가하는 방법을 설명합니다.

시작하기 전에

이 절차를 수행하기 전에 하나 이상의 디렉터리 번호를 정의해야 합니다.

프로시저

단계 **1** 콜 라우팅 > 라우트/헌트 > 회선 그룹을 선택합니다.

단계 **2** 구성원을 추가할 회선 그룹을 찾습니다.

단계 **3** 디렉터리 번호를 찾아야 하는 경우, [파티션] 드롭다운 목록 상자에서 라우트 파티션을 선택하고 [디렉터리 번호 포함] 필드에 검색 문자열을 입력한 다음 [찾기]를 클릭합니다. 파티션에 속하는 모든 디렉터리 번호를 찾으려면 [디렉터리 번호 포함] 필드를 비워 두고 [찾기]를 클릭합니다.

[사용 가능한 DN/라우트 파티션] 목록 상자에 일치하는 디렉터리 번호 목록이 표시됩니다.

단계 **4** [사용 가능한 DN/라우트 파티션] 목록 상자에서 추가할 디렉터리 번호를 선택하고 [회선 그룹에 추가]를 클릭하여 [선택한 DN/라우트 파티션] 목록 상자로 이동합니다. 이 회선 그룹에 추가할 각 구성원에 대해 이 단계를 반복합니다.

단계 **5** [선택한 DN/라우트 파티션] 목록 상자에서 이 회선 그룹에서 새 디렉터리 번호를 액세스할 순서를 선택합니다. 순서를 변경하려면 디렉터리 번호를 클릭하고 목록 상자 오른쪽에 있는 위쪽 및 아래쪽 화살표를 클릭하여 디렉터리 번호의 순서를 변경합니다.

단계 **6** [저장]을 클릭하여 새 디렉터리 번호를 추가하고 이 회선 그룹의 디렉터리 번호 순서를 업데이트합니다.

회선 그룹에서 구성원 제거

새 회선 그룹 또는 기존 회선 그룹에서 구성원을 제거할 수 있습니다. 다음 절차에서는 기존 회선 그룹에서 디렉터리 번호를 제거하는 방법을 설명합니다.

프로시저

단계 **1** 콜 라우팅 > 라우트/헌트 > 회선 그룹을 선택합니다.

단계 **2** 디렉터리 번호를 제거하려는 회선 그룹을 찾습니다.

단계 **3** [선택한 DN/라우트 파티션] 목록 상자에서 삭제할 디렉터리 번호를 선택하고 목록 상자 아래의 아래쪽 화살표를 클릭하여 디렉터리 번호를 [제거된 DN/라우트 파티션] 목록 상자로 이동합니다. 이 회선 그룹에서 제거하려는 각 구성원마다 이 단계를 반복합니다.

단계 **4** 구성원을 제거하려면 [저장]을 클릭합니다.

21 장

헌트 파일럿 구성

헌트 파일럿 개요

헌트 파일럿은 회선 그룹의 전화기 또는 디렉터리 번호 그룹으로 통화를 라우팅할 수 있는 번호 또는 패턴 및 연결된 숫자 조작 세트로 구성됩니다.

헌트 파일럿은 착신 통화에 대한 적합한 라우트(회선 그룹)의 우선순위 목록인 헌트 목록과 함께 작동합니다. 헌트 파일럿 DN으로 통화가 발신되면, 시스템에서 헌트 목록에 지정된 첫 번째 회선 그룹으로 통화를 제공 합니다. 첫 번째 회선 그룹에서 통화에 응답하는 사람이 없는 경우, 시스템에서는 헌트 목록에 지정된 다음 회선 그룹으로 통화를 제공합니다. 회선 그룹은 통화가 그룹 내의 전화기로 분산되는 순서를 제어합니다. 이는 일반적으로 IP 전화기 내선 또는 음성 메일 포트의 특정 내선을 가리킵니다. 회선 그룹은 컴퓨터 텔레포니 통합(CTI) 포트 및 CTI 라우트 포인트를 가리킬 수 없으므로 헌트 파일럿을 사용하여 Cisco CRS(Customer Response Solution) 또는 IP IVR(IP Interactive Voice Response)과 같은 CTI 애플리케이션을 통해 제어되는 엔드포인트에 통화를 분산할 수 없습니다.

헌트 파일럿은 회선 그룹과 헌트 파일럿이 서로 다른 파티션에 있는 경우에도 할당된 회선 그룹에 통화를 분산할 수 있습니다. 헌트 파일럿에 의해 분산된 통화는 모든 파티션과 CSS(발신 검색 공간) 제한 사항을 재정의합니다.

헌트 파일럿 구성 작업 플로우

이러한 작업을 완료하여 시스템에 대한 헌트 파일럿을 구성합니다. 헌트 파일럿은 회선 그룹의 전화기 또는 디렉터리 번호 그룹으로 통화를 라우팅하기 위해 사용될 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	회선 그룹 구성, 224 페이지	여러 전화기가 단일 DN(디렉터리 번호)로 연결되는 통화에 응답할 수 있도록 회선 그룹을 생성합니다.
단계 **2**	헌트 목록 구성, 225 페이지	회선 그룹에 우선순위를 지정하여 헌트 목록을 구성합니다.
단계 **3**	헌트 파일럿 구성, 225 페이지	시스템에서 헌트 목록으로 통화를 연결하기 위해 사용하는 헌트 파일럿 번호 또는 패턴을 구성합니다.

회선 그룹 구성

회선 그룹을 사용하면 여러 전화기에서 단일 디렉터리 번호로 걸려오는 전화를 받을 수 있습니다. 분배 알고리즘은 착신 통화가 그룹의 전화기로 분배되는 순서를 제어합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트/헌트 > 회선 그룹을 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가 를 클릭하여 새 회선 그룹을 만듭니다.
- 찾기를 클릭하고 기존 그룹을 선택합니다.

단계 **3** 회선 그룹 이름을 입력합니다.

단계 **4** 분배 알고리즘 필드에서 통화를 분배하기 위해 사용하려는 알고리즘 유형을 선택합니다.

단계 **5** 회선 그룹에 추가할 회선 그룹 구성원 섹션에서 필드를 구성하여 회선 그룹에 디렉터리 번호를 추가합니다.

a) 추가하려는 디렉터리 번호가 있는 파티션을 선택합니다.
b) (선택 사항) 디렉터리 번호 포함 필드를 완료하여 검색을 필터링합니다.
c) 찾기를 클릭합니다. 파티션의 디렉터리 번호 목록이 상자에 표시됩니다.
d) 사용 가능한 **DN**/라우트 파티션 목록 상자에서 그룹에 추가하려는 디렉터리 번호를 선택하고 회선 그룹에 추가를 클릭합니다.

단계 **6** 회선 그룹 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

헌트 목록 구성

헌트 목록은 회선 그룹의 우선 목록입니다. 시스템에서 헌트 목록을 통해 통화를 라우팅할 경우, 시스템은 헌트 목록에 정의된 순서대로 회선 그룹을 사용합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트/헌트 > 헌트 목록을 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가클릭하여 새 목록을 생성합니다.
- 찾기를 클릭하고 기존 목록을 선택합니다.

단계 **3** 헌트 목록의 이름을 입력합니다.

단계 **4** 헌트 목록에 등록하려는 **Cisco Unified Communications Manager** 그룹을 선택합니다.

단계 **5** 이 헌트 목록 활성화 확인란에 체크 표시를 하여 저장을 클릭하는 즉시 헌트 목록을 활성화합니다.

단계 **6** 헌트 목록이 음성 메일용인 경우 음성 메일용 확인란에 체크 표시합니다.

단계 **7** 저장을 클릭합니다.

단계 **8** 다음과 같이 회선 그룹을 헌트 목록에 추가합니다.

a) 회선 그룹 추가를 클릭합니다.
b) 회선 그룹 드롭다운에서 회선 그룹을 선택하여 헌트 목록에 추가합니다.
c) 저장을 클릭합니다.
d) 회선 그룹을 추가하려면 위의 단계를 반복합니다.

헌트 파일럿 구성

시스템에서 회선 그룹으로 통화를 라우팅하기 위해 사용하는 헌트 파일럿 번호 또는 패턴을 구성합니다.

참고 헌트 파일럿에 사용할 수 있는 와일드카드 및 특수 문자에 대한 자세한 내용은 헌트 파일럿의 와일드카드 및 특수 문자, 226 페이지의 내용을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 라우트/헌트 > 헌트 목록을 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 새로 추가 를 클릭하여 새 헌트 파일럿을 만듭니다.
- 찾기를 클릭하고 기존 헌트 목록을 선택합니다.

단계 **3** 헌트 파일럿 필드에 통화를 라우팅하기 위해 사용하려는 번호 또는 패턴을 입력합니다.

단계 **4** 헌트 목록 드롭다운에서 헌트 파일럿 번호와 일치하는 통화를 연결하려는 헌트 목록을 선택합니다.

단계 **5** 포트 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **6** 통화 대기열을 활성화하려면 대기열 통화 확인란에 체크 표시하고 대기 섹션에서 필드를 구성합니다.

단계 **7** 통화, 연결된 상대방 또는 착신자에게 적용하려는 번호 변환 패턴을 할당합니다.

단계 **8** 저장을 클릭합니다.

헌트 파일럿의 와일드카드 및 특수 문자

헌트 파일럿의 와일드카드 및 특수 문자를 사용하면 헌트 파일럿에서 숫자 범위(주소)를 매칭시킬 수 있습니다. 이러한 와일드카드 및 특수 문자를 사용하여 Cisco Unified Communications Manager에서 인접 시스템으로 보내기 전에 번호를 조작할 수 있게 해주는 지침을 작성할 수도 있습니다.

다음 표에서는 Cisco Unified Communications Manager에서 지원하는 와일드카드 및 특수 문자에 대해 설명합니다.

표 ***20:*** 와일드카드 및 특수 문자

문자	설명	예
@	at 특수문자(@) 와일드카드는 모든 국가 번호 지정 플랜 번호와 일치합니다. 각 라우트 패턴에는 @ 와일드카드가 하나만 있을 수 있습니다.	라우트 패턴 9.@은 국가 번호 지정 플랜에서 인식하는 모든 숫자를 라우트 또는 차단합니다. 다음 라우트 패턴의 예는 @ 와일드카드가 포함된 국가 번호 지정 플랜 번호를 표시합니다. • 0 • 1411 • 19725551234 • 101028819725551234 • 01133123456789
X	X 와일드카드는 범위 0에서 9까지의 모든 단일 숫자와 일치합니다.	라우트 패턴 9XXX는 9000 ~ 9999 범위의 모든 숫자를 라우트 또는 차단합니다.
!	느낌표 (!) 와일드카드는 0 ~ 9 범위에 있는 하나 이상의 숫자와 일치합니다.	라우트 패턴 91!는 910 ~ 91999999999999999999999 범위에 있는 모든 숫자를 라우트 또는 차단합니다.

문자	설명	예
?	물음표 표시 (?) 와일드카드는 선행 숫자 또는 와일드카드 값이 0회 이상 발생에 일치합니다. 참고 물음표 표시(??) 와일드 카드를 사용하는 경우 두 번째 물음표가 빈 입력과 일치하지 않습니다. 라우터 패턴 예: *33X?*X?*X?#	라우트 패턴 91X?는 91 ~ 919999999999999999999 범위에 있는 모든 숫자를 라우트 또는 차단 합니다.
+	더하기 기호 (+) 와일드카드는 선행 숫자 또는 와일드카드 값이 1회 이상 발생에 일치 합니다.	라우트 패턴 91X+는 910 ~ 919999999999999999999 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
[ ]	대괄호 ([ ]) 문자는 여러 값을 포함합니다.	라우트 패턴 813510 [012345]은 8135100~8135105 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
-	대괄호와 함께 사용되는 하이픈 (-) 문자는 여러 값을 나타냅니다.	라우트 패턴 813510[0-5]은 8135100~8135105 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
^	대괄호와 함께 사용되는 circumflex (^) 문자는 여러 값을 무효화합니다. 여는 괄호 ([) 뒤에 나오는 첫 번째 문자인지 확인합니다. 각 라우트 패턴에는 하나의 ^ 문자만 사용될 수 있습니다.	라우트 패턴 813510[^0-5]은 8135106 ~ 8135109 범위에 있는 모든 숫자를 라우트 또는 차단합니다.
.	구분 기호로 사용되는 점 (.) 문자는 디렉터리 번호와 Cisco Unified Communications Manager 액세스 코드를 구분합니다. 이 특수 문자를 폐기 숫자 지침과 함께 사용하여 Cisco Unified Communications Manager 액세스 코드를 제거한 다음 해당 번호를 인접 시스템으로 전송합니다. 각 라우트 패턴에는 점 (.) 문자가 하나만 있을 수 있습니다.	라우트 패턴 9.@은 국가 번호 지정 플랜 통화의 Cisco Unified Communications Manager 액세스 코드로 초기 9를 식별합니다.

문자	설명	예
*	별표 (*) 문자는 전화 건 특수 번호에 추가 숫자를 제공할 수 있습니다.	디렉터리 지원을 위해 내부 운영자에게 액세스를 제공하도록 라우트 패턴 *411을 구성할 수 있습니다.
#	번호 기호 (#) 문자는 다이얼링 시퀀스의 종료를 식별합니다. # 문자가 패턴의 마지막 문자인지 확인합니다.	라우트 패턴 901181910555#는 국가 번호 지정 플랜 내에서 발신된 국제 번호를 라우트 또는 차단합니다. 마지막 5 이후 나오는 # 문자는이 숫자를 시퀀스의 마지막 숫자로 식별합니다.
\+	백슬래시 앞에 나오는 더하기 기호(\+)는 국제 이스케이프 문자 +를 구성하려고 함을 나타냅니다.	\+를 사용하는 것은 국제 이스케이프 문자 +가 와일드카드가 아니라 전화 번호에 있는 기호로 사용됨을 의미합니다.

헌트 파일럿의 성능 및 확장성

다음과 같은 성능 및 확장성 제한 사항이 적용됩니다.

- 단일 Unified CM 클러스터는 최대 15,000개 헌트 목록 디바이스를 지원합니다.
- 단일 Unified CM 가입자는 노드별로 통화 대기가 활성화된 최대 100개의 헌트 파일럿을 지원합니다.
- 헌트 목록 디바이스는 각 헌트 목록에 10개 IP Phone이 있는 1500개 헌트 목록 조합, 각 헌트 목록에 20개 IP Phone이 있는 750개 헌트 목록 조합 또는 비슷한 조합일 수 있습니다.

참고 통화 커버리지에 대해 브로드캐스트 알고리즘을 사용하는 경우, 헌트 목록 디바이스의 수는 BHCA(최번시 통화 시도) 수에 따라 제한을 받습니다. 10대의 전화기를 포함하고 브로드캐스트 알고리즘을 사용하는 헌트 목록이나 헌트 그룹을 가리키는 헌트 파일럿에서 BHCA 10은 BHCA 10인 10대의 전화기와 동일합니다.

- 대기열에 32명의 발신자가 허용되도록 구성할 경우, 통화 대기가 활성화된 헌트 파일럿의 최대 수는 Unified CM 가입자 노드당 100개입니다. 노드당 대기열 슬롯의 총 수(결합된 노드에서 모든 통화 대기열 활성화 헌트 파일럿에 대해 "대기열에 허용되는 최대 발신자 수"의 값)는 3200으로 제한됩니다. 각 헌트 파일럿에 대해 대기열에 있는 최대 동시 발신자의 수는 100입니다. 이는 헌트 파일럿 당 100명의 발신자가 대기열에서 허용되고 최대 헌트 파일럿의 수가 32로 감소한다는 의미입니다. 모든 헌트 리스트 전반에 걸친 최대 설정원 수는 통화 대기가 활성화되어도 변하지 않습니다.
- 구성할 수 있는 각 헌트 파일럿에 대한 대기열의 최대 대기 시간은 0-3600초 범위입니다(기본값 900). 헌트 목록에서 수를 늘리면 Unified Communications Magager 서비스 매개변수에 지정된 다이얼 플랜 초기화 타이머를 늘려야 할 수 있습니다. 1500개 헌트 목록이 구성되어 있으면 다이얼 플랜 초기화 타이머를 600초로 설정하시는 것을 권장합니다.

- 통화 대기와 함께 브로드캐스트 알고리즘을 사용할 때 단일 회선 그룹에 35개 미만의 디렉터리 번호를 사용하는 것이 좋습니다. 또한 브로드캐스트 회선 그룹의 수는 BHCC(통화 중 시간 통화 완료율)에 따라 달라집니다. 통합 CM 시스템에 여러 개의 브로드캐스트 회선 그룹이 있는 경우 회선 그룹의 최대 디렉터리 번호 수는 35 미만이어야 합니다. 모든 브로드캐스트 회선 그룹에 대한 BHCA(최번시 통화 시도)의 수는 초당 설정된 35회 통화를 초과하지 않아야 합니다.

헌트 파일럿 상호 작용 및 제한 사항

기능	상호 작용 및 제한 사항
SNR(단일 번호 연락)과 헌트 그룹	헌트 그룹이 구성되어 있고 헌트 그룹이 가리키는 하나 이상의 디렉터리 번호에 SNR(단일 번호 도달)이 또한 활성화되어 있는 경우, 헌트 그룹의 모든 디바이스가 로그인되어 있지 않으면 통화는 SNR 원격 대상으로 확장되지 않습니다. 헌트 그룹 내의 각 디바이스의 경우, 해당 디바이스에 대한 전화기 설정 창에서 헌트 그룹에 로그인됨 확인란에 체크 표시가 되어 있어야만 합니다.
통화 대기시키기	통화 대기는 헌트 파일럿의 하위 기능입니다. 통화 대기가 활성화되어 있고 특정 헌트 파일럿에 대한 착신 통화 요구 사항이 통화 응답에 사용할 수 있는 헌트 구성원의 수를 초과하는 경우, 시스템에서 헌트 구성원이 해당 통화에 응답할 수 있을 때까지 착신 통화를 대기시킵니다. 대기 중에 발신자에게 재생되는 알림 및 음악 대기를 구성할 수 있습니다. 구성에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 기능 구성 설명서의 '통화 대기 구성' 장을 참조하십시오.
Unified Mobility	헌트 파일럿에서 Unified Mobility 디바이스를 구성하는 것은 권장하지 않습니다.

통화가 분배되지 않음

표 ***21:*** 통화가 순환 알고리즘과 함께 배포되지 않고 있습니다.

제한 사항	설명
통화가 BOT 및 TCT 디바이스를 사용하는 회선 그룹의 순환 알고리즘에서 올바르게 배포되지 않고 있습니다.	통화가 로그오프 상태의 에이전트에게 확장되고 "**Huntlogout**" 유형 이외의 다른 거부 유형으로 통화가 거부될 때가 그러한 경우입니다. 그런 다음 인덱스가 증가 하지 않으며 통화가 이전 통화에 응답 한 동일한 에이전트에 게 전달 됩니다.

제한 사항	설명
회선 그룹의 순환 알고리즘에서는 통화가 올바르게 배포 되지 않습니다.	통화를 순환 알고리즘으로 배포 하는 동안 에이전트가 통화 중일 때 통화는 다음으로 사용 가능한 에이전트 (예: 통화 중 에이전트 대신 통화에 응답)으로 확장 됩니다. 참고 동시에 여러 통화를 진행하는 경우 사용 가능한 다음 에이전트가 통화에 응답합니다.

22 장

ILS(Intercluster Lookup Service) 구성

ILS 개요

Cisco ILS(Intercluster Lookup Service)를 사용하면 데이터를 공유하는 원격 Cisco Unified Communications Manager 클러스터의 다중 클러스터 네트워크를 쉽게 생성할 수 있습니다.

ILS를 사용하면 관리자가 인터클러스터 연결을 수동으로 구성해야 할 필요가 없습니다. 허브 클러스터에 ILS를 구성하고 나면, 새 클러스터에서 ILS를 활성화하고 새 클러스터가 기존 허브를 향하게 만들어 새 클러스터를 연결할 수 있습니다. ILS는 클러스터를 자동으로 연결하고 두 클러스터가 더 큰 ILS 네트워크의 토폴로지를 인식하도록 만듭니다.

ILS 네트워크 구성 요소

ILS 네트워크는 다음 구성 요소로 이루어집니다.

- 허브 클러스터—허브 클러스터는 automesh 기능을 사용하여 ILS 네트워크의 백본을 형성하여 다른 허브 클러스터와의 전체 메시 토폴로지를 생성합니다. 허브 클러스터는 다양한 기능을 위해 ILS 네트워크 상에서 정보를 릴레이하고 공유합니다.
- 스포크 클러스터—스포크 클러스터는 로컬 허브 클러스터에만 연결되며, 다른 허브 또는 스포크 클러스터와와는 직접 연결되지 않습니다. 스포크 클러스터는 로컬 허브에 의존하여 네트워크 상에서 정보를 공유 및 릴레이합니다.
- 전역 다이얼 플랜에서 가져온 카탈로그—전역 다이얼 플랜 복제가 구성된 경우 그리고 Cisco TelePresence Video Communications 서버 또는 타사 통화 제어 시스템과 상호 작용 중인 경우, 이 선택적 구성 요소가 적용됩니다. 다른 시스템에서 내보낸 CSV 파일에서 디렉터리 URI 또는 +E.164 번호 카탈로그를 수동으로 가져오면, ILS 네트워크의 사용자가 다른 시스템의 사용자에게 전화를 걸 수 있습니다.

클러스터 보기

ILS의 원격 클러스터 보기 기능을 사용하여 네트워크를 매핑할 수 있습니다. 각각의 클러스터에서는 네트워크 내 각 클러스터 상태의 원격 클러스터를 알려주는 업데이트 메시지, 착신자 피어 정보 벡터를 교환합니다. 업데이트 메시지에는 다음을 포함하여 네트워크 상의 알려진 클러스터 정보가 포함되어 있습니다.

- 클러스터 ID
- 퍼블리셔의 피어 ID
- 클러스터 설명 및 버전
- 호스트의 FQDN(Fully Qualified Domain name)
- ILS가 활성화된 클러스터 노드의 IP 주소 및 호스트네임

기능 지원

전역 다이얼 플랜 복제 및 Extension Mobility 로밍과 같은 기능은 ILS에 따라 클러스터에서 다이얼 플랜 정보를 공유하는 인터클러스터 네트워크를 생성합니다. 이렇게 하면 화상 통화, URI 다이얼링 및 인터클러스터 이동성을 사용하여 인터클러스터 통화 네트워크를 설정할 수 있습니다.

ILS는 또한 IM and Presence 중앙 클러스터를 여러 텔레포니 클러스터에 연결하는 경우 IM and Presence 서비스의 중앙 집중식 구축에도 사용됩니다. ILS는 IM and Presence 중앙 클러스터와 텔레포니 인터클러스터의 연결을 생성하기 위해 사용됩니다.

ILS 네트워킹 용량

다음은 ILS 네트워크를 계획할 때 염두에 두어야 하는 권장 용량입니다.

- ILS 네트워킹은 허브당 30개의 스포크 클러스터(최대 200개까지 가능)가 포함된 최대 10개의 허브 클러스터까지 지원합니다. 허브 및 스포크 조합 토폴로지는 각 클러스터 내에서 생성된 여러 TCP 연결을 방지하기 위해 사용됩니다.
- 허브 및 스포크 클러스터를 최대값 이상으로 활용하면 성능이 영향을 받을 수 있습니다. 단일 허브에 너무 많은 스포크 클러스터를 추가하면 메모리 또는 CPU 처리의 양을 늘릴 수 있는 추가 연결이 생성됩니다. 20개가 넘는 스포크 클러스터를 사용하여 허브 클러스터에 연결하는 것이 좋습니다.
- ILS 네트워킹은 시스템에 추가 CPU 처리를 추가합니다. CPU 사용률과 동기화 시간은 클러스터 전체에서 동기화되고 있는 레코드의 수에 따라 달라집니다. 허브 및 스포크 토폴로지를 계획하는 경우, 허브 클러스터에 로드를 처리하기 위한 CPU가 있는지 확인하십시오.

참고 이러한 권장 사항은 시스템 테스트에 기반하고 있으며 리소스 활용을 고려하여 수행합니다. 시스템에서 이러한 권장 사항을 초과하는 것을 막지는 않지만, 그렇게 할 경우 리소스 초과 활용의 위험이 발생할 수 있습니다. Cisco에서는 최적 성능 보장을 위해 위의 용량을 권장합니다.

ILS 구성 작업 플로우

이 작업을 완료하여 ILS 네트워크를 설정합니다.

시작하기 전에

허브 클러스터와 스포크 클러스터로 사용할 클러스터를 알 수 있도록 ILS 토폴로지를 반드시 계획해야 합니다.

프로시저

	명령 또는 동작	목적
단계 1	클러스터 ID 구성, 233 페이지	ILS 네트워크 내의 각 클러스터에는 고유한 클러스터 ID가 있어야 합니다.
단계 2	ILS 구성, 233 페이지	네트워크의 여러 클러스터에서 ILS를 구성하고 활성화합니다.
단계 3	ILS가 실행 중인지 확인, 235 페이지	ILS 네트워크가 제대로 작동 중인지 확인하십시오.
단계 4	원격 클러스터 보기 구성, 235 페이지	ILS 네트워크에 대한 원격 클러스터 보기를 구성합니다.

클러스터 ID 구성

ILS 네트워크 내의 각 클러스터에는 고유한 클러스터 ID가 있어야 합니다. 원격 클러스터에서 클러스터 ID에 대한 기본 **StandAloneCluster** 값을 유지하는 경우, ILS가 작동하지 않습니다.

프로시저

단계 1 게시자 노드에서 Cisco Unified CM 관리에 로그인합니다.
단계 2 시스템 > 엔터프라이즈 매개 변수를 선택합니다.
단계 3 클러스터 **ID** 값을 클러스터를 고유하게 식별하는 값으로 설정합니다.
단계 4 저장을 클릭합니다.
단계 5 각 클러스터의 퍼블리셔 노드에서 이 절차를 반복합니다.

ILS 구성

이 절차를 사용하여 네트워크에서 ILS(Intercluster Lookup Service) 를 활성화하고 구성합니다.

참고 구성하는 첫 번째 클러스터가 반드시 허브 클러스터가 되어야 합니다.

프로시저

단계 **1** 퍼블리셔 노드에서 Cisco Unified CM 관리에 로그인합니다.

단계 **2** 고급 기능 > **ILS** 구성을 선택합니다.

단계 **3** 역할 드롭다운 목록 상자에서 설정 중인 클러스터의 유형에 따라 허브 클러스터 또는 스포크 클러스터를 선택합니다.

단계 **4** 전역 다이얼 플랜 복제를 활성화하려는 경우, 원격 클러스터와 전역 다이얼 플랜 복제 데이터 교환 확인란에 체크 표시합니다.

참고 URI 패턴(`user@domain`)을 알릴 때 **SIP** 프로필 구성 창에서 다이얼 문자열 해석 필드를 항상 모든 다이얼 문자열을 **URI** 주소로 취급으로 설정하여 디바이스에서 사용자 섹션의 번호로만 된 다이얼 URI 설정 패턴을 디렉토리 번호 패턴으로 전화를 걸지 않도록해야 합니다. 또는 ILS를 통해 사용자 섹션의 텍스트 문자열을 포함한 URI 패턴만 알릴 수 있습니다.

단계 **5** 네트워크의 여러 인터클러스터에 **ILS** 인증 세부 정보를 구성합니다.

- TLS 인증을 위해 **TLS** 인증서 사용 확인란에 체크 표시합니다. 이 옵션을 사용하는 경우 클러스터의 노드 간에 CA 서명 인증서도 반드시 교환해야 합니다.
- TLS 사용 여부에 관계없이 암호 인증을 위해 암호 사용 확인란에 체크 표시하고 암호 상세 정보를 입력합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** **ILS** 클러스터 등록 팝업에서 등록 세부 정보를 구성합니다.

a) 등록 서버 텍스트 상자에 이 클러스터를 연결할 허브 클러스터의 게시자 노드 IP 주소 또는 FQDN을 입력합니다. 이것이 네트워크의 첫 번째 허브 클러스터인 경우, 필드를 비워 둘 수 있습니다.
b) 이 클러스터 확인란에 퍼블리셔의 인터클러스터 **Lookup** 서비스 **(ILS)** 활성화가 선택되었는지 확인하십시오.
c) 확인을 클릭합니다.

단계 **8** ILS 네트워크에 추가하려는 각 클러스터의 퍼블리셔게 노드에서 이 절차를 반복합니다. 새 클러스터를 허브 또는 스포크 클러스터로 추가 합니다.

참고 구성한 동기화 값에 따라 클러스터 정보가 네트워크 전체에 전파되는 동안 지연이 발생할 수 있습니다.

클러스터간에 TLS(전송 계층 보안) 인증을 사용하도록 선택한 경우 ILS 네트워크의 각 클러스터 퍼블리셔 노드간에 Tomcat 인증서를 교환하십시오. [Cisco Unified Operating System 관리]에서 벌크 인증서 관리 기능을 사용하여 다음을 수행합니다.

- 각 클러스터의 게시자 노드에서 중앙 위치로 인증서 내보내기
- ILS 네트워크에서 내보낸 인증서 통합
- 네트워크의 각 클러스터에 있는 게시자 노드로 인증서 가져오기

자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서의 "인증서 관리" 장을 참조하십시오.

ILS가 실행 중인지 확인

이 절차를 사용하여 ILS 네트워크가 실행 중인지 확인하십시오.

프로시저

단계 **1** 전화 통신 클러스터의 게시자 노드에 로그인합니다.

단계 **2** Cisco Unified CM 관리에서 고급 기능 > **ILS** 구성을 선택합니다.

단계 **3** **ILS** 클러스터 및 전역 다이얼 플랜 가져온 카탈로그 섹션을 선택합니다. ILS 네트워크 토폴로지가 나타나야 합니다.

원격 클러스터 보기 구성

이 절차를 사용하여 ILS 네트워크에 대한 원격 클러스터 보기를 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 고급 기능 > 클러스터 보기를 선택합니다.

단계 **2** 원격 클러스터 찾기 및 나열 창에서 이전에 생성된 원격 클러스터를 선택합니다.

단계 **3** 원격 클러스터 서비스 구성 창에서는 해당 확인란에 체크 표시하여 원격 클러스터에 대한 EMCC(익스텐션 모빌리티 크로스 클러스터), TFTP 및 RSVP 에이전트와 같은 서비스를 구성할 수 있습니다.

단계 **4** 저장을 클릭합니다.

ILS 상호 작용 및 제한 사항

ILS 상호 작용

표 22: ILS 상호 작용

기능	상호 작용
클러스터 검색	ILS 클러스터 검색으로 Cisco Unified Communications Manager 클러스터에서는 원격 클러스터에 대해 동적으로 배울 수 있으며, 관리자가 인터클러스터 연결을 수동으로 구성할 필요도 없습니다. ILS 네트워크에서 각각의 클러스터는 네트워크 내 각 클러스터 상태의 원격 클러스터를 알리도록 설계된 업데이트 메시지, 착신자 피어 정보 벡터를 교환합니다. 업데이트 메시지에는 다음을 포함하여 네트워크 상의 알려진 클러스터 정보가 포함되어 있습니다. • 클러스터 ID • 클러스터 설명 및 버전 • 호스트의 완전히 정규화된 도메인 이름 • ILS가 활성화된 클러스터 노드의 IP 주소 및 호스트네임 고급 기능 > 클러스터 보기를 선택하면 ILS 클러스터 검색 기능은 자동으로 Cisco Unified CM 관리에서 볼 수 있는 원격 클러스터 목록을 채웁니다. 이 창에서는 원격 클러스터에 대해 인터클러스터 내선 이동, TFTP 및 RSVP 에이전트와 같은 서비스를 구성할 수 있습니다. 참고 클러스터 보기에 표시된 대로 원격 클러스터의 FQDN(Fully Qualified Domain name)은 ILS 검색이 작동할 수 있도록 해결 가능한 DNS여야만 합니다.
전역 다이얼 플랜 복제	전역 다이얼 플랜 복제가 ILS 네트워크에서 사용되면 ILS 네트워크의 원격 클러스터가 다음을 포함한 전역 다이얼 플랜 데이터를 공유합니다. • 디렉터리 URI • 대체 번호 • 대체 번호 패턴 • 라우트 문자열 • PSTN 페일오버 번호
인바운드 통화 차단	ILS 기반 네트워크에서 발신자 번호에 근거하여 인바운드 통화를 차단하려는 경우, 발신자의 CSS에 SIP 라우트 패턴의 파티션을 반드시 포함해야 합니다. 예를 들어, 해당 통화가 SIP 트렁크에서 발생한 경우 SIP 트렁크 인바운드 CSS에 SIP 라우트 패턴의 파티션이 있어야만 합니다.

ILS 제한 사항

표 *23: ILS* 제한 사항

제한 사항	설명
ILS 서비스	ILS 서비스는 Unified Communications Manager 퍼블리셔 노드에서만 실행됩니다.
클러스터	허브 클러스터에는 스포크가 많이 있을 수 있지만 스포크 클러스터에는 허브 클러스터가 하나만 있을 수 있습니다.
ILS 네트워크	타사 통화 제어 시스템을 ILS 네트워크에 연결할 수 없습니다.
클러스터 가져오기	타사 카탈로그를 허브 클러스터로만 가져올 수 있습니다.
중복 URI	설정된 ILS 클러스터에 다른 원격 클러스터의 중복 URI가 포함되어 있는 경우 그리고 특정 통화가 해당 URI로 발신된 경우, URI가 우선 데이터베이스로 설정 및 삽입된 클러스터로 라우팅됩니다.
데이터베이스 복제 상태	전역 다이얼 플랜 데이터가 ILS 네트워크에서 성공적으로 교환되지만, 데이터베이스 복제 상태를 완료할 때까지 ILS 수신 클러스터에서 설정된 정보를 데이터베이스에 쓰지 않습니다.
가져오기	가져온 타사 디렉터리 URI 및 패턴의 경우, CSV 파일 형식이 관리 창 샘플 파일에 표시된 대로 정확한 syntax(명령문)와 일치해야만 합니다. 그렇지 않으면 가져오기가 실패합니다.
ILS 허브	ILS 네트워크에 추가 허브 클러스터를 추가하는 경우, 기본 ILS 허브 노드에 대해 다음 조건이 충족되는지 확인하십시오. • 클러스터 ID는 ILS 클러스터의 모든 허브 노드에서 고유합니다. • FQDN(Fully Qualified Domain name)이 구성됩니다. • UDS 및 EM 서비스가 ILS 클러스터의 모든 허브 노드에서 실행 중입니다. • DNS 기본 및 역방향 분석이 정상 작동합니다. • 모든 허브 노드에서 통합된 Tomcat 인증서를 가져옵니다. 그렇지 않으면 클러스터를 재부팅 하거나 오류를 수정한 후에도 원격 클러스터 찾기 및 나열 창에 "버전" 정보가 표시되지 않습니다. 이 문제를 해결 하려면 ILS 네트워크에서 허브 클러스터를 제거하고, 위의 요구 사항을 준수하고, 허브 클러스터를 ILS 네트워크에 다시 추가합니다.

23 장

전역 다이얼 플랜 복제 구성

전역 다이얼 플랜 복제 개요

전역 다이얼 플랜 복제를 사용하면 다이얼링을 위해 URI 다이얼링, 엔터프라이즈 번호 또는 E.164 번호를 사용하는 화상 통화를 통해 인터클러스터 VoIP 네트워크를 쉽게 설정할 수 있습니다.

전역 다이얼 플랜 복제는 ILS 네트워크의 원격 클러스터에 전역 다이얼 플랜 데이터 요소를 복제하여 ILS(Intercluster Lookup Service) 를 활용합니다. ILS 네트워크의 각 클러스터는 홈 클러스터에 대한 라우트 문자열과 함께 다른 클러스터의 전역 다이얼 플랜 요소를 학습합니다.

ILS를 통해 전역 알림

전역 다이얼 플랜 복제는 다음 다이얼 플랜 요소를 ILS 네트워크에 알려 원격 클러스터에서 이 데이터를 다음과 같이 복제합니다.

- 디렉터리 **URI**—로컬 클러스터에서 이메일 스타일 디렉터리 URI(예: alice@cisco.com)를 프로비저닝합니다. URI 다이얼링은 전화를 거는 사용자 중심적인 방법을 제공합니다. 전역 다이얼 플랜 복제를 사용 하면 디렉터리 uri의 로컬 카탈로그를 ILS 네트워크의 다른 클러스터에 광고 하여 인터클러스터 URI 다이얼링를 활성화할 수 있습니다.
- 엔터프라이즈 및 **E.164** 대체 번호—대체 번호는 원래 디렉터리 번호에 숫자 추가 지침으로 마스크를 적용하여 생성된 원래 내선 번호의 별칭입니다. 대체 번호를 사용하면 ILS 네트워크의 어떤 곳에서도 전화를 걸 수 있습니다. 대체 번호에는 두 가지 유형이 있습니다. 로컬 클러스터에서 대체 번호를 프로비저닝한 다음, 각 번호를 ILS 네트워크에 알리거나 여러 대체 번호를 요약하는 알려진 번호 패턴을 구성하고 해당 패턴을 ILS 네트워크에 알릴 수 있습니다.
- 알려진 패턴—알려진 패턴은 여러 엔터프라이즈 대체 번호 또는 +E.164 대체 번호를 요약합니다. 원격 클러스터에서 데이터베이스 공간을 절감하기 위해 개별 대체 번호 대신 ILS 네트워크 전역에 패턴을 복제할 수 있습니다. 알려진 패턴은 ILS 네트워크의 원격 클러스터에서만 사용됩니다. 따라서 이러한 패턴을 사용하여 로컬 통화를 라우팅할 수 없습니다.

- **PSTN** 페일오버 번호—이 옵션을 사용하면 엔터프라이즈 대체 번호 또는 E.164 대체 번호를 PSTN 페일오버 번호로 할당할 수 있습니다. 전역 다이얼 플랜 요소로의 콜 라우팅이 VoIP 채널을 통해 실패하는 경우, 페일오버 번호가 대체 라우팅 방법을 제공합니다. 원격 클러스터에서 PSTN 페일오버를 적절한 게이트웨이로 라우팅하는 라우트 패턴을 구성해야 합니다.
- 라우트 문자열—각 클러스터에는 전역 다이얼 플랜 카탈로그와 함께 복제되는 라우트 문자열이 있습니다. 라우트 문자열은 디렉터리 URI 또는 대체 번호에 대한 홈 클러스터를 식별합니다. 인터클러스터 통화를 위해서는, 각 원격 클러스터에서 라우트 문자열을 홈 클러스터로 라우팅하는 SIP 라우트 패턴을 구성해야만 합니다.
- 설정된 전역 다이얼 플랜 데이터—복제된 데이터가 ILS 네트워크의 모든 클러스터에 도달할 수 있도록 각 클러스터는 다른 클러스터에서 학습된 카달로그와 함께 프로비저닝된 전역 다이얼 플랜 데이터를 복제합니다.
- 가져온 전역 다이얼 플랜 데이터— Cisco Unified Communications Manager를 Cisco TelePresence Video Communications Server 또는 타사의 통화 제어 시스템과 상호 운용하고 있는 경우, 다른 시스템에서 csv 파일로 전역 다이얼 플랜들 내보낸 다음 해당 csv 파일을 ILS 네트워크의 허브 클러스터로 가져옵니다. 전역 다이얼 플랜 복제는 가져온 카탈로그를 ILS 네트워크의 다른 클러스터로 복제하여, 다른 시스템에 등록된 디렉터리 URI 및 대체 번호로 전화를 걸 수 있습니다.

샘플 전역 다이얼 플랜 매핑

다음 예에서는 내선 번호 4001에 매핑되는 샘플 전체 다이얼 플랜 데이터 요소를 보여줍니다. 호라우팅이 올바르게 설정되었다고 가정할 때 이러한 번호로 전화를 걸면 내선 번호 4001이 울립니다.

- 엔터프라이즈 대체 번호—4001 내선 번호에 적용된 5XXXX의 번호 마스크가 엔터프라이즈 대체 번호 54001을 생성합니다.
- E164 대체 번호— 4001 내선 번호에 적용된 1972555XXXX 번호 마스크가 +E.164 대체 번호 19725554001을 생성 합니다.
- PSTN 페일오버—엔터프라이즈 대체 번호 또는 + E.164 대체 번호를 PSTN 페일오버으로 할당하고 통화를 적절한 게이트웨이로 라우팅합니다.
- 알려진 패턴—패턴 54XXX를 사용하여 54000-54999 범위에 있는 모든 엔터프라이즈 대체 번호를 요약할 수 있습니다. 엔터프라이즈 및 + E.164 대체 번호에 대한 패턴을 생성할 수 있습니다.
- 디렉터리 URI—alice@cisco.com

참고 디렉터리 URI는 디렉터리 번호 또는 엔드 유저에게 할당될 수 있습니다. 엔드 유저와 연결된 디렉터리 URI는 사용자의 기본 내선 번호(디렉터리 번호)에도 연결되며, 할당된 경우 기본 내선 번호가 울립니다.

URI 다이얼링

URI 다이얼링은 발신자가 디렉터리 URI를 다이얼 문자열로 사용하여 전화를 걸 수 있도록 허용하는 전역 다이얼 플랜 복제의 하위 기능입니다. 디렉터리 URI는 이메일 주소처럼 보이는 영숫자 텍스트 문자열(예: alice@cisco.com)입니다.

URI가 이메일 주소와 유사하지만 디렉터리 URI는 그 자체로 라우팅이 가능한 엔터티가 아닙니다. 로컬 통화의 경우, 디렉터리 URI가 발신자의 CSS(발신 검색 공간) 내에 있는 파티션에 있을 경우에만 디렉터리 URI에 대한 통화가 라우팅될 수 있습니다. 인터클러스터 통화의 경우, 시스템에서 전역 다이얼 플랜 복제으로 복제된 클러스터 라우트 문자열을 가져와서 SIP 라우트 패턴과 라우트 문자열을 일치시켜 봅니다.

디렉터리 URI 유형

디렉터리 URI에는 두 가지 유형이 있으며, 이 유형은 디렉터리 URI를 프로비저닝하는 방법에 따라 결정됩니다.

- 사용자 기반 URI—디렉터리 URI가 엔드 유저 구성의 사용자에게 할당됩니다. 이러한 모든 URI는 로컬 디렉터리 URI 파티션(삭제할 수 없는 로컬 파티션)에 자동으로 할당됩니다. 사용자에게 기본 내선 번호가 있는 경우에도, URI는 해당 내선 번호에 대한 기본 URI로 디렉터리 번호 구성에도 표시됩니다.
- 회선 기반 URI—최대 5개의 추가 디렉터리 URI를 디렉터리 번호 구성 창에서 디렉터리 번호로 직접 할당할 수 있습니다. 이러한 URI의 경우 모든 로컬 파티션을 할당할 수 있습니다.

디렉터리 URI 형식

디렉터리 URI는 @ 기호로 구분된 사용자 및 호스트 주소로 구성된 영숫자 문자열입니다.

Cisco Unified Communications Manager는 디렉터리 URI에 대해 다음 형식을 지원합니다.

- user@domain(예: joe@cisco.com)
- user@ip_address(예: joe@10.10.10.1)

시스템에서는 디렉터리 URI의 사용자 부분(@ 기호 이전의 부분)에서 다음 형식을 지원합니다.

- 허용되는 문자: a-z, A-Z, 0-9, !, $, %, &, *, _, +, ~, -, =, , ?, , ‘, ,, ., /, (and) .
- 사용자 부분의 최대 길이는 47자입니다.
- 디렉터리 URI가 데이터베이스에 저장될 경우 Cisco Unified Communications Manager에서 다음 문자에 퍼센트 인코딩을 자동으로 적용합니다.

  # % ^ ` { } | \ : ” < > [ ] \ ‘ 및 공백.

참고 기본값으로 디렉터리 URI의 사용자 부분은 대소문자를 구분합니다. **URI** 조회 정책 엔터프라이즈 매개변수를 편집하여 대소문자를 구분하지 않도록 사용자 부분을 편집할 수 있습니다.

퍼센트 인코딩을 적용하면 디렉터리 URI의 숫자 길이가 증가합니다. 예를 들어, 디렉터리 URI로 joe smith#@cisco.com(20자)을 입력하면 Unified Communications Manager에서 디렉터리 URI를 데이터베이스에 joe%20smith%23@cisco.com(24자)으로 저장합니다. 데이터베이스 제한 사항으로 인해, 디렉터리 **URI** 필드의 최대 길이는 254자입니다.

Cisco Unified Communications Manager는 디렉터리 URI의 호스트 부분(@ 기호 다음 부분)에 다음 형식을 지원합니다.

- IPv4 주소 또는 정규화된 도메인 이름을 지원합니다.
- 허용되는 문자는 영숫자 문자, 하이픈(-) 및 점(.)입니다.
- 호스트 부분은 하이픈(-)으로 시작되거나 끝날 수 없습니다.
- 호스트 부분은 두 개의 점을 연속해서 포함할 수 없습니다.
- 호스트 부분의 최소 길이는 2자입니다.
- 호스트 부분은 대소문자를 구분하지 않습니다.

참고 **Cisco Unified Communications Manager** 관리 내에서, 벌크 관리를 사용하여 큰따옴표 또는 쉼표가 포함된 디렉터리 URI가 들어 있는 CSV 파일을 가져올 때는, 전체 디렉터리 URI를 큰따옴표로 묶어야 합니다.

URI로 통화 착신 전환

- 실물 전화기에서는 URI로 통화 착신 전환이 불가능합니다.
- URI로 통화 착신 전환은 Unified Communications Manager데이터베이스에 URI가 이미 있는 경우 응용프로그램을 통해서만 설정할 수 있습니다. URI가 데이터베이스에 없는 경우 응용프로그램은 통화 착신 전환을 설정하는 동안 "통화 착신 전환 설정 실패 /n 새 번호로 통화 착신 전환 실패" 오류를 출력합니다.
- URI가 데이터베이스에 있는지 여부나 Unified Communications Manager 관리 페이지를 통하지 않아도 모든 URI에 대해 통화 착신 전환을 설정할 수 있습니다.
- **Cisco** 통합 커뮤니케이션 자가 관리 포털 > 최종 사용자 페이지에서 데이터베이스에 있는지 여부에 관계 없이 모든 URI에 대한 통화 착신 전환을 설정할 수 있습니다. 다음 문자를 입력할 때 '백분율 인코딩'을 사용해야 합니다 **# % ^ ` { } | \ : ? < > [ ]** \ ‘. 예를 들어 **%3A**는 **:**를 나타내는 데 사용되며 **%20**은 공백을 나타내는 데 사용됩니다.

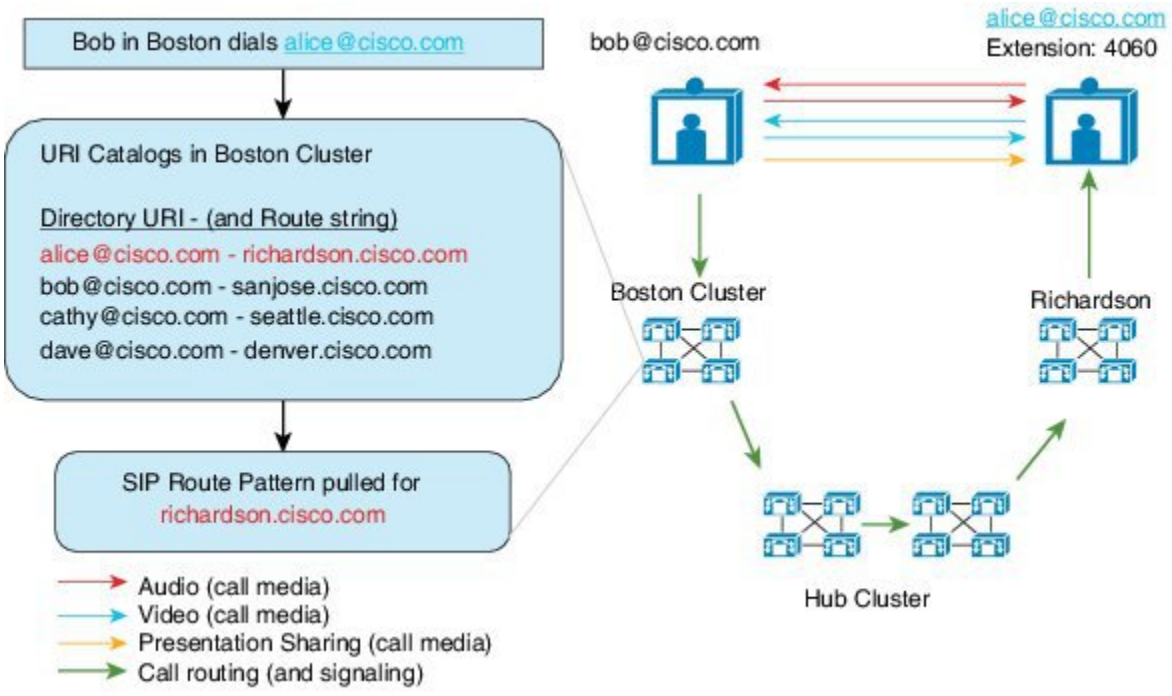
- URI "mobile: 12345@cisco.com"로 통화 착신 전환을 해야 하는 경우, **Cisco** 통합 커뮤니케이션 자가 관리 포털 > 최종 사용자 페이지의 통화 착신 전화 섹션에 "**mobile%3A%2012345@cisco.com**"을 제공해야 합니다.

전역 다이얼 플랜 복제를 위한 콜 라우팅

인터클러스터 통화의 경우, 전역 다이얼 플랜 데이터가 파티션 및 CSS(발신 검색 공간)을 통해 라우트됩니다. 로컬 디렉터리 URI, 엔터프라이즈 대체 번호 또는 E.164 대체 번호로의 통화가 작동되려면, 발신자가 사용 중인 CSS(발신 검색 공간)에 있는 파티션에 URI 또는 번호가 있어야만 합니다.

인터클러스터 통화는 전역 다이얼 플랜 복제가 알려주는 클러스터 라우트 문자열을 사용하여 착신자의 홈 클러스터로 통화를 전송합니다. 발신자가 다른 클러스터에 있는 디렉터리 URI 또는 대체 번호로 전화를 걸면, 시스템에서 연결된 라우트 문자열을 가져오고 라우트 문자열에 대한 SIP 라우트 패턴과 일치시킨 다음, SIP 라우트 패턴에서 지정한 대상으로 통화를 전송합니다. 이 작업을 수행하려면 원격 클러스터의 SIP 라우트 패턴을 구성하여 SIP 라우트 문자열을 홈 클러스터로 다시 라우트해야만 합니다.

콜 라우팅이 실패할 경우 시스템에서 연결된 PSTN 페일오버 번호를 사용할 수도 있습니다. 그러나 PSTN 페일오버 통화를 적절한 게이트웨이로 보낼 수 있도록 원격 클러스터에서 라우트 패턴을 구성해야 합니다.



GDPR(전역 다이얼 플랜 복제) 사전 요건

필수 조치:

- Cisco ILS(Intercluster Lookup Service) 구성
- 전역 다이얼 플랜을 구축할 방법을 다음과 같이 계획합니다.
  - 사용자에 대한 디렉터리 URI를 프로비저닝하여 URI 다이얼링을 구축할 것입니까? 전역 다이얼 플랜 복제를 사용하여 ILS 네트워크에서 디렉터리 URI를 복제할 수 있습니다.
  - 대체 번호 다이얼리을 구축할 것입니까? 엔터프라이즈 대체 번호 또는 E.164 대체 번호를 사용할 것입니까? 어떤 것을 PSTN 페일오버으로 사용할 것입니까?
  - 대체 번호를 구축할 경우, 번호 지정 플랜을 계획합니다. 대규모 네트워크의 경우 개별 대체 번호가 아닌 ILS 네트워크에 번호 패턴을 알려 데이터베이스 공간 및 대역폭을 절약할 수 있습니다.

전역 다이얼 플랜 복제 구성 작업 플로우

이 작업을 완료하여 전역 다이얼 플랜 복제 및 URI 다이얼링을 구성합니다. ILS 네트워크의 각 클러스터에서 이러한 작업을 완료해야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	전역 다이얼 플랜 복제를 위한 ILS 지원 활성화, 245 페이지	로컬 클러스터에서 전역 다이얼 플랜 복제에 대한 지원을 활성화합니다.
단계 **2**	SIP 프로파일 구성, 245 페이지	전역 다이얼 플랜 복제 및 URI 다이얼링을 지원하는 SIP 설정을 구성합니다.
단계 **3**	URI 다이얼링을 위한 SIP 트렁크 구성, 246 페이지	URI 다이얼링을 위해 시스템에서 디렉터리 URI, 디렉터리 번호 또는 혼합 주소를 연락처 헤더에 삽입할지 여부를 구성합니다.
단계 **4**	SIP 라우트 패턴 구성, 247 페이지	인터클러스터 라우팅을 위해 설정된 라우트 문자열을 홈 클러스터로 다시 라우팅하는 SIP 라우트 패턴을 각 클러스터에서 구성합니다.
단계 **5**	설정된 데이터에 대한 데이터베이스 한도 설정, 247 페이지	ILS에서 로컬 데이터베이스에 생성할 수 있는 데이터의 양에 대한 상한을 설정합니다.
단계 **6**	설정된 번호 및 패턴에 대한 파티션 할당, 248 페이지	엔터프라이즈 대체 번호, + E.164 대체 번호 및 설정된 번호 패턴에 대한 라우트 파티션을 할당합니다.
단계 **7**	대체 번호에 대해 광고된 패턴 설정, 249 페이지	(선택 사항) 일련의 엔터프라이즈 또는 +E.164 대체 번호가 요약된 번호 패턴을 알립니다.

	명령 또는 동작	목적
단계 **8**	설정된 패턴 차단, 249 페이지	(선택 사항) 특정 번호 또는 번호 패턴으로 통화를 차단 하는 패턴을 구성합니다. 이 구성은 로컬로 적용 되며 ILS 네트워크에 복제 되지 않습니다.
단계 **9**	전역 다이얼 플랜 데이터 가져오기, 251 페이지	(선택 사항) Cisco TelePresence Video Communication Server 또는 타사 통화 제어 시스템과 상호 운용 중인 경우, 다른 시스템의 디렉터리 URI 카탈로그, +E.164 번호 및 PSTN 페일오버 번호를 ILS 네트워크의 허브 클러스터로로 가져옵니다.
단계 **10**	전역 다이얼 플랜 데이터 프로비저닝, 250 페이지	디렉터리 번호에 디렉터리 URI, 엔터프라이즈 대체 번호 및 +E.164 대체 번호를 할당합니다. 참고 사용자가 복수인 경우, LDAP 디렉터리 동기화 또는 벌크 관리를 사용하여 단일 작업에서 다수의 사용자에 대한 전역 다이얼 플랜 데이터를 할당합니다. 이 설명서의 사용자 프로비저닝 섹션을 참조하십시오.

전역 다이얼 플랜 복제를 위한 ILS 지원 활성화

로컬 클러스터에서 전역 다이얼 플랜 복제를 위한 ILS 지원을 활성화하려면, 이 절차를 따르십시오.

프로시저

단계 **1** Cisco Unified Communications Manager 퍼블리셔 노드에 로그인합니다.
단계 **2** Cisco Unified CM 관리에서 고급 기능 > **ILS** 구성을 선택합니다.
단계 **3** 원격 클러스터와 전역 다이얼 플랜 복제 데이터 교환 확인란을 선택합니다.
단계 **4** 광고된 라우트 문자열 텍스트 상자에서 로컬 클러스터에 라우트 문자열을 입력합니다.
단계 **5** 저장을 클릭합니다.

SIP 프로파일 구성

이 절차를 사용하여 네트워크에서 SIP 프로파일을 편집하여 전역 다이얼 플랜 복제 및 URI 다이얼링을 지원합니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 **2** 찾기를 클릭하고 기존 SIP 프로파일을 선택합니다.

단계 **3** 다이얼 문자열 해석 드롭다운에서 시스템에서 사용하는 정책을 구성하여 통화를 디렉터리 URI로 또는 디렉터리 번호로 라우팅할 것인지 여부를 판단합니다.

- 모든 다이얼 문자열을 항상 URI 주소로 취급
- 전화 번호는 0–9, A–D, * 및 +로 구성됩니다(그 외는 URI 주소로 취급됨).
- 전화 번호는 0–9, * 및 +로 구성됩니다(그 외는 URI 주소로 취급됨). 이것이 기본 옵션입니다.

단계 **4** **SIP** 요청 시 **FQDN(Fully Qualified Domain name)** 사용 확인란에 체크 표시합니다.

단계 **5** (선택 사항) 트렁크별 구성에서 **Cisco** Unified Border Element에서 인터클러스터 통화를 라우팅할 수 있으려는 경우, **ILS** 설정된 대상 라우트 문자열 보내기 확인란에 체크 표시합니다.

단계 **6** 저장을 클릭합니다.

URI 다이얼링을 위한 SIP 트렁크 구성

URI 다이얼링을 구축하는 경우, 네트워크의 SIP 트렁크에 대한 연락처 헤더 주소 지정 정책을 구성합니다. Cisco Unified Communications Manager에서 발신 SIP 메시지의 SIP ID 헤더에 디렉터리 번호, 디렉터리 URI 또는 디렉터리 번호와 디렉터리 URI를 모두 포함하는 혼합 주소를 삽입할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 트렁크를 선택합니다.

단계 **2** 찾기를 클릭하고 기존 SIP 트렁크를 선택합니다.

단계 **3** 아웃 바운드 통화 영역에서 발신자 및 연결된 상대 정보 형식 드롭다운 목록에서 다음 중 하나를 선택합니다.

- 연결된 상대의 **DN**만 전달—발신 SIP 메시지에서 Unified Communications Manager에서 발신자의 디렉터리 번호를 SIP 연락처 헤더 정보에 삽입합니다. 이 값이 기본 설정입니다.
- 연결된 상대의 **URI**만 전달**(**사용 가능한 경우**)**—발신 SIP 메시지에서 Unified Communications Manager에서 착신자의 디렉터리 URI를 SIP 연락처 헤더에 삽입합니다. 디렉토리 URI를 사용할 수 없는 경우 Unified Communications Manager가 디렉토리 번호를 대신 삽입합니다.
- 연결된 상대의 **URI** 및 **DN** 전달**(**사용 가능한 경우**)**—발신 SIP 메시지에서 Unified Communications Manager에서 발신자의 디렉터리 URI 및 디렉터리 번호를 포함하는 혼합 주소를 SIP 연락처 헤더에 삽입합니다. 디렉터리 URI를 사용할 수 없는 경우 Unified Communications Manager는 디렉터리 번호만 포함합니다.

단계 **4** 저장을 클릭합니다.

SIP 라우트 패턴 구성

전역 다이얼 플랜 복제 및 URI 다이얼링을 사용한 클러스터간 콜 라우팅을 위해서는, 설정된 라우트 문자열을 홈 클러스터로 전송하는 SIP 라우트 패턴을 반드시 구성해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > **SIP** 라우트 패턴을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 패턴 사용 드롭다운에서 도메인 라우팅을 선택합니다.

단계 **4** IPv4 또는 IPv6 중 무엇은 구축하는지에 따라 **IPv4** 주소 또는 **IPv6** 주소 텍스트 상자에 라우트 문자열을 입력합니다.

단계 **5** **SIP** 트렁크/라우트 목록에서 라우터가 라우트 문자열의 홈 클러스터로 돌아갈 수 있도록 다음 홉 클러스터로 이어지는 SIP 트렁크 또는 라우트 목록을 선택합니다.

단계 **6** **SIP** 라우트 패턴 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

단계 **8** 설정된 각 라우트 문자열에 대한 SIP 라우트 패턴을 생성합니다.

단계 **9** ILS 네트워크의 각 클러스터에 대해 이러한 작업을 반복합니다.

참고 SIP 라우트 패턴 이름에 대시가 포함된 경우, 대시 사이에 숫자 값이 없는지 확인하십시오. 그러나 대시가 두 개 이상 있는 경우, 문자와 숫자 또는 문자만을 조합하여 사용할 수 있습니다. SIP 라우트 패턴의 예는 다음과 같습니다.

올바른 패턴**:**

- abc-1d-efg.xyz.com
- 123-abc-456.xyz.com

잘못된 패턴**:**

- abc-123-def.xyz.com
- 1bc-2-3ef.xyz.com

설정된 데이터에 대한 데이터베이스 한도 설정

데이터베이스 한도를 설정하여 Unified Communications Manager에서 로컬 데이터베이스에 대해 작성할 수 있는 설정된 개체의 수를 결정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 매개변수를 구성하려는 서버를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco ILS(Intercluster Lookup Service) (**활성**)**를 선택합니다. 서비스가 활성화 상태가 나타나지 않으면, Cisco Unified Serviceability에서 해당 서비스가 활성화되어 있는지 확인해야 합니다.

단계 **4** 클러스터 수준 매개변수**(ILS)**섹션에서 데이터베이스에서 설정된 개체의 **ILS** 최대 수 서비스 매개변수에 대한 상한을 설정합니다.

단계 **5** 저장을 클릭합니다.

참고 이 서비스 매개변수는 Unified Communications Manager가 ILS를 통해 설정한 데이터를 데이터베이스에 작성할 수 있는 최대 횟수를 결정합니다. 이 서비스 매개변수의 기본값은 100,000이며 최대값은 1,000,00입니다.

이 서비스 매개변수를 현재 데이터베이스에 저장된 ILS 설정 항목의 수보다 작은 값으로 줄일 경우, Cisco Unified Communications Manager에서 추가 ILS 설정 개체를 데이터베이스에 작성하지 않습니다. 그러나 기존 데이터베이스 항목은 그대로 유지 됩니다.

설정된 번호 및 패턴에 대한 파티션 할당

설정된 번호와 설정된 패턴을 하나의 파티션에 할당해야 합니다. 자체 파티션을 정의하거나 사전 정의된 기본 파티션을 사용할 수 있습니다. Unified Communications Manager에는 설정된 대체 번호와 번호 패턴에 대해 다음과 같은 사전 정의된 파티션이 설치되어 있습니다.

- 전체 설정된 엔터프라이즈 번호.
- 전체 설정된 E.164 번호.
- 전체 설정된 엔터프라이즈 패턴.
- 전체 설정된 E.164 패턴.

참고 설정된 번호 또는 설정된 패턴을 NULL 파티션에 할당할 수 없습니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 전역 다이얼 플랜 복제 > 설정된 번호 및 패턴에 대한 파티션을 선택합니다.

단계 **2** 설정된 번호 및 패턴에 대한 파티션 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **3** 저장을 클릭합니다.

참고 라우트 파티션은 발신자가 사용하는 발신 검색 공간에도 존재해야 파티션의 번호로 전화를 걸 수 있습니다.

대체 번호에 대해 광고된 패턴 설정

광고된 패턴을 사용하여 엔터프라이즈 대체 번호 범위 또는 E.164 대체 번호를 요약합니다. 패턴을 ILS 네트워크에 광고하여 인터클러스터 통화를 패턴과 일치하는 번호로 활성화할 수 있습니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 전역 다이얼 플랜 복제 > 광고된 패턴을 선택합니다.

단계 **2** 광고된 패턴 찾기 및 나열 창에서 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 패턴을 선택합니다.
- 새로 추가를 클릭하여 새 패턴을 생성합니다.

단계 **3** 패턴 필드에서 번호 패턴을 입력합니다. 예를 들어, 54XXX는 54000 - 54999 사이의 숫자 범위를 요약합니다.

단계 **4** 패턴 유형 필드에서 패턴 유형: 엔터프라이즈 번호 패턴 또는 **E.164** 번호 패턴을 선택합니다.

단계 **5** 라디오 버튼에서 PSTN 페일오버를 적용할지 여부를 선택합니다.

- **PSTN** 페일오버를 사용하지 않음
- **PSTN** 페일오버로 패턴 사용
- **PSTN** 페일오버에 대한 패턴 및 숫자 앞에 추가—이 옵션을 선택하는 경우, **PSTN** 페일오버 스트립 숫자 및 **PSTN** 페일오버 앞자리 숫자에 숫자를 입력합니다.

단계 **6** 저장을 클릭합니다.

설정된 패턴 차단

로컬 클러스터가 특정 엔터프라이즈 대체 번호, +E.164 대체 번호 또는 ILS를 통해 설정된 번호 패턴으로 통화를 라우트할 수 없도록 방지하는 차단 규칙을 설정하려는 경우, 이 선택적 작업을 완료합니다.

설정된 번호 또는 설정된 패턴으로 통화를 전송하기 전에 먼저 ILS에서 로컬 차단 규칙이 다이얼 문자열과 일치하는지 확인합니다. 차단 규칙이 일치하면 Cisco Unified Communications Manager는 통화를 라우팅하지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 전역 다이얼 플랜 복제 > 설정된 번호 및 패턴 차단을 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭하고 편집할 기존 차간 규칙을 선택합니다.
- 새로 추가를 클릭하여 새 차단 규칙을 생성합니다.

단계 **3** 패턴 필드에서 차단하려는 패턴 또는 번호를 입력합니다. 예를 들어, 206XXXXXXX를 사용하여 2065551212로의 통화를 차단할 수 있습니다.

단계 **4** 다이얼 문자열 접두사에 따라 통화를 차단하려는 경우, 접두사를 입력합니다.

단계 **5** 통화가 특정 클러스터로 전송되지 않도록 차단하려면, 클러스터의 클러스터 **ID**를 입력합니다.

단계 **6** 패턴 유형 드롭다운 목록에서 차단 규칙을 적용하려는 방법을 선택합니다.

- 모두— 차단 규칙이 엔터프라이즈 번호 패턴과 +E.164 패턴에 모두 적용되는 경우, 이 옵션을 선택합니다.
- 엔터프라이즈 패턴— 차단 규칙이 엔터프라이즈 번호 패턴에만 적용되는 경우, 이 옵션을 선택합니다.
- **+E.164** 패턴—차단 규칙이 +E.164 번호 패턴에만 적용되는 경우, 이 옵션을 선택합니다.

단계 **7** 저장을 클릭합니다.

전역 다이얼 플랜 데이터 프로비저닝

이 절차를 사용하여 디렉터리 URI, 엔터프라이즈 대체 번호, +E.164 대체 번호 및 PSTN 페일오버 규칙을 디렉터리 번호에 추가합니다.

참고 사용자 수가 대량인 경우, 범용 회선 템플릿을 구성하고 LDAP 동기화 또는 벌크 관리와 같은 프로비저닝 도구로 템플릿을 적용하여 단일 작업에서 대량의 사용자에 대한 전역 다이얼 플랜 데이터를 프로비저닝합니다. 이 책자의 사용자 프로비저닝 섹션을 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 디렉터리 번호를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 전역 다이얼 플랜 데이터를 추가하려는 기존 디렉터리 번호를 선택합니다.
- 새로 추가를 클릭하여 새 디렉터리 번호를 생성합니다.

단계 **3** 새 번호를 생성 중인 경우 디렉터리 번호를 입력하고 저장을 클릭합니다.

단계 **4** 엔터프라이즈 대체 번호를 추가하려면, 엔터프라이즈 대체 번호 추가 버튼을 클릭하고 다음을 수행합니다.

a) 번호 마스크를 입력합니다. 예를 들어, 5XXXX는 4001의 대체 번호입니다. 결과 엔터프라이즈 대체 번호(54001)가 대체 번호 필드에 표시됩니다.
b) 로컬 라우트 파티션에 추가 확인란에 체크 표시를 하여 로컬 라우트 파티션에 추가합니다.
c) 라우트 파티션 드롭다운에서 파티션을 선택합니다.
d) 이 대체 번호를 ILS 네트워크에 알리려는 경우, **ILS**를 통해 전역으로 알림에 체크 표시합니다.

참고 엔터프라이즈 대체 번호 또는 +E.164 대체 번호가 패턴 범위와 일치하는 알림 패턴을 구성하는 경우, 대체 번호를 개별적으로 알릴 필요가 없습니다.

단계 **5** +E.164 대체 번호를 추가하려면 **+E.164** 대체 번호 추가를 클릭하고 다음을 수행합니다.

a) 번호 마스크를 입력합니다. 예를 들어 1972555XXXX는 내선 번호 4001의 대체 번호입니다. 결과 +E.164 대체 번호(19725554001)가 대체 번호 필드에 표시됩니다.
b) 로컬 라우트 파티션에 추가 확인란에 체크 표시를 하여 로컬 라우트 파티션에 추가합니다.
c) 라우트 파티션 드롭다운에서 파티션을 선택합니다.
d) 이 대체 번호를 ILS 네트워크에 알리려는 경우, **ILS**를 통해 전역으로 알림에 체크 표시합니다.

단계 **6** 디렉터리 **URI** 섹션에서 디렉터리 URI를 이 디렉터리 번호에 다음과 같이 추가합니다.

a) **URI** 필드에 디렉터리 URI를 입력합니다. 예를 들어, alice@cisco.com입니다.
b) 파티션 드롭다운에서 디렉터리 URI를 로컬 파티션에 할당합니다.
c) 광고 된 카탈로그에이 디렉터리 URI를 포함 하려면 [ILS를 통해 전역 광고] 확인란에 체크 표시합니다.
d) 행 추가를 클릭하여 추가 디렉터리 URI를 추가합니다. 최대 5개의 디렉터리 URI를 추가할 수 있습니다.

단계 **7** 알려진 페일오버 번호 필드에서 엔터프라이즈 대체 번호 또는 +E.164 대체 번호를 PSTN 페일오버으로 선택합니다.

단계 **8** 디렉터리 번호 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **9** 저장을 클릭합니다.

전역 다이얼 플랜 데이터 가져오기

Cisco TelePresence Video Communications Server, 타사 통화 제어 시스템 또는 ILS를 실행하고 있지 않은 다른 시스템과 상호 운용하는 경우, 이 절차를 사용합니다. 디렉터리 URI, +E.164 패턴 및 PSTN 페일오버 규칙의 카탈로그를 다른 시스템에서 ILS 네트워크의 허브 클러스터로 가져올 수 있습니다. ILS는 클러스터에서 다른 시스템으로 전화를 걸 수 있도록 ILS 네트워크 전체에서 카탈로그를 복제합니다.

시작하기 전에

다른 시스템의 다이얼 플랜 카탈로그를 CSV 파일로 내보냅니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 전역 다이얼 플랜 복제 > 가져온 전역 다이얼 플랜 카탈로그를 선택합니다.

단계 **2** 가져온 전역 다이얼 플랜 카탈로그 창에서 다음 작업 중 하나를 수행합니다.

- 찾기를 클릭하고 결과 목록에서 기존 카탈로그를 선택합니다.
- 새로 추가를 클릭하여 새 카탈로그를 추가합니다.

단계 **3** 가져온 전역 다이얼 플랜 카탈로그 설정 창의 이름 필드에서 가져올 카탈로그를 식별하는 고유한 이름을 입력합니다.

단계 **4** (선택 사항) 설명 필드에 카탈로그에 대한 설명을 입력합니다.

단계 **5** 라우트 문자열 필드에서 카탈로그를 가져오는 시스템에 대한 라우트 문자열을 만듭니다.

참고 라우트 문자열은 최대 길이가 250자인 영숫자일 수 있으며 점과 대시를 포함할 수 있습니다.

단계 **6** 저장을 클릭합니다.

단계 **7** Cisco Unified CM 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.

- 새로 추가를 클릭합니다.
- 찾아보기를 클릭하고 가져올 카탈로그의 CSV 파일을 선택합니다.

참고 가져오기에 사용하는 CSV 파일이 Cisco Unified Communications Manager의 버전과 호환되는지 확인합니다. 예를 들어 버전 9.0(1)로 가져올 수 있는 호환되는 CSV 파일이 버전 10.0(1)과는 호환되지 않습니다.

단계 **8** 대상 선택 드롭다운 목록에서 가져온 디렉터리 **URI** 및 패턴을 선택합니다.

단계 **9** 트랜잭션 유형 선택 드롭다운 목록에서 가져온 디렉터리 **URI** 및 패턴 삽입을 선택합니다.

단계 **10** 저장을 클릭합니다.

단계 **11** Cisco Unified CM 관리에서 벌크 관리 > 디렉터리 **URI** 및 패턴 > 가져온 디렉터리 **URI** 및 패턴 삽입을 선택합니다.

단계 **12** 파일 이름 드롭다운 목록에서 가져올 카탈로그가 포함된 CSV 파일을 선택합니다.

단계 **13** 가져온 디렉터리 **URI** 카탈로그 드롭다운 목록에서 가져온 전역 다이얼 플랜 카탈로그 창에서 이름을 지정한 카탈로그를 선택합니다.

단계 **14** 작업 설명 텍스트 상자에 실행하려는 작업의 이름을 입력합니다.

단계 **15** 다음 단계 중 하나를 수행합니다.

- 지금 작업을 실행하려는 경우, 즉시 실행 옵션을 선택하고 제출을 클릭합니다.
- 지정된 시간에 작업을 실행하도록 일정을 잡으려는 경우, 나중에 실행 라디오 버튼을 선택하고 제출을 클릭합니다.

참고 나중에 실행 옵션을 선택하는 경우, [벌크 관리 작업 스케줄러]를 사용하여 언제 작업을 실행할지 일정을 잡아야만 합니다.

Cisco Unified Communications Manager에서는 가져온 +E.164 패턴을 모두 전역 설정된 +E.164 패턴 파티션에 저장합니다.

참고 모든 디렉터리 URI, +E.164 번호 패턴 및 연결된 PSTN 페일오버 규칙을 CSV 파일로 내보내는 방법에 대해 설명합니다. 이 CSV 파일은 다른 통화 제어 시스템으로 가져올 수 있습니다. 자세한 내용은 벌크 관리 > 디렉터리 **URI** 및 패턴 > 로컬 디렉터리 **URI** 및 패턴 메뉴를 참조하십시오.

전역 다이얼 플랜 복제 상호 작용 및 제한 사항

다음 표에는 전역 다이얼 플랜 복제 및 URI 다이얼링에 대한 몇 가지 기능 상호 작용에 대한 내용이 요약되어 있습니다.

기능	상호 작용 및 제한 사항
디렉터리 URI 및 +E.164 패턴 내보내기	로컬 클러스터에 구성된 모든 디렉터리 URI 및 +E.164 번호 패턴을 내보낸 다음, 이를 다른 시스템으로 가져올 수 있는 csv 파일로 내보낼 수도 있습니다. **1.** Cisco Unified CM 관리에서 벌크 관리 > 디렉터리 **URI** 및 패턴 > 로컬 디렉터리 **URI** 및 패턴 내보내기를 선택합니다. **2.** 다음 라디오 버튼 중 하나를 클릭하여 내보내기 파일에 첨부할 도메인 이름을 정의합니다. • 조직 최상위 도메인—이 라디오 버튼을 클릭하여 내보내기 파일 도메인 이름을 위해 조직 최상위 도메인 엔터프라이즈 매개변수의 값을 사용합니다. • 라우트 문자열 도메인—이 라디오 버튼을 클릭하여 내보내기 파일 도메인 이름을 위해 ILS 구성에 구성된 대로 라우트 문자열 필드의 값을 사용합니다. • 사용자 지정 도메인—이 라디오 버튼을 클릭하여 내보내기 파일에 첨부할 사용자 지정된 도메인 이름을 생성합니다. 이 옵션을 선택한 경우, 도메인 이름 텍스트 상자에 도메인 이름을 입력합니다. **3.** 로컬 디렉토리 **URI** 및 패턴 내보내기 버튼을 클릭합니다. **4.** CSV 파일을 로컬 드라이브에 저장합니다.

기능	상호 작용 및 제한 사항
URI 다이얼링을 사용한 파티셔닝	디렉터리 URI를 사용한 파티셔닝은 디렉터리 URI를 프로비저닝하는 방법에 따라 달라집니다. • 엔드 유저 구성에서 엔드 유저에게 할당된 사용자 기반 디렉터리 URI의 경우, 로컬 삭제 불가능한 디렉터리 URI 파티션이 URI에 자동으로 할당됩니다. 다른 파티션은 할당할 수 없지만, 디렉터리 **URI** 별칭 파티션 엔터프라이즈 매개변수를 구성하여 관리자가 관리하는 파티션을 로컬 디렉터리 URI 파티션에 대한 별칭으로 사용할 수 있습니다. • URI가 디렉터리 번호 구성의 디렉터리 번호에 직접 할당된 회선 기반 디렉터리 URI의 경우, 각 URI를 로컬 파티션에 개별적으로 할당할 수 있습니다. LDAP 동기화 및 벌크 관리와 같은 도구를 사용하여 디렉터리 URI를 프로비저닝하는 경우: • LDAP 동기화를 통해 프로비저닝된 디렉터리 URI는 사용자에 기반하며 엔드 유저 구성에서 사용자에게 할당됩니다. 이러한 URI는 로컬 디렉터리 URI 파티션에 할당됩니다. 사용자에게 기본 내선 번호가 있는 경우, URI는 디렉터리 번호 구성에 기본 URI로도 표시됩니다. 그러나 할당된 파티션은 디렉터리 URI 파티션입니다. • 벌크 관리를 통해 프로비저닝된 디렉터리 URI의 경우, 업데이트 적용 방식에 따라 달라집니다. 예를 들어, `bat` 스프레드시트를 사용하여 csv 가져오기 파일을 생성 하는 경우 스프레드시트에서 사용자 또는 사용자 업데이트 탭을 사용하여 디렉터리 URI를 추가 하면 사용자가 기반 uri가 됩니다. 그러나 파일 형식 생성을 클릭할 때 나타나는 회선 필드 옵션을 통해 디렉터리 URI를 추가하는 경우, URI를 디렉터리 번호에 할당하고 로컬 파티션을 URI에 바로 할당할 수 있습니다.
디렉터리 URI 대/소문자 구분	기본값으로 디렉터리 URI의 사용자 부분(@ 앞의 부문)은 대소문자를 구분합니다. URI 조회 정책 엔터프라이즈 매개변수를 편집하여 사용자가 대소문자를 구분할 수 있도록 설정 할 수 있습니다.
발신 검색 공간	디렉터리 URI, 엔터프라이즈 대체 번호 및 + E.164 대체 번호로 연결이 가능하려면 발신자의 발신 검색 공간에서 사용할 수 있는 파티션에 있어야만 합니다.

기능	상호 작용 및 제한 사항
URI 다이얼링으로 숫자 변환	숫자 변환을 사용하고 인터클러스터 URI 다이얼링을 구축하는 경우, 전화기 구성 또는 전화기에서 사용하는 디바이스 풀에 대해 숫자 변환을 적용합니다. • 개별 전화기의 경우 원격 번호 섹션의 발신자 변환 **CSS** 필드에 변환을 적용합니다. • 디바이스풀의 경우, 디바이스 모빌리티 관련 정보의 발신자 변환 **CSS** 필드에 대해 변환을 적용할 수 있습니다. 참고 로밍 디바이스의 경우, 디바이스 풀 발신자 변환 **CSS** 사용 확인란의 선택이 전화기 구성 창에서 해제되어 있는 경우에도 디바이스 풀 설정에서 전화기 구성을 재정의합니다.

24 장

발신자 정규화

발신자 정규화 개요

발신자 정규화를 통해 전화 번호를 전역화 및 지역화할 수 있으므로 적절한 발신 번호 표시가 전화기에 표시됩니다. 발신자 정규화는 일부 전화기의 전화걸기 기능을 향상하고 통화가 여러 지리적 위치로 라우팅될 때 콜백 기능을 향상시킵니다. 이 기능을 사용하면 전화기의 통화 로그 디렉터리에서 디렉터리 번호를 수정하지 않고서도 전화기에서 통화를 반환할 수 있도록 전역 발신자 번호를 로컬 변형에 매핑할 수 있습니다.

발신자 번호의 전역화

Cisco Unified CM 관리에서 발신자 번호 유형 및 접두사를 구성하면, Cisco Unified Communications Manager를 설정하여 착신 전화에 표시되는 발신자 번호를 국제 국가 코드와 같은 접두사를 포함하는 전역화된 버전으로 다시 포맷하여, 세계 어디에서도 해당 번호로 전화를 걸 수 있습니다.

Cisco Unified Communications Manager에서는 라우트 패턴 또는 변환 패턴과 같은 다양한 번호 패턴을 사용하여 발신자 번호 유형의 값과 함께 전화 번호를 전역화합니다. 예를 들어, Cisco Unified Communications Manager를 구성하여 가입자 발신자 번호 유형을 사용하여 069XXXXXXX의 로컬 독일어 전화 번호를 선택하여 해당 번호를 독일 국가 코드 및 도시 코드가 포함된 + 49 40 69XXXXXXX로 전역화할 수 있습니다.

여러 지리적 위치로 라우팅된 통화의 경우, 각 라우팅 경로에 적용되는 여러 변환 설정을 통해 각 통화 경로에 대한 발신자 번호를 고유하게 전역화할 수 있습니다. 예를 들어, 또한 Cisco Unified Communications Manager를 구성하여 전화기가 전화기 화면에 로컬 번호를 그리고 전화기의 통화 로그 디렉터리에 전역화된 번호를 표시할 수 있습니다. 전화기 사용자가 전화를 걸기 전에 전화기에서 통화 로그 디렉터리 항목을 편집할 필요가 없도록, 전역 발신자 번호를 로컬 변형에 매핑합니다.

발신자 번호 지역화

발신자 번호를 최종적으로 표시하려면, 각 발신자 번호 유형(국내, 국제, 가입자 및 알 수 없음)에 대한 발신자 변환 패턴을 구성하고 해당 통화에 대한 발신자 번호 유형에 따른 접두사 지침을 적용할 수 있습니다. 이렇게 하면 Cisco Unified Communications Manager에서 착신 전화에 표시되는 발신자 번호가 불필요한 국가 코드 및 국제 액세스 코드를 포함하지 않는 로컬 번호가 될 수 있도록 발신자 전화 번호를 다시 포맷할 수 있습니다.

예를 들어, 수신 통화가 + 49 40 69XXXXXXX의 전역화된 번호와 함께 PSTN에서 수신되었다고 가정해 봅시다. 이 때 + 49는 국가 코드, 40은 도시 코드를 나타내고 발신자 번호 유형은 가입자가됩니다. Cisco Unified Communications Managers는 발신자 번호 변환 패턴을 사용하여 그리고 국가 코드, 도시 코드 및 접두사 0 추가 제거에 대한 지침을 함께 사용하여 설정할 수 있습니다. 지침을 적용한 후에는 발신자 번호가 069XXXXXXX로 착신 전화기에 표시됩니다.

전역화된 발신자 번호를 로컬 버전으로 매핑

전화기 사용자가 전화를 걸기 전에 전화기에서 통화 로그 디렉터리 항목을 편집할 필요가 없게 하려면, 라우트 패턴과 착신자 변환 패턴을 사용하여 전역 발신자 번호를 로컬 버전에 매핑합니다. 이렇게 하면 착신자가 통화를 반환할 때 Cisco Unified Communications Manager에서 올바른 게이트웨이로 통화를 라우팅할 수 있습니다.

전역 발신자 번호를 매핑하면 콜백 기능이 개선되어, 착신자가 전화기의 통화 로그 디렉터리에서 디렉터리 번호를 수정할 필요가 없는 상태로 통화를 반환할 수 있게 됩니다.

발신자 정규화 사전 요건

발신자 정규화를 구성하기 전에 Cisco Unified Serviceability에서 **Cisco CallManager** 서비스를 활성화하십시오. 자세한 내용은 *Cisco Unified Serviceability* 관리 설명서를 참조하십시오.

Cisco Unified Communications Manager에서 발신자 번호 유형을 결정하려는 경우, 원하는 통화와 일치하는 발신자 번호 유형 값을 할당하는 패턴을 구성합니다. 다음 구성 창에서 패턴을 만들고 적용할 수 있습니다.

- 라우트 패턴
- 헌트 파일럿
- 변환 패턴
- 발신자 번호 변환 패턴

참고 발신자 변환은 원래 발신자에 대해서만 작동합니다. 리다이렉트 번호에 대한 모든 수정 사항은 전환 헤더에만 영향을 미칩니다. SIP 트렁크 장에서 구성을 검토하고 SIP 트렁크에 전환 헤더를 추가합니다.

발신자 정규화 구성 작업 플로우

발신자 정규화 접두사와 숫자 제거 규칙이 Unified Communications Manager에서 여러 방식으로 적용될 수 있습니다. 예를 들어, 디바이스 풀, 라우트 패턴, 변환 패턴, 헌트 파일럿, 게이트웨이 및 트렁크에 숫자 변환을 적용할 수 있습니다. 숫자 변환을 적용하는 방식은 다이얼 플랜, 디바이스 및 트렁크를 구축하는 방법에 따라 달라집니다. 자세한 내용은 다이얼 플랜, 라우트 패턴, 변환 패턴 및 변환 패턴과 관련된 항목을 검토하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	Unified Communications Manager에서 발신자 번호 유형을 결정하도록 하려는 경우, 패턴을 만들고 원하는 통화와 일치 하는 발신자 번호 유형을 구성합니다. 다음 구성 창에서 패턴을 만들고 적용할 수 있습니다. • 라우트 패턴 • 헌트 파일럿 • 변환 패턴 • 발신자 번호 변환 패턴	
단계 **2**	발신자 번호 전역화, 259 페이지	PSTN을 통해 도달하는 착신 통화의 경우, 발신자 번호를 전역화 하는 설정을 구성합니다.
단계 **3**	CSS(발신 검색 공간) 설정, 260 페이지	파티션 및 CSS(발신 검색 공간)을 설정합니다.
단계 **4**	발신자 변환 패턴 생성, 261 페이지	발신자 번호를 전역화되거나 지역화된 버전으로 변환하는 발신자 변환 패턴을 생성하고 각 패턴을 파티션에 할당합니다.
단계 **5**	발신자 변환 패턴을 CSS(발신 검색 공간)에 적용, 261 페이지	수신 발신자 변환 CSS를 디바이스 풀, 게이트웨이 및 트렁크와 같은 디바이스에 적용합니다.

발신자 번호 전역화

PSTN을 통해 수신되는 착신 통화의 경우 발신자 번호를 전역화하는 설정을 구성합니다. 발신자 번호를 전역화하고 디바이스 풀 또는 개별 디바이스에 적용하는 설정을 적용할 수 있습니다. 또는 클러스터 수준에 근거하여 발신자 정규화 설정을 적용하는 서비스 매개변수를 구성할 수 있습니다.

발신자 번호를 전역화하려면, 다음 단계를 수행합니다.

프로시저

단계 **1** 특정 디바이스에 발신자 정규화 설정을 적용하려면 다음 단계를 수행합니다.

a) 설정을 적용하려는 디바이스에 대한 구성 창을 엽니다 (예: 디바이스 풀, 게이트웨이, 전화기 및 트렁크).

b) [구성] 창의 [수신 발신자 설정] 섹션에서 각 발신자 번호 유형에 대한 접두사 및 Strip Digits 지침을 적용합니다.

참고 Cisco Unified Communications Manager에서 통화와 관련된 통화 착신 전환, 통화 지정 보류, 음성 메시지, CDR 데이터를 비롯한 보조 서비스와 같은 모든 추가 작업을 위해 발신자 번호 필드에 접두사를 포함합니다.

단계 **2** 서비스 매개변수를 사용하여 모든 디바이스에 대한 발신자 번호를 클러스터 수준으로 전역화하려는 경우, 다음 단계를 수행합니다.

a) Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

b) 서버 드롭다운 목록에서 서비스를 실행하려는 서버를 선택합니다.

c) 서비스 드롭다운 목록에서 Cisco CallManager를 선택합니다.

d) 고급을 클릭합니다.

e) 전화기, MGCP 게이트웨이 또는 H.323 게이트웨이에 대해 클러스터 수준을 기반으로 적용할 수 있는 다음과 같은 매개변수에 대한 값을 구성합니다.

- 발신자 수신 국가 번호 접두사
- 발신자 수신 국제 번호 접두사
- 알 수 없는 발신자 수신 번호 접두사
- 발신자 수신 가입자 번호 접두사

참고 Cisco Unified Communications Manager에서 특정 전화기에 클러스터 수준 서비스 매개변수 설정을 적용하려면, 디바이스 및 디바이스 풀 수준에서 모두 해당 전화기에 대한 접두사 설정을 기본 옵션으로 설정해야만 합니다.

CSS(발신 검색 공간) 설정

CSS(발신 검색 공간)을 설정하는 경우 이 절차를 사용하여 발신자 정규화 기능을 처리합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 제어 클래스 > 파티션을 선택합니다.

단계 **2** 네트워크에 대한 파티션을 만듭니다.

단계 **3** Cisco Unified CM 관리에서 콜 라우팅 > 제어 클래스 > **CSS(**발신 검색 공간**)**을 선택합니다.

단계 **4** 발신자 변환 패턴에 대한 CSS(발신 검색 공간)을 만듭니다.

단계 **5** 각 CSS(발신 검색 공간)에 대해 발신 검색 공간에 파티션을 할당합니다.

발신자 변환 패턴 생성

발신자 변환 패턴을 사용하여 발신자 정규화 기능을 처리하는 경우 이 절차를 사용합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 변환 패턴 > 발신자 변환 패턴을 선택합니다.

단계 **2** 변환 패턴을 생성합니다.

단계 **3** 생성하는 각 발신자 변환 패턴에 대해 발신자 번호를 전역화하거나 지역화하는 접두사 또는 숫자 제거 명령을 할당합니다.

단계 **4** 각 발신자 변환 패턴에 대해 발신 검색 공간 중 하나에 연결된 파티션을 할당합니다.

발신자 변환 패턴을 **CSS(**발신 검색 공간**)**에 적용

디바이스의 경우, 수신 발신자 변환 CSS를 디바이스 풀, 게이트웨이 및 트렁크와 같은 디바이스에 할당합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 발신자 변환을 적용하려는 디바이스에 적용되는 구성 창을 선택합니다.

- 게이트웨이
- 트렁크
- 디바이스 풀

단계 **2** 발신자 번호를 지역화하려면, 발신 검색 공간 드롭다운 목록 상자에서 적용하려는 발신자 변환 패턴을 포함한 CSS를 선택합니다.

참고 디바이스 풀에 대해 CSS를 구성하는 경우, 해당 디바이스 풀을 전화기에도 적용해야 합니다.

단계 **3** 발신자 번호를 전역화하려면, 수신 발신자 설정 섹션에서 적용하려는 발신자 변환 패턴을 포함한 CSS(발신 검색 공간)을 선택합니다.

발신자 정규화 서비스 매개변수 예

다음 서비스 매개변수를 전화기, MGCP 게이트웨이 또는 H.323 게이트웨이에 대해 클러스터 수준을 기반으로 적용할 수 있습니다. 특정 디바이스에서 클러스터 수준 매개변수를 사용할 수 있으려면, 디바이스 구성의 접두사를 기본값으로 설정해야 합니다.

- 발신자 수신 국가 번호 접두사
- 발신자 수신 국제 번호 접두사
- 알 수 없는 발신자 수신 번호 접두사
- 발신자 수신 가입자 번호 접두사

다음 표에서는 접두사 및 숫자 제거 구성의 예와 이러한 값을 사용하여 발신자 번호의 표시를 변환하는 방법의 예를 제공합니다. 서비스 매개변수 구성의 경우, 콜론 뒤의 숫자는 발신자 번호의 시작 부분에서 제거할 자릿수를 나타내고 콜론 뒤의 숫자는 발신자 번호의 시작 부분에 추가할 접두사를 나타냅니다.

표 ***24:*** 발신자 번호 정규화 서비스 매개변수 예

최초 발신 번호	서비스 매개변수 값	설명	최종 발신 번호
04423452345	+:1	첫 번째 숫자 제거 및 + 접두사 추가	+4423452345
04423452345	:2	처음 두 자리 숫자 제거	423452345
552345	+1:6	처음 6자리 숫자 제거 및 +1 접두사 추가	+1
552345	+1:8	사용 가능 숫자 보다 더 많이 제거되어 최종 번호가 비어 있음	
552345	123	접두사 123 추가	123552345
비어 있음	+1:2	발신 번호가 빈 경우, 접두사 적용되지 않음	비어 있음
0442345	:26	발신자 정규화에서 24자릿수만 제거하도록 허용	Cisco Unified Communications Manager에서 구성을 허용하지 않음

발신자 정규화 상호 작용 및 제한 사항

발신자 정규화 상호 작용

다음 표에서는 발신자 정규화 기능과의 기능 상호 작용에 대해 설명합니다.

기능	상호 작용
호전환된 통화	일부 전송된 통화에 대해 발신자 정규화가 지원되지 않을 수 있습니다. 그 이유는 전송 기능이 통화 중 업데이트에 의존하고 발신자 정규화가 각 통화 홉에 대해 최초 통화 설정 시 발생할 수 있기 때문입니다. 다음은 전송에 대해 발신자 정규화가 작동하는 방식에 대한 예입니다. 내선 번호가 12345이고 전화 번호가 972 500 2345인 전화기 A에서 내선 번호가 54321이고 전화 번호가 972 500 4321인 전화기 B로 전화를 겁니다. 전화기 B에 발신자 번호 12345가 표시되지만, 전화기 B에서 해당 통화를 San Jose 게이트웨이를 통해 전화기 C로 전송합니다. 최초 전송 중에 전화기 C는 972 500 4321의 발신자 번호를 표시하지만, 전송이 완료된 후에는 전화기 C에서 전화기 A에 대한 발신자 번호를 12345로 표시합니다.
착신 전환 통화	착신 전환 통화는 전역화 및 지역화된 발신자 번호를 지원합니다. 예를 들어, 전화기 F의 발신자가 PSTN을 통해 Dallas의 전화기 G에 전화를 걸지만, 전화기 G는 San Jose의 전화기 H로 착신 전환됩니다. 수신되는 Dallas 게이트웨이에서 발신자 번호는 555-5555/가입자로 표시되지만 해당 통화는 San Jose 게이트웨이로 착신 전환됩니다. Dallas의 발신 통화는 972 555 5555으로 표시됩니다. 수신되는 San Jose 게이트웨이에서 +1이 첫 글자로 오며 전화기 F에 발신 번호 +1 972 555 5555가 표시됩니다.
통화 세부 정보 레코드	발신자 정규화가 CDR(통화 세부 정보)과 작동하는 방식에 대한 자세한 내용은 *Cisco Unified Communications Manager* 통화 세부 정보 레코드 관리 설명서를 참조하십시오.
Cisco Unified Communications Manager Assistant	발신자 정규화 기능을 구성할 경우, Cisco Unified Communications Manager Assistant에서 지역화 및 전역화된 통화를 자동으로 지원합니다. Cisco Unified Communications Manager Assistant의 사용자 인터페이스에는 지역화된 발신자 번호가 표시될 수 있습니다. 또한 관리자에 대한 착신 통화의 경우 Cisco Unified Communications Manager Assistant에서는 필터 패턴 일치가 발생할 때 지역화된 발신자 번호와 전역화된 발신자 번호를 표시할 수 있습니다. Cisco Unified Communications Manager Assistant 구성에 대한 자세한 내용은, http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

기능	상호 작용
Cisco Unity Connection	Cisco Unity Connection에서는 국제이스케이프 문자(+)를 지원하지 않습니다. 따라서 Cisco Unity Connection에 대한 통화에 +가 포함되지 않도록 해야만 음성 메시지 기능이 정상적으로 작동합니다. Cisco Unity Connection을 정상 작동하려면 이 애플리케이션을 디바이스로 간주하고 +가 이 음성 사서함 애플리케이션으로 전송되지 않도록 발신자 변환을 구성하십시오. Cisco Unity Connection 서버가 북미 기반 다이얼 플랜을 사용할 경우 Cisco Unity Connection에서 발신자 번호를 수신하기 전에 발신자 번호를 naNP 형식으로 지역화하십시오. Cisco Unified Communications Manager 관리에는 음성 사서함 포트를 위한 발신자 변환 옵션이 없으므로 음성 사서함 포트와 연결된 디바이스 풀에 발신자 번호 변환을 구성해야 합니다. 발신자 번호를 지역화하려면 음성 사서함 애플리케이션이 실시간 회신과 같은 특정 기능을 위해 번호를 쉽게 재다이얼할 수 있도록 액세스 코드에 대한 접두사를 추가하는 것을 고려하십시오. 예를 들어, +12225551234를 912225551234로 변환하고 국제 번호 +4423453456을 90114423453456으로 변환하여 국제 이스케이프 코드를 포함할 수 있습니다.
디바이스 이동성	전화기 구성 창에서 [디바이스 풀 발신자 변환 CSS 사용] 확인란이 선택되지 않은 경우에도 로밍 디바이스 풀의 발신자 변환 CSS는 동일한 DMG(디바이스 이동성 그룹) 내의 전화기 로밍 디바이스 수준 구성을 무시합니다. 다음 예는 현재 San Jose에서 로밍 중인 Dallas의 홈 위치를 사용하여 발신자 정규화가 전화기의 디바이스 이동성에서 작동하는 방식을 보여줍니다. 전화기가 San Jose에서 로밍할 때 Dallas의 972 500 1212 <national>에서 PSTN을 통해 통화가 도달합니다. 수신되는 San Jose 게이트웨이에서 발신자 번호는 전역 형식인 +1 408 500 1212로 변환됩니다. 현재 San Jose에 있는 전화기에서는 발신자 번호가 1 972 500 1212로 표시됩니다. San Jose에서 전화기가 로밍할 때, San Jose의 7자리 다이얼 지역의 500 1212 <Subscriber>에서 PSTN을 통해 통화가 도달합니다. 수신되는 San Jose 게이트웨이에서 발신자 번호는 전역 형식인 +1 408 500 1212로 변환됩니다. 현재 San Jose에 있는 전화기에서는 발신자 번호가 9 500 1212 표시됩니다.

발신자 정규화 제한 사항

다음 표에는 Cisco Unified Communications Manager의 특정 기능 및 시스템 구성 요소가와 발신자 정규화 기능이 갖는 제한 사항이 표시되어 있습니다.

표 **25:** 발신자 정규화 제한 사항

기능	제한 사항
공유 회선	공유 회선에 대해 표시되는 발신자 번호는 Cisco Unified Communications Manager의 통화 제어 이벤트의 순서에 따라 달라집니다. 공유 회선에서 잘못된 지역화된 발신자 번호가 표시되는 것을 방지하려면, 특히 공유 회선이 지리적으로 서로 다른 위치에서 발생하는 경우, 동일한 회선을 공유하는 서로 다른 디바이스에 대해 동일한 발신자 변환 CSS를 구성하도록해야 합니다.
SIP 트렁크 및 MGCP 게이트웨이	SIP 트렁크와 MGCP 게이트웨이는 통화에 대해 국제 이스케이프 문자, +를 전송하는 기능을 지원하지만, H.323 게이트웨이는 +를 지원하지 않습니다. QSIG 트렁크는 +를 전송하려고 시도하지 않습니다. +를 지원하는 게이트웨이를 통한 발신 통화의 경우, Cisco Unified Communications Manager는 전화 건 숫자와 함께 +를 게이트웨이로 보낼 수 있습니다. +를 지원하지 않는 게이트웨이를 통한 발신 통화의 경우, Cisco Unified Communications Manager가 통화 정보를 게이트웨이로 전송할 때 국제 이스케이프 문자 +는 제거됩니다.
SIP	SIP는 번호 유형을 지원하지 않으므로, SIP 트렁크를 통한 통화는 발신자 번호 유형 [알 수 없음]에 대해 수신 번호 설정만 지원합니다.
QSIG	QSIG 구성은 보통 일관된 다이얼 플랜을 지원합니다. QSIG를 사용하는 경우, 번호와 접두사의 변환이 기능 상호작용 문제를 일으킬 수 있습니다.
발신자 변환 CSS	발신자 번호를 지역화하기 위해서는 해당 디바이스가 숫자 분석을 사용하여 변환을 적용해야 합니다. [발신자 변환 CSS]를 없음으로 구성하면 변환이 일치하지 않으며 적용되지 않습니다. 라우팅에 사용되지 않는 비 Null 파티션에서 발신자 변환 패턴을 구성해야 합니다.
T1-CAS 및 FXO 포트	게이트웨이의 T1-CAS 및 FXO 포트에는 발신자 변환 CSS 설정이 적용되지 않습니다.
Cisco Unity Connection	Cisco Unity Connection에서는 국제이스케이프 문자(+)를 지원하지 않습니다. 따라서 Cisco Unity Connection에 대한 통화에 +가 포함되지 않도록 해야만 음성 메시지 기능이 정상적으로 작동합니다. Cisco Unity Connection에 대한 자세한 내용은 http://www.cisco.com/c/en/us/products/unified-communications/unity-connection/index.html을 참조하십시오.

25 장

다이얼 규칙 구성

다이얼 규칙 개요

Unified CM에서는 다음과 같은 유형의 다이얼 규칙을 지원합니다.

- 애플리케이션 다이얼 규칙: 관리자는 애플리케이션 다이얼 규칙을 사용하여 Cisco web dialer 및 Cisco Unified Communications Manager Assistant와 같은 애플리케이션에 대한 다이얼 규칙의 우선순위를 추가하고 정렬합니다.
- 디렉터리 조회 다이얼 규칙: 관리자는 디렉터리 조회 다이얼 규칙을 사용하여 발신자 식별 번호를 변환하고 Cisco Unified Communications Manager Assistant와 같은 애플리케이션에서 어시스턴트 콘솔의 디렉터리 검색을 수행합니다.
- **SIP** 다이얼 규칙: 관리자는 SIP 다이얼 규칙을 사용하여 시스템 번호 분석 및 라우팅을 수행합니다. 관리자가 SIP 다이얼 규칙을 구성하고 통화 처리가 진행되 전에 SIP 다이얼 규칙을 Cisco Unified IP Phone에 추가합니다.

다이얼 규칙 사전 요건

- SIP 다이얼 규칙 구성의 경우, 디바이스에서 SIP를 실행해야만 합니다.
- 관리자는 SIP 다이얼 규칙을 디바이스에 연결합니다. Cisco IP 전화기 7911, 7940, 7941, 7960, 7961, 7970 및 7971

다이얼 규칙 구성 작업 플로우

프로시저

	명령 또는 동작	목적
단계 **1**	애플리케이션 다이얼 규칙 구성, 268 페이지	애플리케이션 다이얼 규칙을 구성하여 Cisco web 전화 걸기 및 Cisco Unified Communications Manager Assistant와 같은 애플리케이션에 대한 다이얼 규칙의 우선순위를 추가하고 정렬합니다.
단계 **2**	디렉터리 조회 다이얼 규칙 구성, 269 페이지	디렉터리 조회 다이얼 규칙을 구성하여 발신자 식별 번호를 디렉터리에서 조회할 수 있는 번호로 변환합니다.
단계 **3**	SIP 다이얼 규칙 구성, 270 페이지	Sip 다이얼 규칙 구성을 사용하여 SIP를 실행하는 전화기에 대한 다이얼 플랜을 구성합니다.
단계 **4**	다이얼 규칙 우선순위 재지정, 273 페이지	(선택 사항) 두 개 이상의 다이얼 규칙이 있는 경우, Cisco Unified Communications Manager 관리 창에서 다이얼 규칙의 우선순위를 변경합니다.

애플리케이션 다이얼 규칙 구성

Cisco Unified Communications Manager에서는 Cisco Web Dialer 및 Cisco Unified Communications Manager Assistant와 같이 애플리케이션 다이얼 규칙의 우선순위를 추가 및 정렬할 수 있는 애플리케이션 다이얼 규칙을 지원합니다. 애플리케이션 다이얼 규칙은 사용자가 전화를 건 전화 번호에서 번호를 자동으로 제거하거나 해당 번호로 번호를 추가합니다. 예를 들면. 다이얼 규칙은 7자리 전화 번호 앞에 숫자 9를 자동으로 추가하여 외선 액세스를 제공합니다.

참고 Cisco Unified Communications Manager에서는 CTI 원격 디바이스에 대한 애플리케이션 다이얼 규칙을 모든 원격 대상 번호에 자동으로 적용합니다.

다음 절차를 수행하여 새 애플리케이션 다이얼 규칙을 추가하거나 기존 애플리케이션 다이얼 규칙을 업데이트합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 다이얼 규칙 > 애플리케이션 다이얼 규칙을 선택합니다.

단계 **2** 애플리케이션 다이얼 규칙 찾기 및 나열 창에서 다음 단계 중 하나를 수행합니다.

- 새로 추가를 클릭합니다.
- 찾기를 클릭하고 기존 애플리케이션 다이얼 규칙을 선택합니다.

단계 **3** 애플리케이션 다이얼 규칙 구성 창에서 필드를 구성합니다. 필드에 대한 상세 설명은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

다음 작업을 수행하십시오.

- 디렉터리 조회 다이얼 규칙 구성, 269 페이지
- SIP 다이얼 규칙 구성, 270 페이지

디렉터리 조회 다이얼 규칙 구성

디렉터리 조회 다이얼 규칙은 발신자 식별 번호를 디렉터리에서 조회할 수 있는 번호로 변환합니다. 각 규칙은 시작 자리와 번호의 길이에 따라 변환할 번호를 지정합니다. 예를 들면 10자리 전화 번호에서 지역 번호와 2개의 접두사 번호를 자동으로 제거(4085551212를 51212로 변환)하는 디렉터리 조회 다이얼 규칙을 만들 수 있습니다.

다음 절차를 수행하여 새 디렉터리 조화 다이얼 규칙을 추가하거나 기존 디렉터리 조회 다이얼 규칙을 업데이트합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 다이얼 규칙 > 디렉터리 조회 다이얼 규칙을 선택합니다.

단계 **2** 디렉터리 조회 다이얼 규칙 찾기 및 나열 창에서 다음 단계 중 하나를 수행합니다.

- 새로 추가를 클릭합니다.
- 찾기를 클릭하고 기존 디렉터리 조회 다이얼 규칙을 선택합니다.

단계 **3** 디렉터리 조회 다이얼 규칙 구성 창에서 필드를 구성합니다. 필드에 대한 상세 설명은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

다음에 수행할 작업

SIP 다이얼 규칙 구성, 270 페이지

SIP 다이얼 규칙 구성

SIP 다이얼 규칙은 SIP를 실행하는 Cisco IP 전화기에 대한 로컬 다이얼 플랜을 제공하므로 사용자가 키를 누르거나 타이머를 기다리지 않아도 통화가 처리됩니다. 관리자가 SIP 다이얼 규칙을 구성하여 SIP를 실행하는 전화기에 적용합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	SIP 다이얼 규칙 설정, 271 페이지	SIP 다이얼 규칙을 구성 및 업데이트하고 SIP를 실행하는 전화기와 연결합니다.
단계 **2**	SIP 다이얼 규칙 재설정, 272 페이지	SIP 다이얼 규칙이 업데이트될 때 SIP를 실행하고 있는 전화기를 재설정하거나 다시 시작하여, 전화기가 새 SIP 다이얼 규칙으로 업데이트되도록 합니다.
단계 **3**	SIP 다이얼 규칙 설정과 SIP 전화기 동기화, 273 페이지	(선택 사항) 구성이 변경된 SIP 다이얼 규칙과 SIP 전화기를 동기화하면, 방해를 최소화하는 방식으로 미처리 구성 설정에 적용됩니다. 예를 들어, 일부 영향을 받는 SIP 전화기에서는 재설정/다시 시작이 필요 없을 수도 있습니다.)

관련 항목

패턴 형식, 271 페이지

패턴 형식

표 ***26: SIP*** 다이얼 규칙에 대한 패턴 형식

다이얼 규칙 패턴	값
7940_7960_OTHER	• 마침표(.)는 모든 문자와 매칭됩니다. • 파운드 기호(#)는 종료 키로 작동하므로 눌러 매칭시킨 후에만 종료를 적용할 수 있습니다. 또는 별표(*)도 종료 키로 사용할 수 있습니다. 참고 7940_7960_OTHER에 유효하려면 패턴 필드에서 파운드 기호를 구성해야 합니다. • 별표(*)는 한 개 이상의 문자와 일치하며 와일드카드 문자로 처리됩니다. * 앞에 백슬래시(\) 이스케이프 시퀀스를 지정하여(즉, *) 이 와일드카드를 오버라이드할 수 있습니다. 전화기에서 \가 자동으로 제거되므로 발신 다이얼 문자열에는 \가 나타나지 않습니다. *가 다이얼 문자로 수신되는 경우 이 문자는 와일드카드 *와 마침표(.)와 일치합니다. • 쉼표(,)가 수신되면 전화기에서 보조 신호음을 생성합니다. 예를 들면, 7은 7로 시작하는 모든 4자리 DN과 일치합니다. 8은 8과 일치하며 보조 다이얼톤(기본값)을 재생한 다음, 5자리 임의의 DN과 일치합니다.

SIP 다이얼 규칙 설정

SIP를 실행하는 전화기에 대한 다이얼 플랜을 구성하려면 다음을 수행합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 다이얼 규칙 > **SIP** 다이얼 규칙을 선택합니다.

단계 **2** **SIP** 다이얼 규칙 찾기 및 나열 창에서, 다음 단계 중 하나를 수행합니다.

- 새로 추가를 클릭합니다.
- 찾기를 클릭하고 기존 SIP 다이얼 규칙을 선택합니다.

단계 **3** **SIP** 다이얼 규칙 구성 창에서 필드를 구성합니다. 필드에 대한 상세 설명은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

참고 Cisco Unified Communications Manager 관리에서 SIP 다이얼 규칙을 추가하거나 업데이트하는 경우 Cisco TFTP 서비스에서 모든 전화기 구성 파일을 다시 작성하므로 Cisco TFTP 서비스가 실행되는 서버에서 특히, 여러 전화기기 포함된 대형 시스템인 경우 CPU 사용이 급격히 늡니다. CPU 사용이 급격히 늘지 않게 하려면 유지 보수 기간 중에 SIP 다이얼 규칙을 추가 또는 업데이트하거나 구성을 변경하기 전에 Cisco Unified Serviceability에서 Cisco TFTP 서비스를 일시적으로 중지합니다. Cisco TFTP 서비스를 중지하는 경우에는 SIP 다이얼 규칙을 추가 또는 업데이트한 후 Cisco Unified Serviceability에서 서비스를 재시작해야 합니다.

다음에 수행할 작업

SIP 다이얼 규칙 재설정, 272 페이지

관련 항목

패턴 형식, 271 페이지

SIP 다이얼 규칙 재설정

다음 절차를 수행하여 SIP 다이얼 규칙이 업데이트될 때 SIP가 실행되고 있는 전화기를 재설정하거나 다시 시작하여 전화기가 새 SIP 다이얼 규칙으로 업데이트되도록 합니다.

시작하기 전에

SIP 다이얼 규칙 설정, 271 페이지

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 다이얼 규칙 > 애플리케이션 다이얼 규칙을 선택합니다.

단계 **2** **SIP** 다이얼 규칙 찾기 및 나열 창에서 찾기를 클릭하고 재설정하려는 기존 SIP 다이얼 규칙을 선택합니다.

단계 **3** **SIP** 다이얼 규칙 구성 창에서 재설정을 클릭합니다.

단계 **4** 디바이스 재설정 대화 상자에서 다음 작업 중 하나를 수행합니다.

- 선택한 디바이스를 종료하지 않고 다시 시작하고 해당 디바이스를 Cisco Unified Communications Manager에 등록하려면, 다시 시작을 클릭합니다.
- 디바이스를 종료한 다음 다시 시작하려면, 재설정을 클릭합니다.
- 어떤 작업도 수행하지 않은 상태로 [디바이스 재설정] 대화 상자를 닫으려면, 닫기를 클릭합니다.

관리자가 SIP 다이얼 규칙을 구성하여 SIP를 실행하는 실행하는 전화기에 적용하고 나면, 데이터베이스에서 TFTP 서버에 알림을 전송하여, SIP를 실행하는 전화기에 대한 새 구성 파일 세트를 작성할 수 있습니다. TFTP 서버에서 새 구성 파일에 대해 Cisco Unified Communications Manager에 알리고 업

데이트된 구성 파일이 전화기로 전송됩니다. 자세한 내용은 SIP를 실행하는 Cisco Unified IP Phone에 대한 **TFTP** 서버 구성을 참조하십시오.

다음에 수행할 작업

SIP 다이얼 규칙 설정과 SIP 전화기 동기화, 273 페이지

SIP 다이얼 규칙 설정과 SIP 전화기 동기화

구성이 변경된 SIP 다이얼 규칙과 SIP 전화기를 동기화하려면 다음 절차를 수행합니다.

시작하기 전에

SIP 다이얼 규칙 재설정, 272 페이지

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 다이얼 규칙 > **SIP** 다이얼 규칙을 선택합니다.

단계 **2** **SIP** 다이얼 규칙 찾기 및 나열 창에서 찾기를 클릭하고 해당 SIP 전화를 동기화하려는 기존 SIP 다이얼 규칙을 선택합니다.

단계 **3** 추가 구성을 변경하고 저장을 **SIP** 다이얼 규칙 구성에서 클릭합니다.

단계 **4** 구성 적용을 클릭합니다.

단계 **5** 확인을 클릭합니다.

다이얼 규칙 우선순위 재지정

다이얼 규칙 구성 창에서 다이얼 규칙의 우선 순위를 추가하고 정렬하려면 다음과 같이 진행합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 콜 라우팅 > 다이얼 규칙을 선택합니다.

단계 **2** 다음 중 하나 선택:

- 애플리케이션 다이얼 규칙
- 디렉터리 조회 다이얼 규칙
- **SIP** 다이얼 규칙

단계 **3** 찾기 및 나열 창에서 다이얼 규칙을 선택하고 다이얼 규칙 이름을 클릭합니다.
다이얼 규칙 구성 창이 나타납니다.

단계 **4** 위쪽 및 아래쪽 화살표를 사용하여 다이얼 규칙을 목록 위 또는 아래로 이동합니다.
단계 **5** 우선 순위를 모두 지정한 경우, 저장을 클릭합니다.

다이얼 규칙 상호 작용 및 제한 사항

SIP 다이얼 규칙 상호 작용

SIP 다이얼 규칙 상호 작용

Cisco Unified IP Phone	상호 작용
SIP를 실행하는 7911, 7941, 7961, 7970 및 7971	이들 전화기에서는 7940_7960_OTHER 다이얼 규칙 패턴을 사용합니다. KPML(Key Press Markup Language)을 사용하면 숫자를 Cisco Unified Communications Manager에 숫자 단위로 보낼 수 있지만, SIP 다이얼 규칙을 사용하면 전화기에서 숫자 패턴을 로컬로 수집한 다음 Cisco Unified Communications Manager에 보낼 수 있습니다. SIP 다이얼 규칙을 구성하지 않은 경우, KPML이 사용됩니다. Cisco 통합 커뮤니케이션 매니저의 성능을 높이려면 즉, 처리되는 통화 수를 늘리려면 관리자가 SIP 다이얼 규칙을 구성하는 것이 좋습니다.
SIP를 실행하는 7940 및 7960	이들 전화기는 7940_7960_OTHER 다이얼 규칙 패턴을 사용하며 KPML은 지원하지 않습니다. 관리자가 이러한 전화기의 SIP 다이얼 플랜을 구성하지 않는 경우 사용자는 숫자를 Cisco Unified Communications Manager에 보내 처리할 때까지 지정된 시간 동안 기다려야 합니다. 이렇게 하면 실제 통화 처리가 지연됩니다.

디렉터리 조회 다이얼 규칙 제한 사항

디렉터리 조회 다이얼 규칙 제한 사항

필드	제한 사항
번호 시작	이 필드는 숫자와 +, * 및 # 문자만 지원합니다. 길이는 100자를 초과할 수 없습니다.

필드	제한 사항
자릿수	이 필드는 숫자만 지원하며, 이 필드의 값은 패턴 필드에 지정된 패턴의 길이 보다 작을 수는 없습니다.
제거할 총 자릿수	이 필드는 숫자만 지원하며 이 필드의 값은 자릿수 필드의 값을 초과할 수 없습니다.
패턴을 포함한 접두사	필드 접두사로는 숫자와 +, * 및 # 문자만 지원됩니다. 길이는 100자를 초과할 수 없습니다. 참고 다이얼 규칙의 경우 제거해야 할 총 자릿수 필드 및 패턴을 포함한 접두사 필드를 모두 비워 둘 수는 없습니다.

III 부

애플리케이션 통합

26 장

Cisco 애플리케이션 통합

Cisco Unity Connection

음성 메시지 및 메시징 시스템의 설정을 시작할 때는 사용자 추가, 기능 활성화 및 Cisco Unified Communications Manager와 Cisco Unity Connection의 통합을 위해 가지고 있는 옵션에 대해 알아 두십시오.

Cisco Unified Communications Manager와 통합되면 Cisco Unity Connection(음성 메시지 및 메시징 시스템)에서 AXL 서비스 또는 LDAP 통합을 통해 수동으로 설정하는 사용자를 위한 음성 메시지 기능을 제공합니다. 메일 박스에서 음성 메시지를 수신한 후에 사용자는 전화에서 메시지 대기 조명을 수신합니다. 사용자는 내부 또는 외부 통화를 통해 음성 메시지 시스템에 액세스하여 메시지를 검색, 듣기, 회신, 전달 및 삭제할 수 있습니다.

시스템에서 바로 연결되어 있는 메시지 시스템과 게이트웨이 기반 메시지 시스템을 모두 지원합니다. 바로 연결되어 있는 음성 메시지 시스템은 패킷 프로토콜을 사용하여 Cisco Unified Communications Manager와 통신합니다. 게이트웨이 기반 음성 메시지 시스템은 Cisco 게이트웨이에 연결되는 아날로그 또는 디지털 트렁크를 통해 Cisco Unified Communications Manager에 접속합니다.

Unified Communications Manager와 Cisco Unity Connection을 통합하면, 사용자를 위한 다음과 같은 기능을 설정할 수 있습니다.

- 개인 착신 전환 인사말
- 통화 착신 전환 인사말
- 발신자 ID

- 간단한 메시지 액세스(사용자는 ID를 입력하지 않고서도 메시지를 검색할 수 있음, Cisco Unity Connection에서 통화가 시작된 내선 번호에 근거하여 사용자를 식별함, 암호가 필요할 수 있음)
- 식별된 사용자 메시(Cisco Unity Connection에서 통화가 시작된 내선 번호에 기반하여 착신된 내부 통화가 진행되는 동안 메시지를 남긴 사용자를 자동으로 식별합니다)
- 메시지 대기 표시(MWI)
- Cisco Unified Communications Manager와 Cisco Unity Connection 서버 사이의 안전한 SIP 트렁크 통합을 설정하려면 Cisco Unified Communications Manager 클러스터가 혼합 모드로 설정되어 있어야 합니다.

Cisco Unified Communications Manager는 다음 인터페이스 중 하나를 통해 Cisco Unity Connection과 상호 작용합니다.

- SIP 트렁크—SIP를 사용하여 Cisco Unity Connection과 Unified Communications Manager를 통합할 수 있습니다. 기존 통합과 관련된 복수의 SCCP 포트 대신, SIP는 Unity Connection 서버당 한 대의 트렁크를 사용합니다. SIP 통합에서 요구 사항을 제거하여 음성 메일 포트 및 메시지 대기 표시(MWI)용 디렉터리 번호를 설정합니다.
- SCCP 프로토콜—음성 메일 포트를 생성하여 직접 조정되는 음성 메시지 시스템으로 인터페이스를 구성합니다. 이것들이 Unified Communications Manager와 Cisco Unity Connection 사이의 링크를 설정합니다.

  음성 메시지 시스템으로 전달된 복수의 자발적 통화를 처리하려면 복수의 음성 메일 포트를 생성하고 해당 포트를 회선 그룹에 놓고 해당 회선 그룹을 라우팅/헌트 리스트에 놓습니다.

  Cisco Unified Communications Manager에서 Cisco Unity Connection에 의해 해석되는 SCCP 메시지를 생성합니다. 음성 메일 시스템에서 메시지 대기 ON/OFF 번호를 통화하여 메시지 대기 표시(MWI)를 보냅니다.

  음성 메일 포트와 Cisco Unity SCCP 디바이스에 대한 보안을 구성할 때 각 다비이스에서 다른 디바이스의 인증서를 수락한 후에 인증된 디바이스에 대해 TLS connection(악수)이 열립니다. 마찬가지로 시스템에서 디바이스간 SRTP 스트림을 전송합니다. 즉, 암호화를 위해 디바이스를 구성할 경우에 해당됩니다.

  디바이스 보안 모드가 인증 또는 암호화로 설정되어 있으면 Cisco Unity TSP가 Cisco Unified Communications Manager로 Unified Communications Manager TLS 포트를 통해 연결됩니다. 보안 모드가 Non-secure 상태이면 Cisco Unity TSP가 Cisco Communications Manager에 Unified Communications Manager SCCP 포트를 통해 연결됩니다.

시스템과 통합하기 위한 Cisco Unity Connection 설정에 대한 자세한 내용은 *Cisco Unity Connection*을 위한 *Cisco Unified Communications Manager SCCP* 통합 가이드 또는 *Cisco Unity Connection*을 위한 *Cisco Unified Communications Manager SIP* 트렁크 통합 가이드 를 http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-installation-and-configuration-guides-list.html에서 참조하십시오.

PIN 동기화 활성화

이 절차를 사용하여 엔드 유저가 동일한 PIN을 사용하여 Extension Mobility, Conference Now, Mobile Connect 및 Cisco Unity Connection 음성 메일에 로그인할 수 있도록 PIN 동기화를 활성화합니다.

참고 Cisco Unity Connection과 Cisco Unified Communications Manager 간의 PINn 동기화는 Cisco Unified Communications Manager 퍼블리셔 데이터베이스 서버가 실행 중이고 데이터베이스 복제를 완료한 경우에만 성공합니다. Cisco Unity Connection에서 PIN 동기화에 실패하면 다음 오류 메시지가 표시됩니다. `CUCM에서 PIN 업데이트에 실패했습니다. 이유: PIN을 가져오는 동안 오류가 발생했습니다.`

PIN 동기화가 활성화되고 엔드 유저가 PIN을 변경하는 경우, PIN이 Cisco Unified Communications Manager에서 업데이트됩니다. 이는 구성된 Unity Connection 애플리케이션 서버 중 하나 이상에서 PIN 업데이트가 성공했을 때만 발생합니다.

참고 PIN 동기화를 적용하려면 관리자는 기능을 성공적으로 활성화한 후 사용자에게 PIN을 변경하도록 만들어야만 합니다.

시작하기 전에

이 절차에서는 사용자가 이미 Cisco Unity Connection의 애플리케이션 서버 연결이 설정되어 있는 것으로 가정합니다. 그렇지 않은 경우, 새 애플리케이션 서버를 추가하는 방법에 대한 자세한 내용은 관련 주제 섹션을 참조하십시오.

PIN 동기화 기능을 활성화하려면, 먼저 Cisco Unity Server 연결에 대한 유효한 인증서를 Cisco Unified OS 관리 페이지에서 Cisco Unified Communications Manager tomcat-trust로 업로드해야 합니다. 인증서 업로드 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html의 *Cisco Unified Communications Manager* 관리 설명서에서 "보안 인증서 관리" 장을 참조하십시오.

Cisco Unity Connection 서버의 사용자 ID는 Cisco Unified Communications Manager 내의 사용자 ID와 일치해야만 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 애플리케이션 서버를 선택합니다.

단계 **2** Cisco Unity Connection에 대해 설정하는 애플리케이션 서버를 선택합니다.

단계 **3** [엔드 유저 **PIN** 동기화 활성화] 확인란에 체크 표시 합니다.

단계 **4** 저장을 클릭합니다.

관련 항목

애플리케이션 서버 구성

Cisco Expressway

Cisco Unified Communications Manager는 Cisco Expressway를 통합하여 Cisco Unified Communications 모바일 및 원격 액세스를 제공합니다. Cisco Unified Communications 모바일 및 원격 액세스는 Cisco Collaboration Edge Architecture의 핵심 부분입니다. Cisco Jabber와 같은 엔드포인트가 엔터프라이즈 네트워크에 없는 경우, 엔드포인트를 통해 Cisco Unified Communications Manager(Unified CM)에서 제공하는 등록, 통화 제어, 프로비저닝, 메시징 및 프레즌스 서비스를 사용할 수 있습니다. Expressway에서 Unified CM 등록을 위한 보안 방화벽 통과 및 회선 측 지원을 제공합니다.

전체 솔루션은 다음과 같은 기능을 제공합니다.

- 오프프레미스 액세스—Cisco Jabber 및 EX/MX/SX 시리즈 클라이언트 네트워크 외부에서 일관된 경험.
- 보안—비즈니스 간 통신 보호
- 클라우드 서비스—풍부한 Webex 통합 및 서비스 공급자 패키지를 제공하는 엔터프라이즈급 유연성 및 확장 가능 솔루션.
- 게이트웨이 및 상호운용성 서비스—미디어 및 신호 정규화, 비표준 엔드포인트 지원.

구축에 대한 상세 설명은 *Cisco Expressway*를 통한 모바일 및 원격 액세스 구축 설명서를 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html에서 참조하십시오.

Cisco Emergency Responder

Cisco Emergency Responder(Emergency Responder)에서 전화 통신 네트워크 상에서 응급 전화의 관리를 지원하며, 그 결과 이러한 전화에 효과적으로 대응할 수 있고 응급 전화 취급에 대한 현지 법령을 준수할 수 있습니다. 북미에서 이러한 현지 법령은 "강화된 911," 또는 E911로 부릅니다. 기타 국가 및 로캘에도 유사한 법령이 있습니다.

응급 전화 법령이 국가, 지방, 주 또는 자치 구역 내의 장소에 따라 달라질 수 있으므로, Emergency Responder에서 특정 현지 요구 사항에 따라 응급 전화 구성을 설정할 수 있는 유연성을 제공합니다. 그러나 법령은 장소에 따라 달라지며, 보안 요구 사항도 회사에 따라 달라집니다. 따라서 반드시 보안 및 법적 필요에 대해 연구한 다음 Emergency Responder를 구축해야 합니다.

Cisco Emergency Responder를 설치하고 Cisco Unified Communications Manager와 통합하는 방법에 대한 자세한 내용은 *Cisco Emergency Responder* 관리 설명서를 https://www.cisco.com/c/en/us/support/unified-communications/emergency-responder/products-maintenance-guides-list.html에서 참조하십시오.

Cisco Unified Communications Manager의 기능 지원

다음 Cisco Unified Communications Manager 기능은 Cisco Emergency Responder와의 통합을 지원합니다. Cisco Unified Communications Manager에 대한 이러한 기능 설정 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager*에 대한 기능 설정 가이드를 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 참조하십시오.

- 위치 인식
- 비상 통화 처리기

Cisco Paging Server

Cisco Paging Server와 통합하기 위해 Cisco Unified Communications Manager를 구성하여 Cisco IP 전화기와 여러 엔트포인트에 대한 페이징 서비스를 제공할 수 있습니다. Cisco Paging Server 제품은 InformaCast Virtual Appliance를 통해 제공되며, 다음과 같은 구축 옵션을 제공합니다.

- 기본 페이징—전화기 간 및 그룹 라이브 오디오 페이징을 Cisco IP 전화기에 제공합니다. 시스템의 모든 사용자는 기본 페이지를 만들고 수신하는 데 참가할 수 있습니다.
- 고급 알림—텍스트 및 라이브 또는 사전 녹음된 오디오 메시지를 사용하여 무한대의 전화기에 연결할 수 있는 종합 기능을 갖춘 고급 알림 솔루션을 제공합니다.

Cisco Paging Server에 대한 자세한 내용 및 설명서는 https://www.cisco.com/c/en/us/products/unified-communications/paging-server/index.html을 참조하십시오.

구성

기본 페이징 또는 고급 알림을 위해 Cisco Unified Communications Manager를 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager*에 대한 기능 구성 설명서의 "페이징" 장을 참조하십시오.

Cisco Unified Contact Center Enterprise

시스템에서 Cisco Unified Contact Center Enterprise(Unified CCE)를 사용하여 지능형 콜 라우팅, 네트워크-투-데스크톱 CTI(Computer Telephony Integration), 다중 채널 연락처 관리를 IP 네트워크의 컨택 센터 에이전트로 통합할 수 있습니다. Unified CCE에서는 고급 분산 컨택 센터를 신속하게 구축할 수 있도록 소프트웨어 IP ACD(자동 통화 분산)를 Cisco Unified Communications과 결합합니다.

시스템에 통합하도록 Unified CCE를 구성하는 방법에 대한 자세한 작업 내용은, http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html에서 *Cisco Unified Contact Center Enterprise* 설치 및 업그레이드 설명서를 참조하십시오.

Cisco Unified Contact Center Express

Cisco Unified Contact Center Express(Unified CCX)는 단일 또는 이중 서버 구축으로 패키지된 대규모 컨택 센터의 기능을 시스템에 제공합니다. Unified CCX는 최대 400명의 동시 에이전트, 42명의 감독자, 150개의 에이전트 그룹 및 150개의 스킬 그룹으로 확장됩니다. 여기에는 이 메일, 채팅, 발신 통화, 착신 전화, 인력 최적화 및 보고서 기능이 포함됩니다.

Unified CCX는 Unified CCX를 대신하여 모든 컨택 센터 통화를 관리 하는 Unified Communication Manager와 함께 작동합니다. 헬프 데스크로 전화가 걸려오면, 통화 시스템에서는 해당 번호가 Unified CCX 애플리케이션 서버에 대해 지정된 것으로 인식합니다. 이 구성을 사용하여 Unified CCX에서 착신 통화를 수신하고 걸려온 내선 번호에 따라 요청을 처리합니다. 스크립트는 프롬프트를 재생하고 숫자를 수집하며, 필요한 경우 발신자의 정보를 사용하여 적절한 에이전트를 선택합니다. 할당된 에이전트를 사용할 수 없는 경우 해당 통화는 적절 한 대기열에 배치되고 녹음된 메시지나 음악이 발신자에 게 스트리밍됩니다. 에이전트를 사용할 수 있게 되면, 즉시 Unified CCX에서 Unified Communications Manager에게 에이전트의 전화기로 전화를 걸 것을 지시합니다.

에이전트가 수신하면 관련 통화 컨텍스트가 에이전트의 데스크톱 애플리케이션에 제공됩니다. 이 단계를 통해 에이전트가 고객을 지원하기 위한 적절한 정보를 보유하게 됩니다.

시스템과 통합하기 위해 Unified CCX를 구성하는 방법에 대한 자세한 내용은 http://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-express/products-installation-and-configuration-guides-list.html에서 *Cisco Unified CCX* 관리 설명서를 참조하십시오.

고급 QoS APIC-EM Controller

APIC-EM 컨트롤러에서는 네트워크 트래픽 관리용 중앙 시스템을 제공하여 혼잡한 네트워크에서도 항상 대역폭을 보유하여 커뮤니케이션을 유지할 수 있게 해줍니다. Cisco Unified Communications Manager를 설정하여 APIC-EM 컨트롤러를 사용하여 SIP 미디어 플로우를 관리할 수 있습니다. 이를 통해 제공받는 이점은 다음과 같습니다.

- QoS 관리를 중앙에서 집중 처리함으로써, DSCP 값을 할당하기 위한 엔드포인트에 대한 필요를 없애 줍니다.
- 서로 다른 미디어 흐름에 대한 차등 QoS 처리를 적용합니다. 예를 들면, 비디오에 비해 오디오를 우선시하여 네트워크 대역폭이 낮을 때 조차도 기본 오디오 커뮤니케이션이 항상 유지되도록 보장할 수 있습니다.
- SIP 프로파일 외부 QoS 설정을 통해 어떤 사용자가 APIC-EM을 사용할지 타겟팅할 수 있습니다. 예를 들면, Cisco Unified IP Phone 사용자가 Cisco Unified Communications Manager에서 DSCP 설정을 사용하는 동안, Cisco Jabber 사용자가 APIC-EM을 사용하여 미디어 플로우를 관리하도록 할 수 있습니다.

구성 상세 정보

APIC_EM Controller와 통합하기 위해 Cisco Unified Communications Manager를 구성하는 방법에 대한 내용을 포함한 추가적인 상세 정보는, *Cisco Unified Communications Manager*에 대한 기능 설정 가이드의 "APIC-EM Controller로 QoS 구성" 장을 참조하십시오.

Cisco WebDialer 서버 구성

입력할 문자 수를 제한하는 **WebDialer** 목록 서비스 매개변수의 대체 방법으로 Cisco WebDialer 애플리케이션 서버를 구성합니다. 애플리케이션 서버 구성 창에서 Cisco WebDialer 애플리케이션 서버를 추가하면, Cisco WebDialer Web 서비스의 서비스 매개변수 구성 창에 있는 [WebDialers 목록] 필드에 서버가 표시됩니다. Cisco WebDialer 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에서 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 애플리케이션 서버를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 애플리케이션 서버 유형 드롭다운 목록에서 **Cisco WebDialer**를 선택한 다음, 저장을 클릭합니다.

단계 **4** 호스트네임 또는 **IP** 주소 필드에 WebDialer 서버의 호스트네임 또는 IP 주소를 입력합니다.

단계 **5** 리디렉터 노드 드롭다운 목록에서 **< None >** 또는 특정 Unified Communications Manager 노드를 선택합니다.

< None >인 경우 WebDialer 서버가 모든 노드에 적용됩니다.

단계 **6** 저장을 클릭합니다.

단계 **7** Cisco Unified Serviceability에서 도구제어 센터 > - 기능 서비스를 선택합니다.

단계 **8** **Cisco WebDialer** 웹 서비스 라디오 버튼을 클릭합니다.

단계 **9** 재시작을 클릭합니다.

27 장

CTI 애플리케이션 구성

CTI 애플리케이션 개요

컴퓨터 텔레포니 통합(CTI)를 사용하여 전화 통화를 걸고 받고 관리하면서 컴퓨터 처리 기능을 사용할 수 있습니다. CTI 애플리케이션을 사용하면 발신자 ID를 사용하여 데이터베이스에서 고객 정보를 검색하는 것과 같은 작업을 수행하고, IVR(대화형 음성 응답) 시스템에서 수집한 정보로 작업하여 고객의 통화를 해당 정보와 함께 해당 고객 서비스 담당자에게 라우팅할 수 있습니다.

라우트 포인트에서 통화에 대한 미디어를 종료하려는 애플리케이션에서 통화 별로 통화에 대한 미디어 및 포트를 지정해야만 합니다. CTI 애플리케이션은 정적 또는 동적 IP 주소 및 포트 번호를 사용하여 CTI 포트 및 CTI 라우트 포인트의 미디어를 종료할 수 있습니다.

이 장에서는 Cisco Unified Communications Manager를 구성하여 CTI 애플리케이션을 작동하는 방법에 대해 설명합니다. 특정 애플리케이션을 구성하는 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

몇 가지 사용 가능한 Cisco CTI 애플리케이션은 다음과 같습니다.

- Cisco IP Communicator: 컴퓨터를 통화 추적, 데스크톱 협업 및 온라인 디렉터리에서 원클릭 다이얼링이 추가된 완전한 기능을 갖춘 전화기로 전환하는 데스크톱 애플리케이션입니다.
- Cisco Unified Communications Manager 자동 응답: Cisco Unified Communications Manager와 연동하여 특정 전화의 내선에서 전화를 받고 발신자가 해당 내선을 선택할 수 있습니다.
- Cisco Web Dialer: Cisco IP 전화기를 사용하여 웹과 데스크톱 애플리케이션에서 전화를 걸 수 있습니다.
- Cisco Unified Communications Manager Assistant: 관리자와 어시스턴트를 활성화하여 더 효율적으로 협력할 수 있습니다. 이 기능은 콜 라우팅 서비스, 관리자와 어시스턴트를 위한 전화기 기능 개선사항 및 주로 어시스턴트가 사용하는 Assistant Console 인터페이스로 구성됩니다.

참고 어떤 Unified Communications Manager CTI 애플리케이션이 SIP IP 전화기를 지원하는지 확인하려면, 애플리케이션에 따른 설명서를 참조하십시오.

CTI 라우트 포인트 개요

CTI 라우트 포인트 가상 디바이스는 애플리케이션 제어 전환을 위해 여러 개의 동시 통화를 수신할 수 있습니다. 사용자가 애플리케이션에 액세스하기 위해 통화할 수 있는 CTI 라우트 포인트에 하나 이상의 회선을 구성할 수 있습니다. 애플리케이션은 라우트 포인트에서 통화에 응답할 수 있고, CTI 포트 또는 IP 전화기로 통화를 전환할 수도 있습니다. CTI 애플리케이션에서 리디렉트 API를 사용하여 통화를 전환하도록 요청하는 경우, Cisco Unified Communications Manager에서 전환된 상대방의 회선/디바이스 발신 검색 공간에 대한 구성을 사용합니다.

CTI 라우트 포인트를 사용하여 다음을 수행할 수 있습니다.

- 전화 받기
- 복수의 활성 통화 걸기 및 받기
- 통화 재전송
- 통화 보류
- 통화 보류 해제
- 통화 취소

Cisco Unified Communications Manager의 CTI 리던던시

클러스터에서 Unified Communications Manager 노드가 실패하면, CTIManager에서 다른 Unified Communications Manager 노드에서 이들 디바이스를 다시 열어 해당 CTI 포트 및 라우트 포인트를 복구합니다. 애플리케이션에 전화 디바이스가 열려 있는 경우, CTIManager에서는 전화기가 다른 Unified Communications Manager로 페일오버될 때 전화기도 다시 엽니다. Cisco IP Phone이 다른 Unified Communications Manager로 페일오버되지 않는 경우, CTIMManager에서 전화기 또는 전화기의 회선을 열 수 없습니다. CTIManager에서 디바이스 풀에 할당된 Unified Communications Manager 그룹을 사용하여, 애플리케이션이 열려 있는 CTI 디바이스 및 전화기를 복구하기 위해 어떤 Unified Communications Manager를 사용할지를 결정합니다.

CTIManager의 CTI 리던던시

CTIManager에 장애가 발생하면 CTIManager에 연결된 애플리케이션에서 다른 CTIManager에서 이러한 디바이스를 다시 열어 영향을 받는 리소스를 복구할 수 있습니다. 애플리케이션에서는 애플리케이션을 설정할 때 기본 및 백업으로 정의된 CTIManager를 기준으로 사용할 CTIManager를 결정합니다(애플리케이션에서 지원하는 경우). 애플리케이션에서 새 CTIManager에 연결하면 이전에 열었던 디바이스와 회선이 다시 열릴 수 있습니다. 애플리케이션은 전화기가 새 Unified Communications

Manager으로 새롭게 연결되기 전에 Cisco IP 전화기를 다시 열 수 있습니다. 그러나 홈재설정이 완료될 때까지 전화기를 제어할 수 없습니다.

참고 애플리케이션에서 서비스로 복귀할 때 기본 CTIManager로 새로 연결되지 않습니다. 애플리케이션을 다시 시작하거나 백업 CTIManager에서 장애가 발생한 경우, 애플리케이션이 기본 CTIManager로 복구됩니다.

애플리케이션 실패에 대한 CTI 리던던시

애플리케이션(TAPI/JTAPI 또는 CTIManager에 직접 연결되는 애플리케이션)이 실패하면, CTIManager에서 애플리케이션을 닫고 CTI 포트 및 라우트 포인트에서 종결되지 않은 통화를 구성된 통화 착신 전환 실패(CFOF) 번호로 재전송합니다. CTIManager에서는 또한 애플리케이션에서 이러한 디바이스를 복구하고 재등록할 때까지 이러한 CTI 포트 및 라우트 포인트로의 후속 통화를 구성된 통화 착신 응답 없음(CFna) 번호로 라우팅합니다.

CTI 애플리케이션 사전 요건

CTI 애플리케이션에 대한 Cisco Unified Communications Manager를 구성하려면 먼저 디바이스 풀이 구성해야 합니다.

각 CTI 애플리케이션에 대한 IP 전화기를 추가하고 구성합니다. IP 전화기 추가 및 구성에 대한 자세한 내용은 Cisco Unified IP Phone를 참조하십시오.

CTI 애플리케이션을 사용할 엔드 유저 및 애플리케이션 사용자를 구성합니다.

컴퓨터 텔레포니 통합(CTI)는 IPv4 및 IPv6 주소를 지원할 수 있는 JTAPI 및 TAPI 인터페이스를 통해 IP 주소 정보를 제공합니다. IPv6 주소를 지원하려면 애플리케이션에서 IPv6을 지원하는 JTAPI/TAPI 클라이언트 인터페이스 버전을 사용하고 있는지 확인하십시오.

CTI 애플리케이션 작업 플로우 구성

CTI 애플리케이션을 위해 Cisco Unified Communications Manager를 구성하려면 다음 작업을 수행합니다.

프로시저

	명령 또는 동작	목적
단계 1	CTIManager 서비스 활성화, 290 페이지	아직 활성화되지 않은 경우, 해당 서버에서 CTIManager 서비스를 활성화합니다.

	명령 또는 동작	목적
단계 2	CTIManager 및 Cisco Unified Communications Manager 서비스 매개변수 구성, 291 페이지	CTI 슈퍼 공급업체 기능과 함께 사용되는 CTIManager 고급 클러스터 수준 서비스 매개변수를 구성합니다.
단계 3	CTI 라우트 포인트를 구성 하려면 다음 절차를 수행합니다. • CTI 라우트 포인트 구성, 292 페이지 • 새 통화 수락 타이머 구성, 292 페이지 • 동시 활성 통화 구성, 292 페이지 • CTI 라우트 포인트 동기화, 293 페이지	애플리케이션 제어 전환을 위해 여러 건의 동시 통화를 수신할 수 있는 하나 이상의 CTI 라우트 포인트 가상 디바이스를 구성합니다.
단계 4	CTI 디바이스 디렉터리 번호 구성, 293 페이지	CTI 디바이스에 대한 디렉터리 번호를 구성합니다.
단계 5	디바이스를 그룹에 연결, 294 페이지	애플리케이션 사용자 및 엔드 유저를 위해 애플리케이션에서 사용하는 모든 디바이스를 해당 Cisco Unified Communications Manager 그룹에 (디바이스 풀을 통해) 연결합니다.
단계 6	엔드 유저 및 애플리케이션 사용자 추가, 294 페이지	CTI 애플리케이션에서 엔드 유저 및 애플리케이션 사용자를 표준 CTI 활성 사용자 그룹에 추가하여 Cisco Unified Communications Manager 시스템에서 구성된 CTI 제어 디바이스를 제어할 수 있도록 허용합니다.
단계 7	(선택 사항) 애플리케이션 장애에 대한 CTI 리던던시 구성, 296 페이지	CTI 관리자가 애플리케이션에서 연속 두 번 이내로 메시지를 수신하는 간격을 다음과 같이 정의합니다.

CTIManager 서비스 활성화

프로시저

단계 1 Cisco Unified 서비스 가용성에서 도구서비스 활성화를 선택합니다. >
단계 2 서버 드롭다운 목록에서 노드를 선택합니다.
단계 3 CM 서비스 섹션에서 **Cisco CTIManager** 확인란에 체크 표시합니다.
단계 4 저장을 클릭합니다.

CTIManager 및 Cisco Unified Communications Manager 서비스 매개변수 구성

CTI 슈퍼 공급업체 기능과 함께 사용되는 CTIManager 고급 클러스터 수준 서비스 매개변수를 구성합니다.

참고 구성된 제한 사항을 초과하는 경우, CTI에서 알람을 생성하지만, 애플리케이션은 추가 디바이스를 통해 계속해서 작동합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 Cisco CTIManager(활성)를 선택합니다.

단계 **4** 서비스 매개변수 구성 창에서 고급을 클릭합니다.

단계 **5** 공급업체 당 최대 디바이스 필드에 단일 CTI 애플리케이션에서 열 수 있는 최대 디바이스의 수를 입력합니다. 기본값은 2000대의 디바이스입니다.

단계 **6** [노드당 최대 디바이스] 필드에 모든 CTI 애플리케이션에서 Unified Communications Manager 시스템의 모든 CTIManager 노드에서 열 수 있는 최대 디바이스의 수를 입력합니다. 기본값은 800대의 디바이스입니다.

단계 **7** 저장을 클릭합니다.

CTI 라우트 포인트 작업 플로우 구성

프로시저

	명령 또는 동작	목적
단계 **1**	CTI 라우트 포인트 구성, 292 페이지	새로 추가하거나, 기존 CTI 라우트 포인트를 수정합니다.
단계 **2**	새 통화 수락 타이머 구성, 292 페이지	라우트 포인트에 통화가 도달하면 애플리케이션에서 지정된 시간 내에 처리(수락, 응답, 재전송)되도록, 새로운 통화 수락 타이머를 구성합니다.
단계 **3**	동시 활성 통화 구성, 292 페이지	라우트 포인트에서 동시 활성 통화의 수를 구성합니다.

	명령 또는 동작	목적
단계 4	선택 사항: CTI 라우트 포인트 동기화, 293 페이지	최근 구성 변경 사항과 CTI 경로 포인트를 동기화하면, 방해를 최소화하는 방식으로 모든 미처리 구성 설정이 적용됩니다. (예를 들어, 일부 해당 디바이스에서는 재설정/다시 시작이 필요 없을 수 있습니다.)

CTI 라우트 포인트 구성

새로 추가하거나, 기존 CTI 라우트 포인트를 수정합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.

단계 2 다음 작업 중 하나를 수행합니다.

- 새로 추가를 클릭하여 새 게이트웨이를 추가합니다.
- 찾기를 클릭하고 결과 목록에서 CTI 라우트 포인트를 선택 하 여 기존 CTI 라우트 포인트에 대한 설정을 수정 하 고 검색 기준을 입력합니다.

단계 3 **CTI** 라우트 포인트 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 4 저장을 클릭합니다.

새 통화 수락 타이머 구성

라우트 포인트에 통화가 도달하면 애플리케이션에서 지정된 시간 내에 처리(수락, 응답, 재전송)되도록, 새로운 통화 수락 타이머를 구성합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 2 서버 드롭다운 목록에서 노드를 선택합니다.

단계 3 서비스 드롭다운 목록에서 **Cisco CallManager(**활성**)**를 선택합니다.

단계 4 **CTI** 새 통화 수락 타이머 필드에서 통화 응답에 허용하려는 시간을 지정합니다. 기본값은 4입니다.

단계 5 저장을 클릭합니다.

동시 활성 통화 구성

라우트 포인트에서 동시 활성 통화의 수를 구성합니다.

참고 Cisco CallManager TSP(전화 통신 서비스 제공자)를 사용하여 CTI 포트 디바이스를 제어하기 위해 TAPI 애플리케이션을 사용하려고 계획 중인 경우, CTI 포트 디바이스 당 한 회선만 구성할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 디렉터리 번호를 선택합니다.
단계 **2** 디렉터리 번호 구성 창에서 새로 추가를 클릭합니다.
단계 **3** 필수 필드를 입력합니다.
단계 **4** 저장을 클릭합니다.

CTI 라우트 포인트 동기화

최근 구성 변경 사항과 CTI 경로 포인트를 동기화하면, 방해를 최소화하는 방식으로 모든 미처리 구성 설정이 적용됩니다. (예를 들어, 일부 해당 디바이스에서는 재설정/다시 시작이 필요 없을 수 있습니다.)

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.
단계 **2** **CTI** 라우트 포인트 찾기 및 나열 창에서 찾기를 클릭하여 CTI 라우트 패턴 목록을 표시합니다.
단계 **3** 동기화할 CTI 라우트 포인트 옆의 확인란에 체크 표시합니다. 창에 있는 CTI 라우트 포인트를 모두 선택하려면 일치하는 레코드 제목 표시줄의 확인란에 체크 표시합니다.
단계 **4** 선택한 항목에 구성 적용을 클릭합니다.
단계 **5** 확인을 클릭합니다.

CTI 디바이스 디렉터리 번호 구성

CTI 디바이스에 대한 디렉터리 번호를 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 콜 라우팅 > 디렉터리 번호를 선택합니다.
단계 **2** 디렉터리 번호 나열 및 찾기 창에서 새로 추가를 클릭합니다.
단계 **3** 디렉터리 번호 구성 창에서 필수 필드를 입력합니다.

단계 **4** 저장을 클릭합니다.

디바이스를 그룹에 연결

애플리케이션 사용자 및 엔드 유저를 위해 애플리케이션에서 사용하는 모든 디바이스를 해당 Cisco Unified Communications Manager 그룹에 (디바이스 풀을 통해) 연결합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 애플리케이션 사용자를 클릭합니다.

단계 **2** 애플리케이션 사용자 찾기 및 나열 창에서 새로 추가를 클릭합니다. 이렇게 하면 애플리케이션 사용자 설정 창이 나옵니다.

단계 **3** 디바이스 정보 창에서 사용 가능한 디바이스 목록에서 제어된 디바이스 목록으로 이동하여 해당 디바이스를 연결합니다.

단계 **4** 저장을 클릭합니다.

단계 **5** 엔드 유저의 디바이스를 연결하려면 사용자 관리 > 엔드 유저를 클릭합니다.

단계 **6** 2 ~ 4 단계를 반복합니다.

엔드 유저 및 애플리케이션 사용자 추가

CTI 애플리케이션에서 엔드 유저 및 애플리케이션 사용자를 표준 CTI 활성 사용자 그룹에 추가하여 Cisco Unified Communications Manager 시스템에서 구성된 CTI 제어 디바이스를 제어할 수 있도록 허용합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 액세스 제어 그룹을 선택합니다.

단계 **2** 엑세스 컨트롤 그룹 찾기 및 나열 창에서 찾기를 클릭하여 액세스 제어 그룹의 현재 목록을 표시합니다.

단계 **3** 표준 **CTI** 활성화를 클릭합니다. 그러면 이 그룹에 대한 액세스 제어 그룹 설정 창이 표시됩니다. 모든 CTI 사용자가 표준 CTI 활성화 사용자 그룹에 포함되어 있는지 확인하십시오. 이용 가능한 그룹의 전체 목록 및 관련 기능에 대해서는 액세스 제어 그룹 설정 옵션을 참조하십시오.

단계 **4** 엔드 유저를 추가하려면 그룹에 엔드 유저 추가를 클릭하거나, 애플리케이션 사용자를 추가하려면 그룹에 앱 사용자 추가를 클릭합니다.

단계 **5** 찾기를 클릭하여 현재 사용자 목록을 표시합니다.

단계 **6** 표준 CTI 활성화 사용자 그룹에 할당하려는 사용자를 확인합니다.

단계 **7** 선택한 항목 추가를 클릭합니다.

액세스 제어 그룹 구성 옵션

참고 CTI 애플리케이션에서 할당된 지정 사용자 그룹을 지원해야 합니다.

참고 [모든 디바이스의 표준 CTI 허용 제어] 사용자 그룹에 연결된 사용자는 표준 CTI 보안 연결 사용자 그룹에도 연결되어 있을 것을 권장합니다.

참고 다음 표에 나열된 모든 역할이 제대로 작동하려면 제어되는 장치 아래에 특정 장치를 추가해야 합니다.

필드	설명
표준 CTI 통화 모니터링 허용	이 사용자 그룹을 통해 애플리케이션에서 통화를 모니터링할 수 있습니다.
표준 CTI 통화 지정보류 모니터링 허용	이 사용자 그룹을 사용하면 애플리케이션에서 통화가 모든 통화 대기 디렉터리 번호로 대기/대기 해제될 때 알림을 받을 수 있습니다.
표준 CTI 통화 녹음 허용	이 사용자 그룹을 사용하면 애플리케이션에서 통화를 녹음할 수 있습니다.
표준 CTI 발신 번호 수정 허용	이 사용자 그룹을 사용하면 애플리케이션에서 지원되는 CTI 애플리케이션의 발신자 번호를 수정할 수 있습니다.
표준 CTI 모든 디바이스 제어 허용	이 사용자 그룹을 사용하면 애플리케이션에서 시스템의 CTI 제어 가능 디바이스를 제어 또는 모니터링할 수 있습니다.
표준 CTI SRTP 키 자료 수신 허용	이 사용자 그룹을 사용하면 애플리케이션에서 암호화된 미디어 스트림을 해독하기 위해 필요한 정보를 받을 수 있습니다. 이 그룹은 일반적으로 녹음 및 모니터링을 위해 사용됩니다.
표준 CTI 활성화	모든 CTI 애플리케이션에 필요한 이 사용자 그룹을 사용하면 애플리케이션에서 Cisco Unified Communications Manager에 연결하고 CTI 기능에 액세스할 수 있습니다.

필드	설명
표준 CTI 보안 연결	이 그룹에 포함되면 애플리케이션에 Cisco Unified Communications Manager에 대한 보안(TLS) CTI 연결이 있고 Cisco Unified Communications Manager 클러스터 보안이 활성화되어 있어야 합니다.

애플리케이션 장애에 대한 CTI 리던던시 구성

CTI 관리자가 애플리케이션에서 연속 두 번 이내로 메시지를 수신하는 간격을 다음과 같이 정의합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **Cisco CTIManager(**활성**)**를 선택합니다.

단계 **4** 서비스 매개변수 구성 창에서 고급을 클릭합니다.

단계 **5** 애플리케이션 하트 비트 최소 간격 필드에 최소 간격에 대한 시간을 입력합니다. 기본값은 5입니다.

단계 **6** 애플리케이션 하트 비트 최대 간격 필드에 최대 간격에 대한 시간을 입력합니다. 기본값은 3600입니다.

단계 **7** 저장을 클릭합니다.

IV 부

엔드 유저 프로비저닝

28 장

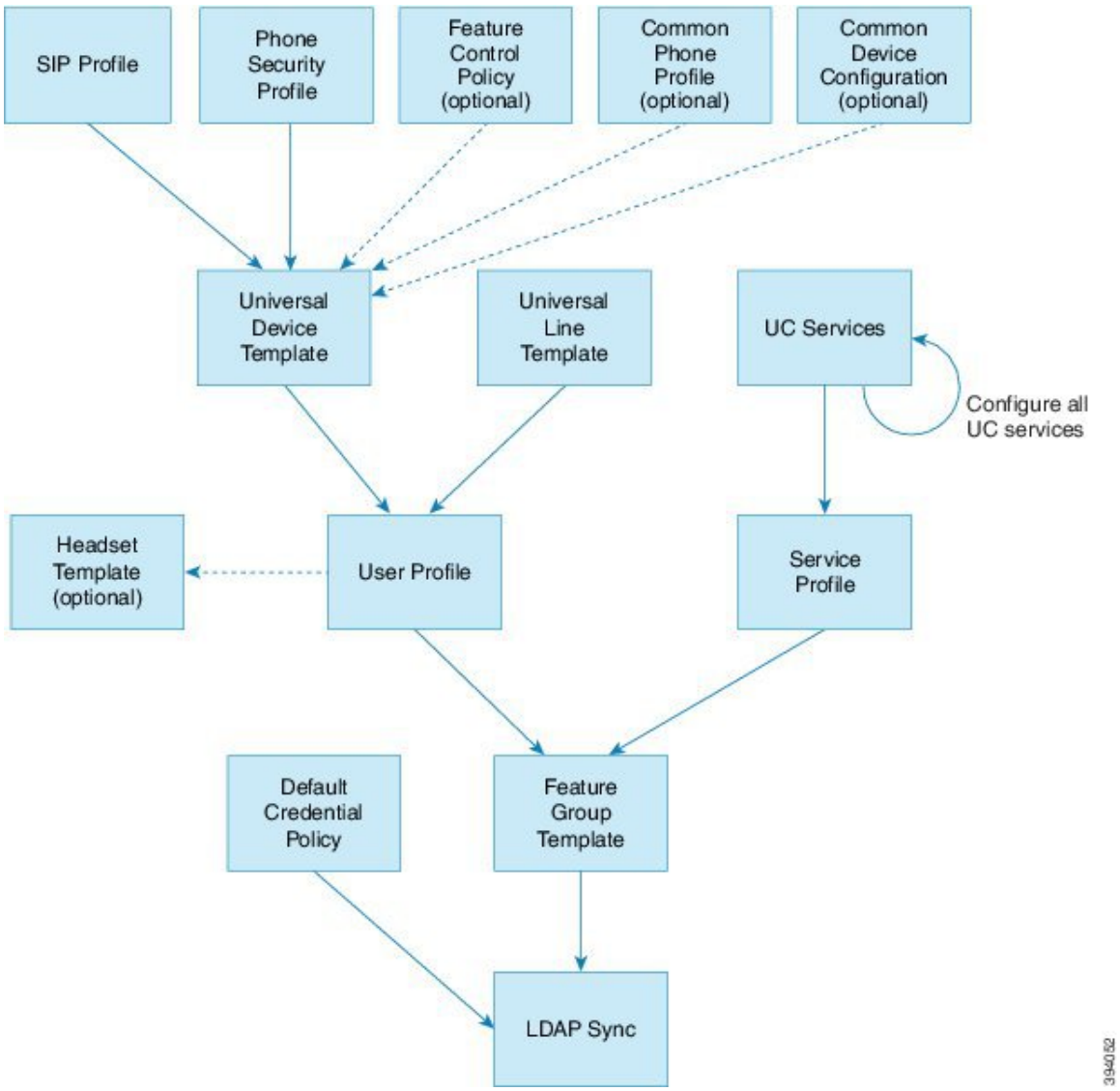
프로비저닝 프로파일 구성

프로비저닝 프로파일 개요

Unified Communications Manager에는 새 사용자에게 할당할 수 있는 일련의 프로파일 및 템플릿이 포함되어 있습니다. 이러한 프로파일 및 일반 설정을 미리 설정한 경우, 새 사용자를 프로비저닝하고 디바이스를 할당할 때는 적용되는 설정에 따라 사용자 및 디바이스가 자동으로 구성됩니다.

사용자를 프로비저닝할 경우, 필요한 설정을 포함하는 사용자 프로파일 및 서비스 프로파일에 사용자를 연결합니다. 또한 사용자에 대한 디바이스를 추가할 때에도, 사용자의 사용자 프로파일에 연결된 범용 회선 및 범용 디바이스 템플릿을 사용하여 디바이스 및 디렉터리 번호가 신속하게 구성됩니다.

다음과 같은 프로파일 및 템플릿을 사용하여 사용자의 필요에 따라 사용자 및 엔드포인트에 일반 설정을 적용할 수 있습니다.



프로비저닝 프로파일 작업 플로우

프로비저닝할 사용자와 디바이스의 수가 대량인 경우, 특정 그룹의 사용자에게 적용되는 템플릿 및 일반 설정을 사용하여 사용자 프로파일 및 서비스 프로파일을 설정하여 구성 프로세스를 단순화할 수 있습니다(예: 고객 지원).

사용자를 프로비저닝할 경우, 필요한 설정을 포함하는 사용자 프로파일 및 서비스 프로파일에 사용자를 연결합니다. 또한 사용자에 대한 디바이스를 추가할 때에도, 사용자의 사용자 프로파일에 연결된 범용 회선 및 범용 디바이스 템플릿을 사용하여 디바이스 및 디렉터리 번호가 신속하게 구성됩니다.

다음과 같은 프로파일 및 템플릿을 사용하여 사용자의 필요에 따라 사용자 및 엔드포인트에 일반 설정을 적용할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	SIP 프로파일 구성, 302 페이지	구축하는 SIP 엔드포인트와 연결되는 일반 SIP 설정을 구성합니다.
단계 **2**	전화기 보안 프로파일 구성, 303 페이지	프로비저닝된 엔드포인트에 할당될 보안 프로파일을 구성합니다. TLS 및 TFTP 암호화와 같은 설정을 할당합니다.
단계 **3**	기능 제어 정책 생성, 303 페이지	선택 사항. 이 정책을 사용하여 특정 기능을 활성화하고 전화기 소프트 키의 모양을 조정할 수 있습니다.
단계 **4**	일반 전화기 프로파일 생성, 304 페이지	선택 사항. 이 프로파일을 사용하여 엔드포인트 그룹에 할당할 수 있는 프로파일에 TFTP 데이터 및 제품별 구성 기본값을 할당합니다.
단계 **5**	일반 디바이스 설정 구성, 305 페이지	선택 사항. 이 구성을 사용하여 엔드포인트에 사용자별 설정 및 IPv6 기본 설정을 할당합니다.
단계 **6**	범용 디바이스 템플릿 구성, 306 페이지	이 템플릿에는 새롭게 프로비저닝된 전화기를 구성하는 데 사용되는 일반 설정이 포함되어 있습니다. 이 템플릿에 구성한 프로파일을 할당할 수도 있습니다.
단계 **7**	범용 회선 템플릿 구성, 306 페이지	이 템플릿에는 새롭게 프로비저닝된 내선 번호를 구성하는 데 사용되는 일반 설정이 포함되어 있습니다. 내선 번호에 대해 엔터프라이즈 및 E.164 번호를 구성할 수도 있습니다.
단계 **8**	사용자 프로파일 구성, 307 페이지	새롭게 프로비저닝된 사용자에 대한 디바이스 템플릿, 회선 템플릿 및 일반 설정을 사용하여 사용자 프로파일을 설정합니다.
단계 **9**	헤드셋 템플릿 구성, 308 페이지	선택 사항. Cisco 헤드셋을 사용하여 헤드셋 템플릿을 구성하고 설정된 사용자 프로파일에 할당하려는 경우.
단계 **10**	UC 서비스 구성, 309 페이지	IM and Presence 서비스 및 디렉터리 서비스와 같은 UC 서비스를 구성합니다.
단계 **11**	서비스 프로파일 구성, 310 페이지	프로비저닝된 사용자에게 할당하려는 UC 서비스를 포함하는 서비스 프로파일을 생성합니다.

	명령 또는 동작	목적
단계 **12**	기능 그룹 템플릿 구성, 311 페이지	LDAP 동기화를 위해, 사용자 프로파일 및 서비스 프로파일을 LDAP 동기화 사용자에게 할당할 수 있는 기능 그룹 템플릿에 추가합니다.
단계 **13**	기본 자격 증명 정책 구성, 312 페이지	새롭게 프로비저닝된 사용자에게 할당할 자격 증명 정책을 구성합니다.

다음에 수행할 작업

- LDAP 동기화를 설정하여 새 사용자를 프로비저닝합니다.
- LDAP를 구축하고 있지 않는 경우, 벌크 관리를 사용하여 대량으로 사용자를 프로비저닝할 수 있습니다.

SIP 프로파일 구성

이 절차를 사용하여 SIP 디바이스에 할당할 수 있는 공통 SIP 설정으로 SIP 프로파일을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 기존 프로파일을 편집하려면, 찾기를 클릭하고 SIP 프로파일을 선택합니다.
- 새 프로파일을 추가하려면 새로 추가를 클릭합니다.

단계 **3** 프로파일의 이름을 입력합니다.

단계 **4** URI 다이얼링을 구축 중인 경우, 다이얼 문자열 해석을 구성하여 시스템에서 통화를 디렉터리 URI 또는 전화 번호로 처리할지 여부에 대해 시스템에 지시합니다.

단계 **5** 전화기에 사용되는 매개변수에서 DSCP 설정을 완료하여 이 프로파일을 사용하는 통화 유형에 대한 QoS 처리를 정의합니다.

단계 **6** (선택 사항) 정규화 스크립트를 할당해야 하는 경우, 정규화 스크립트 드롭다운 목록에서 기본 스크립트 중 하나를 선택합니다.

참고 스크립트를 직접 만들 수도 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

단계 **7** 이 프로 파일에서 IPv4 및 IPv6 스택을 모두 동시에 지원하게 하려는 경우, **AnaT** 활성화 확인란에 체크 표시합니다.

단계 **8** 사용자가 프레젠테이션을 공유할 수 있게 하려는 경우, **BFCP**를 사용하여 프레젠테이션 공유 허용 확인란에 체크 표시합니다.

단계 **9** SIP 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **10** 저장을 클릭합니다.

전화기 보안 프로파일 구성

엔드포인트에 대한 TLS 신호 처리, CAPF 및 다이제스트 인증 요구 사항과 같은 보안 기능을 활성화하려는 경우, 엔드포인트에 적용할 수 있는 새 보안 프로파일을 구성해야 합니다.

참고 프로비저닝된 디바이스에 SIP 전화기 보안 프로파일을 적용하지 않으면, 기본값으로 디바이스에서 비보안 프로파일을 사용합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 보안 > 전화기 보안 프로파일에 체크 표시합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화기 보안 프로파일 유형 드롭다운 목록에서 범용 디바이스 템플릿을 선택하여 디바이스 템플릿을 통해 프로비저닝할 때 사용할 수 있는 프로파일을 생성합니다.

참고 선택적으로 특정 디바이스 모델에 대한 보안 프로파일을 만들 수도 있습니다.

단계 **4** 프로토콜을 선택합니다.

단계 **5** 프로파일에 대한 적절한 이름을 이름 필드에 입력합니다.

단계 **6** TLS 신호 처리를 사용하여 디바이스에 연결하려면 디바이스 보안 모드를 인증 또는 암호화로, 전송 유형을 **TLS**로 설정합니다.

단계 **7** (선택 사항) 전화기에서 다이제스트 인증을 사용하려면 **OAuth** 인증 활성화 확인란에 체크 표시합니다.

단계 **8** (선택 사항) 암호화된 TFTP를 사용하려면 **TFTP** 암호화 구성 확인란에 체크 표시합니다.

단계 **9** 전화기 보안 프로파일 구성 창에서 남아 있는 필드를 완료해야 합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **10** 저장을 클릭합니다.

기능 제어 정책 생성

다음 단계에 따라 기능 제어 정책을 만듭니다. 이 정책을 사용하여 특정 기능을 활성화 또는 비활성화하여 전화기에 표시되는 소프트 키의 모양을 조정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 기능 제어 정책을 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 기존 정책에 대한 설정을 수정하려면 검색 기준을 입력하고 찾기를 클릭하여 결과 목록에서 정책을 선택합니다.
- 새 정책을 추가하려면 새로 추가를 클릭합니다.

기능 제어 정책 구성 창이 표시됩니다.

단계 **3** 이름 필드에 기능 제어 정책의 이름을 입력합니다.

단계 **4** 설명 필드에 기능 제어 정책에 대한 간단한 설명을 입력합니다.

단계 **5** 나열된 각 기능에 대해 기능 제어 섹션에서 시스템 기본값을 재정의할지 여부와 해당 설정을 활성화 또는 비활성화할지 여부를 선택합니다.

- 기능이 기본값으로 활성화되어 있는 경우 이 설정을 비활성화하려면, 기본값 재정의에서 확인란에 체크 표시하고 설정 활성화에서 확인란에 체크 표시를 해제합니다.
- 기능이 기본값으로 비활성화되어 있는 경우 이 설정을 활성화하려면, 기본값 재정의에서 확인란에 체크 표시하고 설정 활성화에서 확인란에 체크 표시합니다.

단계 **6** 저장을 클릭합니다.

일반 전화기 프로파일 생성

일반 전화기 프로파일은 프로파일을 사용하는 전화기에 대한 TFTP 데이터 및 제품별 구성 기본값을 구성하기 위해 사용할 수 있는 선택적 프로파일입니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 전화기 프로파일 메뉴 경로를 선택하여 일반 전화기 프로파일을 구성합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 프로파일의 이름을 입력합니다.

단계 **4** 프로파일에 대한 설명을 입력합니다.

단계 **5** 이 프로파일을 사용하는 전화기에 기능 제어 정책을 설정하는 경우, 드롭다운 목록에서 정책을 선택합니다.

단계 **6** 일반 전화기 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 제품별 구성 레이아웃에서 필드를 구성합니다. 필드 설명의 경우, (?)를 클릭하여 필드별 도움말을 확인합니다.

단계 **8** (선택 사항) 모바일 및 원격 액세스 전화기에 대해 ICE(상호 연결 설정)를 활성화하려는 경우, 다음을 수행합니다.

a) ICE 드롭다운을 활성화 됨으로 설정합니다.

b) 기본 후보 유형을 다음 중 하나로 설정합니다.

- 호스트—호스트 디바이스에서 IP 주소를 선택하여 가져온 후보입니다. 이것이 기본값입니다.
- 서버 재귀—STUN 요청을 전송하여 가져온 IP 주소 및 포트 후보입니다. 일반적으로 이것은 naT의 공용 IP 주소를 나타낼 수 있습니다.
- **Relayed**—TURN 서버에서 가져온 IP 주소 및 포트 후보입니다. IP 주소 및 포트는 해당 미디어가 TURN 서버를 통해 릴레이될 수 있도록 TURN 서버에 상주합니다.

c) 나머지 ICE 필드를 구성합니다.

단계 **9** 저장을 클릭합니다.

일반 디바이스 설정 구성

일반 디바이스 구성은 사용자별 기능 특성 세트로 이루어집니다. IPv6을 구축하는 경우, 이 구성을 사용하여 SIP 트렁크 또는 SCCP 전화기에 대한 IPv6 기본 설정을 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 디바이스 구성을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** SIP 트렁크, SIP 전화기 또는 SCCP 전화기의 경우, **IP** 주소 지정 모드 드롭다운 목록에 대한 값을 다음과 같이 선택합니다.

- **IPv4** 전용—디바이스에서 미디어 및 신호 처리에 IPv4 주소만 사용합니다.
- **IPv6** 전용—디바이스에서 미디어 및 신호 처리에 IPv6 주소만 사용합니다.
- **IPv4** 및 **IPv6(**기본값**)**—디바이스는 듀얼 스택 디바이스로 어떤 것이든 사용할 수 있는 IP 주소 유형을 사용합니다. 해당 디바이스에 두 IP 주소 유형이 모두 구성된 경우, 신호 처리를 위해 디바이스에서 신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 설정을 사용하고 미디어를 위해 디바이스에서 미디어를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수를 사용합니다.

단계 **4** 이전 단계에서 IPv6을 구성한 경우, 신호 처리를 위한 **IP** 주소 지정 모드 드롭다운 목록에 대해 IP 주소 지정 기본 설정을 다음과 같이 구성합니다.

- **IPv4** —이중 스택 디바이스는 신호 처리를 위해 IPv4 주소를 선호합니다.
- **IPv6** —이중 스택 디바이스는 신호 처리를 위해 IPv6 주소를 선호합니다.

- 시스템 기본값 사용—신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수에 대한 설정을 사용합니다.

단계 **5** 일반 디바이스 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

범용 디바이스 템플릿 구성

범용 디바이스 템플릿을 사용하면 구성 설정을 새로 프로비저닝된 디바이스에 쉽게 적용할 수 있습니다. 프로비저닝된 디바이스는 범용 디바이스 템플릿의 설정을 사용합니다. 서로 다른 사용자 그룹의 요구 사항을 충족하도록 서로 다른 디바이스 템플릿을 구성할 수 있습니다. 이 템플릿에 구성한 프로파일을 할당할 수도 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 디바이스 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 필수 필드인

a) 템플릿에 대한 디바이스 설명을 입력합니다.
b) 드롭다운 목록에서 디바이스 풀을 선택합니다.
c) 드롭다운 목록에서 디바이스 보안 프로파일을 선택합니다.
d) 드롭다운 목록에서 **SIP** 프로파일을 선택합니다.
e) 드롭다운 목록에서 전화기 버튼 템플릿을 선택합니다.

단계 **4** 범용 디바이스 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **5** 전화기 설정 아래에서 다음 옵션 필드를 완성합니다.

a) 일반 전화기 프로파일을 구성한 경우 프로파일을 할당합니다.
b) 일반 디바이스 구성을 구성한 경우 구성을 할당합니다.
c) 기능 제어 정책을 구성한 경우 정책을 할당합니다.

단계 **6** 저장을 클릭합니다.

범용 회선 템플릿 구성

범용 회선 템플릿을 사용하면 새로 할당된 디렉터리 번호에 일반 설정을 쉽게 적용할 수 있습니다. 서로 다른 사용자 그룹의 요구 사항을 충족하도록 서로 다른 템플릿을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 회선 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 범용 회선 템플릿 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 대체 번호를 사용하여 전역 다이얼 플랜 복제를 배포하는 경우 엔터프라이즈 대체 번호와 **+E.164** 대체 번호 섹션을 확장하고 다음을 수행합니다.

a) 엔터프라이즈 대체 번호 추가 버튼 및/또는 **+E.164** 대체 번호 추가 버튼을 클릭합니다.

b) 대체 번호에 할당하는 데 사용할 번호 마스크를 추가합니다. 예를 들어, 4자리 내선 번호는 5XXXX를 엔터프라이즈 번호 마스크로 사용하고 1972555XXXX를 +E.164 대체 번호 마스크로 사용할 수 있습니다.

c) 대체 번호를 할당할 파티션을 할당합니다.

d) ILS를 통해 이 번호를 광고하려면 **ILS**를 통해 전역으로 광고 확인란에 체크 표시합니다. 광고된 패턴을 사용하여 대체 번호 범위를 요약하는 경우 개별 대체 번호를 광고할 필요가 없습니다.

e) **PSTN** 페일오버 섹션을 확장하고 일반 콜 라우팅이 실패하는 경우 사용할 PSTN 페일오버으로 엔터프라이즈 번호 또는 **+E.164** 대체 번호를 선택합니다.

단계 **5** 저장을 클릭합니다.

사용자 프로파일 구성

사용자 프로파일을 통해 범용 회선 및 범용 디바이스 템플릿을 사용자에게 할당합니다. 서로 다른 사용자 그룹에 대한 여러 사용자 프로파일을 구성합니다. 이 서비스 프로파일을 사용하는 사용자에 대한 셀프 프로비저닝을 활성화할 수도 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.사용자 관리 > 사용자 설정 > 사용자 프로파일.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 사용자 프로파일의 이름 및 설명을 입력합니다.

단계 **4** 사용자의 데스크폰, 모바일 및 데스크탑 디바이스 및 원격 대상/디바이스 프로파일에 적용할 유니버셜 디바이스 템플릿을 할당합니다.

단계 **5** 이 사용자 프로파일의 사용자에 대한 전화 회선에 적용할 범용 회선 템플릿을 할당합니다.

단계 **6** 이 사용자 프로파일의 사용자가 자신의 전화기를 프로비저닝하는 데 셀프 프로비저닝 기능을 사용할 있도록하려면 다음을 수행합니다.

a) 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.

b) 최종 사용자가 이렇게 많은 전화기를 가지고 있으면 프로비저닝 제한 필드에 사용자가 프로비저닝하도록 허용되는 전화기의 최대 수를 입력합니다. 최대값은 20입니다.

c) 다른 엔드 유저에게 이미 할당된 전화의 프로비저닝 허용 확인란에 체크 표시하여 이 프로파일에 연결된 사용자에게 이미 다른 사용자가 소유하는 디바이스를 마이그레이션 또는 재할당할 권한이 있는지 여부를 결정합니다. 기본값으로 이 확인란은 선택되어 있지 않습니다.

단계 **7** 이 사용자 프로파일과 연결된 Cisco Jabber 사용자가 모바일 및 원격 액세스 기능을 사용할 수 있도록 하려면 모바일 및 원격 액세스 활성화 확인란에 체크 표시합니다.

참고
- 기본적으로 이 확인란은 선택되어 있습니다. 이 확인란의 체크 표시를 취소하면 클라이언트 정책 섹션이 비활성화되고 기본값으로 서비스 클라이언트 없음 정책 옵션이 선택됩니다.
- 이 설정은 OAuth 새로 고침 로그인을 사용하는 Cisco Jabber 사용자의 경우에만 필수입니다. 비 Jabber 사용자는 이 설정이 없어도 모바일 및 원격 액세스를 사용할 수 있습니다. 모바일 및 원격 액세스 기능은 Jabber 모바일 및 원격 액세스 사용자에 대해서만 적용 가능하며, 다른 엔드포인트 또는 클라이언트에게는 적용되지 않습니다.

단계 **8** 이 사용자 프로파일에 대해 Jabber 정책을 할당합니다. 데스크톱 클라이언트 정책 및 모바일 클라이언트 정책 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 서비스 없음 - 이 정책은 모든 Cisco Jabber 서비스에 대한 액세스를 비활성화합니다.
- IM & 프레즌스만 해당—이 정책은 인스턴트 메시징 및 프레즌스 기능을 활성화합니다.
- IM & 프레즌스, 음성 및 영상 통화—이 정책은 음성 또는 영상 디바이스가 있는 모든 사용자에 대해 인스턴트 메시징, 프레즌스, 음성 메일 및 전화 회의 기능을 활성화합니다. 이것이 기본 옵션입니다.

참고 Jabber 데스크톱 클라이언트는 Windows용 Cisco Jabber와 Mac용 Cisco Jabber 사용자를 포함합니다. Jabber 모바일 클라이언트는 iPad 및 iPhone용 Cisco Jabber 사용자와 Android용 Cisco Jabber 사용자를 포함합니다.

단계 **9** 사용자가 Unified Communications 셀프 서비스 포털을 통해 내선 이동 또는 인터클러스터 내선 이동에 대한 최대 로그인 시간을 설정하도록 허용하려면 엔드 유저가 내선 이동을 최대 로그인 시간을 설정하도록 허용 확인란에 체크 표시합니다.

참고 기본적으로 최종 사용자가 **Extension Mobility**를 최대 로그인 시간을 설정하도록 허용 확인란은 선택 해제되어 있습니다.

단계 **10** 저장을 클릭합니다.

헤드셋 템플릿 구성

이 절차를 사용하여 Cisco 헤드셋에 적용할 수 있는 사용자 지정된 설정으로 헤드셋 템플릿을 구성합니다. 사용자 지정 템플릿을 만들거나 시스템 정의 표준 기본 헤드셋 템플릿을 사용할 수 있습니다.

참고 표준 기본 헤드셋 구성 템플릿은 시스템 정의 템플릿입니다. 표준 기본 헤드셋 템플릿에 새 사용자 프로파일을 할당할 수 있지만 템플릿을 편집할 수는 없습니다. 기본적으로 모든 사용자 프로파일은 이 템플릿에 할당됩니다. 이 템플릿에서 사용자 프로파일의 연결을 해제하려면 프로파일을 새 템플릿에 할당해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 헤드셋 > 헤드셋 템플릿을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 기존 템플릿을 편집하려면 템플릿을 선택합니다.
- 새 템플릿을 만들려면 기존 템플릿을 선택하고 복사를 클릭합니다. 기존 설정이 새 템플릿에 적용됩니다.

단계 **3** 템플릿에 대한 이름 및 설명을 추가합니다.

단계 **4** 모델 및 펌웨어 설정] 아래에서 이 템플릿에 적용할 사용자 지정된 헤드셋 설정을 할당합니다. 새 설정을 추가하려면 추가 버튼을 클릭하고 설정을 구성합니다.

단계 **5** 위쪽 및 아래쪽 화살표를 사용하여 이 템플릿에 할당하려는 사용자 프로파일을 할당된 사용자 프로파일 목록 상자로 이동합니다. 해당 프로파일에 할당된 모든 사용자도 이 헤드셋 템플릿에 할당됩니다.

단계 **6** 저장을 클릭합니다.

단계 **7** 기본값으로 설정 버튼을 사용하여 기본 템플릿 설정으로 돌아갑니다.

단계 **8** 구성 적용을 클릭합니다.

표준 기본 헤드셋 구성 템플릿의 경우 구성 적용 버튼이 다음 항목에 적용됩니다.

- 할당된 사용자 프로파일 목록에 추가한 사용자가 소유한 디바이스
- 익명의 디바이스

사용자 지정된 헤드셋 구성 템플릿의 경우 구성 적용 버튼은 할당된 사용자 프로파일 목록에 추가한 사용자가 소유한 디바이스에만 적용됩니다.

UC 서비스 구성

이 절차를 사용하여 사용자가 사용할 UC 서비스 연결을 구성합니다. 다음 UC 서비스에 대한 연결을 구성할 수 있습니다.

- 음성 메일
- 메일 저장소

- 전화회의
- 디렉터리
- IM and Presence Service
- CTI
- 화상 회의 예약 포털
- Jabber 클라이언트 구성(jabber-config.xml)

참고 이 필드는 구성하는 UC 서비스에 따라 달라질 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리>사용자 설정>**UC** 서비스를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** [UC 서비스 유형] 드롭다운에서 구성하려는 UC 서비스를 선택하고 다음을 클릭합니다.

단계 **4** 제품 유형을 선택합니다.

단계 **5** 서비스의 이름을 입력합니다.

단계 **6** 서비스가 홈 인 서버의 호스트네임 또는 **IP** 주소를 입력합니다.

단계 **7** 포트 및 프로토콜 정보를 완료합니다.

단계 **8** 나머지 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오. 필드 옵션은 구축하는 UC 서비스에 따라 달라집니다.

단계 **9** 저장을 클릭합니다.

단계 **10** 필요한 모든 UC 서비스를 프로비저닝할 때까지 이 절차를 반복합니다.

참고 여러 서버에 서비스를 배치하려면 다른 서버를 가리키는 다른 UC 서비스 연결을 구성합니다. 예를 들어, IM and Presence Service 중앙 집중식 구축을 통해 서로 다른 IM 및 Presence 노드를 가리키는 여러 IM Presence UC 서비스를 구성하는 것이 좋습니다. 모든 UC 연결을 구성한 후에는 서비스 프로파일에 추가할 수 있습니다.

서비스 프로파일 구성

프로파일을 사용하는 엔드 유저에 게 할당하려는 UC 서비스를 포함한 서비스 프로파일을 구성합니다.

시작하기 전에

Unified Communications(UC) 서비스를 설정해야만 이들 서비스를 서비스 프로파일에 추가할 수 있습니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 서비스 프로파일을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 선택한 서비스 프로파일 구성에 대한 이름을 입력합니다.

단계 **4** 선택한 서비스 프로파일 구성에 대한 설명을 입력합니다.

단계 **5** 이 프로파일의 일부가 되려는 각 UC 서비스의 경우, 해당 서비스에 대한 기본, 보조 및 **3**차 연결을 할당합니다.

단계 **6** 서비스 프로파일 구성 창에서 나머지 필드를 완료합니다. 자세한 필드 설명은 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

기능 그룹 템플릿 구성

기능 그룹 템플릿은 프로비저닝된 사용자를 위해 전화기, 회선 및 기능을 신속하게 구성하도록 도와 시스템 구축을 지원합니다. 회사 LDAP 디렉터리에서 사용자를 동기화하는 경우 사용자가 디렉터리에서 동기화할 사용자 프로파일 및 서비스 프로파일을 사용하여 기능 그룹 템플릿을 구성합니다. 이 템플릿을 통해 동기화된 사용자에 대한 IM and Presence Service를 활성화할 수도 있습니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 기능 그룹 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 기능 그룹 템플릿에 대한 이름 및 설명을 입력합니다.

단계 **4** 이 템플릿을 사용하는 모든 사용자에 대해 로컬 클러스터를 홈 클러스터로 사용하려는 경우 홈 클러스터 확인란을 선택합니다.

단계 **5** 이 템플릿을 사용하는 사용자가 인스턴트 메시징 및 프레전스 정보를 교환하도록 하려면 **Unified CM IM and Presence**에 대해 사용자 활성화 확인란을 선택합니다.

단계 **6** 드롭다운 목록에서 서비스 프로파일 및 사용자 프로파일을 선택합니다.

단계 **7** 기능 그룹 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

기능 그룹 템플릿을 LDAP 디렉터리 동기화와 연결하여 템플릿의 설정을 동기화된 최종 사용자에게 적용합니다.

기본 자격 증명 정책 구성

이 절차를 사용하여 새롭게 프로비저닝된 사용자에게 적용되는 클러스터 수준 기본 자격 증명 정책을 구성합니다. 다음과 같은 각각의 자격 증명 유형에 대해 별도의 자격 증명 정책을 적용할 수 있습니다.

- 애플리케이션 사용자 암호
- 엔드 유저 암호
- 엔드 유저 PIN

프로시저

단계 **1** 자격 증명 정책에 대한 설정을 다음과 같이 구성합니다.

a) Cisco Unified CM 관리에서사용자 관리 > 사용자 설정 > 인증서 정책을 선택합니다.
b) 다음 중 하나를 수행합니다.
   - 찾기를 클릭하고 기존 인증서 정책을 선택합니다.
   - 새로 추가를 클릭하여 새 인증서 정책을 생성합니다.
c) 시스템에서 ABCD 또는 123456과 같이 쉽게 해킹되는 암호를 확인할 수 있게 하려는 경우, 단순한 암호 확인 확인란에 체크 표시합니다.
d) 인증서 정책 구성 창에서 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
e) 저장을 클릭합니다.
f) 다른 자격 증명 유형 중 하나에 대해 다른 자격 증명 정책을 생성하려는 경우, 이러한 단계를 반복합니다.

단계 **2** 다음 자격 증명 유형 중 하나에 자격 증명 정책을 다음과 같이 적용합니다.

a) Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 자격 증명 정책 기본값을 선택합니다.
b) 자격 증명 정책을 적용하려는 자격 증명 유형을 선택합니다.
c) 자격 증명 정책 드롭다운에서 이 자격 증명 유형에 적용하려는 자격 증명 정책을 선택합니다. 예를 들어, 자신이 생성한 자격 증명 정책을 선택할 수 있습니다.
d) 자격 증명 변경 및 자격 증명 확인 필드 모두에 기본 암호를 입력합니다. 사용자는 다음 로그인 시 이러한 암호를 입력해야 합니다.
e) 자격 증명 정책 기본 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
f) 저장을 클릭합니다.

g) 다른 자격 증명 유형 중 하나에 대한 자격 증명 정책을 할당하려는 경우, 이러한 단계를 반복합니다.

참고 개별 사용자의 경우, 해당 사용자에 대한 엔드 유저 구성 창 또는 애플리케이션 사용자 구성 창에서 특정 사용자 자격 증명으로 정책을 할당할 수도 있습니다. 자격 증명 유형(암호 또는 PIN)에 인접한 자격 증명 편집 버튼을 클릭하여 해당 사용자 자격 증명에 대한 자격 증명 구성 설정을 엽니다.

29 장

LDAP 동기화 구성

LDAP 동기화 개요

LDAP(Lightweight Directory Access Protocol) 동기화를 사용하면 시스템의 최종 사용자를 프로비저닝하고 구성할 수 있습니다. LDAP 동기화 중 시스템은 외부 LDAP 디렉터리의 사용자 목록 및 관련 사용자 데이터를 Unified Communications Manager 데이터베이스로 가져옵니다. 가져오는 동안 최종 사용자를 구성할 수도 있습니다.

참고 Unified Communications Manager는 LDAPS(SSL이 있는 LDAP)를 지원하지만 StartTLS가 있는 LDAP는 지원하지 않습니다. LDAP 서버 인증서를 Unified Communications Manager에 Tomcat-Trust로 업로드하십시오.

지원되는 LDAP 디렉터리에 대한 정보는 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스의 호환성 매트릭스를 참조하십시오.

LDAP 동기화는 다음과 같은 기능을 광고합니다.

- 최종 사용자 가져오기—초기 시스템 설정 중에 LDAP 동기화를 사용하여 사용자 목록을 회사 LDAP 디렉토리에서 Unified Communications Manager 데이터베이스로 가져올 수 있습니다. 기능 그룹 템플릿, 사용자 프로파일, 서비스 프로파일, 범용 디바이스 및 회선 템플릿 등의 항목을 미리 구성한 경우에는 사용자에게 구성을 적용하고 동기화 프로세스 중에 구성된 디렉터리 번호와 디렉터리 URI를 할당할 수 있습니다. LDAP 동기화 프로세스는 사용자 및 사용자 특정 데이터 목록을 가져오고 사용자가 설정한 구성 템플릿을 적용합니다.

참고 초기 동기화가 이미 발생한 후에는 LDAP 동기화를 편집할 수 없습니다.

- 예약된 업데이트—예약된 간격으로 여러 LDAP 디렉터리와 동기화하도록 Unified Communications Manager를 구성하여 데이터베이스가 정기적으로 업데이트되고 사용자 데이터가 최신 상태로 유지되도록 할 수 있습니다.
- 최종 사용자 인증—Cisco Unified Communications Manager 데이터베이스가 아닌 LDAP 디렉터리에 대해 최종 사용자 암호를 인증하도록 시스템을 구성할 수 있습니다. LDAP 인증은 회사가 모든 회사 애플리케이션에 대해 최종 사용자에게 단일 암호를 할당하는 기능을 제공합니다. 이 기능은 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.
- **Cisco** 모바일 및 원격 액세스 클라이언트와 엔드포인트에 대한 디렉터리 서버 사용자 검색— 엔터프라이즈 방화벽 외부에서 작동하는 경우에도 회사 디렉터리 서버를 검색할 수 있습니다. 이 기능을 활성화하면 사용자 데이터 서비스(UDS)가 프록시로 작동하고 사용자 검색 요청을 Unified Communications Manager 데이터베이스로 보내는 대신 회사 디렉터리로 보냅니다.

LDAP 동기화 필수 조건

필수 작업

LDAP 디렉터리에서 최종 사용자를 가져오기 전에 다음 작업을 완료하십시오.

- 사용자 액세스 구성 사용자에게 할당하려는 액세스 제어 그룹을 선택합니다. 대부분의 구축에서는 기본 그룹이면 충분합니다. 역할 및 그룹을 사용자 지정해야 하는 경우, 관리 설명서의 '사용자 액세스 관리' 장을 참조하십시오.
- 새로 프로비저닝된 사용자에게 기본으로 적용되는 인증 정책에 대한 기본 인증서를 구성합니다.
- LDAP 디렉터리에서 사용자를 동기화하고 있는 경우, 사용자의 전화기 및 전화기 내선 번호에 할당하려는 사용자 프로파일, 서비스 프로파일 및 범용 회선 및 디바이스 템플릿 설정을 포함하는 기능 그룹 템플릿을 설정했는지 확인하십시오.

참고 데이터를 시스템과 동기화하려는 사용자의 경우, 활성 디렉터리 서버의 이메일 ID 필드가 고유한 항목인지 또는 공백으로 남겨져 있는지 확인하십시오.

LDAP 동기화 구성 작업 흐름

다음 작업을 사용하여 외부 LDAP 디렉터리에서 사용자 목록을 가져와서 Unified Communications Manager 데이터베이스로 가져올 수 있습니다.

참고 이미 LDAP 디렉터리를 한 번 동기화한 경우 외부 LDAP 디렉터리의 새 항목을 계속 동기화할 수 있지만 Unified Communications Manager의 새 구성을 LDAP 디렉터리 동기화에 추가할 수는 없습니다. 이 경우 사용자 업데이트 또는 사용자 삽입과 같은 벌크 관리 도구 및 메뉴를 사용할 수 있습니다. *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco DirSync 서비스 활성화, 317 페이지	Cisco Unified 서비스 가용성에 로그인하고 Cisco DirSync 서비스를 활성화합니다.
단계 **2**	LDAP 디렉터리 동기화 활성화, 318 페이지	Unified Communications Manager에서 LDAP 디렉터리 동기화를 활성화합니다.
단계 **3**	LDAP 필터 만들기, 318 페이지	선택 사항. Unified Communications Manager가 회사 LDAP 디렉터리의 사용자 하위 집합만 동기화하도록 하려면 LDAP 필터를 만듭니다.
단계 **4**	LDAP 디렉터리 동기화 구성, 319 페이지	필드 설정, LDAP 서버 위치, 동기화 일정 및 액세스 제어 그룹, 기능 그룹 템플릿 및 기본 내선 번호에 대한 할당과 같은 LDAP 디렉터리 동기화 설정을 구성합니다.
단계 **5**	엔터프라이즈 디렉터리 사용자 검색 구성, 321 페이지	선택 사항. 엔터프라이즈 디렉터리 서버 사용자 검색을 위해 시스템을 구성합니다. 이 절차에 따라 데이터베이스 대신 엔터프라이즈 디렉터리 서버에 대한 사용자 검색을 수행하도록 시스템의 전화기 및 클라이언트를 구성하십시오.
단계 **6**	LDAP 인증 구성, 322 페이지	선택 사항. 최종 사용자 암호 인증에 LDAP 디렉터리를 사용하려면 LDAP 인증 설정을 구성합니다.
단계 **7**	LDAP 계약 서비스 매개 변수 사용자 지정, 323 페이지	선택 사항. 선택 사항 LDAP 동기화 서비스 매개 변수를 구성합니다. 대부분의 구축의 경우 기본값으로 충분합니다.

Cisco DirSync 서비스 활성화

이 절차를 수행하여 Cisco Unified 서비스 가용성에서 Cisco DirSync 서비스를 활성화하십시오. 회사 LDAP 디렉터리에서 최종 사용자 설정을 동기화하려면 이 서비스를 활성화하십시오.

프로시저

단계 **1** Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 게시자 노드를 선택합니다.

단계 **3** 디렉터리 서비스 아래에서 **Cisco DirSync** 라디오 버튼을 클릭합니다.

단계 **4** 저장을 클릭합니다.

LDAP 디렉터리 동기화 활성화

회사 LDAP 디렉터리의 최종 사용자 설정을 동기화하기 위해 Unified Communications Manager를 구성하려는 경우, 이 절차를 수행합니다.

참고 이미 LDAP 디렉터리를 한 번 동기화한 경우 외부 LDAP 디렉터리의 새 사용자를 계속 동기화할 수 있지만 Unified Communications Manager의 새 구성을 LDAP 디렉터리 동기화에 추가할 수는 없습니다. 또한 기능 그룹 템플릿 또는 사용자 프로파일과 같은 기본 구성 항목에 편집을 추가할 수도 없습니다. 한 번의 LDAP 동기화를 이미 완료하고 다른 설정을 사용하여 사용자를 추가하려는 경우, 사용자 업데이트 또는 사용자 삽입과 같은 벌크 관리 메뉴를 사용할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 시스템을 선택합니다.

단계 **2** Cisco Unified Communications Manager가 LDAP 디렉터리에서 사용자를 가져오게 하려는 경우, **LDAP** 서버와 동기화 활성화 확인란을 선택합니다.

단계 **3** **LDAP** 서버 유형 드롭다운 목록에서 회사에서 사용하는 LDAP 디렉터리 서버 유형을 선택합니다.

단계 **4** 사용자 **ID**의 **LDAP** 특성 드롭다운 목록에서 Unified Communications Manager가 최종 사용자 설정 창의 사용자 **ID** 필드에 대해 동기화할 회사 LDAP 디렉터리에서 속성을 선택합니다.

단계 **5** 저장을 클릭합니다.

LDAP 필터 만들기

LDAP 디렉터리에서 사용자의 하위 집합으로 LDAP 동기화를 제한하기 위해 LDAP 필터를 만들 수 있습니다. LDAP 디렉터리에 LDAP 필터를 적용하면 Unified Communications Manager는 LDAP 디렉터리에서 필터와 일치하는 사용자만 가져옵니다.

참고 구성하는 모든 LDAP 필터는 RFC4515에 지정된 LDAP 검색 필터 표준을 준수하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 필터를 선택합니다.

단계 **2** 새로 추가를 클릭하여 새 LDAP 필터를 만듭니다.

단계 **3** 필터 이름 텍스트 상자에 LDAP 필터의 이름을 입력합니다.

단계 **4** 필터 텍스트 상자에 필터를 입력합니다. 필터에는 최대 1024자의 UTF-8 문자를 사용할 수 있으며 괄호 ()로 묶어 주어야 합니다.

단계 **5** 저장을 클릭합니다.

LDAP 디렉터리 동기화 구성

이 절차를 사용하여 LDAP 디렉터리와 동기화하도록 Unified Communications Manager를 구성합니다. LDAP 디렉터리 동기화를 사용하면 최종 사용자 데이터를 외부 LDAP 디렉터리에서 Unified Communications Manager 데이터베이스로 가져와 최종 사용자 구성 창에 표시할 수 있습니다. 범용 회선 및 장치 템플릿을 사용 하는 설정 기능 그룹 템플릿이 있는 경우 새로 프로비저닝된 사용자 및 해당 내선 번호에 대한 설정을 자동으로 할당할 수 있습니다.

팁 액세스 제어 그룹 또는 기능 그룹 템플릿을 할당하는 경우 LDAP 필터를 사용하여 동일한 구성 요구 사항을 가진 사용자 그룹으로 가져오기를 제한할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 LDAP 디렉터리를 선택합니다.
- 새로 추가를 클릭하여 새 LDAP 디렉터리를 만듭니다.

단계 **3** **LDAP** 디렉터리 구성에서 다음을 입력합니다.

a) **LDAP** 구성 이름 필드에서 LDAP 디렉터리에 고유한 이름을 할당합니다.

b) **LDAP** 관리자 고유 이름 필드에 LDAP 디렉터리 서버에 액세스할 수 있는 사용자 ID를 입력합니다.

c) 암호 세부 정보를 입력하고 확인합니다.

d) [**LDAP** 사용자 검색 공간] 필드에 검색 공간 세부 정보를 입력합니다.

e) [사용자 사용자에 대한 **LDAP** 사용자 정의 필터] 필드에서 사용자만 또는 사용자 및 그룹 중 하나를 선택합니다.

f) (선택 사항) 가져 오기를 특정 프로파일을 충족하는 사용자의 하위 집합으로만 제한하려는 경우 그룹에 대한 **LDAP** 사용자 정의 필터 드롭다운 목록에서 LDAP 필터를 선택합니다.

단계 **4** **LDAP** 디렉터리 동기화 일정 필드에서 Unified Communications Manager가 데이터를 외부 LDAP 디렉터리와 동기화하는 데 사용하는 일정을 만듭니다.

단계 **5** 동기화할 표준 사용자 필드 섹션을 완성합니다. 각 최종 사용자 필드에 대한 LDAP 특성을 선택합니다. 동기화 프로세스는 Unified Communications Manager의 최종 사용자 필드에 LDAP 특성의 값을 할당합니다.

단계 **6** URI 다이얼을 배포 하는 경우 사용자의 기본 디렉터리 URI 주소에 사용 될 LDAP 특성을 할당 하십시오.

단계 **7** 동기화 할 사용자 정의 사용자 필드 섹션에서 필수 LDAP 특성을 사용하여 사용자 정의 사용자 필드 이름을 입력합니다.

단계 **8** 가져온 최종 사용자를 모든 가져온 최종 사용자에 공통된 액세스 제어 그룹에 할당하려면 다음을 수행하십시오.

a) 액세스 제어 그룹에 추가를 클릭합니다.

b) 팝업 창에서 가져온 최종 사용자에게 할당할 각 액세스 제어 그룹에 해당하는 확인란을 클릭합니다.

c) 선택한 항목 추가를 클릭합니다.

단계 **9** 기능 그룹 템플릿을 할당하려면 기능 그룹 템플릿 드롭다운 목록에서 해당 템플릿을 선택합니다.

참고 최종 사용자는 사용자가 없을 때만 처음으로 할당된 기능 그룹 템플릿과 동기화됩니다. 기존 기능 그룹 템플릿이 수정되고 연결된 LDAP에 대해 전체 동기화가 수행되는 경우 수정 사항이 업데이트되지 않습니다.

단계 **10** 가져온 전화 번호에 마스크를 적용하여 기본 내선 번호를 할당하려면 다음을 수행하십시오.

a) 동기화된 전화 번호에 마스크를 적용하여 삽입된 사용자에 대한 새 회선 만들기 확인란을 선택합니다.

b) 마스크를 입력합니다. 예를 들어, 가져온 전화 번호가 8889945인 경우 11XX의 마스크는 기본 내선 번호 1145를 만듭니다.

단계 **11** 디렉터리 번호 풀에서 기본 내선 번호를 할당하려면 다음을 수행하십시오.

a) 동기화된 **LDAP** 전화 번호를 기준으로 새 회선이 만들어지지 않은 경우 풀 목록에서 새 회선 할당 확인란을 선택합니다.

b) **DN** 풀 시작 및 **DN** 풀 끝 텍스트 상자에 기본 내선 번호를 선택할 수 있는 디렉터리 번호의 범위를 입력합니다.

단계 **12** (선택사항) Jabber 엔드포인트 프로비저닝 섹션에서 Jabber 장치를 생성하려는 경우 다음 드롭다운에서 자동 프로비저닝에 필요한 Jabber 장치 중 하나를 선택합니다:

- Android용 Cisco 이중 모드(BOT)
- iPhone용 Cisco 이중 모드(TCT)
- 태블릿용 Cisco Jabber(TAB)
- Cisco Unified 클라이언트 서비스 프레임워크(CSF)

참고 **LDAP**에 다시 쓰기 옵션을 사용하면 Unified CM에서 선택한 기본 DN을 LDAP 서버에 다시 쓸 수 있습니다. 다시 쓰기에 사용할 수 있는 LDAP 특성은 **telephoneNumber**, **ipPhone** 및 **mobile**입니다.

단계 **13** **LDAP** 서버 정보 섹션에 LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **14** TKS를 사용하여 LDAP 서버에 대한 보안 연결을 생성하려면 **TLS** 사용 확인란을 선택합니다.

참고 Tomcat을 다시 시작한 후 보안 포트를 통해 사용자를 동기화하려고 하면 사용자가 동기화되지 않는 경우가 있습니다. 사용자 동기화가 성공적으로 이루어지려면 Cisco DirSync 서비스를 다시 시작해야 합니다.

단계 **15** 저장을 클릭합니다.

단계 **16** LDAP 동기화를 완료 하려면 지금 전체 동기화 수행을 클릭합니다. 그렇지 않으면 예약된 동기화를 기다릴 수 있습니다.

참고 LDAP에서 사용자를 삭제 하면 24 시간 후에 자동으로 Unified Communications Manager에서 해당 사용자가 제거 됩니다. 뿐만 아니라, 삭제 된 사용자가 다음 장치 중 하나에 대한 이동성 사용자로 구성된 경우 이러한 비활성 장치도 자동으로 삭제 됩니다.

- 원격 대상 프로파일
- 원격 대상 프로파일 템플릿
- 모바일 스마트 클라이언트
- CTI 원격 디바이스
- Spark 원격 디바이스
- Nokia S60
- iPhone용 Cisco 이중 모드
- IMS 통합 모바일(기본)
- 통신사업자 통합 모바일
- Android용 Cisco 이중 모드

엔터프라이즈 디렉터리 사용자 검색 구성

이 절차를 사용하여 데이터베이스 대신 엔터프라이즈 디렉터리 서버에 대한 사용자 검색을 수행하도록 시스템의 전화기 및 클라이언트를 구성하십시오.

시작하기 전에

- LDAP 사용자 검색을 위해 선택하는 1차, 2차 및 3차 서버가 Unified Communications Manager 가입자 노드에 연결할 수 있는 네트워크인지 확인하십시오.
- 시스템 > **LDAP** > **LDAP** 시스템에서 **LDAP** 시스템 설정 창의 **LDAP** 서버 유형 드롭다운 목록에서 LDAP 서버 유형을 설정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 검색을 선택합니다.

단계 **2** 엔터프라이즈 LDAP 디렉터리 서버를 사용하여 사용자 검색을 수행할 수있도록 하려면 엔터프라이즈 디렉터리 서버에 대한 사용자 검색 활성화 확인란을 선택합니다.

단계 **3** **LDAP** 검색 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

참고 OpenLDAP 서버에서 회의실 객체로 표시된 회의실을 검색하려면 사용자 지정 필터를 (objectClass=intOrgPerson)(objectClass=rooms))로 구성합니다. 따라서 Cisco Jabber 클라이언트가 이름으로 회의실을 검색하고 회의실과 연결된 번호로 전화를 걸 수 있습니다.

회의실 객체에 대해 OpenLDAP 서버에 **givenName** or **sn** or **mail** or **displayName** 또는 **telephonenumber** 특성이 구성된 경우 회의실을 검색할 수 있습니다.

LDAP 인증 구성

회사 LDAP 디렉터리에 할당된 암호에 대해 최종 사용자 암호가 인증되도록 LDAP 인증을 활성화하려면 이 절차를 수행하십시오. 이 구성은 최종 사용자 암호에만 적용되며 최종 사용자 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 인증을 선택합니다.

단계 **2** 사용자 인증에 LDAP 디렉터리를 사용하려면 최종 사용자에 대한 **LDAP** 인증 확인란을 선택합니다.

단계 **3** **LDAP** 관리자 고유 이름 필드에 LDAP 디렉터리에 대한 액세스 권한이 있는 LDAP 관리자의 사용자 ID를 입력합니다.

단계 **4** 암호 확인 필드에 LDAP 관리자의 암호를 입력합니다.

단계 **5** [**LDAP** 사용자 검색 기준] 필드에 검색 조건을 입력합니다.

단계 **6** **LDAP** 서버 정보 섹션에 LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **7** TKS를 사용하여 LDAP 서버에 대한 보안 연결을 생성하려면 **TLS** 사용 확인란을 선택합니다.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

LDAP 계약 서비스 매개 변수 사용자 지정, 323 페이지

LDAP 계약 서비스 매개 변수 사용자 지정

LDAP 계약에 대한 시스템 수준 설정을 사용자 지정하는 서비스 파라미터를 구성하려면 이 절차를 수행하십시오. 이러한 서비스 파라미터를 구성하지 않을 경우 Unified Communications Manager는 LDAP 디렉터리 통합에 대한 기본 설정을 적용합니다. 파라미터에 대한 설명을 보려면 사용자 인터페이스에서 파라미터 이름을 클릭합니다.

서비스 파라미터를 사용하여 아래 설정을 사용자 지정할 수 있습니다.

- 계약의 최대 수—기본값은 20입니다.
- 최대 호스트 수—기본값은 3입니다.
- 호스트 장애 발생 시 재시도 지연(초)—호스트 장애의 기본값은 5입니다.
- **HotList** 장애 발생 시 재시도 지연(분)—hostlist 실패의 기본값은 10입니다.
- **LDAP** 연결 시간 초과(초)—기본값은 5입니다.
- 지연된 동기화 시작 시간(분)—기본값은 5입니다.
- 사용자 고객 맵 감사 시간

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 파라미터를 선택합니다.
단계 **2** 서버 드롭다운 목록 상자에서 게시자 노드를 선택합니다.
단계 **3** 서비스 드롭다운 목록 상자에서 **Cisco DirSync**를 선택합니다.
단계 **4** Cisco DirSync 서비스 매개 변수 값을 구성합니다.
단계 **5** 저장을 클릭합니다.

30 장

벌크 관리 도구를 사용하여 사용자 및 디바이스 프로비저닝

벌크 관리 도구 개요

BAT(Bulk Administration Tool)는 웹 기반 애플리케이션으로, Unified Communications Manager 데이터베이스에 벌크 트랜잭션을 수행하는 데 사용할 수 있습니다. BAT를 사용하여 다수의 유사한 전화기, 사용자 또는 포트를 동시에 추가, 업데이트 또는 삭제할 수 있습니다.

참고 [벌크 관리] 메뉴는 Unified Communications Manager 서버의 첫 번째 노드에만 표시됩니다.

Cisco BPS(Bulk Provision Service)는 Cisco Unified CM 관리의 [벌크 관리] 메뉴를 통해 제출되는 모든 작업을 관리 및 유지합니다. Cisco Unified Serviceability에서 이 서비스를 시작할 수 있습니다. Unified Communications Manager의 첫 번째 노드에서만 Cisco BPS를 활성화해야 합니다.

BAT를 사용하여 다음을 수행할 수 있습니다.

- 많은 수의 전화기를 일괄적으로 추가, 업데이트 또는 삭제합니다
- 새 전화기 그룹을 추가할 수 있는 일반 전화기 속성을 정의합니다
- 새 BAT 전화기 템플릿을 생성합니다
- 새 사용자 그룹을 추가하고 사용자를 전화기 및 기타 IP 텔레포니 디바이스에 연결합니다
- BAT 스프레드시트에서 사용자 CSV 데이터 파일을 생성합니다
- 전화기 및 사용자를 일괄적으로 추가하기 위해 CSV 데이터 파일을 생성합니다
- Unified Communications Manager 데이터베이스와 디렉터리에 전화기와 사용자 그룹을 추가합니다

벌크 관리 도구 사전 요건

- 사용자 및 서비스 프로파일 구성

벌크 관리 도구 작업 플로우

프로시저

	명령 또는 동작	목적
단계 **1**	데이터베이스에 전화기 추가, 327 페이지	BAT를 사용하여 Unified Communications Manager 데이터베이스에 전화기 및 다른 IP 텔레포니 디바이스를 대량으로 추가합니다.
단계 **2**	새 BAT 전화 템플릿 생성, 328 페이지	새 BAT 전화 템플릿을 생성할 수 있습니다.
단계 **3**	BAT 스프레드시트를 사용하여 전화기 CSV 데이터 파일 생성, 332 페이지	BAT에 사용하도록 설계된 .xls 스프레드시트를 사용하여 새 전화기 또는 IP 텔레포니 디바이스를 시스템에 추가할 수 있습니다.
단계 **4**	텍스트 편집기를 사용한 사용자 지정 전화기 파일 형식 생성, 335 페이지	텍스트 편집기를 사용하여 텍스트 기반 CSV 데이터 파일의 사용자 지정 전화기 파일 형식을 생성할 수 있습니다.
단계 **5**	Unified Communications Manager에 전화기 삽입, 336 페이지	전화기, Cisco VGC Phone, CTI 포트 또는 H.323 클라이언트를 Cisco Unified Communications Manager 데이터베이스에 추가할 수 있습니다.
단계 **6**	사용자 추가, 338 페이지	BAT를 사용하여 일단의 새 사용자를 추가하고 사용자를 전화기 및 기타 IP 텔레포니 디바이스에 연결할 수 있습니다.
단계 **7**	BAT 스프레드시트에서 사용자 CSV 데이터 파일 생성, 338 페이지	BAT 스프레드시트에서 Unified Communications Manager 데이터베이스에 새 사용자를 추가하기 위한 세부 정보를 제공한 후 CSV 데이터 파일로 변환할 수 있습니다.
단계 **8**	Unified Communications Manager 데이터베이스에 사용자 삽입, 339 페이지	CSV 데이터 파일을 사용하여 Unified Communications Manager 데이터베이스에 사용자 그룹을 추가할 수 있습니다.
단계 **9**	전화기 및 사용자 파일 형식 추가, 341 페이지	텍스트 기반 CSV 데이터 파일로 전화기 및 사용자 파일 형식을 추가할 수 있습니다. CSV 데이터 파일이 생성된 후 파일 형식을 텍스

	명령 또는 동작	목적
		트 기반 CSV 데이터 파일과 연결해야 합니다.
단계 **10**	Unified Communications Manager에 전화기 및 사용자 삽입, 342 페이지	Unified Communications Manager 데이터베이스와 디렉터리에 전화기와 사용자 그룹을 추가할 수 있습니다.

데이터베이스에 전화기 추가

BAT를 사용하여 일괄로 Unified Communications Manager 데이터베이스에 전화기 및 다른 IP 텔레포니 디바이스를 추가할 때 각 회선에 대해 여러 회선, 서비스 및 바로 통화를 추가할 수 있습니다. CTI 포트 및 H.323 클라이언트를 추가할 수도 있습니다.

전화기에 대한 CSV 데이터 파일을 생성하는 두 가지 옵션이 있습니다.

- BAT 스프레드시트(BAT.xlt)를 사용하여 CSV 형식에 데이터를 내보냅니다.
- 텍스트 편집기를 사용하여 CSV 형식으로 텍스트 파일을 만듭니다(숙련된 사용자에게 해당).

프로시저

단계 **1** 일괄 관리 > 전화기 > 전화 템플릿을 선택합니다.

전화 템플릿 찾기 및 나열 창이 표시됩니다.

단계 **2** 전화 템플릿을 삽입하기 위한 CSV 데이터 파일을 생성합니다.

다음 옵션 중 하나를 수행합니다.

a) BAT 스프레드시트를 사용하여 CSV 데이터 파일을 생성합니다.
b) 다음과 같이 텍스트 편집기를 사용하여 CSV 데이터 파일을 생성합니다.

1. 일괄 관리 > 전화기 > 전화기 파일 형식 > 파일 형식 생성을 선택합니다.
2. 텍스트 편집기를 사용하여 사용할 파일 형식을 따르는 전화기에 대한 CSV 데이터 파일을 생성합니다.
3. 텍스트 기반 파일 형식을 CSV 데이터 파일과 연결하려면 일괄 관리 > 전화기 > 전화기 파일 형식 > 파일 형식 추가를 선택합니다.

단계 **3** 일괄 관리 > 전화기 > 전화기 확인을 선택합니다.

단계 **4** 전화기 레코드를 Unified Communications Manager 데이터베이스에 삽입하려면 일괄 관리 > 전화기 > 전화기 삽입을 선택합니다.

새 BAT 전화 템플릿 생성

새 BAT 전화 템플릿을 생성할 수 있습니다. 전화 템플릿을 생성한 후 회선, 서비스, 바로 통화 등을 추가할 수 있습니다.

프로시저

단계 1 일괄 관리 > 전화기 > 전화 템플릿을 선택합니다.

단계 2 새로 추가를 클릭합니다. 새 전화 템플릿 추가 창이 표시됩니다.

단계 3 전화기 유형 드롭다운 목록에서 템플릿을 생성할 전화기 모델을 선택합니다. 다음을 클릭합니다.

단계 4 디바이스 프로토콜 선택 드롭다운 목록에서 디바이스 프로토콜을 선택합니다. 다음을 클릭합니다.

전화 템플릿 구성 창이 선택한 디바이스 유형에 대한 필드 및 기본 항목과 함께 표시됩니다.

단계 5 템플릿 이름 필드에 템플릿의 이름을 입력합니다.

이름에는 최대 50자의 영숫자 문자가 포함될 수 있습니다.

단계 6 [디바이스 정보] 영역에 이 배치에 공통적으로 사용될 전화기 설정을 입력합니다.

일부 전화기 모델 및 디바이스 유형에는 표에 나열된 모든 특성이 없습니다. 모든 특성에 대한 정보는 전화기 모델 설명서를 참조하십시오.

단계 7 이 BAT 전화 템플릿에 대한 모든 설정을 입력한 후 저장을 클릭합니다.

[상태]에 트랜잭션이 완료되었다고 표시되면 회선 특성을 추가할 수 있습니다.

BAT 템플릿에 전화기 회선 추가 또는 업데이트

BAT 템플릿에 하나 이상의 회선을 추가하거나 기존 회선을 업데이트할 수 있습니다. BAT 템플릿에 사용 중인 버튼 템플릿에 따라 추가하거나 업데이트할 수 있는 회선 수가 결정됩니다. 여러 회선이 있는 기본 전화 템플릿을 생성할 수 있습니다. 그런 다음, 표준 템플릿을 사용하여 단일 회선 또는 표준 템플릿에 있는 회선 수까지를 포함하는 전화기를 추가할 수 있습니다. 이 배치의 모든 전화기 또는 사용자 장치 프로파일은 선택한 설정을 사용합니다.

회선 템플릿 값에는 영숫자를 사용하는 것이 좋습니다. 숫자가 지정되는 경우 실제 디렉토리 번호와 충돌할 가능성이 있습니다. 이렇게 하면 그룹 당겨받기 번호 및 통화 지정보류 번호와 같은 기능과의 충돌을 피할 수 있습니다.

BAT 템플릿에 대해 표시되는 최대 회선 수는 모델과 BAT 전화 템플릿을 생성할 때 선택한 단추 템플릿에 따라 다릅니다. 일부 Cisco UnifiedIPPhone 모델의 경우, Cisco UnifiedIPPhone 서비스 및 단축 다이알을 템플릿에 추가할 수도 있습니다.

프로시저

단계 1 회선을 추가하려는 전화 템플릿을 찾습니다.

단계 2 전화 템플릿 설정 창의 연결 정보 영역에서 회선 [1] 새 DN 추가를 클릭합니다.

회선 템플릿 구성 창이 표시됩니다.

단계 3 회선 설정에 대한 적절한 값을 입력하거나 선택합니다.

단계 4 저장을 클릭합니다.

단계 5 추가 회선에 대한 설정을 추가하려면 단계 2, 328 페이지에서 단계 4, 329 페이지까지 반복합니다.

회선 템플릿 설정 창의 상단 오른쪽 모서리에 있는 관련 링크 드롭다운 목록표에서 찾기/목록으로 돌아가기를 선택하면 회선 템플릿 찾기 및 나열 창이 표시됩니다.

a) 기존 회선 템플릿을 찾으려면 적절한 검색 기준을 입력하고 찾기를 클릭합니다.

b) 새 회선 템플릿을 추가하려면 새로 추가를 클릭합니다.

BAT 템플릿에 IP 서비스 추가 또는 업데이트

BAT 템플릿에 이 기능을 바로 포함하는 Cisco Unified IPPhone 모델의 Cisco Unified IPPhone 서비스에 가입할 수 있습니다. 사용자 또는 전화기를 IP 서비스에 일괄 가입하려면 IP 서비스가 일반 서비스 매개 변수를 포함해야 하고 전화 템플릿을 통해 가입되어야 합니다. 고유한 서비스 매개변수가 있는 IP 서비스에 일괄 가입할 수 없습니다. 고유한 매개변수를 사용하는 서비스의 경우 CSV 파일을 사용합니다.

프로시저

단계 1 IP 서비스를 추가하려는 전화 템플릿을 찾습니다.

단계 2 전화 템플릿 설정 창의 연결 정보 영역에서 새 **SURL** 추가를 클릭합니다.
팝업 창이 표시됩니다. 이 창에서 사용 가능한 Cisco Unified IPPhone 서비스에 가입할 수 있습니다.

단계 3 서비스 선택 드롭다운 목록표에서 모든 전화기가 가입될 서비스를 선택합니다. 서비스 설명 상자에 선택한 서비스에 대한 세부 정보가 표시됩니다.

단계 4 다음을 클릭합니다.

단계 5 필요한 경우 서비스 이름 필드의 서비스 이름을 수정합니다.

단계 6 선택된 서비스를 템플릿에 연결하거나 템플릿에 서비스를 더 추가합니다.

a) 이러한 전화기 서비스를 전화 템플릿에 연결하려면 저장을 클릭합니다.

b) 서비스를 더 추가하려면 단계 3, 329 페이지에서 단계 6, 329 페이지까지 반복합니다.

c) 모든 서비스를 템플릿에 추가하려면 업데이트를 클릭합니다.

선택된 템플릿에 대한 서비스 추가 또는 업데이트를 완료한 후 다음 단계를 계속합니다.

단계 7 팝업 창을 닫습니다.

BAT 템플릿에 바로 호출 추가 또는 업데이트

전화기 버튼 템플릿이 바로 통화 버튼을 제공하는 경우 전화기 및 Cisco VGC 전화기의 BAT 템플릿에 바로 통화를 추가하고 업데이트할 수 있습니다. BAT 템플릿에 사용되는 전화기 버튼 템플릿에 따라 사용 가능한 바로 통화 버튼의 수가 결정됩니다.

프로시저

단계 **1** 바로 통화를 추가하려는 전화 템플릿을 찾습니다.

단계 **2** 전화 템플릿 구성 창에서 다음 중 하나를 수행합니다.

a) 연결 정보 영역에서 새 **SD** 추가를 클릭합니다.

b) 창의 상단 오른쪽 모서리에 있는 관련 링크 드롭다운 목록표에서 바로 단축 다이얼 추가/업데이트를 선택합니다.

팝업 창이 표시됩니다. 이 창에서 Cisco Unified IPPhone 및 확장 모듈에 대한 단축 다이얼 버튼을 지정할 수 있습니다.

단계 **3** 단축 다이얼 설정 영역에서 액세스 또는 장거리 코드를 포함한 전화 번호를 번호 필드에 입력합니다.

참고 전화 번호를 입력할 때, 해당되는 경우 전화 번호 다음에 FAC(강제 인증 코드)/CMC(클라이언트 매터 코드)를 입력할 수 있습니다. 전화 번호, FAC, CMC를 순차적으로 입력하거나 쉼표(,)로 구분하여 입력할 수 있습니다. 바로 통화에는 PIN, 암호 또는 통화가 연결된 후 DTMF 숫자로 전송될 다른 숫자가 포함될 수 있습니다. 바로 통화를 통해 연결하는 동안 일시 중지해야 하는 경우 하나 이상의 쉼표(,)를 입력할 수 있습니다. 여기서 각 쉼표는 2초 동안의 일시 중지를 나타냅니다. 통화가 연결되고 쉼표 수에 해당하는 적절한 일시 중지 기간이 입력되면 DTMF 숫자가 전송됩니다.

단계 **4** 레이블 필드에서 바로 통화 번호에 해당하는 레이블을 입력합니다.

단계 **5** 단축 다이얼 설정 영역에서 적용 가능한 IP 전화기 모델에 대한 단축된 바로 통화를 설정할 수 있습니다. 단계 3, 330 페이지를 반복합니다.

단계 **6** 저장을 클릭합니다.
BAT가 템플릿에 바로 호출 설정을 삽입하고 팝업 창이 닫힙니다.

BAT 템플릿에 통화 중 램프 필드 추가 또는 업데이트

전화기 버튼 템플릿이 바로 통화 버튼을 제공하는 경우 전화기 및 Cisco VGC 전화기의 BAT 템플릿에 통화 중 램프 필드 바로 통화를 추가하고 업데이트할 수 있습니다. BAT 템플릿에 사용 중인 전화기 버튼 템플릿에 따라 사용 가능한 BLF SD 버튼의 수가 결정됩니다.

프로시저

단계 **1** 바로 통화를 추가하려는 전화 템플릿을 찾습니다.

단계 **2** 전화 템플릿 구성 창에서 다음 중 하나를 수행합니다.

a) 연결 정보 영역에서 새 **BLF SD** 추가를 클릭합니다.

b) 창의 상단 오른쪽 모서리에 있는 관련 링크 드롭다운 목록에서 통화 중 램프 필드 바로 통화 추가/업데이트를 선택합니다.

팝업 창이 표시됩니다. 이 창에서 Cisco Unified IPPhone 및 확장 모듈에 대한 BLF SD(통화 중 램프 필드 바로 통화) 버튼을 할당할 수 있습니다.

단계 **3** 바로 통화 설정 영역의 대상 필드에 액세스 또는 장거리 코드를 포함하는 대상을 입력합니다.

단계 **4** 드롭다운 목록에서 디렉토리 번호를 선택합니다. 찾기를 클릭하여 디렉토리 번호를 검색할 수 있습니다.

단계 **5** 레이블 필드에서 BLF SD 번호에 해당하는 레이블을 입력합니다.

단계 **6** 저장을 클릭합니다.
BAT가 템플릿에 BLF SD 설정을 삽입하고 팝업 창이 닫힙니다.

BAT 템플릿에 통화 중 램프 필드 직접 통화 지정보류 추가 또는 업데이트

전화기 버튼 템플릿이 바로 통화 버튼을 제공하는 경우 전화기 및 Cisco VGC 전화기의 BAT 템플릿에 BLF(통화 중 램프 필드) 직접 통화 지정보류를 추가하고 업데이트할 수 있습니다. 이 BAT 템플릿에 사용 중인 전화기 버튼 템플릿에 따라 사용 가능한 BLF 직접 통화 지정보류 버튼의 수가 결정됩니다.

프로시저

단계 **1** BLF 단축 직접 통화 지정보류를 추가하려는 전화 템플릿을 찾습니다.

단계 **2** 전화 템플릿 구성 창에서 다음 중 하나를 수행합니다.

a) 연결 정보 영역에서 새 **BLF** 통화 전환 보류 추가를 클릭합니다.

b) 창의 상단 오른쪽 모서리에 있는 관련 링크 드롭다운 목록표에서 **BLF** 통화 전환 보류 추가/업데이트를 선택합니다.

팝업 창이 표시됩니다. 이 창에서 Cisco 통합 IP 전화 및 확장 모듈에 대한 BLF 직접 통화 지정보류 버튼을 지정할 수 있습니다.

단계 **3** 할당되지 않은 통화 중 램프 필드/직접 통화 지정보류 설정 영역의 드롭다운 목록에서 디렉토리 번호를 선택합니다. 찾기를 클릭하여 디렉토리 번호를 검색할 수 있습니다.

단계 **4** 레이블 필드에서 BLF 직접 통화 지정보류 번호에 해당하는 레이블을 입력합니다.

단계 **5** 저장을 클릭합니다.
BAT가 템플릿에 BLF 직접 통화 지정보류 설정을 삽입하고 팝업 창이 닫힙니다.

BAT 템플릿에 인터콤 템플릿 추가 또는 업데이트

하나 이상의 인터컴 템플릿을 BAT 템플릿에 추가하거나 BAT 템플릿의 기존 인터컴 템플릿을 업데이트할 수 있습니다. BAT 템플릿에 사용 중인 해당 버튼 템플릿에 따라 추가하거나 업데이트할 수 있는 회선의 수가 결정됩니다. 여러 회선이 있는 표준 전화 템플릿을 생성할 수 있습니다. 그런 다음, 표준 템플릿을 사용하여 단일 회선 또는 표준 템플릿에 있는 회선 수까지를 포함하는 전화기를 추가할 수 있습니다. 이 배치의 모든 전화기 또는 사용자 장치 프로파일은 인터콤 템플릿에 대해 선택한 설정을 사용합니다.

인터컴 템플릿에는 영숫자를 사용하는 것이 좋습니다. 숫자가 지정되는 경우 실제 디렉토리 번호와 충돌할 가능성이 있습니다. 이렇게 하면 그룹 당겨받기 번호 및 통화 지정보류 번호와 같은 기능과의 충돌을 피할 수 있습니다.

BAT 템플릿에 대해 표시되는 최대 회선 수는 모델과 BAT 전화 템플릿을 생성할 때 선택한 단추 템플릿에 따라 다릅니다. 일부 Cisco UnifiedIPPhone 모델의 경우, Cisco UnifiedIPPhone 서비스 및 단축 다이알을 템플릿에 추가할 수도 있습니다.

프로시저

단계 **1** 인터콤 템플릿을 추가하려는 전화 템플릿을 찾습니다.

단계 **2** 전화 템플릿 구성 창의 연결 정보 영역에서 인터컴 **[1] -** 새 인터컴 추가를 클릭합니다.
인터컴 템플릿 구성 창이 표시됩니다.

단계 **3** 인터컴 템플릿에 설정에 대한 적절한 값을 입력하거나 선택합니다.

단계 **4** 저장을 클릭합니다.
BAT가 인터컴 템플릿을 전화 템플릿 구성에 추가합니다.

단계 **5** 추가 인터컴 템플릿에 대한 설정을 추가하려면 단계 2, 332 페이지에서 단계 4, 332 페이지를 반복합니다.

인터컴 템플릿 설정 창의 상단 오른쪽 모서리에 있는 관련 링크 드롭다운 목록표에서 찾기/목록으로 돌아가기를 선택하면 인터컴 디렉토리 번호 찾기 및 나열 창이 표시됩니다.

참고 인터컴 템플릿 설정 창의 상단 오른쪽 모서리에 있는 관련 링크 드롭다운 목록표에서 찾기/목록으로 돌아가기를 선택하면 인터컴 디렉토리 번호 찾기 및 나열 창이 표시됩니다.

a) 기존 인터컴 디렉토리 번호를 찾으려면 적절한 검색 기준을 입력하고 찾기를 클릭합니다.
b) 새 인터컴 디렉토리 번호를 추가하려면 인터컴 디렉토리 번호 찾기 및 나열 창에서 새로 추가를 클릭합니다.

BAT 스프레드시트를 사용하여 전화기 CSV 데이터 파일 생성

BAT 스프레드시트를 사용하여 CSV 데이터 파일을 생성합니다. 스프레드시트 내에 파일 형식을 정의할 수 있으며 BAT 스프레드시트에서 데이터 파일 형식을 사용하여 CSV 데이터 파일에 대한 필드를 표시합니다.

참고 필드 중 하나에 쉼표를 입력하면 BAT 형식으로 내보낼 때 BAT.xlt가 해당 필드 항목을 큰따옴표로 묶습니다.

BAT 스프레드시트에 공백 행을 입력하면 시스템에서 비어 있는 행을 파일의 끝으로 처리하고 공백 행 다음에 입력한 데이터는 BAT 형식으로 변환하지 않습니다.

CTI 포트를 추가할 때 [더미 MAC 주소] 옵션을 사용할 수 있습니다. 이 옵션은 또는Cisco 통합 커뮤니케이션 매니저 관리 Unified CM 자동 등록 전화기 도구를 사용하여 나중에 수동으로 업데이트할 수 있는 더미 MAC 주소 형식으로 각 CTI 포트에 고유한 디바이스 이름을 제공합니다. H.323 클라이언트, VGC 전화기 또는 VGC 가상 전화기에는 [더미 MAC 주소] 옵션을 사용하지 마십시오.

[더미 MAC 주소] 옵션이 자동으로 다음 형식의 더미 MAC 주소를 생성합니다.

XXXXXXXXXXXX

여기서 X는 12자 길이의 16진수(0~9 및 A~F)를 나타냅니다.

주의 BAT 스프레드시트에서 전화기에 대해 정의한 회선 및 바로 통화 수가 BAT 전화 템플릿에 정의된 수를 초과해서는 안 됩니다. 그렇지 않으면 CSV 데이터 파일 및 BAT 템플릿을 삽입하려고 시도할 때 오류가 발생합니다.

BAT 스프레드시트에서 모든 필드의 편집을 완료한 후 내용을 CSV 형식의 데이터 파일로 내보낼 수 있습니다. 내보낸 CSV 형식의 데이터 파일에 다음과 같은 기본 파일 이름이 할당됩니다.

`<tabname>-<timestamp>.txt`

여기서 `<tabname>`은 생성한 입력 파일의 유형(예: 전화기)을 나타내고 `<timestamp>`는 파일이 생성된 정확한 날짜 및 시간을 나타냅니다.

내보낸 파일을 로컬 워크스테이션에 저장한 후 CSV 형식 데이터 파일의 이름을 바꿀 수 있습니다.

참고 쉼표가 포함된 CSV 파일 이름(예: abcd,e.txt)을 서버에 업로드할 수 없습니다Unified Communications Manager.

프로시저

단계 **1** BAT 스프레드시트를 열려면 BAT.xlt 파일을 찾아서 두 번 클릭합니다.

단계 **2** 메시지가 표시될 때 스프레드시트 기능을 사용하려면 매크로 사용을 클릭합니다.

단계 **3** 전화기 옵션을 표시하려면 스프레드시트의 아래쪽에 있는 전화기 탭을 클릭합니다.

단계 **4** 다음 디바이스 유형 중 하나에 대한 라디오 버튼을 선택합니다.

선택하는 디바이스 유형에 따라 BAT 스프레드시트의 데이터에 대한 확인 기준이 결정됩니다.

- 전화기
- CTI 포트
- H.323 Client
- VGC 전화기
- VGC 가상 전화기
- Cisco IP Communicator Phone

스프레드시트에 선택한 디바이스에 사용 가능한 옵션이 표시됩니다. 예를 들어, 전화기를 선택하면 전화기 회선 수 및 바로 통화 수에 대한 필드가 표시됩니다.

단계 **5** BAT 스프레드시트에 표시할 각 전화기에 대한 디바이스 및 회선 필드를 선택합니다. 다음을 수행하십시오.

a) 파일 형식 생성을 클릭합니다.
b) 디바이스 필드를 선택하려면 디바이스 필드 상자에서 디바이스 필드 이름을 클릭한 후 화살표를 클릭하여 필드를 선택한 디바이스 필드 상자로 이동합니다.

   CSV 데이터 파일에 **MAC** 주소/디바이스 이름 및 설명이 포함되어야 하므로 이러한 필드는 항상 선택되어 있습니다.

   팁 목록에서 항목의 범위를 선택하려면 **Shift** 키를 누른 채로 선택합니다. 랜덤 필드 이름을 선택하려면 **Ctrl** 키를 누른 채로 필드 이름을 클릭합니다.

c) 회선 필드 상자에서 회선 필드 이름을 클릭하고 화살표를 클릭하여 필드를 선택한 회선 필드 상자로 이동합니다.

   팁 선택한 회선 및 디바이스 상자의 항목 순서를 변경하려면 항목을 선택하고 위쪽 및 아래쪽 화살표를 사용하여 목록에서 필드를 위로 또는 아래로 이동합니다.

d) 기존 CSV 형식을 덮어쓸지 여부를 묻는 메시지가 표시됩니다. CSV 데이터 파일 형식을 수정하려면 생성을 클릭합니다.
e) 확인을 클릭합니다.
   선택한 필드에 대한 새 열이 지정한 순서대로 BAT 스프레드시트에 표시됩니다.

단계 **6** 오른쪽으로 스크롤하여 전화기 회선 수 상자를 찾고 전화기의 회선 수를 입력합니다.

참고 입력하는 회선 수가 BAT 템플릿에 구성된 회선 수를 초과해서는 안 됩니다.

단계 **7** 전화기의 경우 최대 바로 통화 수 상자에 바로 통화 버튼의 수를 입력해야 합니다.

참고 입력하는 바로 통화 수가 BAT 템플릿에 구성된 바로 통화 수를 초과해서는 안 됩니다.

이 수를 입력하면 각 바로 호출 번호에 대한 열이 표시됩니다.

단계 **8** 최대 **BLF** 바로 통화 수 상자에 BLF(통화 중 램프 필드) 바로 통화 버튼의 수를 입력합니다.
이 수를 입력하면 각 BLF 바로 통화 번호에 대한 열이 표시됩니다.

단계 **9** 스프레드시트의 각 행에 개별 전화기의 데이터를 입력합니다.

모든 필수 필드와 관련된 선택적 필드를 완료합니다. 각 열 제목에는 필드의 길이와 필드가 필수 또는 선택 사항인지가 지정됩니다. 전화기 필드 설명은 온라인 도움말을 참조하십시오.

단계 **10** 각 전화기의 MAC 주소를 입력하지 않은 경우 더미 **MAC** 주소 생성 확인란에 체크 표시합니다.

주의 H.323 클라이언트, VGC 전화기 또는 VGC 가상 전화기에는 [더미 MAC 주소] 옵션을 사용하지 마십시오.

단계 **11** BAT Excel 스프레드시트의 데이터를 CSV 형식의 데이터 파일로 전환하려면 **BAT** 형식으로 내보내기를 클릭합니다.

팁 내보낸 CSV 데이터 파일을 읽는 방법에 대한 자세한 내용을 보려면 BAT의 전화기 삽입 창에서 샘플 파일 보기 링크를 클릭합니다.

시스템에서 기본 파일명 <tabname>-<timestamp>.txt를 사용하여 로컬 워크스테이션의 선택한 폴더에 파일을 저장합니다.

텍스트 편집기를 사용한 사용자 지정 전화기 파일 형식 생성

텍스트 편집기를 사용하여 텍스트 기반 CSV 데이터 파일의 사용자 지정 전화기 파일 형식을 생성할 수 있습니다.

프로시저

단계 **1** 일괄 관리 > 전화기 > 전화기 파일 형식 > 파일 형식 생성을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 형식 이름 필드에 이 사용자 정의 형식의 이름을 입력합니다.

단계 **4** 사용자 지정 파일 형식에 표시될 필드를 선택합니다. 다음을 수행하십시오.

a) 디바이스 필드를 선택하려면 디바이스 필드 상자에서 디바이스 필드 이름을 클릭한 후 화살표를 클릭하여 필드를 선택한 디바이스 필드 상자로 이동합니다.

CSV 데이터 파일에 **MAC** 주소/디바이스 이름 및 설명이 포함되어야 하므로 이러한 필드는 항상 선택되어 있습니다.

팁 목록에서 항목의 범위를 선택하려면 **Shift** 키를 누른 채로 선택합니다. 랜덤 필드 이름을 선택하려면 **Ctrl** 키를 누른 채로 필드 이름을 클릭합니다.

b) 회선 필드 상자에서 회선 필드 이름을 클릭하고 화살표를 클릭하여 필드를 선택한 회선 필드 상자로 이동합니다.

c) 인터컴 **DN** 필드 상자에서 인터컴 DN 필드 이름을 클릭하고 화살표를 클릭하여 필드를 선택한 인터컴 **DN** 필드 순서 상자로 이동합니다.

팁 선택한 회선 필드, 선택한 디바이스 필드 및 선택한 인터컴 **DN** 필드 순서 상자의 항목 순서를 변경할 수 있습니다. 항목을 선택하고 위쪽 및 아래쪽 화살표를 사용하여 목록에서 필드를 위로 또는 아래로 이동합니다.

단계 **5** **IP** 전화 서비스 최대값 영역에 다음 필드의 최대값을 입력합니다.

- 최대 바로 통화 수
- 최대 BLF 바로 통화 수
- 최대 BLF 직접 통화 지정보류 수
- 최대 IP 전화 서비스 수
- 최대 IP 전화 서비스 매개변수 수

단계 **6** 저장을 클릭합니다.

사용자 정의 파일 형식의 이름이 전화기 파일 형식 찾기 및 나열 창의 파일 형식 이름 목록에 표시됩니다.

Unified Communications Manager에 전화기 삽입

Unified Communications Manager 데이터베이스에 전화기 레코드를 삽입할 때 대상 CSV 데이터 파일을 정의하고 전화기 레코드가 삽입되는 방법을 정의합니다. 아래 나열된 작업 중 하나 이상을 수행하여 기존 전화기 레코드를 덮어쓰거나, 업로드 중에 레코드를 삽입할 수 있습니다.

- 기존 모든 단축 다이얼을 삭제한 후 새 단축 다이얼을 추가해야 합니다.
- 기존 모든 단축 다이얼을 삭제한 후 새 단축 다이얼을 추가해야 합니다.
- 새로운 BLF 직접 통화 지정보류를 추가하기 전에 기존 모든 BLF 직접 통화 지정보류를 삭제해야 합니다.
- 새 서비스를 추가하기 전에 기존에 가입한 모든 서비스를 삭제해야 합니다.

참고 전화기 레코드의 유효성이 확인되어야 삽입할 수 있습니다.

참고 BAT에는 [디렉토리 번호 URI] 필드에 다음과 같은 형식으로 디렉토리 번호를 입력해야 합니다.

디렉토리 번호 1에 URI 1, 디렉토리 번호 1에 URI 1 라우트 파티션(URI 1은 디렉토리 번호 1의 기본 번호)

더미 MAC 주소 옵션을 사용할 수 있습니다. CTI 포트를 추가할 때 이 옵션은 Cisco 통합 커뮤니케이션 매니저 관리 또는 Unified CM 자동 등록 전화기 도구를 사용하여 나중에 수동으로 업데이트할 수 있는 더미 MAC 주소 형식으로 각 CTI 포트에 고유한 디바이스 이름을 제공합니다. H.323 클라이언트, VGC 전화기 또는 VGC 가상 전화기에는 [더미 MAC 주소] 옵션을 사용하지 마십시오.

[더미 MAC 주소] 옵션이 자동으로 다음 형식의 더미 MAC 주소를 생성합니다.

XXXXXXXXXXXX

여기서 X는 12자 길이의 16진수(0~9 및 A~F)를 나타냅니다.

시작하기 전에

- 추가하려는 디바이스에 사용할 수 있는 Unified Communications Manager 일괄 관리(BAT) 전화 템플릿이 있어야 합니다. 데이터 파일 업로드 대상과 방법을 선택할 수 있습니다. 전화기 레코드의 유효성이 확인되어야 삽입할 수 있습니다.
- 전화기 또는 다른 IP 텔레포니 장치에 대한 고유한 세부 정보를 포함하는 CSV(쉼표로 구분된 값) 형식의 데이터 파일이 있어야 합니다.

프로시저

단계 **1** 일괄 관리 > 전화기 > 전화기 삽입을 선택합니다.

단계 **2** 업로드하려는 전화기 레코드의 파일 형식 유형을 지정합니다.

a) 사용자 지정된 파일 형식을 사용하는 전화기 레코드를 삽입하려면 전화 삽입 특정 세부 정보 라디오 버튼을 클릭하고 단계 3, 337 페이지 및 단계 5, 337 페이지를 계속 진행합니다.

b) 모든 세부 정보 옵션을 사용하여 생성된 내보낸 전화기 파일에서 전화기 레코드를 삽입하려면 전화 삽입 모든 세부 정보 라디오 버튼을 클릭합니다.

단계 **3** 파일 이름 드롭다운 목록표에서 특정 일괄 트랜잭션에 대해 생성한 CSV 데이터 파일을 선택합니다. 그런 다음 선택한 사용자 지정 파일로 전화기를 업데이트할 수 있도록 사용자 지정 파일로 전화 업데이트 허용 확인란에 체크 표시합니다.

단계 **4** 삽입할 파일에 포함되어 있는 정보로 기존 전화기 설정을 덮어쓰려면 기존 구성 무시 확인란에 체크 표시합니다. 그런 다음, 업로드 중에 수행할 업로드 작업 옆의 확인란에 체크 표시합니다.

기존 구성 무시 확인란에 체크 표시하면 다음과 같은 업로드 작업을 선택할 수 있습니다.

- 기존 모든 단축 다이얼을 삭제한 후 새 단축 다이얼을 추가해야 합니다.
- 기존 모든 단축 다이얼을 삭제한 후 새 단축 다이얼을 추가해야 합니다.
- 새로운 BLF 직접 통화 지정보류를 추가하기 전에 기존 모든 BLF 직접 통화 지정보류를 삭제해야 합니다.
- 새 서비스를 추가하기 전에 기존에 가입한 모든 서비스를 삭제해야 합니다.

참고 업로드가 진행되는 동안 이 레코드를 CSV 데이터 파일의 기존 레코드에 추가하려면 해당 확인란에 체크 표시하지 않은 상태로 둡니다.

단계 **5** 특정 세부 정보 옵션의 경우, 전화 템플릿 이름 드롭다운 목록에서 이 유형의 일괄 트랜잭션에 대해 생성한 BAT 전화 템플릿을 선택합니다.

주의 CSV 데이터 파일에 개별 MAC 주소를 입력하지 않은 경우에는 더미 **MAC** 주소 생성 확인란을 선택해야 합니다. 이 정보는 나중에 수동으로 업데이트할 수 있습니다. 단계 8, 337 페이지로 건너뜁니다. 데이터 입력 파일에 MAC 주소 또는 장치 이름을 입력한 경우에는 이 옵션을 선택하지 마십시오.

사용자에게 할당된 전화기의 MAC 주소를 모르는 경우에는 이 옵션을 선택합니다. 전화기가 연결되면 MAC 주소가 해당 장치에 등록됩니다.

단계 **6** 작업 정보 영역에 작업 설명을 입력합니다.

단계 **7** 삽입 방법을 선택합니다. 다음 중 하나를 수행합니다.

a) 즉시 전화기 레코드를 삽입하려면 즉시 실행을 클릭합니다.

b) 나중에 전화기 레코드를 삽입하려면 나중에 실행을 클릭합니다.

단계 **8** 전화기 레코드 삽입 작업을 만들려면 제출을 클릭합니다.

작업 구성 창을 사용하여 이 작업을 예약하거나 이 작업을 활성화합니다.

다음에 수행할 작업

삽입된 전화기의 유형이 Cisco Unified Mobile Communicator인 경우에는 삽입 작업이 완료된 후에 디바이스를 다시 설정해야 합니다. 벌크 관리 > 전화기 > 전화 재설정/재시작 옵션을 사용하여 전화기를 다시 설정할 수 있습니다.

사용자 추가

BAT 스프레드시트를 사용하여 일괄로 Unified Communications Manager 데이터베이스에 새 사용자를 추가하려면 CSV 데이터 파일을 생성해야 합니다. Cisco IP SoftPhone과 같이 CTI 포트가 필요한 애플리케이션을 가진 사용자의 경우, BAT가 CTI 포트를 기존 사용자와 연결할 수 있습니다.

프로시저

단계 **1** 추가할 각 사용자의 개별 값을 정의하기 위한 CSV(쉼표로 구분된 값) 데이터 파일을 생성합니다.

단계 **2** BAT를 사용하여 사용자를 Unified Communications Manager 데이터베이스에 삽입합니다.

BAT 스프레드시트에서 사용자 CSV 데이터 파일 생성

BAT 스프레드시트에서 Unified Communications Manager 데이터베이스에 새 사용자를 추가하기 위한 세부 정보를 제공한 후 CSV 데이터 파일로 변환할 수 있습니다.

참고 BAT 스프레드시트에 공백 행을 입력하면 시스템에서 비어 있는 행을 파일의 끝으로 처리하고 공백 행 다음에 입력한 데이터는 BAT 형식으로 변환하지 않습니다.

BAT 스프레드시트에서 사용자를 추가하기 위한 필드 편집을 완료한 후 내용을 CSV 형식의 데이터 파일로 내보낼 수 있습니다. 내보낸 CSV 형식의 데이터 파일에 다음과 같은 기본 파일 이름이 할당됩니다.

```
<tabname>-<timestamp>.txt
```

여기서 <tabname>은 생성한 입력 파일의 유형(예: 전화기)을 나타내고 <timestamp>는 파일이 생성된 정확한 날짜 및 시간을 나타냅니다.

내보낸 파일을 로컬 워크스테이션에 저장한 후 CSV 형식 데이터 파일의 이름을 바꿀 수 있습니다. 필드 중 하나에 쉼표를 입력하면 BAT 형식으로 내보낼 때 BAT.xlt가 해당 필드 항목을 큰따옴표로 묶습니다.

참고 쉼표가 포함된 CSV 파일 이름(예: abcd,e.txt)을 Unified Communications Manager 서버에 업로드할 수 없습니다.

프로시저

단계 **1** BAT 스프레드시트를 열려면 BAT.xlt 파일을 찾아서 두 번 클릭합니다.

단계 **2** 메시지가 표시될 때 스프레드시트 기능을 사용하려면 매크로 사용을 클릭합니다.

단계 **3** 사용자를 추가하려면 스프레드시트의 아래쪽에 있는 사용자 탭을 클릭합니다.

단계 **4** 모든 필수 필드와 관련된 선택적 필드를 완료합니다. 각 열 제목에는 필드의 길이와 필드가 필수 또는 선택 사항인지가 지정됩니다.

각 행에서 온라인 도움말 파일에 설명된 대로 정보를 입력합니다.

- 사용자에게 여러 디바이스가 있는 경우 디바이스마다 한 번씩 [디바이스 이름] 필드가 반복되어야 합니다.
- 새 사용자와 연결될 추가 디바이스 이름을 입력하려면 제어된 디바이스 수 텍스트 상자에 값을 입력합니다.

참고 CTI 포트, ATA 포트 및 H.323 클라이언트를 포함한 모든 디바이스를 사용자와 연결할 수 있습니다.

단계 **5** 새 사용자와 연결될 추가 디바이스 이름을 입력하려면 제어된 디바이스 수 텍스트 상자에 값을 입력합니다.

단계 **6** BAT Excel 스프레드시트의 데이터를 CSV 형식의 데이터 파일로 전환하려면 **BAT** 형식으로 내보내기를 클릭합니다.

시스템에서 기본 파일명 <tabname>-<timestamp>.txt를 사용하여 C:\XLSDataFiles에 파일을 저장합니다. 또는 찾아보기를 사용하여 다른 기존 폴더에 파일을 저장합니다.

팁 내보낸 CSV 데이터 파일을 읽는 방법에 대한 자세한 내용을 보려면 BAT의 사용자 삽입 창에서 샘플 파일 보기 링크를 클릭합니다.

다음에 수행할 작업

BAT에서 데이터 파일에 액세스할 수 있도록 CSV 데이터 파일을 Unified Communications Manager 데이터베이스 서버의 첫 번째 노드에 업로드해야 합니다.

Unified Communications Manager 데이터베이스에 사용자 삽입

CSV 데이터 파일을 사용하여 Unified Communications Manager 데이터베이스에 사용자 그룹을 추가할 수 있습니다. 사용자 삽입을 위해 CSV 파일에서 입력하는 필드 값은 사용자 템플릿에 제공된 값을 덮어씁니다.

주의 자격 증명 정책에 “단순 암호 확인”이 활성화되어 있고 사용자 템플릿의 암호가 사용자 ID일 경우, 해당 사용자 ID가 단순 암호에 필요한 기준을 만족하지 못하면 BAT를 통해 사용자를 삽입하는 작업에 실패할 수 있습니다.

제어된 디바이스 선택에서 디바이스를 선택하지 않고 기본 내선 번호를 구성하여 BAT를 통해 사용자를 삽입할 수 있습니다. 이렇게 하려면 BAT를 사용하여 사용자를 삽입하기 전에 Unified Communications Manager에 DN이 미리 채워져 있어야 합니다. 다음 단계에서는 DN 미리 채우기 과정에 대해 간단하게 설명합니다.

1. DN 페이지에서 사용자의 기본 내선 번호에 연결되는 DN 범위를 만듭니다.
2. 기본 내선 번호가 구성된 BAT 템플릿을 만듭니다(동일한 DN이 미리 채워져 있어야 함).
3. 다음 절차에 따라 BAT를 사용하여 사용자를 삽입합니다.

시작하기 전에

UTF-8 인코딩 형식으로 저장되어 있고 사용자 이름, 제어된 디바이스 이름, 디렉토리 번호가 포함된 CSV 데이터 파일이 있어야 합니다. 다음 방법 중 하나로 CSV 데이터 파일을 만들 수 있습니다.

- CSV 형식으로 변환되는 BAT 스프레드시트 사용
- 사용자 데이터의 내보내기 파일을 생성하는 내보내기 유틸리티 사용

참고 내보낸 BAT 파일을 사용하여 사용자를 삽입하려고 하면 둘 이상의 파일에서 일부 내보낸 사용자에 대해 “사용자 ID가 이미 프레즌스합니다”라는 오류 메시지가 표시됩니다. 예를 들어, 첫 번째 회선 관리자 목록과 사용자 목록 둘 다에 동일한 관리자 사용자 ID가 있을 수 있습니다.

프로시저

단계 **1** 일괄 관리 > 사용자 > 사용자 삽입을 선택합니다.

단계 **2** 파일 이름 필드에서 이 일괄 트랜잭션에 대해 생성한 CSV 데이터 파일을 선택합니다.

단계 **3** 내보내기 유틸리티를 사용하여 CSV 데이터 파일을 만든 경우에는 사용자 내보내기로 생성된 파일 확인란에 체크 표시합니다.

단계 **4** 사용자 템플릿 이름 드롭다운 목록에서 이 삽입 작업에 사용할 사용자 템플릿을 선택합니다.

참고 Unified Communications Manager 데이터베이스에 사용자 프로필, 제어된 디바이스 이름, 디렉토리 번호가 있어야 합니다. 제어된 디바이스의 전체 이름이 입력되어 있어야 합니다. 디바이스 이름에 MAC 주소만 포함되어 있는 경우에는 BAT가 프레즌스하지 않는 디바이스 오류 메시지를 표시합니다.

단계 **5** 작업 정보 영역에 작업 설명을 입력합니다.

단계 **6** 삽입 방법을 선택합니다. 다음 중 하나를 수행합니다.

a) 사용자 레코드를 즉시 삽입하려면 즉시 실행을 클릭합니다.
b) 사용자 레코드를 나중에 삽입하려면 나중에 실행을 클릭합니다.

단계 **7** 사용자 레코드 삽입 작업을 만들려면 제출을 클릭합니다.
이 작업을 예약하거나활성화하려면 벌크 관리 주 메뉴의 [작업 스케줄러] 옵션을 사용합니다.

BAT 스프레드시트를 사용하여 전화기 및 사용자 추가

전화기 및 사용자를 일괄로 추가하기 위한 CSV 데이터 파일을 생성합니다.

프로시저

단계 **1** BAT 스프레드시트를 열려면 BAT.xlt 파일을 찾아서 두 번 클릭합니다.
BAT.xlt 파일을 다운로드할 수 있습니다.

단계 **2** 메시지가 표시될 때 스프레드시트 기능을 사용하려면 매크로 사용을 클릭합니다.

단계 **3** 스프레드시트의 아래쪽에 있는 전화기-사용자 탭을 클릭합니다.

단계 **4** BAT 스프레드시트를 사용하여 전화기 CSV 데이터 파일 생성, 332 페이지의 4~10단계에 따릅니다.

전화기 및 사용자 파일 형식 추가

텍스트 기반 CSV 데이터 파일로 전화기 및 사용자 파일 형식을 추가할 수 있습니다. CSV 데이터 파일이 생성된 후 파일 형식을 텍스트 기반 CSV 데이터 파일과 연결해야 합니다. 파일 형식을 CSV 파일과 연결한 후 각 필드의 이름이 CSV 데이터 파일의 첫 번째 레코드로 표시됩니다. 이 정보를 사용하여 각 필드의 값을 올바른 순서로 입력했는지 확인할 수 있습니다.

시작하기 전에

업데이트할 각 사용자의 개별 값을 정의하는 CSV 데이터 파일을 생성해야 합니다.

텍스트 편집기를 사용하여 CSV 데이터 파일을 생성한 경우 텍스트 기반 파일에 값을 입력하기 위한 파일 형식이 생성됩니다. 파일 형식에 지정된 순서대로 텍스트 파일에 값을 입력합니다.

프로시저

단계 **1** 일괄 관리 > 전화기 및 사용자 > 전화기 및 사용자 파일 형식 > 파일 형식 할당을 선택합니다.
파일 형식 추가 구성 창이 표시됩니다.

단계 **2** 파일 이름 필드에서 이 트랜잭션에 대해 생성한 텍스트 기반 CSV 파일을 선택합니다.

단계 **3** 형식 파일 이름 필드에서 이 유형의 일괄 트랜잭션에 대해 생성한 파일 형식을 선택합니다.

단계 **4** 일치하는 파일 형식을 CSV 데이터 파일과 연결하기 위한 작업을 생성하려면 제출을 클릭합니다.

단계 **5** 이 작업을 예약하거나 활성화하려면 일괄 관리 주 메뉴의 작업 스케줄러 옵션을 사용합니다.

참고 파일 형식을 추가할 때 사용자 필드가 자동으로 추가됩니다.

Unified Communications Manager에 전화기 및 사용자 삽입

Unified Communications Manager 데이터베이스와 디렉토리에 전화기와 사용자 그룹을 추가할 수 있습니다.

참고 전화기 레코드의 유효성이 확인되어야 삽입할 수 있습니다.

더미 MAC 주소 옵션을 사용할 수 있습니다. CTI 포트를 추가할 때 이 옵션은 Cisco 통합 커뮤니케이션 매니저 관리 또는 UnifiedCM 자동 등록 전화기 도구를 사용하여 나중에 수동으로 업데이트할 수 있는 더미 MAC 주소 형식으로 각 CTI 포트에 고유한 디바이스 이름을 제공합니다. H.323 클라이언트, VGC 전화기 또는 VGC 가상 전화기에는 [더미 MAC 주소] 옵션을 사용하지 마십시오.

[더미 MAC 주소] 옵션이 자동으로 다음 형식의 더미 MAC 주소를 생성합니다.

XXXXXXXXXXXX

여기서 X는 12자 길이의 16진수(0~9 및 A~F)를 나타냅니다.

시작하기 전에

1. CSV(쉼표로 구분된 값) 데이터 파일을 만들어 사용자와 함께 삽입할 각 전화기의 개별 값을 정의합니다. BAT 스프레드시트(BAT.xlt)를 사용하여 CSV 데이터 파일을 만들어 전화기 및 사용자를 추가하거나, CSV 형식으로 사용자 지정 텍스트 파일을 만들어 전화기 및 사용자 조합을 추가할 수 있습니다.
2. 파일 형식을 CSV 데이터 파일과 연결합니다.
3. 전화기 및 사용자 레코드의 유효성을 확인합니다.

프로시저

단계 **1** 일괄 관리 > 전화기 및 사용자 > 전화기 및 사용자 삽입을 선택합니다.

단계 **2** 파일 이름 필드에서 이 일괄 트랜잭션에 대해 생성한 CSV 데이터 파일을 선택합니다.

단계 **3** 전화 템플릿 이름 필드에서 이 트랜잭션에 사용한 BAT 전화 템플릿을 선택합니다.

주의 CSV 데이터 파일에 개별 MAC 주소를 입력하지 않은 경우에는 더미 **MAC** 주소 생성 확인란을 선택해야 합니다. 이 정보는 나중에 수동으로 업데이트할 수 있습니다. 데이터 입력 파일에 MAC 주소 또는 장치 이름을 입력한 경우에는 이 옵션을 선택하지 마십시오.

사용자에게 할당된 전화기의 MAC 주소를 모르는 경우에는 이 옵션을 선택합니다. 전화기가 연결되면 MAC 주소가 해당 장치에 등록됩니다.

단계 **4** 사용자 템플릿 이름 필드에서 이 트랜잭션에 사용한 BAT 사용자 템플릿을 선택합니다.

단계 **5** 작업 정보 영역에 작업 설명을 입력합니다.

단계 **6** 삽입 방법을 선택합니다. 다음 중 하나를 수행합니다.

a) 전화기 및 사용자를 즉시 삽입하려면 즉시 실행을 클릭합니다.

b) 전화기 및 사용자를 나중에 삽입하려면 나중에 실행을 클릭합니다.

단계 **7** 전화기 및 사용자 레코드 삽입 작업을 만들려면 제출을 클릭합니다.

이 작업을 예약 및 활성화하려면 벌크 관리 주 메뉴의 [작업 스케줄러] 옵션을 사용합니다.

V 부

프로비저닝 엔드포인트

31 장

엔드포인트 구성

엔드포인트 프로비저닝 기본값

이 파트의 정보를 사용하여 엔드포인트 디바이스와 사용자를 엔드포인트에 연결하는 방법을 구성합니다.

Unified Communications Manager에는 엔드포인트를 추가하기 전에 프로비저닝할 수 있는 디바이스 기본값 세트가 포함되어 있습니다. 이러한 디바이스 기본 설정을 미리 설정하면, 새 사용자와 디바이스를 언제 프로비저닝할 것인지가 적용된 설정에 따라 자동으로 구성됩니다.

다음은 엔드포인트 프로비저닝에 대한 두 개의 기본 구성입니다.

- 디바이스 기본값 구성
- 엔터프라이즈 전화기 설정 구성

엔드포인트 프로비저닝 기본값 사전 요건

엔드포인트 등록을 위해 구성된 포트를 확인합니다. Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM**로 이동하여 서버를 선택하고 구성된 포트 설정을 확인합니다.

참고 대부분의 경우 기본 설정에서 포트를 변경할 필요가 없습니다.

엔드포인트 프로비저닝 기본값 작업 플로우

다음 작업 플로우를 완료하여 시스템에 대한 디바이스를 구성합니다.

프로시저

	명령 또는 동작	목적
단계 1	디바이스 기본값 구성, 348 페이지	Unified Communications Manager 노드를 통해 자동 등록되는 디바이스에 적용되는 기본 설정을 변경할 수 있습니다. 각 디바이스 유형에는 특정한 기본값 세트가 있습니다.
단계 2	디바이스 프로파일 구성, 351 페이지	선택 사항. 특정 사용자를 위해 특정 디바이스와 연결하는 속성 세트로 구성된 디바이스 프로파일을 구성할 수 있습니다.
단계 3	기본 디바이스 프로파일 구성, 349 페이지	사용자가 사용자 디바이스 프로파일이 없는 전화기에 로그인할 때마다 전화기에 적용되는 기본 디바이스 프로파일을 구성할 수 있습니다.
단계 4	기본 디바이스 프로파일에 대한 소프트 키 템플릿 구성, 350 페이지	선택 사항. 기본 디바이스 프로파일을 소프트 키 템플릿에 추가할 수 있습니다.
단계 5	엔터프라이즈 전화기 구성, 352 페이지	같은 클러스터의 모든 전화기에 적용되는 기본 엔터프라이즈 전화기 설정을 구성할 수 있습니다.

디바이스 기본값 구성

디바이스 기본값 설정 업데이트

이 절차를 사용하여 기본 펌웨어 로드, 기본 디바이스 풀, 소프트키 템플릿 및 재등록 방법: 자동 등록 또는 활성화 코드를 할당할 수 있도록 허용하는 디바이스 기본 설정을 구성합니다.

시작하기 전에

시스템에 적용되는 다음 작업을 모두 수행한 후에 디바이스 기본 설정을 업데이트해야 합니다.

- 디바이스에 대한 새 펌웨어 파일을 TFTP 서버에 추가합니다.
- 디바이스 기본값을 사용하여 디렉터리에 존재하지 않는 펌웨어 로드를 할당하면 해당 디바이스에서 할당된 펌웨어를 로드할 수 없습니다.

- 새 디바이스 풀을 구성합니다. 디바이스가 전화기인 경우 새 전화기 템플릿을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 디바이스 기본값을 선택합니다.

단계 **2** 디바이스 기본값 설정 창에서 업데이트하려는 디바이스 유형에 해당하는 설정을 수정한 다음, 저장을 클릭합니다. 필드 설명은 온라인 도움말을 참조하십시오.

- 로드 정보
- 디바이스풀
- 전화 템플릿

단계 **3** 디바이스 이름 좌측에 표시된 재설정 아이콘을 클릭하여 그런 유형의 모든 디바이스를 재설정하고, 클러스터의 모든 노드에서 그런 유형의 모든 디바이스에 새 기본값을 로드합니다.

모든 디바이스를 재설정하지 않을 경우, 노드에서 자동 등록되는 새로운 디바이스만 업데이트된 기본값으로 설정됩니다.

기본 디바이스 프로파일 구성

전화기는 사용자가 사용자 디바이스 프로파일이 없는 전화기에 로그인할 때마다 기본 디바이스 프로파일을 적용합니다.

기본 디바이스 프로파일에는 디바이스 유형(전화기), 사용자 로캘, 전화기 버튼 템플릿, 소프트키 템플릿, MLPP(Multilevel Precedence and Preemption) 정보가 포함됩니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 창에서 디바이스 > 디바이스 설정 > 기본 디바이스 프로파일을 선택합니다.

단계 **2** 기본 디바이스 프로파일 구성 창의 디바이스 프로파일 유형 드롭다운 목록에서 해당 Cisco Unified IP Phone를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 디바이스 프로토콜 드롭다운 목록에서 해당 프로토콜을 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 디바이스 프로파일 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

기본 디바이스 프로파일에 대한 소프트 키 템플릿 구성

Cisco Unified Communications Manager에는 통화 처리 및 애플리케이션을 위한 표준 소프트키 템플릿이 있습니다. 사용자 정의 소프트키 템플릿을 만드는 경우 표준 템플릿을 복사하고 필요한 대로 내용을 수정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 디바이스 설정 > 소프트키 템플릿.

단계 **2** 새 소프트키 템플릿을 생성하려면 다음 단계를 수행합니다. 그렇지 않으면 다음 단계로 진행합니다.

a) 새로 추가를 클릭합니다.
b) 기본 템플릿을 선택하고 복사를 클릭합니다.
c) 소프트키 템플릿 이름 필드에 템플릿의 새 이름을 입력합니다.
d) 저장을 클릭합니다.

단계 **3** 다음 단계를 수행하여 기존 템플릿에 소프트키를 추가합니다.

a) 찾기를 클릭하고 검색 기준을 입력합니다.
b) 필요한 기존 템플릿을 선택합니다.

단계 **4** 이 소프트키 템플릿을 표준 소프트키 템플릿으로 지정하려면 기본 소프트키 템플릿 확인란을 선택합니다.

참고 소프트키 템플릿을 기본 소프트키 템플릿으로 지정하는 경우 먼저 기본값 지정을 제거하지 않는 한 이 소프트키 템플릿을 삭제할 수 없습니다.

단계 **5** 오른쪽 상단의 관련 링크 드롭다운 목록에서 소프트키 레이아웃 설정을 선택하고 이동을 클릭합니다.

단계 **6** 구성할 통화 상태 선택 드롭다운 목록에서 소프트키가 표시할 통화 상태를 선택합니다.

단계 **7** 선택되지 않은 소프트키 목록에서 소프트키를 선택하고 오른쪽 화살표를 클릭하여 소프트키를 선택한 소프트키 목록으로 이동합니다. 위쪽 및 아래쪽 화살표를 사용하여 새 소프트키의 위치를 변경합니다.

단계 **8** 이전 단계를 반복하여 추가 통화 상태로 소프트키를 표시합니다.

단계 **9** 저장을 클릭합니다.

단계 **10** 다음 작업 중 하나를 수행합니다.

- 이미 디바이스와 연결되어 있는 템플릿을 수정한 경우 구성 적용을 클릭하여 디바이스를 다시 시작합니다.
- 새 소프트키 템플릿을 생성한 경우 템플릿을 디바이스에 연결하고 다시 시작합니다. 자세한 내용은 소프트키 템플릿을 일반 디바이스 구성에 추가 및 소프트키 템플릿을 전화기와 연결 섹션을 참조하십시오.

다음에 수행할 작업

다음 구성 창 중 하나에서 [소프트 키 템플릿] 드롭다운에서 템플릿을 선택하여 사용자 지정된 소프트키 템플릿을 디바이스에 적용할 수 있습니다.

- 전화기 구성
- 범용 디바이스 템플릿
- BAT 템플릿
- 일반 디바이스 구성
- 디바이스 프로파일
- 기본 디바이스 프로파일
- UDP 프로파일

디바이스 프로파일 구성

디바이스 프로파일은 특정 디바이스와 연결된 속성 세트로 구성됩니다. 생성한 디바이스 프로파일을 엔드 유저에 연결하여 Cisco Extension Mobility 기능을 사용할 수 있습니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 창에서 디바이스 > 디바이스 설정 > 디바이스 프로파일을 선택합니다.

단계 **2** 디바이스 프로파일 구성 창에서 **[** 디바이스 프로파일 유형**]** 드롭다운 목록에서 해당 Cisco Unified IP Phone를 선택합니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 디바이스 프로토콜 드롭다운 목록에서 해당 프로토콜을 선택합니다.

단계 **5** 다음을 클릭합니다.

단계 **6** 전화기 버튼 템플릿 드롭다운 목록에서 템플릿을 선택합니다.

단계 **7** (선택 사항) 소프트 키 템플릿 드롭다운 목록에서 소프트키 템플릿을 선택합니다.

단계 **8** 디바이스 프로파일 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **9** 저장을 클릭합니다.

참고 Cisco Extension Mobility을 설정하기 위해 디바이스 프로파일을 사용하는 방법에 대한 자세한 내용은, *Cisco Unified Communications Manager* 기능 구성 설명서, 릴리스 *1.5(1)SU1* 을 참조하십시오.

엔터프라이즈 전화기 구성

엔터프라이즈 전화기 설정 구성

이 절차를 사용하여 네트워크의 전화기에서 사용할 수 있는 기본 제품별 구성 필드 설정을 구성합니다.

이 창에서 설정한 매개변수는 다양한 디바이스의 [일반 전화기 프로파일 구성] 창 및 [전화기 구성] 창에도 나타날 수 있습니다. 이렇게 동일한 매개변수를 다른 창에서도 설정하는 경우 1) [전화기 구성] 창 설정, 2) [일반 전화기 프로파일] 창 설정, 3) [엔터프라이즈 전화기 구성] 창 설정 순으로 우선 적용되는 설정이 결정됩니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 엔터프라이즈 전화기 구성을 선택합니다.

단계 **2** 제품별 구성 레이아웃 섹션에서 필수 필드를 입력합니다.

모든 엔터프라이즈 전화기 매개변수에 대한 설명을 보려면 엔터프라이즈 전화기 매개변수 구성 창에서 ? 버튼을 클릭합니다.

단계 **3** 엔터프라이즈 전화기 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

전화기 구성

이러한 단계를 수행하여 수동으로 전화기를 Unified Communications Manager 데이터베이스에 추가합니다. 자동 등록를 사용하는 경우, 이러한 단계를 수행할 필요가 없습니다. 자동 등록을 선택하는 경우, Unified Communications Manager에서 자동으로 전화기를 추가하고 디렉터리 번호를 할당합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화기 유형 드롭다운 목록에서 해당 Cisco IP 전화기 모델을 선택합니다.

단계 **4** 다음을 클릭합니다.

단계 **5** 디바이스 프로토콜 선택 드롭다운 목록에서 다음 중 하나를 선택합니다.

- **SCCP**
- **SIP**

단계 **6** 다음을 클릭합니다.

단계 **7** 전화기 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

참고 보안 프로파일에 구성된 CAPF 설정은 [전화기 구성] 창에 표시되는 CAPF(Certificate Authority Proxy Function) 설정과 관련이 있습니다. MIC(Manufacturer-Installed Certificate) 또는 LSC(Locally Significant Certificate)가 포함되는 인증서 작업에 대해 CAPF 설정을 구성해야 합니다. [전화기 구성] 창에서 업데이트하는 CAPF 설정이 보안 프로파일 CAPF 설정에 영향을 미치는 방법에 대한 자세한 내용은 Cisco Unified Communications Manager 보안 설명서를 참조하십시오.

단계 **8** 저장을 클릭합니다.

단계 **9** 연결 영역에서 회선 **[1]** - 새 **DN** 추가를 클릭합니다.

단계 **10** 디렉터리 번호 필드에서 전화기와 연결하려는 디렉터리 번호를 입력합니다.

단계 **11** 저장을 클릭합니다.

셀프 서비스 포털

셀프 서비스 포털은 새 전화기를 프로비저닝 하 고 구성 하기 위한 배포 프로세스의 일부로 사용할 수 있습니다.

- 엔드 유저는 포털을 사용하여 전화기에 대한 기능 및 설정을 사용자 지정할 수 있습니다.
- 디바이스 활성화 코드 온보딩을 사용하면 사용자가 포털을 사용하여 전화기를 활성화할 수 있는 옵션을 갖게 됩니다.
- 사용자는 또한 포털을 사용하여 자신의 단일 번호 도달(SNR) 원격 대상을 셀프 프로비저닝할 수도 있습니다.

엔드 유저는 먼저 액세스 권한을 설정하고 난 다음 포털을 사용할 수 있습니다. 포털 설정 방법에 대한 자세한 내용은 *Cisco Unified Communications Manager*에 대한 기능 구성 설명서의 "셀프 서비스 포털" 장을 참조하십시오.

32 장

CAPF 구성

CAPF(Certificate Authority Proxy Function) 설정

CAPF(Certificate Authority Proxy Function)는 LSC(Locally Significant Certificate)를 발급하고 Cisco 엔드포인트를 인증하는 Cisco 독점 서비스입니다. CAPF 서비스는 Unified Communications Manager에서 실행되며 다음 작업을 수행합니다.

- 지원되는 Cisco Unified IP Phone에 LSC를 발급합니다.
- 혼합 모드가 활성화된 경우 전화기를 인증합니다.
- 전화기에 대한 기존 LSC를 업그레이드합니다.
- 보기 및 문제해결을 위해 전화기 인증서를 검색합니다.

CAPF 실행 모드

다음 모드에서 작동하도록 CAPF를 구성할 수 있습니다.

- CAPF(Cisco Authority Proxy Function)—Unified Communications Manager의 CAPF 서비스는 CAPF 서비스에서 자체 서명한 LSC를 발급합니다. 이것이 기본 모드입니다.
- 온라인 CA—이 옵션을 사용하여 전화기에 대한 외부 온라인 CA 서명 LSC를 확보합니다. CAPF 서비스는 자동으로 외부 CA에 연결됩니다. CSR이 제출되면 CA는 서명 후 CA 서명된 LSC를 자동으로 반환합니다.
- 오프라인 CA—오프라인 외부 CA를 사용하여 전화기의 LSC를 서명하려는 경우, 이 옵션을 사용합니다. 이 옵션을 사용하려면 LSC를 수동으로 다운로드하여 CA에 제출한 다음, CA 서명 인증서가 준비되고 나면 이를 업로드해야 합니다.

참고 타사 CA를 사용하여 LSC에 서명하려는 경우, Cisco에서는 프로세스가 자동화되고 훨씬 더 빨라져 문제가 발생할 가능성이 적기 때문에 온라인 **CA**를 오프라인 **CA** 대신 사용할 것을 권장합니다.

CAPF 서비스인증서

Unified Communications Manager가 설치되면 CAPF 서비스가 자동으로 설치되고 CAPF에 따른 시스템 인증서가 생성됩니다. 보안이 적용되면 Cisco CTL 클라이언트에서 인증서를 모든 클러스터 노드에 복사합니다.

전화기 인증서 유형

Cisco에서는 전화기에 다음과 같은 전화기 X.509v3 인증서 유형을 사용합니다.

- LSC(Locally Significant Certificate)—CAPF(Certificate Authority Proxy Function)와 관련된 필수 구성 작업을 수행한 후 지원되는 전화기에 설치되는 인증서입니다. 인증 또는 암호화를 위한 디바이스 보안 모드를 구성하고 나면 LSC가 Unified Communications Manager와 전화기 간의 연결을 보호합니다.

참고 온라인 CA의 경우, LSC 유효성은 CA에 기반하며 CA가 허용하는 한 사용할 수 있습니다.

- MIC(Manufacturing Installed Certificate)—Cisco Manufacturing에서 지원되는 전화기 모델에 MIC를 자동으로 설치합니다. 제조업체에서 설치한 인증서는 LSC 설치를 위해 Cisco CAPF(Certificate Authority Proxy Function)를 인증합니다. 제조업체에서 설치한 인증서를 덮어쓰기하거나 삭제할 수 없습니다.

참고 Cisco에서는 LSC 설치용으로만 MIC(Manufacturer Installed Certificate)를 사용할 것을 권장합니다. Cisco에서는 LSC를 지원하여 Unified Communications Manager와 TLS 연결을 인증합니다. MIC 루트 인증서의 보안이 침해될 수 있으므로, TLS 인증을 위해 MIC를 사용하기 위해 또는 다른 목적으로 전화기를 구성하는 고객은 이러한 위험을 감수해야 합니다. MIC의 보안이 침해된 경우 Cisco에서는 어떤 책임도 지지 않습니다.

CAPF를 통한 **LSC** 세대

CAPF를 구성한 후에는 전화기에 구성된 인증 문자열을 추가합니다. 전화기와 CAPF 간에 키 및 인증서 교환이 발생하고 다음과 같은 상황이 발생합니다.

- 전화기에서 구성된 인증 방법을 사용하여 CAPF에 대해 자체 인증을 진행합니다.

- 전화기에서 공개-개인 키 쌍을 생성합니다.
- 전화기에서 서명된 메시지로 공개 키를 CAPF로 착신 전송합니다.
- 개인 키는 전화기에 남아 있으며 외부에 절대 공개되지 않습니다.
- CAPF에서 전화기 인증서에 서명하고 서명된 메시지로 전화기에 인증서를 보냅니다.

참고 전화기 사용자가 인증서 작업을 중단하거나 전화기의 작동 상태를 볼 수 있으니, 주의하십시오.

참고 우선 순위가 낮게 설정되어 있는 키 생성을 통해 작업 수행 중에도 전화기가 작동할 수 있습니다. 인증 생성 중에 전화기가 작동하더라도 추가 TLS 트래픽으로 인해 전화기에 대한 최소 통화 처리 중단이 발생할 수 있습니다. 예를 들어, 설치가 끝날 때 인증서가 플래시에 기록되면 오디오 결함이 발생할 수 있습니다.

CAPF 사전 요건

LSC 생성을 위해 CAPF(Certificate Authority Proxy Function)를 구성하기 전에 다음 작업을 수행합니다.

- 타사 CA를 사용하여 LSC에 서명하려는 경우, 외부에서 CA를 구성합니다.
- 전화기 인증 방법을 계획합니다.
- LSC를 생성하기 전에 다음을 갖추고 있는지 확인하십시오.
  - Unified Communications Manager 릴리스 12.5 이상.
  - 인증서에 CAPF를 사용하는 엔드포인트(Cisco IP 전화기 및 Jabber 포함).
  - Microsoft Windows Server 2012 및 2016.
  - DNS(Domain name Service)가 구성되어 있습니다.
- 이 노트는 릴리스 14 SU2부터 적용할 수 있습니다.

참고 CAPF 인증서의 경우 다음 기본 X509 확장을 포함해야 합니다.

X509v3 기본 제약조건:

CA:TRUE, pathlen:0

X509v3 키 사용:

디지털 서명, 인증서 서명

CAPF 인증서에 이러한 확장이 누락된 경우 TLS 연결이 실패하게 됩니다.

- CA 루트 및 HTTPS 인증서를 업로드한 다음 LSC를 생성해야 합니다. 보안 SIP 연결 중에, HTTPS 인증서는 CAPF-trust를 통과하고 CA 루트 인증서는 CAPF-trust 및 CallManager-trust를 통과합니다. IIS(인터넷 정보 서비스)에서 HTTPS 인증서를 호스팅합니다. CA 루트 인증서는 CSR(인증서 서명 요청)에 서명하기 위해 사용됩니다.

  다음은 인증서를 업로드해야 할 경우에 대한 시나리오입니다.

  표 ***27:*** 인증서 업로드 시나리오

시나리오	결과
CA 루트 인증서 및 HTTPS 인증서는 동일합니다.	CA 루트 인증서를 업로드합니다.
CA 루트 인증서 및 HTTPS 인증서는 서로 다르며, HTTPS 인증서는 동일한 CA 루트 인증서에서 발급합니다.	CA 루트 인증서를 업로드합니다.
중간 CA 및 HTTPS 인증서는 서로 다르며, CA 루트 인증서에서 발급합니다.	CA 루트 인증서를 업로드합니다.
CA 루트 및 HTTPS 인증서가 서로 다르며, 동일한 CA 루트 인증서에서 발급합니다.	CA 루트 및 HTTPS 인증서를 업로드합니다.

참고 여러 인증서를 동시에 생성하면 통화 처리 중단이 발생할 수 있기 때문에 예약된 유지보수 일정 안에 CAPF를 사용하실 것을 강력하게 권장합니다.

CAPF(Certificate Authority Proxy Function) 구성 작업 플로우

다음 작업을 완료하여 엔드포인트에 대한 LSC를 발행하도록 CAPF(Certificate Authority Proxy Function)을 구성합니다.

참고 새 CAPF 인증서를 다시 생성하거나 업로드하고 나면 CAPF 서비스를 다시 시작할 필요가 없습니다.

프로시저

	명령 또는 동작	목적
단계 1	타사 CA 루트 인증서 업로드	LSC를 타사 CA 서명을 받게하려면 CA 루트 인증서 체인을 CAPF-trust 저장소에 업로드합니다. 그렇지 않은 경우 이 작업을 생략할 수 있습니다.
단계 2	CA(인증기관) 루트 인증서 업로드 , 360 페이지	CA 루트 인증서를 Trust 저장소에Unified Communications Manager 업로 합니다.
단계 3	온라인 CA(인증기관) 설정 구성, 361 페이지	이 절차를 사용하여 전화기 LSC 인증서를 생성합니다.
단계 4	오프라인 CA(인증기관) 설정 구성	이 절차를 사용하여 오프라인 CA를 사용하는 전화기 LSC 인증서를 생성합니다.
단계 5	CAPF 서비스 활성화 또는 재시작	CAPF 시스템 설정을 구성한 후에 필수 CAPF 서비스를 활성화합니다.
단계 6	다음 절차 중 하나를 사용하여 Unified Communications Manager에서 CAPF 설정을 구성합니다. • 범용 디바이스 템플릿에서 CAPF 설정 구성, 364 페이지 • 벌크 관리자를 통한 CAPF 설정 업데이트, 365 페이지 • 전화기에 대한 CAPF 설정 구성, 366 페이지	다음 옵션 중 하나를 사용하여 CAPF 설정을 전화기 구성에 추가합니다. • LDAP 디렉터리를 동기화하지 않은 경우, CAPF 설정을 범용 디바이스 템플릿에 추가하고 초기 LDAP 동기화를 통해 설정을 적용합니다. • 벌크 관리 도구를 사용하여 단일 작업에서 여러 전화기에 CAPF 설정을 적용합니다. • 전화기 별로 CAPF 설정을 적용할 수 있습니다.
단계 7	KeepAlive 타이머 설정, 367 페이지	(선택 사항) CAPF 엔드포인트 연결에 대한 keepalive 값을 설정하여 방화벽에 의해 시간이 초과되지 않도록 합니다. 기본값은 15분입니다.

타사 **CA** 루트 인증서 업로드

CA 루트 인증서를 CAPF-trust 저장소 및 Unified Communications Manager trust 저장소에 업로드하여 외부 CA를 사용하여 LSC 인증서에 서명합니다.

참고 타사 CA를 사용하여 LSC에 서명하지 않으려면 이 작업을 건너뜁니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서 용도 드롭다운 목록에서 **CAPF-trust**를 선택합니다.
단계 **4** 인증서에 대한 설명을 입력합니다. 예를 들어, 외부 **LSC** 서명 **CA**에 대한 인증서입니다.
단계 **5** 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.
단계 **6** 업로드를 클릭합니다.
단계 **7** 이 작업을 반복하여 인증서 용도에 대한 **callmanager-trust**에 인증서를 업로드합니다.

CA(인증기관**)** 루트 인증서 업로드

참고 중간 또는 루트 CA 인증서의 일반 이름에 'CAPF−' 하위 문자열이 포함되어 있지 않은지 확인하십시오. 'CAPF−' 일반 이름은 CAPF 인증서용으로 예약되어 있습니다.

프로시저

단계 **1** Cisco Unified OS 관리에서 보안 > 인증서 관리를 선택합니다.
단계 **2** 인증서/인증서 체인 업로드를 클릭합니다.
단계 **3** 인증서 용도 드롭다운 목록에서 **callManager-trust**를 선택합니다.
단계 **4** 인증서에 대한 설명을 입력합니다. 예를 들어, 외부 **LSC** 서명 **CA**에 대한 인증서입니다.
단계 **5** 찾아보기를 클릭하고 파일을 탐색한 다음 열기를 클릭합니다.
단계 **6** 업로드를 클릭합니다.

중요 이 노트는 릴리스 14 SU2부터 적용할 수 있습니다.

참고 모든 루트 또는 중간 CA 인증서의 경우에는 다음과 같은 기본 X509 확장이 포함되어야 합니다.

X509v3 기본 제약조건:

CA:TRUE, pathlen:0

X509v3 키 사용:

디지털 서명, 인증서 서명

인증서에 이러한 확장이 누락된 경우 TLS 연결이 실패하게 됩니다.

중요 이 노트는 릴리스 14 SU3부터 IPSec 인증서에 대해서만 적용됩니다.

참고 CA 서명 IPSec 인증서의 경우 다음 확장을 포함하지 않아야 합니다.

X509v3 기본 제약조건:

CA:TRUE

온라인 **CA(**인증기관**)** 설정 구성

Unified Communications Manager에서 이 절차를 사용하여 온라인 CAPF를 사용하여 전화기 LSC를 생성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다.

단계 **2** 서버 드롭다운 목록에서CAPF(Certificate Authority Proxy Function)(활성) 서비스를 활성화한 노드를 선택합니다.

단계 **3** 서비스 드롭다운 목록에서 **CAPF(Certificate Authority Proxy Function)(**활성**)**을 선택합니다. 서비스 이름 옆에 "활성"이라는 단어가 표시되는지 확인하십시오.

단계 **4** 엔드포인트 대상 인증서 발급자 드롭다운 목록에서 온라인 **CA**를 선택합니다. CA 서명 인증서의 경우, 온라인 CA를 사용하는 것이 좋습니다.

단계 **5** 인증서 유효 기간**(**일**)** 필드에 1 ~ 1825 사이의 숫자를 입력하여 CAPF에서 발급한 인증서가 유효한 날짜의 수를 나타냅니다.

단계 **6** 온라인 **CA** 매개변수 섹션에서 다음 매개변수를 설정하여 온라인 CA 섹션에 대한 연결을 생성합니다.

- 온라인 CA 호스트네임—제목 이름 또는 CN(공통 이름)이 HTTPS 인증서의 FQDN(Fully Qualified Domain name)과 동일해야 합니다.

  참고 구성된 호스트네임은 Microsoft CA에서 실행되는 IIS(인터넷 정보 서비스)에서 호스팅하는 HTTP 인증서의 CN(공통 이름)과 동일 합니다.

- 온라인 CA 포트 - 온라인 CA에 대한 포트 번호를 입력합니다(예: 443).

- 온라인 CA 템플릿—템플릿의 이름을 입력합니다. Microsoft CA가 템플릿을 만듭니다.

  참고 이 필드는 온라인 CA 유형이 Microsoft CA인 경우에만 활성화됩니다.

- 온라인 CA 유형 - 엔드포인트 인증서의 자동 등록을 위해 Microsoft CA 또는 EST 지원 CA를 선택합니다.
  - Microsoft CA - CA가 디지털 인증서를 장치에 할당하는 Microsoft CA인 경우 이 옵션을 사용합니다.

    참고 FIPSS 활성화 모드는 Microsoft CA에서 지원되지 않습니다.

    - 중요 릴리스 14SU2부터 지원됩니다.

    EST 지원 CA - CA가 자동 등록을 위해 내장 EST 서버 모드를 지원하는 경우 이 옵션을 사용합니다.

- 온라인 CA 사용자 이름—CA 서버의 사용자 이름을 입력합니다.
- 온라인 CA 암호—CA 서버의 사용자 이름에 대한 암호를 입력합니다.
- 인증서 등록 프로파일 레이블 - 유효한 문자가 포함된 EST 지원 CA에 대한 디지털 ID를 입력합니다.

  참고 이 필드는 온라인 CA 유형이 EST 지원 CA인 경우에만 활성화됩니다.

단계 **7** 나머지 CAPF 서비스 매개변수를 완료합니다. 매개변수 이름을 클릭하여 서비스 매개변수 도움말 시스템을 봅니다.

단계 **8** 저장을 클릭합니다.

단계 **9** **CAPF(Certificate Authority Proxy Function)**를 다시 시작하여 변경 사항을 적용합니다. 그러면 Cisco 인증서 등록 서비스가 자동으로 다시 시작됩니다.

현재 온라인 **CA** 제한 사항

- CA 서버에서 영어 이외의 다른 언어를 사용하는 경우, 온라인 CA 기능이 작동하지 않습니다. CA 서버는 영어로만 응답해야 합니다.
- 온라인 CA 기능은 CA를 사용한 mTLS 인증을 지원하지 않습니다.
- LSC 작업에 온라인 CA를 사용하는 동안 LSC 인증서에 '디지털 서명' 및 '키 암호화' 키 사용이 제공되지 않을 경우 디바이스 보안 등록이 실패합니다.
- LSC 작업에 온라인 CA를 사용하는 동안 LSC 인증서에 '디지털 서명' 및 '키 암호화'를 제공하지 않을 경우 디바이스 보안 등록이 실패합니다.

오프라인 CA(인증기관) 설정 구성

오프라인 CA를 사용하여 전화기 LSC 인증서를 생성하기로 결정한 경우, 이 고급 프로세스를 수행합니다.

참고 오프라인 CA 옵션은 무수한 수동 단계와 관련이 있어 온라인 CA에 비해 시간이 더 오래 소요됩니다. 인증서 생성 및 전송 프로세스 중에 문제가 발생하는 경우(예: 네트워크 중단 또는 전화 재설정) 프로세스를 다시 시작합니다.

프로시저

단계 1 타사 CA(인증기관)에서 루트 인증서 체인을 다운로드합니다.

단계 2 Unified Communications Manager에서 필수 신뢰(CallManager trust CAPF trust)에 루트 인증서 체인을 업로드합니다.

단계 3 Unified Communications Manager을(를) 구성하여 엔드포인트에 인증서 발급 서비스 매개변수를 오프라인 CA로 설정하여 오프라인 CA를 사용합니다.

단계 4 전화기 LSC에 대한 **CSR**을 생성합니다.

단계 5 **CSR**을 인증기관에 보냅니다

단계 6 **CSR**에서 서명된 인증서를 가져옵니다.

오프라인 CA를 사용하여 전화기 LSC를 생성하는 방법에 대한 자세한 예는 CUCM 타사 CA 서명 LSC 생성 및 가져오기 구성을 참조하십시오.

CAPF 서비스 활성화 또는 재시작

CAPF 시스템 설정을 구성한 후에 필수 CAPF 서비스를 활성화합니다. CAPF 서비스가 이미 활성화된 경우 다시 시작합니다.

프로시저

단계 1 Cisco 유니파이드 Serviceability에서 도구 > 서비스 활성화를 선택합니다.

단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택하고 이동을 클릭합니다.

단계 3 [보안 서비스] 창에서 적용되는 서비스를 확인하십시오.

- **Cisco Certificate** 등록 서비스—온라인 CA를 사용하는 경우 이 서비스를 선택하고, 그렇지 않은 경우 선택하지 않은 상태로 둡니다.
- **CAPF(Certificate Authority Proxy Function)**—체크 표시되어 있지 않은 경우(비활성 상태), 이 서비스를 선택합니다. 서비스가 이미 활성화된 경우 다시 시작합니다.

단계 **4** 모든 설정을 수정한 경우, 저장을 클릭합니다.

단계 **5** **CAPF(Certificate Authority Proxy Function)**서비스가 이미 선택된 된 경우(활성 상태), 다음과 같이 다시 시작합니다.

a) 관련 링크 드롭다운 목록에서 컨트롤 센터 - 기능 서비스를 선택하고 이동을 클릭합니다.
b) 보안 설정 창에서 **CCAPF(Certificate Authority Proxy Function)**를 선택하고 재시작을 클릭합니다.

단계 **6** 다음 절차 중 하나를 완료하여 개별 전화기 대비 CAPF 설정을 구성합니다.

a) 범용 디바이스 템플릿에서 CAPF 설정 구성, 364 페이지
b) 벌크 관리자를 통한 CAPF 설정 업데이트, 365 페이지
c) 전화기에 대한 CAPF 설정 구성, 366 페이지

범용 디바이스 템플릿에서 **CAPF** 설정 구성

이 절차를 사용하여 범용 디바이스 템플릿에 CAPF 설정을 구성합니다. 기능 그룹 템플릿 구성을 통해 LDAP 디렉터리 동기화에 대해 템플릿을 적용합니다. 템플릿의 CAPF 설정은 이 템플릿을 사용하는 모든 동기화된 디바이스에 적용됩니다.

참고 동기화되지 않은 LDAP 디렉터리에 범용 디바이스 템플릿을 추가만 할 수 있습니다. 초기 LDAP 동기화가 발생한 경우, 벌크 관리를 사용하여 전화기를 업데이트합니다. 자세한 내용은 벌크 관리자를 통한 CAPF 설정 업데이트, 365 페이지를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 디바이스 템플릿을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 템플릿을 선택합니다.
- 새로 추가를 클릭합니다.

단계 **3** **CAPF(Certificate Authority Proxy Function)** 설정 영역을 확장합니다.

단계 **4** 인증서 작업 드롭다운 목록에서 설치/업그레이드를 선택합니다.

단계 **5** 인증 모드 드롭다운 목록 메뉴에서 디바이스가 자체 인증할 수 있는 옵션을 선택합니다.

단계 **6** 인증 문자열을 사용하기로 선택한 경우, 텍스트 상자에 인증 문자열을 입력하거나 문자열 생성을 클릭하여 시스템에서 문자열을 생성합니다.

참고 이 문자열이 디바이스 자체에 구성지 않은 경우 인증이 실패합니다.

단계 **7** 나머지 필드에서 키 정보를 구성합니다. 필드에 대해 도움이 필요한 경우, 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

참고 이 템플릿을 사용하는 디바이스를 이 절차에서 할당한 것과 동일한 인증 방법으로 구성했는지 확인하십시오. 그렇지 않으면 디바이스 인증이 실패합니다. 전화기 인증 구성 방법에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

단계 **9** 이 프로파일을 사용하는 디바이스에 템플릿 설정을 적용합니다.

a) 기능 그룹 템플릿 구성에 범용 디바이스 템플릿을 추가합니다.
b) 기능 그룹 템플릿을 동기화되지 않은 LDAP 디렉터리 구성에 추가합니다.
c) LDAP 동기화를 완료합니다. CAPF 설정은 동기화된 모든 디바이스에 적용됩니다.

기능 그룹 템플릿 및 LDAP 디렉터리 구성에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "엔드 유저 구성" 섹션을 참조하십시오.

벌크 관리자를 통한 CAPF 설정 업데이트

벌크 관리의 전화기 업데이트 쿼리를 사용하여 단일 작업에서 많은 기존 전화기에 대한 CAPF 설정 및 LSC 인증서를 구성합니다.

참고 전화기를 프로비저닝하지 않은 경우, 벌크 관리의 전화기 삽입 메뉴를 사용하여 CSV 파일의 CAPF 설정으로 새 전화기를 프로비저닝합니다. CSV 파일에서 전화기를 삽입하는 방법에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서의 "전화기 삽입" 섹션을 참조하십시오.

이 절차에서 추가하려는 것과 동일한 문자열 및 인증 방법을 사용하여 전화기를 구성하였는지 확인하십시오. 그렇지 않으면 전화기가 CAPF에 인증되지 않습니다. 전화기에서 인증을 구성하는 방법에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.벌크 관리 > 전화기 > 전화기 업데이트 > 쿼리.

단계 **2** 필터 옵션을 사용하여 업데이트하려는 전화기로 검색을 제한하고 찾기를 클릭합니다.

예를 들어, 전화기 찾기 위치 드롭다운 목록을 사용하여 모든 전화기를 선택합니다. 여기서 LSC는 특정 날짜 이전에 또는 특정 디바이스 풀 내에서 만료됩니다.

단계 **3** 다음을 클릭합니다.

단계 **4** 로그아웃/재설정/재시작 섹션에서 구성 적용 라디오 버튼을 선택합니다. 작업이 실행되면 CAPF 업데이트가 업데이트된 모든 전화기에 적용됩니다.

단계 **5** **CAPF(Certificate Authority Proxy Function)** 정보에서 인증서 작업 확인란에 체크 표시합니다.

단계 **6** 인증서 작업 드롭다운 목록에서 설치/업그레이드를 선택하여 CAPF가 전화기에 새 LSC 인증서를 설치하도록 합니다.

단계 **7** 인증 모드 드롭다운 목록에서 LSC 설치 중 전화기의 자체 인증 방법을 선택합니다.

참고 전화기에서 동일한 인증 방법을 구성합니다.

단계 **8** 인증 문자열을 인증 모드로 선택한 경우, 다음 단계 중 하나를 완료합니다.

- 각 디바이스에 대한 고유한 인증 문자열을 사용하려는 경우, 각 디바이스에 고유한 인증 문자열 생성을 선택합니다.
- 인증 문자열 텍스트 상자에 문자열을 입력하거나, 모든 디바이스에 대해 동일한 인증 문자열을 사용하려면 문자열 생성을 클릭합니다.

단계 **9** 전화기 업데이트 창의 **CAPF(Certificate Authority Proxy Function)** 정보 섹션에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **10** 작업 정보에서 즉시 실행을 선택합니다.

참고 예약된 시간에 작업을 실행하려면 나중에 실행을 선택합니다. 작업 예약에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 벌크 관리 지침서에서 "예약된 작업 관리" 섹션을 참조하십시오.

단계 **11** 제출을 클릭합니다.

참고 이 절차에서 설정 적용 옵션을 선택하지 않은 경우, 업데이트된 모든 전화기에 대해 전화기 설정 창에서 설정을 적용합니다.

전화기에 대한 **CAPF** 설정 구성

이 절차를 사용하여 개별 전화기의 LSC 인증서에 대한 CAPF 설정을 구성합니다.

참고 벌크 관리 또는 동기화 LDAP 디렉터리를 사용하여 많은 수의 전화기에 CAPF 설정을 적용합니다.

이 절차에서 추가하려는 것과 동일한 문자열 및 인증 방법을 사용하여 전화기를 구성합니다. 그렇지 않으면, 전화기가 CAPF에 자체 인증되지 않습니다. 전화기에서 인증을 구성하는 방법에 대한 자세한 내용은 전화기 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기.

단계 **2** 찾기를 클릭하고 기존 전화기를 선택합니다. 전화기 구성 페이지가 나타납니다.

단계 **3** **CAPF(Certificate Authority Proxy Function)** 정보 창으로 이동합니다.

단계 **4** 인증서 작업 드롭다운 목록에서 CAPF에 대한 설치/업그레이드를 선택하여 전화기에 새 LSC 인증서를 설치합니다.

단계 **5** 인증 모드 드롭다운 목록에서 LSC 설치 중 전화기의 자체 인증 방법을 선택합니다.

참고 동일한 인증 방법을 사용하도록 전화기를 구성해야 합니다.

단계 **6** 텍스트 문자열을 입력하거나 문자열 생성을 클릭하여 인증 문자열을 선택하는 경우 문자열을 생성합니다.

단계 **7** 전화기 설정 페이지의 **CAPF(Certificate Authority Proxy Function)** 정보 창에 있는 나머지 필드에 세부 정보를 입력합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

KeepAlive 타이머 설정

이 절차를 사용하여 CAPF-엔드포인트 연결에 대한 클러스터 수준 keepalive 타이머를 설정하여 방화벽에 의해 연결이 시간 초과되지 않도록 합니다. 타이머의 기본값은 15분입니다. 각 간격 이후 CAPF 서비스는 연결을 계속 유지할 수 있도록 keepalive 신호를 전화기로 보냅니다.

프로시저

단계 **1** 명령줄 인터페이스를 사용하여 퍼블리셔 노드에 로그인합니다.

단계 **2** `Utils capt set keep_alive` CLI 명령을 실행합니다.

단계 **3** 5에서 60(분) 사이의 숫자를 입력하고 입력을 클릭합니다.

CAPF 관리 작업

CAPF를 구성하고 LSC 인증서를 발급한 후에는 다음 작업을 사용하여 LSC 인증서를 지속적으로 관리합니다.

인증서 상태 모니터링

시스템을 구성하여 인증서 상태를 자동으로 모니터링할 수 있습니다. 시스템에서 인증서 만료가 다가오면 이메일을 보내 며, 만료 후에는 인증서를 철회합니다.

인증서 모니터링 확인 작업을 구성하는 방법에 대한 자세한 내용은, "인증서 관리" 관리 장의 인증서 모니터링 및 철회 작업 플로우를 참조하십시오.

오래된 LSC 보고서 실행

이 절차를 사용하여 Cisco Unified Reporting에서 오래된 LSC 보고서를 실행합니다. 오래된 LSC는 엔드포인트 CSR에 대한 응답으로 생성되었지만, 새로운 CSR이 오래된 LSCS가 설치되기 전에 엔드포인트에 의해 생성 되었기 때문에 한 번도 설치된 적이 없었던 인증서입니다.

참고 퍼블리셔 노드에서 `utils capf stale-lsc list` CLI 명령을 실행하여 오래된 LSC 인증서 목록을 가져올 수도 있습니다.

프로시저

단계 **1** Cisco Unified Reporting Administration에서 시스템 보고서를 선택합니다.

단계 **2** 왼쪽 내비게이션 바에서 오래된 **LSC**를 선택합니다.

단계 **3** 새 보고서 생성을 클릭합니다.

보류 중인 **CSR** 목록 조회

이 절차를 사용하여 보류 중인 CAPF CSR 파일 목록을 봅니다. 모든 CSR 파일에는 타임스탬프가 찍혀 있습니다.

프로시저

단계 **1** 명령줄 인터페이스를 사용하여 퍼블리셔 노드에 로그인합니다.

단계 **2** `utils capf csr list` CLI 명령을 실행합니다.
보류기 중인 CSR 파일의 타임스탬프가 찍힌 목록이 표시됩니다.

오래된 **LSC** 인증서 삭제

이 절차를 사용하여 시스템에서 오래된 LSC 인증서를 삭제합니다.

프로시저

단계 **1** 명령줄 인터페이스를 사용하여 퍼블리셔 노드에 로그인합니다.

단계 **2** `utils capf stale-lsc delete all` CLI 명령어 실행
시스템에서 모든 오래된 LSC 인증서를 삭제합니다.

CAPF 시스템 상호 작용 및 제한 사항

기능	상호 작용
인증 문자열	전화기에 대한 CAPF 인증 방법의 경우, 작업 후에 동일한 인증 문자열을 전화기에 입력해야 합니다. 그렇지 않으면 작업이 실패합니다. TFTP 암호화 구성 엔터프라이즈 매개변수가 활성화되어 있고 인증 문자열을 입력하지 못한 경우, 일치하는 인증 문자열이 전화기에 입력될 때까지 전화기가 실패하고 복구되지 않을 수 있습니다.
클러스터 서버 자격 증명	Unified Communications Manager 클러스터의 모든 서버는 동일한 관리자 사용자 이름 및 암호를 사용해야 합니다. 그래야 CAPF에서 클러스터의 모든 서버를 인증할 수 있습니다.
보안 전화기 마이그레이션	보안 전화기가 다른 클러스터로 이동되는 경우, Unified Communications Manager에서는 인증서가 CTL 파일에 존재하지 않는 다른 CAPF에서 발급했기 때문에 전화기에서 전송하는 LSC 인증서를 신뢰하지 않습니다. 보안 전화에서 등록을 진행하게 하려면, 기존 CTL 파일을 삭제합니다. 그런 다음, 설치/업그레이드 옵션을 사용하여 새 CAPF를 통해 새 LSC 인증서를 설치하고 새 CTL 파일에 대한 전화기를 재설정합니다(또는 MIC를 사용합니다). 전화기를 이동하기 전에 [전화기 구성] 창의 [CAPF] 섹션에서 [삭제] 옵션을 사용하여 기존 LSC를 삭제합니다.
Cisco Unified IP Phone 6900 시리즈, 7900 시리즈, 8900 시리즈 및 9900 시리즈	Cisco에서는 Cisco Unified IP Phone 6900 시리즈, 7900 시리즈, 8900 시리즈 및 9900 시리즈를 업그레이드하여 Unified Communications Manager에 대한 TLS 연결을 위해 LSC를 사용할 것과, 예상되는 호환성 문제를 방지하기 위해 CallManager 신뢰 저장소에서 MIC 루트 인증서를 제거할 것을 권장합니다. Unified Communications Manager에 대한 TLS 연결을 위해 MIC를 사용하는 일부 전화기 모델은 등록되지 않을 수도 있습니다. 관리자는 CallManager 신뢰 저장소에서 다음과 같은 MIC 루트 인증서를 제거해야 합니다. • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048

기능	상호 작용
정전	다음 정보는 통신 두절 또는 정전 발생 시 적용됩니다. • 전화기에서 인증서 설치가 진행디는 동안 통신 두절이 발생하는 경우, 전화기는 30초 간격으로 3회 이상 인증서를 가져오려고 시도합니다. 이러한 값은 구성할 수 없습니다. • 전화기에서 CAPF를 사용하여 세션을 시도하는 동안 정신이 발생하는 경우, 전화기에서는 플래시에 저장된 인증 모드를 사용합니다. 즉, 전화기가 다시 부팅된 후에 전화기가 TFTP 서버에서 새 구성 파일을 로드할 수 없는 경우가 이에 해당됩니다. 인증서 작업이 완료되면 시스템에서 바로 해당 값을 소거합니다.
인증서 암호화	Unified Communications Manager 릴리스 11.5(1) SU1에서 시작하여 CAPF 서비스에서 발급한 모든 LSC 인증서는 SHA-256 알고리즘으로 서명됩니다. 따라서 IP 전화기 7900/8900/9900 시리즈 모델은 SHA-256 서명된 LSC 인증서 및 외부 SHA2 ID 인증서(Tomcat, CallManager, CAPF, TVS 등)를 지원합니다. 서명 확인이 필요한 다른 암호화 작업의 경우, SHA-1만 지원됩니다. 참고 소프트웨어 유지보수 종료 또는 단종 단계에 있는 전화기 모델을 사용하는 경우, 11.5(1) SU1 릴리스를 사용하기 전에 Unified Communications Manager를 사용할 것을 강력 권장합니다.

7942 및 7962 전화기를 이용한 CAPF 예

사용자 또는 Unified Communications Manager에서 전화기를 재설정할 때는, CAPF가 Cisco Unified IP Phone 7962 및 7942와 상호 작용하는 방식에 대한 다음 정보를 고려하십시오.

참고 다음 예에서, LSC가 아직 전화기에 존재하지 않고 CAFP 인증 모드에 대해 기존 인증서 사용을 선택한 경우, CAPF 인증서 작업이 실패합니다.

예-비보안 디바이스 보안 모드

이 예에서는, 디바이스 보안 모드를 비보안으로 그리고 CAPF 인증 모드를 **Null** 문자열 사용 또는 기존 인증서 사용**(**우선순위**...)**으로 설정한 후에 전화기가 재설정됩니다. 전화기가 재설정되고 나면, 즉시 기본 Unified Communications Manager에 등록되고 구성 파일을 수신합니다. 그런 다음 전화기가 자동으로 CAPF를 사용하여 세션을 시작하여 LSC를 다운로드합니다. 전화기에서 LSC를 설치한 후에는 디바이스 보안 모드를 인증됨 또는 암호화됨으로 구성합니다.

예-인증된/암호화된 디바이스 보안 모드

이 예에서는, 디바이스 보안 모드를 비보안으로 인증됨 또는 암호화됨으로 그리고 CAPF 인증 모드를 **Null** 문자열 사용 또는 기존 인증서 사용(우선순위...)으로 설정한 후에 전화기가 재설정됩니다. CAPF 세션이 종료되고 전화기에 LSC가 설치될 때까지 전화기는 기본 Unified Communications Manager에 등록되지 않습니다. 세션이 종료되면, 전화기가 등록되고, 즉시 인증됨 또는 암호화됨 모드로 실행됩니다.

이 예에서 인증 문자열 사용을 구성할 수 없습니다. 그 이유는 전화기가 CAPF 서버에 자동으로 연결되지 않아, 전화기에 유효한 LSC가 없는 경우 등록이 실패하기 때문입니다.

IPv6 주소 지정과의 CAPF 상호 작용

CAPF는 IPv4, IPv6 또는 두 가지 유형의 주소를 모두 사용하는 전화기로 인증서를 발급하고 업그레이드할 수 있습니다. IPv6 주소를 사용하는 SCCP를 실행 중인 전화기에 대한 인증서를 발급하거나 업그레이드하려면, Unified Communications Manager 관리에서 IPv6 활성화 서비스 매개변수를 참으로 설정해야 합니다.

전화기가 CAPF에 연결되어 인증서를 가져올 때 CAPF는 [IPv6 활성화] 엔터프라이즈 매개변수에서 구성을 사용하여 전화기에 인증서를 발급 또는 업그레이드할지 여부를 결정합니다. 엔터프라이즈 매개변수가 거짓으로 설정된 경우, CAPF는 IPv6 주소를 사용하는 전화기에서 연결을 무시하거나 거부하며 전화기는 인증서를 수신하지 않습니다.

다음 표에서는 IPv4, IPv6 또는 두 유형의 주소가 있는 전화기가 CAPF에 연결되는 방식에 대해 설명합니다.

표 ***28: IPv6*** 또는 ***IPv4*** 전화기가 ***CAPF***에 연결되는 방법

전화기의 **IP** 모드	전화기의 **IP** 주소	**CAPF IP** 주소	전화기가 **CAPF**에 연결되는 방법
두 개의 스택	IPv4 및 IPv6 사용 가능	IPv4, IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다. 즉, 전화기를 IPv6 주소를 통해 연결할 수 없는 경우, 전화기에서는 IPv4 주소를 사용하여 연결을 시도합니다.
두 개의 스택	IPv4	IPv4, IPv6	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
두 개의 스택	IPv6	IPv4, IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다. 시도가 실패하면 전화기에서 IPv4 주소를 사용하여 CAPF에 연결합니다.
두 개의 스택	IPv4	IPv4	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
두 개의 스택	IPv4 및 IPv6 사용 가능	IPv6	전화기가 IPv6 주소를 사용하여 CAPF에 연결됩니다.

전화기의 IP 모드	전화기의 IP 주소	CAPF IP 주소	전화기가 CAPF에 연결되는 방법
두 개의 스택	IPv4 및 IPv6 사용 가능	IPv4	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
두 개의 스택	IPv4	IPv6	전화기가 CAPF에 연결될 수 없습니다.
두 개의 스택	IPv6	IPv4	전화기가 CAPF에 연결될 수 없습니다.
두 개의 스택	IPv6	IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다.
IPv4 스택	IPv4	IPv4, IPv6	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
IPv6 스택	IPv6	IPv4, IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다.
IPv4 스택	IPv4	IPv4	전화기는 IPv4 주소를 사용하여 CAPF에 연결됩니다.
IPv4 스택	IPv4	IPv6	전화기가 CAPF에 연결될 수 없습니다.
IPv6 스택	IPv6	IPv6	전화기는 IPv6 주소를 사용하여 CAPF에 연결됩니다.
IPv6 스택	IPv6	IPv4	전화기가 CAPF에 연결될 수 없습니다.

33 장

TFTP 서버 구성

프록시 TFTP 구축 개요

프록시 TFTP(Trivial File Transfer Protocol) 서버를 사용하여 네트워크의 엔드포인트에 필요한 구성 파일(예: 다이얼 플랜, 벨소리 파일 및 디바이스 구성 파일)을 제공합니다. TFTP 서버는 구축 시 모든 클러스터에 설치될 수 있으며 여러 클러스터의 엔드포인트에서 요청을 진행할 수 있습니다. DHCP 범위는 구성 파일을 가져오기 위해 사용할 프록시 TFTP 서버의 IP 주소를 지정합니다.

리던던트 및 피어 프록시 TFTP 서버

단일 클러스터 구축의 경우 클러스터에 하나 이상의 프록시 TFTP 서버가 있어야 합니다. 리던던시를 위해 다른 프록시 TFTP 서버를 클러스터에 추가할 수 있습니다. 두 번째 프록시 TFTP 서버는 IPv4에 대한 옵션 150에 추가됩니다. IPv6의 경우, 두 번째 프록시 TFTP 서버를 DHCP 범위에 있는 TFTP 서버 주소 하위 옵션 1에 추가합니다.

다중 클러스터 구축 시에, 최대 3대의 원격 프록시 TFTP 서버를 기본 프록시 TFTP 서버의 피어 클러스터로 지정할 수 있습니다. 이 기능은 많은 DHCP 범위에 대해 한 대의 프록시 TFTP 서버만 구성하거나 하나의 DHCP 범위만 포함하려는 경우에 유용합니다. 기본 프록시 TFTP 서버는 네트워크의 모든 전화기 및 디바이스에 구성 파일을 제공합니다.

각 원격 프록시 TFTP 서버와 기본 프록시 TFTP 서버 간에 피어 관계를 생성해야 합니다.

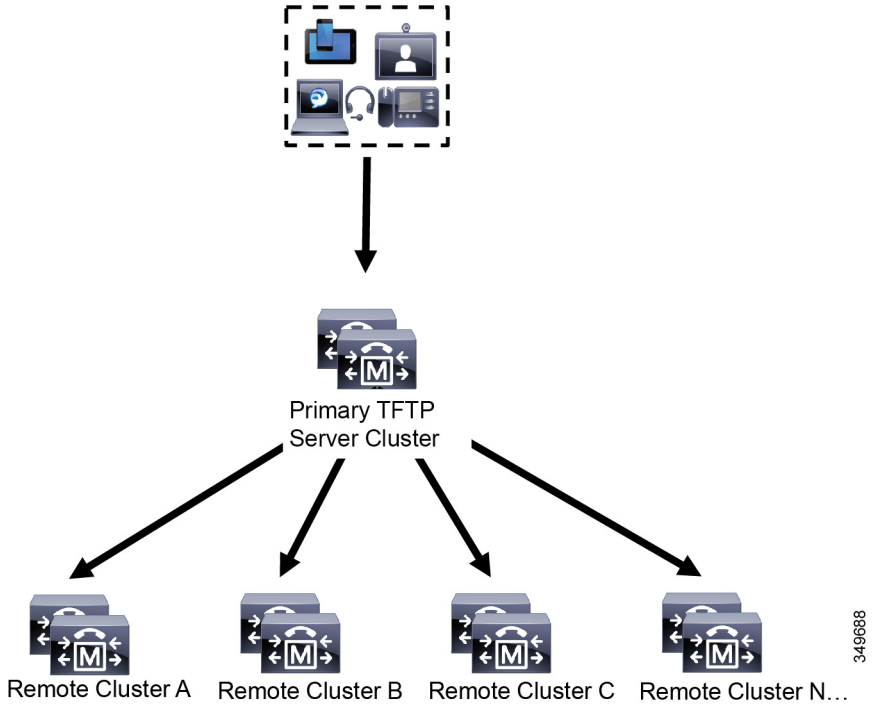
팁 네트워크의 원격 프록시 TFTP 서버 간에 피어 관계를 구성할 경우, 관계 계층 구조를 유지합니다. 루프 생성을 막기 위해 원격 클러스터의 피어 TFTP 서버가 서로를 가리키고 있지 않은지 확인하십시오. 예를 들어, 기본 노드 A가 노드 B 및 C와 피어 관계를 갖는 경우 노드 B와 C 사이에는 피어 관계를 생성하지 말아야 합니다. 이렇게 하면 루프가 생성됩니다.

프록시 TFTP

다중 클러스터 시스템에서 프록시 TFTP 서비스는 단일 기본 TFTP 서버를 통해 여러 클러스터의 TFTP 파일을 제공할 수 있습니다. 프록시 TFTP는 단일 서브넷 또는 VLAN에 여러 클러스터의 전화 또는 여러 클러스터가 동일한 DHCP TFTP 옵션 (150)을 공유하는 시나리오가 포함된 경우, 단일 TFTP 참조로 사용할 수 있습니다.

프록시 TFTP 서비스는 설명한 것처럼 단일 수준 계층 구조로 작동합니다. 더 복잡한 다중 레벨 계층 구조는 지원되지 않습니다.

그림 *7:* 프록시 ***TFTP*** 단일 수준 계층 구조



위 그림에서 디바이스 그룹은 구성 파일에 대해 기본 TFTP 서버에 연결합니다. 디바이스에서 TFTP에 대한 요청을 받으면, 기본 TFTP는 구성 파일 및 원격 클러스터 A, B, C 또는 N(구성된 다른 모든 원격 클러스터)과 같은 원격으로 구성된 모든 클러스터에 대해 자체 로컬 캐시를 조사합니다.

기본 TFTP 서버에 원하는 수의 원격 클러스터를 구성할 수 있습니다. 그러나 각 원격 클러스터에는 최대 3 개의 TFTP IP 주소만 포함될 수 있습니다. 리던던시를 위해 권장되는 설계는 클러스터 당 2개의 TFTP 서버이므로, 리던던시를 위해 주 TFTP 서버의 원격 클러스터 당 2개의 IP 주소입니다.

사용 사례 계획 모범 사례

프록시 TFTP 사용 방법 및 구현 모범 사례를 자세히 설명하고 있는 다음 시나리오를 고려하십시오.

1. 클러스터는 다른 용도로 사용되지 않을 경우 프록시 TFTP 클러스터 역할을 할 수 있습니다. 이 경우 클러스터는 다른 클러스터와 관계가 없으며 통화를 처리하지 않습니다. 이 시나리오에서는 원격 클러스터 TFTP가 수동으로 정의되고 8.0 이전으로의 롤백이 권장됩니다.

참고 이 시나리오에서는 자동 등록이 작동되지 않습니다.

2. 해당 클러스터는 원격 클러스터에 대한 프록시 TFTP 서버 역할을 하기도 하는 원격 클러스터입니다. 원격 클러스터는 수동으로 정의되므로 자동 등록을 활성화하지 않아야 합니다.

IPv4 및 IPv6 디바이스에 대한 TFTP 지원

DHCP 사용자 지정 옵션 150을 사용하도록 IPv4 전화기 및 게이트웨이를 활성화하여 TFTP 서버 IP 주소를 검색하는 것이 좋습니다. 옵션 150을 사용하여 게이트웨이 및 전화기에서 TFTP 서버 IP 주소를 검색합니다. 자세한 내용은 디바이스와 함께 제공되는 설명서를 참조하십시오.

IPv6 네트워크에서 Cisco 공급업체별 DHCPv6 정보를 사용하여 TFTP 서버 IPv6 주소를 엔드포인트에 전달하는 것이 좋습니다. 이런 방식으로 TFTP 서버 IP 주소를 옵션 값으로 구성합니다.

IPv4를 사용하는 일부 엔드포인트 및 IPv6을 사용하는 일부 엔드포인트가 있는 경우, IPv4에 대해 DHCP 사용자 지정 옵션 150을 사용하고 IPv6에 대해 TFTP 서버 주소 하위 옵션 유형 1, Cisco 공급업체별 정보 옵션을 사용하는 것이 좋습니다. TFTP 서버에서 IPv4를 사용하여 요청을 처리하는 동안 엔드포인트에서 IPv6 주소를 얻고 요청을 TFTP 서버에 보내는 경우, TFTP 서버는 IPv6 스택에서 요청을 수신하지 않기 때문에 TFTP 서버에서 요청을 받지 않습니다. 이 경우 엔드포인트를 Cisco Unified Communications Manager에 등록할 수 없습니다.

IPv4 및 IPv6 디바이스에서 TFTP 서버의 IP 주소를 검색하기 위해 사용할 수 있는 다른 방법이 있습니다. 예를 들어, IPv4 디바이스에 대해 DHCP 옵션 066 또는 CiscoCM1를 사용할 수 있습니다. IPv6 디바이스의 경우, 다른 방법으로 TFTP 서비스 하위 옵션 유형 2를 사용하는 것이나 엔드포인트에서 TFTP 서버의 IP 주소를 구성하는 것이 있습니다 이러한 대체 방법은 사용하지 않는 것이 좋습니다. 먼저 Cisco 서비스 제공자에게 문의한 다음 대체 방법을 사용하십시오.

TFTP 구축을 위한 엔드포인트 및 구성 파일

SCCP 전화기, SIP 전화기 및 게이트웨이는 초기화될 때 구성 파일을 요청합니다. 디바이스 구성을 변경할 때마다 업데이트된 구성 파일이 엔드포인트로 전송됩니다.

구성 파일에는 Unified Communications Manager 노드의 우선 순위 목록과 같은 정보, 이러한 노드에 연결하는 데 사용되는 TCP 포트, 기타 실행 파일이 포함되어 있습니다. 일부 엔드포인트의 경우, 구성 파일에 메시지, 디렉터리, 서비스 및 정보와 같은 전화기 버튼에 대한 로캘 정보와 URL이 들어 있습니다. 게이트웨이에 대한 구성 파일에는 디바이스에 필요한 모든 구성 정보가 포함되어 있습니다.

프록시 TFTP의 보안 고려 사항

Cisco 프록시 TFTP 서버는 서명된 또는 서명되지 않은 요청을 모두 처리하며, 비보안 모드 또는 혼합 모드에서 실행됩니다. 프록시 TFTP 서버에서는 전화기에서 파일을 요청할 경우 로컬 파일 시스템이나 데이터베이스를 검색하며, 검색 결과가 없을 경우 원격 클러스터에 요청을 전송합니다. 전화기에서 `ringlist.xml.sgn`, `locale file` 등과 같은 이름을 갖는 공통 파일에 대한 서버를 요청할 경우, 해당 서버는 전화기의 홈 클러스터에서 자체 파일 대신 파일의 로컬 사본을 전송합니다.

프록시 TFTP에서 파일을 수신할 때, 파일의 프록시 서버 서명이 전화기의 ITL(Initial Trust List)과 일치하지 않아 서명 검증이 실패로 돌아가 전화기에서 파일을 거부합니다. 이 문제를 해소하기 위해, 전화기의 SBD(Security by Default)를 비활성화하거나 프록시 TFTP의 CallManager 인증서를 새로운(원격/홈) 클러스터 phone-sast-trust로 가져올 수 있습니다. 그런 다음 전화기를 TVS(Trust Verification Service)에 문의하여 프록시 TFTP 인증서를 신뢰합니다. EMCC가 구축 시 활성화되어 있으면 벌크 인증서 교환이 필요합니다

보안(기본값)을 비활성화하려면 "Cisco Unified IP Phone에 대한 ITL 파일 업데이트" 섹션 Cisco 통합 커뮤니케이션 매니저 보안 설명서의 내용을 참조하십시오.

혼합 모드의 프록시 TFTP

혼합 모드로 실행 중인 원격 클러스터의 TFTP 서버에서 기본 프록시 TFTP 서버 인증서를 Cisco CTL(Certificate Trust List) 파일에 추가해야만 합니다. 그렇지 않으면 보안이 활성화되어 있는 클러스터에 등록하는 엔드포인트가 필요한 파일을 다운로드할 수 없습니다. 이를 위해, 인증서 벌크 가져오기-내보내기를 수행한 이후 CTL 파일을 업데이트합니다.

벌크 인증서 내보내기를 수행하기 위해 인터클러스터에 IP 전화기를 마이그레이션할 때 자세한 내용은, Cisco 통합 커뮤니케이션 매니저 보안 설명서의 "벌크 인증서 내보내기" 섹션을 참조하십시오.

프록시 TFTP 환경에서 클러스트 간에 전화기 이동

프록시 TFTP 환경에서 하나의 원격 클러스터에서 다른 클러스터로 전화기를 이동할 때는, 다음을 수행합니다.

1. 원격 클러스터 B(대상 클러스터)에 전화기 세부 정보를 추가합니다.
2. 원격 클러스터 A(소스 클러스터)에서 전화기 세부 정보를 삭제합니다.

참고 프록시 TFTP에서 전화기 구성은 끝날 때까지 30분 걸립니다. 어떤 파일도 찾을 수 없다는 반응을 피하기 위해, 프록시 클러스터의 TFTP 서비스를 다시 시작할 수 있습니다.

3. 전화기를 재설정하여 원격 클러스터 B에서 구성 파일을 다운로드한 다음 원격 클러스터 B에 등록합니다.

TFTP 서버 구성 작업 플로우

클러스터에 대해 구성된 EMCC(Extension Mobility Cross Cluster)가 있는 경우, 시스템에서 프록시 TFTP 서버를 동적으로 구성하도록 할 수 있습니다. 그렇지 않은 경우, TFTP 서버를 설정하고 보안 모드를 수동으로 설정할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 1	다음 방법 중 하나를 사용하여 TFTP 서버를 설정합니다. • TFTP 서버 동적 구성, 377 페이지 • TFTP 서버 수동 구성, 378 페이지	ILS(Intercluster Lookup Service) 가 구성된 경우, TFTP 서버를 동적으로 설정할 수 있습니다. EMCC를 구성하지 않은 경우, TFTP 서버를 수동으로 설정합니다. 클러스터가 보안 상태인지 비보안 상태인지 나타내야만 합니다. 클러스터는 기본값으로 비보안으로 처리됩니다.
단계 2	(선택 사항) TFTP 서버에 대한 CTL 파일 업데이트, 379 페이지	CTL 클라이언트 플러그 인을 설치 하 고 혼합 모드에서 작동 하는 모든 원격 클러스터에 있는 모든 프록시 TFTP 서버의 Cisco CTL (Certificate Trust List) 파일에 기본 프록시 TFTP 서버를 추가 합니다.
단계 3	(선택 사항) 엔드포인트 디바이스를 지원하는 설명서를 참조하십시오.	프록시 TFTP 구축에 원격 클러스터가 있는 경우, 모든 원격 엔드포인트의 TVL(신뢰 확인 목록)에 프록시 TFTP 서버를 추가합니다.
단계 4	(선택 사항) TFTP 서버에 대한 비 구성 파일 수정, 380 페이지	엔드포인트가 프록시 TFTP 서버에서 요청하는 비구성 파일을 수정할 수 있습니다.
단계 5	(선택 사항) TFTP 서비스 시작 및 중지, 380 페이지	엔드포인트에 대한 수정된 비구성 파일을 업로드한 경우, 프록시 TFTP 노드에서 TFTP 서비스를 중지했다가 다시 시작합니다.
단계 6	(선택 사항) DHCP 서버를 지원하는 설명서를 참조하십시오.	다중 클러스터 구축을 위해 개별 원격 노드에 대한 DHCP 범위를 수정하여 기본 프록시 TFTP 서버의 IP 주소를 포함합니다.

TFTP 서버 동적 구성

네트워크의 ILS(Intercluster Lookup Service) 를 구성한 경우, Cisco 프록시 TFTP 서버를 동적으로 구성할 수 있습니다.

시작하기 전에

네트워크의 EMCC를 구성합니다. 자세한 내용은 Cisco Unified Communications Manager의 기능 및 서비스 설명서를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 참조하십시오.

SIP OAuth가 활성화된 경우 오프 클러스터 Tomcat 인증서의 루트 CA 인증서를 프록시 전화기 엣지 신뢰로 복사해야 합니다.

프로시저

Cisco Unified Communications Manager 관리에서 고급 기능 > 클러스터 보기 > 지금 원격 클러스터 업데이트를 선택합니다. TFTP 서버는 클러스터에 대해 자동으로 구성됩니다.

다음에 수행할 작업

원격 프록시 TFTP 서버를 엔드포인트의 신뢰 확인 목록(TVL)으로 추가해야만 합니다. 그렇지 않으면 원격 클러스터에 있는 프록시 TFTP 서버의 구성 파일을 승인하지 않습니다. 자세한 지침은 엔드포인트 디바이스를 지원하는 설명서를 참조하십시오.

TFTP 서버 수동 구성

EMCC를 구성하지 않은 상태로 네트워크에서 TFTP를 구성하려면 수동 절차를 사용해야만 합니다.

클러스터 보기에서 기본 프록시 TFTP 서버와 기타 TFTP 서버 간에 피어 관계를 설정합니다. 최대 3개의 피어 TFTP 서버를 추가할 수 있습니다.

프록시 TFTP 구축 시 각 원격 TFTP 서버에는 기본 프록시 TFTP 서버에 대한 피어 관계가 포함되어야만 합니다. 루프 생성을 막으려면 원격 클러스터의 피어 TFTP 서버가 서로를 가리키고 있지 않은지 확인하십시오.

시작하기 전에

중요 14SU1 릴리스부터 SIP OAuth가 활성화된 경우 오프 클러스터 Tomcat 인증서의 루트 CA 인증서를 프록시 전화기 엣지 신뢰로 복사해야 합니다.

프로시저

단계 **1** 원격 클러스터를 생성합니다. 다음 작업을 수행합니다.

a) Cisco Unified CM 관리에서 고급 기능 > 클러스터 보기를 선택합니다.
b) 새로 추가를 클릭합니다. 원격 클러스터 구성 창이 나타납니다.
c) TFTP 서버에 대해 최대 50자의 클러스터 ID 및 FQDN(Fully Qualified Domain name)을 입력한 다음, 저장을 클릭합니다.

   클러스터 ID에 대한 유효한 값에는 영숫자 문자, 마침표(.), 하이픈(-)이 포함됩니다. FQDN에 대한 유효한 값에는 영숫자 문자, 마침표(.), 대시(-), 별표(*), 공백이 포함됩니다.

d) (선택 사항) 원격 클러스터 서비스 구성 창에서 최대 128자의 원격 클러스터에 대한 설명을 입력합니다.

   따옴표("), 폐쇄 또는 개방 꺾쇠 괄호(> <), 백슬래시(\), 대시(-), 앰퍼샌드(&) 또는 백분율 기호(%)를 사용하지 마십시오.

단계 2 **TFTP** 확인란에 체크 표시하여 원격 클러스터의 TFTP를 활성화합니다.

단계 3 **TFTP** 를 클릭합니다.

단계 4 원격 클러스터 서비스 수동 재정의 구성] 창에서 원격 서비스 주소 수동 구성을 선택합니다.

단계 5 TFTP 서버의 IP 주소를 입력하여 이들 TFTP 서버에 대한 피어 관계를 만듭니다.

TFTP 서버 IP 주소는 최대 3개까지 입력할 수 있습니다.

단계 6 (선택 사항) 프록시 TFTP 서버가 보안 클러스터에 구축된 경우, 클러스터가 안전하다 확인란에 체크 표시합니다.

단계 7 저장을 클릭합니다.

다음에 수행할 작업

엔드포인트의 TVL(신뢰 확인 목록, Trust Verification Lists)에 원격 TFTP 서버를 추가해야만 합니다. 그렇지 않으면, 원격 클러스터의 프록시 TFTP 서버에서 구성 파일을 승인하지 않습니다. 자세한 지침은 엔드포인트 디바이스를 지원하는 설명서를 참조하십시오.

TFTP 서버에 대한 CTL 파일 업데이트

혼합 모드에 있는 각 클러스터에서 `utils ctl`을 실행하여 퍼블리셔 노드의 CTL 파일을 업데이트합니다. 프록시 TFTP 서버와 모든 인터클러스터에 완전한 보안 네트워크가 확보되었는지 확인하십시오. 즉, 이는 프록시 및 원격 인터클러스터 인증서의 벌크 가져오기 및 내보내기 교환을 의미합니다.

CTLClient를 사용하는 동안 기본 TFTP 서버 또는 기본 TFTP 서버의 IP 주소를 혼합 모드로 실행 중인 원격 클러스터의 모든 TFTP 서버에 대한 Cisco CTL(Certificate Trust List) 파일에 추가해야 합니다. 이렇게 하는 이유는 보안 활성 클러스터의 엔드포인트에서 구성 파일을 성공적으로 다운로드할 수 있도록 지원하기 위해서입니다.

보안 및 Cisco CTL CLI 사용에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 보안 설명서에서 "Cisco CTL 설정 정보" 섹션을 참조하십시오.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.애플리케이션 > 플러그인.

단계 2 설치할 수 있는 모든 플러그인의 목록에 찾기를 클릭합니다.

단계 3 Cisco CTL 클라이언트에 대한 다운로드 링크를 클릭합니다.
시스템에서 TFTP 서버에 저장된 인증서를 디지털 서명한 클라이언트를 설치합니다.

단계 4 TFTP 서버를 재부팅합니다.

TFTP 서버에 대한 비 구성 파일 수정

엔드포인트가 프록시 TFTP 서버에서 요청하는 로드 파일 또는 `RingList.xml`과 같은 비구성 파일을 수정할 수 있습니다. 이 절차를 완료한 후에는 수정된 파일을 프록시 TFTP 서버의 TFTP 디렉터리에 업로드합니다.

프로시저

단계 **1** Cisco Unified Communications 운영체제 관리에서 소프트웨어 업그레이드 > **TFTP** 파일 관리를 선택합니다.
TFTP 파일 관리 창이 나타납니다.

단계 **2** 파일 업로드를 클릭합니다.
파일 업로드 팝업이 나타납니다.

단계 **3** 다음 작업 중 하나를 수행합니다.

- 찾아보기를 클릭하여 업로드할 파일의 디렉터리 위치를 찾습니다.
- 업데이트된 파일의 전체 디렉터리 경로를 디렉터리 필드에 붙여 넣습니다.

단계 **4** 파일 업로드를 클릭하거나 닫기를 클릭하여 파일을 업로드하지 않은 상태로 종료합니다.

다음에 수행할 작업

Cisco Unified Serviceability 관리를 사용하여 프록시 TFTP 노드에서 Cisco TFTP 서비스를 중지했다가 다시 시작합니다.

TFTP 서비스 시작 및 중지

다음 절차를 사용하여 프록시 TFTP 노드에서 TFTP 서비스를 중지하고 다시 시작합니다.

서비스 활성화에 대한 자세한 내용은 *Cisco Unified Serviceability* 관리 설명서를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 참조하십시오.

프로시저

단계 **1** Cisco Unified Serviceability에서 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **2** 제어 센터-기능 서비스 창에서 서버 드롭다운 목록에서 프록시 TFTP 노드를 선택합니다.

단계 **3** **CM** 서비스 영역에서 TFTP 서비스를 선택하고 중지를 클릭합니다.

상태가 변경되어 업데이트된 상태가 반영됩니다.

팁 서비스의 최신 상태를 보려면 새로 고침을 클릭합니다.

단계 **4** **CM** 서비스 영역에서 TFTP 서비스를 선택한 다음 시작을 클릭합니다.

상태가 변경되어 업데이트된 상태가 반영됩니다.

34 장

활성화 코드를 통해 디바이스 온보딩

활성화 코드 개요

활성화 코드를 사용하면 새로 프로비저닝된 전화기를 온보딩하기가 쉬워집니다. 활성화 코드는 사용자가 전화기를 등록하는 동안 반드시 입력해야 하는 16자리 일회용 값입니다. 활성화 코드는 관리자가 각 전화기의 MAC 주소를 수동으로 수집하고 입력할 필요 없이 전화기를 프로비저닝하고 온보딩하는 간단한 방법을 제공합니다. 이 방법은 다수의 전화기, 단일 전화기를 프로비저닝하거나 심지어 기존 전화기를 다시 등록하기 위해 사용 할 수 있는 간단한 자동 등록 대체 방법입니다.

또한 활성화 코드를 사용하여 모바일 및 원격 액세스를 쉽고 안전하게 등록할 수 있도록 모바일 및 원격 액세스 규정 준수 디바이스를 사용할 수도 있습니다.

활성화 코드 디바이스 온보딩은 다음 모드에서 작동합니다.

- 온프레미스
- 모바일 원격 액세스(MRA)

참고 TFTP 프록시 설정에서는 활성화 코드 온보딩 및 MRA를 사용한 엔드포인트 등록을 지원하지 않습니다.

활성화 코드는 다음과 같은 이점을 제공합니다.

- 활성화 코드를 사용하는 온보딩은 새롭게 프로비저닝된 모든 전화기 또는 신뢰할 수 없는 전화기를 Unified Communications Manager에서 평가하고 확인하도록 보장합니다

참고 온보딩 활동을 수행하려면 Cisco 제조 루트 인증서가 CallManager-trust 저장소에 있어야만 합니다.

- 수동으로 실제 MAC 주소를 입력할 필요는 없습니다. 관리자는 더미 MAC 주소를 사용할 수 있으며, 등록 도중 전화기가 실제 MAC 주소로 구성을 자동으로 업데이트 합니다.
- TAPS와 같은 IVR을 구축하여 BAT에서 SEP로 전화기 이름을 변경할 필요는 없습니다.

전화기 사용자는 셀프 서비스 포털을 통해 활성화 코드를 입수할 수 있습니다. 단, 활성화할 준비가 된 전화기 표시 엔터프라이즈 매개변수가 참으로 설정되어 있어야 합니다. 그렇지 않으면 관리자가 전화 사용자에게 코드를 제공해야 합니다.

참고 BAT MAC 주소를 사용하여 프로비저닝할 경우, 활성화 코드는 전화기 모델에 연결됩니다. BAT MAC은 'BAT'로 시작하는 디바이스명에 대한 참조이며, MAC 주소처럼 보이는 임의의 12자의 16진수가 표시됩니다. 디바이스 설정 페이지를 MAC 주소 필드가 빈 상태로 저장할 경우, 이런 형식을 갖는 임의의 이름이 생성됩니다.전화기를 활성화하려면 전화기 모델과 일치하는 활성화 코드를 입력해야 합니다.

추가 보안을 위해 전화기의 실제 MAC 주소로 전화기를 프로비저닝할 수 있습니다. 프로비저닝하는 동안 관리자는 각 전화기의 MAC 주소를 수집하고 입력해야만 하기 때문에 이 옵션은 더 많은 구성을 포함합니다. 하지만 사용자가 전화기의 실제 MAC 주소와 일치하는 활성화 코드를 입력해야 하기 때문에 더 뛰어난 보안을 제공합니다.

기술적 제한으로 인해 활성화 코드를 통한 장치 온보딩은 프록시 TFTP 구축에서 지원되지 않습니다.

온프레미스 모드의 온보딩 프로세스 플로우

다음은 활성화 코드를 통해 온보딩 새 전화기에 대한 프로세스 플로우입니다.

1. 관리자는 사용자가 온보딩에 대한 활성화 코드를 입력하도록 구성을 설정합니다.
2. 관리자가 전화기를 프로비저닝하고 구성합니다. BAT MAC 주소를 사용 중인 경우, 관리자는 실제 MAC 주소를 입력하지 않습니다.
3. 전화기는 DHCP opt 150 또는 전화기 설정에 구성된 대로 대체 TFTP를 통해 TFTP의 IP 주소를 가져옵니다. 전화기는 XMLDefault 파일을 다운로드하고 활성화 코드가 사용 중인 것을 감지합니다.
4. 사용자는 전화기에 활성화 코드를 입력합니다.
5. 전화기에서 활성화 코드 및 제조업체에서 설치한 인증서를 통해 Cisco Unified Communications Manager를 인증합니다.
6. 활성화 코드를 온보딩 전화기에 사용하는 경우 전화기에 TVS 서비스가 필요합니다. ITL 파일은 통합 CM 서버 TCP 포트 2445에서 실행되는 TVS 서비스 인증서를 포함하는 이 TVS 기능을 제공합니다.

7. Cisco Unified Communications Manager에서 실제 MAC 주소로 디바이스 구성을 업데이트합니다. TFTP 서버에서 전화기의 디바이스 구성을 감지하여 전화기를 등록할 수 있도록 허용합니다. 디바이스 등록에는 최대 5분이 소요될 수 있습니다.

참고 온프레미스 활성화 코드 온보딩에 대한 기본 통신 관리자 그룹에는 추가 가입자를 추가하는 것이 좋습니다. 그렇지 않으면, 기본 통신 관리자 그룹의 노드가 다운되면 온보딩 문제가 발생할 수 있습니다.

모바일 및 원격 액세스 모드에서 온보딩 프로세스 플로우

다음은 모바일 및 원격 액세스 모드를 사용할 때 활성화 코드를 통해 새 전화기를 온보딩하기 위한 프로세스 플로우입니다.

1. 관리자는 Cisco Cloud를 사용하여 활성화 코드 온보딩을 활성화하기 위해 클라우드/하이브리드 통신을 구성하고, 모바일 및 원격 액세스 활성화 도메인을 지정합니다.
2. 필요한 경우, 관리자는 추가 모바일 및 원격 액세스 서비스 도메인을 구성합니다.
3. 관리자는 MAC 주소(BAT, AXL, GUI)를 지정하지 않은 상태로 전체 디바이스 구성을 생성합니다. 디바이스 이름은 임의의 BAT MAC 주소입니다.
4. 관리자가 이 디바이스에 대한 활성화 코드를 요청합니다. 디바이스 활성화 서비스에서 클라우드 기반 디바이스 활성화 서비스에서 코드를 요청합니다.
5. 사용자는 셀프 서비스 포털에서 코드를 가져오거나 관리자가 사용자에 코드를 보낼 수 있습니다.
6. 사용자는 전화기에 전원을 공급하고 활성화 코드를 입력합니다.
7. 전화기는 클라우드에서 Expressway의 위치를 학습하고 모바일 및 원격 액세스/Cisco Unified Communications Manager를 인증합니다.
8. 디바이스 활성화 서비스에서 전화기의 MAC 주소로 데이터베이스의 디바이스 구성을 업데이트합니다.

   이제 전화기에서 일반 모바일 및 원격 액세스처럼 TFTP에서 전화기별 구성 파일을 등록하고 가져올 수 있으며, Cisco Unified Communications Manager에 등록할 수 있습니다.

참고 홈 원격 사용자의 작업을 위한 보안 솔루션을 제공하기 위해 TRP가 아닌 Expressway의 모바일 및 원격 접속을 권장합니다.

활성화 코드 사전 요건

릴리스 12.5(1)부터 Cisco IP 전화기 모델(7811, 7821, 7832, 7841, 7861, 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 및 8865NR)은 활성화 코드를 통해 온보딩을 지원합니다.

릴리스 12.5SR3은 온프레미스 및 MRA 모두에 대해 Cisco IP 전화기 모델의 온보딩을 지원합니다.

또한 릴리스 12.5(1)SU1은 Cisco IP 전화기 모델 8832 및 8832NR를 지원합니다.

클라우드 온보딩 프로세스의 경우, Cisco Unified Communications Manager에서 다음 도메인 이름을 확인해야 합니다.

- fos-a.wbx2.com
- idbroker.webex.com
- push.webexconnect.com
- btpush.webexconnect.com

셀프 서비스 포털

사용자가 셀프 서비스 포털을 사용하여 전화기를 온보드하려고 계획하고 있는 경우, 사용자가 액세스 권한을 갖도록 사전에 포털을 설정해야 합니다. 자세한 내용은 *Cisco Unified Communications Manager* 에 대한 기능 구성 설명서의 "셀프 서비스 포털" 장으로 이동하십시오.

온프레미스 모드에서 활성화 코드 작업 플로우를 사용하는 디바이스 온보딩

활성화 코드를 사용하여 새 전화기를 온보딩하기 위해 이러한 작업을 완료합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	디바이스 활성화 서비스 활성화, 387 페이지	**Cisco Device Activation** 서비스가 Cisco Unified Serviceability에서 실행되어야만 합니다.
단계 **2**	등록 방법 설정하여 활성화 코드 사용, 387 페이지	디바이스 기본값에 따라 기본 등록 방법을 설정하여 지원되는 전화기 모델에 대한 활성화 코드를 사용합니다.
단계 **3**	활성화 코드 요구 사항을 사용하여 전화기를 프로비저닝합니다. 다음은 두 가지 프로비저닝 옵션의 예입니다.	Cisco Unified Communications Manager에는 왼쪽의 옵션을 포함하여 다양한 프로비저닝 방법이 있습니다. 어떤 방법을 선택하든 해당 전

	명령 또는 동작	목적
	• 활성화 코드 요구 사항으로 전화기 추가, 388 페이지 • 벌크 관리를 통해 활성화 코드로 전화기 추가, 389 페이지	화기의 전화기 설정 내에서 온보딩에 대한 활성화 코드 필요 확인란이 체크 표시되었는지 확인하십시오.
단계 **4**	전화기 활성화, 392 페이지	사용자에게 활성화 코드를 분배합니다. 전화기를 사용하려면 사용자가 전화기에 코드를 입력해야 합니다.

디바이스 활성화 서비스 활성화

활성화 코드를 사용하려면 Cisoc Unified Serviceability에서 **Cisco** 디바이스 활성화 서비스가 실행되고 있어야만 합니다. 이 절차를 사용하여 서비스가 실행 중인지 확인하십시오.

프로시저

단계 **1** Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.
단계 **2** 서버 드롭다운에서 Unified Communications Manager 퍼블리셔 노드를 선택하고 이동을 클릭합니다.
단계 **3** **CM** 서비스에서 **Cisco** 디바이스 활성화 서비스의 상태가 활성화됨인지 확인하십시오.
단계 **4** 서비스가 실행되고 있지 않은 경우, 인접한 확인란에 체크 표시하고 저장을 클릭합니다.

다음에 수행할 작업

등록 방법 설정하여 활성화 코드 사용, 387 페이지

등록 방법 설정하여 활성화 코드 사용

이 절차를 사용하여 특정 모델 유형의 전화기에서 활성화 코드를 사용하여 Unified Communications Manager에 등록할 수 있도록 시스템 기본값을 구성합니다.

참고 이 절차는 온프레미스 엔드포인트의 온보딩에만 적용됩니다. 디바이스 기본값에서 온보딩 방법 설정은 활성화 코드를 사용하는 모바일 및 원격 액세스 엔드포인트의 온보딩에는 적용되지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 디바이스 기본값을 선택합니다.

단계 **2** 디바이스 기본값 설정 창에서 듀얼 뱅크 정보 섹션에서 등록을 위한 활성화 코드를 사용하는 디바이스 유형을 선택하고, 자동 등록에서 활성화 코드로 구축형 온보딩 방법을 변경합니다.

단계 **3** 저장을 클릭합니다.

참고 디바이스 기본값을 활성화 코드로 설정하고 전화기 유형에 대해 자동 등록이 이전에 사용된 경우, 이어지는 새 전화기 추가는 활성화 코드 온보딩 또는 전화기와 등록의 수동 구성(MAC 주소 사용)을 따라야 합니다.

자세한 내용은 새 전화기를 프로비저닝하기 위해 활성화 코드 요구 사항으로 전화기 추가및 벌크 관리를 통해 활성화 코드로 전화기 추가 섹션을 참조합니다.

활성화 코드 요구 사항으로 전화기 추가

활성화 코드 요구 사항으로 새 전화기를 설정하려면 이 절차를 사용합니다.

시작하기 전에

프로비저닝 프로세스를 더 빠르게 만들기 때문에 적용하려는 설정을 사용하여 범용 디바이스와 회선 템플릿을 구성합니다.

참고 템플릿을 사용하지 않기로 선택하면 새로운 전화를 추가하고 수동으로 설정을 구성하거나 BAT 템플릿을 통해 설정을 추가할 수 있습니다. 각각의 경우에 온보딩 활성화 코드 필요 확인란을 전화 설정 창에서 체크 표시해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.디바이스 > 전화기.

단계 **2** 템플릿에서 새로 추가를 클릭하여 범용 회선 또는 디바이스 템플릿에서 설정을 추가합니다.

단계 **3** 전화 유형 드롭다운 메뉴에서 전화기 모델을 선택합니다.

단계 **4** **MAC** 주소 필드에서 MAC 주소를 입력합니다. 활성화 코드로 더비 MAC 주소 또는 전화기의 실제 MAC 주소를 사용할 수 있습니다.

다음 시나리오에서 전화기의 MAC 주소를 수정할 수 있습니다.

- **BAT{mac}->SEP{mac}**: 접두사에 대한 정확한 디바이스 이름을 알아야 `?BAT?`에서 `?SEP?`으로 저장 즉시 변경할 수 있습니다.
- **SEP{mac}->BAT{mac}:** 접두사에 대한 MAC 주소를 공란으로 두어 `?SEP?`에서 `?BAT?`으로 변경하고 새 디바이스명을 `?BAT?`의 접두사로 변경할 수 있습니다..

활성화 코드가 활성화되어 있는 경우, **MAC** 주소 필드는 공란으로 남겨둘 수 있습니다. 더미 MAC 주소로 자동으로 채워집니다.

단계 **5** 디바이스 템플릿 드롭다운에서 적용하고자 하는 설정이 포함된 기존 범용 디바이스 템플릿과 같은 템플릿을 선택합니다.

단계 **6** 디렉터리 번호 필드에서 기존 디렉터리 번호를 선택하거나 New를 클릭하고 다음을 진행합니다.

a) 새 내선 번호 추가 팝업에서 디렉터리 번호와 적용하고자 하는 설정이 포함된 회선 템플릿을 입력합니다.

b) 저장을 클릭한 다음 닫기를 클릭합니다.
새 내선 번호가 디렉터리 번호 필드에 표시됩니다.

단계 **7** (선택 사항) 사용자 필드에서 이 전화기에 적용하려는 사용자 ID를 선택합니다.

단계 **8** 추가를 클릭합니다.

단계 **9** 온보딩용 활성화 코드 필요 확인란에 체크 표시합니다. 모바일 및 원격 액세스 모드의 경우, 모바일 및 원격 액세스를 통한 활성화 코드 허용 확인란에 체크 표시합니다.

단계 **10** 적용하고자 하는 모든 다른 설정을 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **11** 저장을 클릭한 다음 확인을 클릭합니다.
전화기 설정에서 활성화 코드를 생성합니다. 코드를 보려는 경우 활성화 코드 보기를 클릭합니다.

다음에 수행할 작업

전화기 활성화, 392 페이지

벌크 관리를 통해 활성화 코드로 전화기 추가

이 선택적 작업 플로우에는 벌크 관리 도구의 전화기 삽입 기능을 사용하여 단일 작업에 다수의 전화기를 프로비저닝하는 예가 포함되어 있습니다. 이러한 전화기는 등록을 위해 활성화 코드를 사용합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	BAT 프로비저닝 템플릿 구성, 389 페이지	프로비저닝된 전화기에 적용하려는 설정을 포함한 BAT 템플릿을 구성합니다.
단계 **2**	새 전화기로 CSV 파일 생성, 390 페이지	추가하려는 새 전화기를 포함한 CSV 파일을 생성합니다.
단계 **3**	전화기 삽입, 391 페이지	벌크 관리의 전화기 삽입 기능을 사용하여 새 전화기를 데이터베이스에 추가합니다.

BAT 프로비저닝 템플릿 구성

이 절차를 사용하여 새롭게 프로비저닝된 특정 모델의 전화기에 벌크 관리를 통해 적용할 수 있는 일반 설정으로 전화기 템플릿을 생성합니다.

시작하기 전에

이 절차에서는 사용자가 이미 시스템에 구축되어 있고 사용자가 자신의 요구를 충족하는 디바이스 풀, SIP 프로파일 및 전화기 보안 프로파일을 이미 설정한 것으로 가정합니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 벌크 관리 > 전화기 > 전화기 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화기 유형 드롭다운 목록에서 템플릿을 생성하려는 전화기 모델을 선택합니다.

단계 **4** 템플릿 이름을 입력합니다.

단계 **5** 온보딩용 활성화 코드 필요 확인란에 체크 표시합니다. 모바일 및 원격 액세스 모드의 경우, 모바일 및 원격 액세스를 통한 활성화 코드 허용 확인란에 체크 표시합니다.

단계 **6** 다음과 같은 필수 필드에 대한 값을 구성합니다.

- 디바이스풀
- 전화기 버튼 템플릿
- 소유자 사용자 ID
- 디바이스 보안 프로필
- SIP 프로파일

단계 **7** 전화기 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

새 전화기로 CSV 파일 생성, 390 페이지

새 전화기로 CSV 파일 생성

이 절차를 사용하여 새 전화기로 새 csv 파일을 생성합니다.

참고 csv 파일을 수동으로 생성할 수도 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.

단계 **2** 찾기를 클릭합니다.

단계 **3** **bat.xlt** 스프레드시트를 선택하고 다운로드합니다.

단계 **4** 스프레드시트를 열고 전화기 탭으로 이동합니다.

단계 **5** 새 전화기 세부 정보를 스프레드시트에 추가합니다. 더미 MAC 주소를 사용 중인 경우, MAC 주소 필드를 비워 둡니다. 온보딩용 활성화 코드 필요 확인란에 체크 표시합니다. 모바일 및 원격 액세스 모드의 경우, 모바일 및 원격 액세스를 통한 활성화 코드 허용 확인란에 체크 표시합니다.

단계 **6** 완료하면 **BAT** 형식으로 내보내기를 클릭합니다.

단계 **7** Cisco Unified CM 관리에서 벌크 관리 > 파일 업로드/다운로드를 선택합니다.

단계 **8** csv 파일을 업로드합니다.

a) 새로 추가를 클릭합니다.
b) 파일 선택을 클릭하고 업로드할 csv 파일을 선택합니다.
c) 대상으로 전화기를 선택합니다.
d) 트랜잭션 유형에 대한 전화기 특정 세부 정보 삽입을 선택합니다.
e) 저장을 클릭합니다.

다음에 수행할 작업

전화기 삽입, 391 페이지

전화기 삽입

이 절차를 사용하여 csv 파일의 새 전화기를 삽입합니다.

프로시저

단계 **1** 벌크 관리 > 전화기 > 전화기 삽입을 선택합니다.

단계 **2** 파일 이름 드롭다운에서 자신의 csv 파일을 선택합니다.

단계 **3** 전화기 템플릿 이름 드롭다운에서 생성한 프로비저닝 템플릿을 선택합니다.

단계 **4** 더미 **MAC** 주소 생성 확인란에 체크 표시합니다.

참고 추가 보안을 위해, MAC 주소에 일치하는 전화기에만 활성화 코드가 작동하할 수 있도록, 실제 MAC 주소를 csv 파일에 추가할 수 있습니다. 이 경우 이 확인란을 체크 표시하지 않은 상태로 그대로 둡니다.

단계 **5** 즉시 실행 확인란에 체크 표시하여 해당 작업을 즉시 실행합니다. 나중에 작업을 실행하기로 선택한 경우, 벌크 관리 도구의 작업 스케줄러에서 작업에 대한 일정을 잡아야만 합니다.

단계 **6** 제출을 클릭합니다.

다음에 수행할 작업

전화기 활성화, 392 페이지

전화기 활성화

프로비저닝 이후 전화기를 활성화할 수 있도록 활성화 코드를 전화기 사용자에게 분배합니다. 다음은 활성화 코드를 수집 및 분배하기 위한 두 가지 옵션입니다.

- 셀프 서비스 포털—전화기 사용자는 셀프 서비스 포털에 로그인하여 전화기에 적용되는 활성화 코드를 받을 수 있습니다. 전화기의 코드를 수동으로 입력하거나 전화기의 비디오 카메라를 사용하여 자가 관리에 표시되는 바코드를 스캔할 수 있습니다. 두 방법 중 하나가 작동합니다. 자가 관리를 사용하여 전화기를 활성화하려면 Cisco Unified Communications Manager에서 활성화할 준비가 된 전화기 표시 엔터프라이즈 매개변수를 참으로 설정해야만 합니다(기본 설정).

참고 셀프 서비스 포털에 대한 사용자 액세스 구성 방법에 대한 추가 요구 사항은 *Cisco Unified Communications Manager*에 대한 기능 구성 설명서 "셀프 서비스 포털" 장을 참조하십시오.

- CSV 파일—미처리 사용자 및 활성화 코드 목록을 csv 파일로 내보내 사용자에 게 배포할 수도 있습니다. 절차에 대해서는 활성화 코드 내보내기, 392 페이지를 참조하십시오.

등록 프로세스

전화기 사용자는 전화기에 활성화 코드를 입력해야만 전화기를 사용할 수 있습니다. 전화기 사용자가 전화기에 올바른 활성화 코드를 입력한 후에는 다음과 같은 상황이 발생합니다.

- 전화기가 Cisco Unified Communications Manager를 통해 인증됩니다.
- Cisco Unified Communications Manager의 전화기 구성은 전화기의 실제 MAC 주소를 통해 업데이트됩니다.
- 전화기는 TFTP 서버에서 구성 파일 및 기타 관련 파일을 다운로드하고 Cisco Unified Communications Manager에 등록합니다.

향후 작업

이제 전화기를 사용할 수 있습니다.

활성화 코드 내보내기

이 절차를 사용하여 등록 코드의 csv 파일을 해당 전화기 및 사용자와 함께 내보냅니다. 이 파일을 사용하여 사용자에 게 활성화 코드를 배포할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다.

단계 **2** 관련 링크에서 활성화 코드 내보내기를 선택하고 이동을 클릭합니다.

디바이스 온보딩 작업 플로우(모바일 및 원격 액세스 모드)

이러한 작업을 완료하여 모바일 및 원격 액세스 모드에서 활성화 코드를 사용하여 새로 전화기를 온보딩합니다.

시작하기 전에

Cisco Device Activation 서비스가 Cisco Unified Serviceability에서 실행되어야만 합니다(이 서비스는 기본으로 실행됩니다). 서비스가 실행되고 있는지 확인하려면 디바이스 활성화 서비스 활성화, 387 페이지를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	모바일 및 원격 액세스를 통한 Cisco Cloud 온보딩 활성화, 394 페이지	클라우드 온보딩에서 바우처를 생성하고, 활성화 코드 온보딩을 활성화하고, 모바일 및 원격 액세스 활성화 도메인을 지정합니다.
단계 **2**	모바일 및 원격 액세스 서비스 도메인 구성(선택 사항), 394 페이지	클러스터를 클라우드에 온보딩하여 특정 모바일 및 원격 액세스 활성화 도메인으로 원격 모바일 및 원격 액세스 디바이스 온보딩을 허용합니다.
단계 **3**	사용자 지정 인증서 업로드(선택 사항), 394 페이지	(선택 사항) 사용자 지정 인증서를 사용하려는 경우, 원격 모바일 및 원격 액세스 엔드포인트가 클라우드에서 해당 인증서를 다운로드하여 Expressway에 연결하는 데 사용할 수 있습니다.
단계 **4**	활성화 코드 요구 사항을 사용하여 전화기를 프로비저닝합니다. 다음은 두 가지 프로비저닝 옵션의 샘플입니다. • 활성화 코드 요구 사항으로 전화기 추가, 388 페이지 • 벌크 관리를 통해 활성화 코드로 전화기 추가, 389 페이지	Unified CM 데이터베이스에서 전화기를 프로비저닝해야 합니다. Unified CM에는 이러한 샘플 옵션을 포함하여 사용할 수 있는 다양한 프로비저닝 방법이 있습니다.
단계 **5**	전화기 활성화, 392 페이지	사용자에게 활성화 코드를 분배합니다. 전화기를 사용하려면 사용자가 전화기에 코드를 입력해야 합니다.

모바일 및 원격 액세스를 통한 **Cisco Cloud** 온보딩 활성화

프로시저

단계 **1** 클라우드 기반 디바이스 활성화 서비스에 연결 하기 위해 클러스터(CCMAct 서비스)에 권한을 부여하려면, 바우처 생성 버튼을 클릭하여 바우처를 생성합니다.

단계 **2** 모바일 및 원격 액세스 활성화 도메인을 지정합니다 (이는 모바일 및 원격 액세스 서비스 도메인 목록에 자동으로 복사됩니다).

단계 **3** '모바일 및 원격 액세스 온보딩 활성화' 및 '모바일 및 원격 액세스 온보딩' 확인란에 체크 표시하여 활성화 코드 온보딩을 활성화합니다. '자동 등록'을 사용하여 디바이스 기본값 온보딩을 구성한 경우, '모바일 및 원격 액세스 모드의 전화기에만 작동하므로 '모바일 및 원격 액세스 온보딩 허용' 확인란가 비활성화되었다가 자동으로 체크 표시됩니다. '코드 활성화'를 사용하여 디바이스 기본값 온보딩을 구성한 경우, 두 확인란을 모두 사용할 수 있습니다.

단계 **4** 저장을 클릭합니다.

모바일 및 원격 액세스 서비스 도메인 구성(선택 사항)

전화기에 대한 모바일 및 원격 액세스 서비스 도메인을 구성하려면 다음 절차를 따르십시오.

프로시저

단계 **1** 고급 기능 > 모바일 및 원격 액세스 서비스 도메인을 선택하여 모바일 및 원격 액세스 서비스 도메인 창에 액세스합니다.

단계 **2** 모바일 및 원격 액세스 서비스 도메인 이름을 입력합니다.

단계 **3** 활성화에 사용하는 Expressway-E용 SRV 레코드를 입력합니다.

단계 **4** 선택한 도메인 옆의 기본값 확인란을 체크 표시하여 기본 모바일 및 원격 액세스 서비스 도메인을 선택합니다. 이 도메인은 디바이스풀 수준에서 '< None >'을 선택할 때 사용합니다.

단계 **5** 디펜던시의 수를 나열하기도 하는 해당 레코드의 행에 있는 링크를 사용하여 디펜던시 레코드에 액세스합니다.

사용자 지정 인증서 업로드(선택 사항)

사용자 지정 인증서를 업로드하려면, 아래 절차를 사용합니다.

프로시저

단계 **1** Expressway에 인증서를 업로드합니다. 다른 인증서는 제거하지 마십시오.

단계 **2** 경로 **CUCM OS** 관리>인증서 관리를 사용하여 Unified Communications Manager에 새 인증서를 업로드합니다. “Phone-Edge-trust” 유형을 사용합니다. (Unified Communications Manager에서는 이를 클라우드로 보낸 다음 전화기로 전송하여 Expressway에 액세스합니다.)

단계 **3** 원하는 대로 다른 "Phone-Edge-trust" 유형의 인증서를 모두 제거하여 사용자 지정 인증서가 유일한 사용 중인 인증서가 되게 합니다.

활성화 코드에 대한 추가 작업

다음 표에는 활성화 코드에 필요할 수 있는 추가 작업이 나와 있습니다.

작업	절차
등록된 전화기에 대한 활성화 코드 생성	이미 등록된 전화에 대한 활성화 코드를 생성하려면 다음을 수행합니다. **1.** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다. **2.** 활성화 코드를 생성하려는 전화기에 대한 전화기 구성을 찾고 이를 엽니다. **3.** 온보딩용 활성화 코드 필요 확인란에 체크 표시하고, 저장을 클릭합니다.
미등록 전화기에 대한 활성화 코드 다시 생성	새 전화기에 대한 활성화 프로세스가 실패하는 경우와 같이 미등록 전화기에 대한 새 활성화 코드를 생성하려면, 다음 작업을 수행합니다. **1.** Cisco Unified CM 관리에서 디바이스 > 전화기를 선택합니다. **2.** 활성화 코드를 생성하려는 전화기에 대한 전화기 구성을 찾고 이를 엽니다. **3.** 활성화 코드 릴리스를 클릭합니다. **4.** 새 활성화 코드 생성을 클릭하고, 저장을 클릭합니다.

작업	절차
선택적 활성화 코드 매개변수 설정	활성화 코드에 대한 선택적 서비스 매개변수를 구성하려는 경우, 다음을 수행합니다. **1.** Cisco Unified CM 관리에서 시스템 > 서비스 매개변수를 선택합니다. **2.** 서버 드롭다운 목록에서 퍼블리셔 노드를 선택합니다. **3.** 서비스 드롭다운에서 **Cisco Device Activation** 서비스를 선택합니다. **4.** 다음과 같은 선택적 서비스 매개변수에 대한 값을 구성합니다. 설정에 대한 도움말은 상황별 도움말을 참조하십시오. • 활성화 **TTL(Time to Live)(**시간**)**—활성화 코드가 활성 상태로 유지되는 시간입니다. 기본값 168 • 모바일 및 원격 액세스 활성화 사용—이를 참으로 설정하여 모바일 및 원격 액세스 활성화를 사용합니다. • 모바일 및 원격 액세스 활성화 도메인—모바일 및 원격 액세스 디바이스 활성화가 발생하는 도메인입니다. **5.** 저장을 클릭합니다.

활성화 코드 사용 사례

다음 표에서는 활성화 코드를 통해 디바이스 온보딩을 사용하는 샘플 사용 사례를 보여줍니다.

사용 사례	설명
기존 전화기를 교체합니다	활성화 코드를 사용하면 기존 전화기를 쉽게 교체할 수 있습니다. 예를 들어, 전화기가 손상되면 원격 작업자에게 새 전화기가 필요한 상황을 가정해 보겠습니다. • 관리자가 Unified Communications Manager에서 손상된 전화기에 대한 전화기 구성 설정을 엽니다. • 관리자가 **MAC** 주소를 공백으로 처리하고 온보딩을 위한 활성화 코드 필요 확인란에 체크 표시한 다음, 저장을 클릭합니다. • 사용자는 동일한 전화 모델의 새 전화를 얻고 해당 전화기를 네트워크에 연결합니다. • 사용자는 활성화 코드를 입수하기 위해 자가 관리에 로그인하고 전화기에 코드를 입력합니다. 전화기가 성공적으로 온보드됩니다. 참고 이 시나리오에서는 새로운 전화기 모델이 손상된 전화기와 동일한 모델이기만 하면 사용자가 새 전화기를 온보드할 수 있습니다. 더 안전한 환경에서 관리자가 대체 전화기를 프로비저닝하여 기존 전화기를 교체해야 할 수 있습니다(아래 참조).
활성화 코드를 사용한 새 전화기의 보안 배송	다음과 같이 특정 MAC 주소로 활성화 코드를 지정하여 전화기 배송 프로세스의 보안을 보장할 수 있는 더 뛰어난 보안 환경에서 다음을 수행합니다. • 관리자가 Unified Communications Manager에서 새 전화기를 프로비저닝합니다. • 새 전화기에 대한 전화기 구성 설정에서 관리자는 전화기의 실제 **MAC** 주소를 입력하고 온보딩용 활성화 코드 필요 확인란에 체크 표시합니다. • 관리자가 전화기를 포장하여 사용자에게 배송합니다. • 사용자가 새 전화기를 네트워크에 연결합니다. • 사용자가 활성화 코드를 입수하기 위해 자가 관리에 로그인하여 전화기에 코드를 입력합니다. 전화기가 성공적으로 온보드됩니다. 참고 이 시나리오에서 사용자는 특정 전화기만 온보드할 수 있습니다.

사용 사례	설명
새 전화기의 보안 배송(자동 등록)	활성화 코드 대신 자동 등록 및 TAPS를 사용하여 전화기를 원격 작업자에게 안전하게 배송할 수도 있습니다. • 디바이스 기본 구성에서 관리자는 전화기 모델에 대한 온보딩 방법이 자동 등록인지 반드시 확인하십시오. • 관리자가 Unified Communications Manager에서 새 전화기를 프로비저닝합니다. 새 전화기에 대한 전화기 구성에서 관리자는 전화기의 실제 **MAC** 주소를 공백으로 처리합니다. • 관리자가 전화기를 포장하여 사용자에게 배송합니다. • 사용자는 새 전화기를 네트워크에 연결하여 자동 등록을 진행합니다. • 사용자는 TAPS를 사용하여 자동 등록된 레코드를 이전 레코드로 다시 매핑합니다. 참고 이 시나리오에서는 자동 등록 및 TAPS를 모두 구성해야 합니다.
자동 등록을 통한 전화기 다시 온보딩	디바이스 기본 설정 창의 구축형 온보딩 방법을 통해 특정 전화기 모델에 대한 온보딩 방법을 활성화 코드와 자동 등록 간에 전환할 수 있습니다. 참고 자동 등록을 통해 기존 전화기를 다시 온보드하려는 경우, 데이터베이스에서 자동 등록이 작동하도록 기존 레코드를 삭제해야만 합니다.
모바일 및 원격 액세스 모드에서 사용하기 위한 온프레미스 전화기 온보딩	온프레미스로 전화기를 온보드한 다음, 모바일 및 원격 액세스 모드에서 다시 온보딩하기 위해 전화기를 표시하여 OAuth 연결에서 Expressway로 제공되는 보안과 Expressway에서 Cisco Unified Communications Manager로의 신뢰할 수 있는 연결을 활용할 수 있습니다. '모바일 및 원격 액세스를 통한 활성화 코드 허용'이 활성화된 상태인 이 시나리오에서는 전화기가 온프레미스로 온보드하고, 수신한 OAuth 액세스 토큰의 유효성을 검증하고, 모바일 및 원격 액세스 모드로 전환하고, Expressway와의 통신을 시작합니다. 내부 네트워크가 온프레미스에서 Expressway와의 통신을 허용하지 않는 경우, 전화기는 등록되지 않지만 오프프레미스에 전원이 공급되면 Expressway에 연결될 수 있습니다. 참고 미등록 오프프레미스 전화기는 펌웨어 로드를 업데이트할 수 없습니다. 이 시나리오는 최신 펌웨어를 다운로드하고 활성화 코드 기능을 사용하기 위해 프레미스에 있어야 하는 바로 사용 가능한 전화기의 경우에 유용 합니다. 전화기는 **MRA**를 통한 활성화 코드 허용 확인란에 체크 표시한 경우 MRA 모드로 전환되고 MRA 서비스 도메인 및 OAuth 토큰을 갖게 됩니다.

사용 사례	설명
제로 터치 온보딩을 통한 온프레미스 전화기 온보딩	온프레미스 전화기가 등록되고 보안 프로파일이 OAuth로 구성된 경우, 전화기가 재설정 또는 재시작 시에 액세스 토큰을 가지고 오게 됩니다.

35 장

자동 등록 구성

자동 등록 개요

자동 등록을 사용하면 Unified Communications Manager가 네트워크에 전화기를 연결할 때 자동으로 디렉터리 번호를 새 전화기에 할당할 수 있습니다.

자동 등록이 보안 모드에서 현재 활성화되어 있습니다. 이 기능 개선을 통해 새 전화기를 프로비저닝하면서 클러스트를 보호할 수 있기 때문에 시스템에 더 강력한 보안이 제공됩니다. 또한 새 전화기를 등록하기 위해 클러스터 보안을 비활성화할 필요가 없기 때문에 등록 프로세스가 간단해집니다.

911(비상) 및 0(운영자) 통화만 허용하는 디바이스 풀을 생성하는 경우, 자동 등록이 활성화되어 있을 때 무단 엔드포인트가 네트워크에 연결되는 것을 방지하기 위해 이를 사용할 수 있습니다. 새 엔드포인트는이 풀에 등록 될수 있지만 액세스는 제한되어 있습니다. 네트워크에 등록하기 위해 지속적으로 부팅 되는 무단 액세스는 차단됩니다. 자동 등록한 전화기를 디렉터리 번호에 영향을 주지 않으면서 새 위치로 옮기고 다른 디바이스 풀에 할당할 수 있습니다.

시스템에서 자동 등록 중인 새 전화기가 SIP 또는 SCCP를 실행하고 있는지 알 수 없으므로 자동 등록을 활성화할 때 이를 지정해야만 합니다. SIP 및 SCCP(예: Cisco IP 전화기 7911, 7940, 7941, 7960, 7961, 7970 및 7971)를 모두 지원하는 디바이스는 자동 등록 전화기 프로토콜로 불리는 엔터프라이즈 매개변수에 지정된 프로토콜에 자동 등록됩니다.

단일 프로토콜만 지원하는 디바이스는 해당 프로토콜에 자동 등록됩니다. [자동 등록 전화기 프로토콜] 설정이 재정의됩니다. 예를 들어, SCCP만 지원하는 모든 Cisco IP 전화기는 자동 등록 전화기 프로토콜 매개변수가 SIP로 설정된 경우에도 SCCP에 자동 등록됩니다.

자동 등록을 사용하여 100대 미만의 전화기를 네트워크에 추가할 것이 좋습니다. 100대 이상의 전화기를 추가하려면 BAT(Bulk Administration Tool)를 사용하십시오. 자세한 내용은 *Cisco Unified Communications Manager* 설명서를 http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html에서 참조하십시오.

자동 등록 작업 플로우 구성

자동 등록을 활성화하면 보안 위험이 따라옵니다. 네트워크에 새 엔드포인트를 추가하는 짧은 기간 동안만 자동 등록을 활성화합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	자동 등록에 대한 파티션 구성, 402 페이지	라우트 파티션을 특히 자동 등록용으로 구성하여 자동 등록된 전화기를 내부 통화 용도로만 제한합니다.
단계 **2**	자동 등록용 CSS(발신 검색 공간) 구성, 403 페이지	CSS(발신 검색 공간)을 특히 자동 등록용으로 구성하여 자동 등록된 전화기를 내부 통화로만 제한합니다.
단계 **3**	자동 등록을 위한 디바이스 풀 구성, 404 페이지	자동 등록에 대해 구성된 발신 검색 공간을 사용하는 디바이스 풀을 생성합니다.
단계 **4**	자동 등록을 위한 디바이스 프로토콜 유형 설정, 405 페이지	이 절차를 사용하여 자동 등록 중인 전화기 유형과 일치하도록 프로토콜을 SCCP 또는 SIP로 설정합니다.
단계 **5**	자동 등록 활성화, 406 페이지	자동 등록에 사용할 노드에서 자동 등록을 활성화하고 자동 등록 **Cisco Unified Communications Manager** 그룹 매개변수를 설정하여, 자동 등록에 사용해야 하는 Cisco Unified Communications Manager 그룹에 대해 자동 등록을 활성화합니다.
단계 **6**	자동 등록 비활성화, 408 페이지	새 디바이스의 등록을 완료하자마자 노드에 대한 자동 등록을 비활성화합니다.
단계 **7**	자동 등록 번호 재사용, 408 페이지	(선택 사항) 비활성화된 디바이스에 대한 자동 등록 번호는 재사용할 수 있습니다. 자동 등록 디렉터리 번호의 범위를 재설정하면, 시스템에서 시작 번호부터 다시 검색하도록 강제할 수 있습니다. 사용 가능한 디렉터리 번호는 다시 사용됩니다.

자동 등록에 대한 파티션 구성

라우트 파티션을 특히 자동 등록용으로 구성하여 자동 등록된 전화기를 내부 통화 용도로만 제한합니다.

프로시저

단계 1 Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스 > 파티션.

단계 2 새로 추가를 클릭하여 새 파티션을 생성합니다.

단계 3 파티션 이름, 설명 필드에 경로 플랜에 고유한 파티션 이름을 입력합니다.

파티션 이름에는 영숫자 문자는 물론 공백, 하이픈(-) 및 밑줄(_)을 사용할 수 있습니다. 파티션 이름에 대한 지침은 온라인 도움말을 참조하십시오.

단계 4 파티션 이름 뒤에 쉼표(,)를 입력하고 동일한 줄에 파티션 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자를 입력할 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\), 꺾쇠괄호(<>) 또는 대괄호([ ])는 사용할 수 없습니다.

설명을 입력하지 않으면 Cisco Unified Communications Manager에서 자동으로 이 필드에 파티션 이름을 입력합니다.

단계 5 여러 파티션을 생성하려면 각 파티션 항목마다 한 행을 사용합니다.

단계 6 시간 일정 드롭다운 목록에서 이 파티션과 연결할 시간 일정을 선택합니다.

시간 일정에서는 파티션이 수신 통화를 받을 수 있는 시기를 지정합니다. 없음을 선택하면, 파티션이 항상 활성 상태로 유지됩니다.

단계 7 구성할 다음 라디오 버튼 중 하나를 선택하고 시간대 를 구성합니다.

- 시작 디바이스—이 라디오 버튼을 선택하면 시스템은 발신 디바이스의 표준 시간대를 시간 일정과 비교하여 파티션을 수신 통화를 받는 데 사용할 수 있는지 여부를 확인합니다.
- 특정 표준 시간대—이 라디오 버튼을 선택한 후에 드롭다운 목록에서 표준 시간대를 선택합니다. 시스템은 선택한 표준 시간대를 시간 일정과 비교하여 수신 통화를 받는 데 파티션을 사용할 수 있는지 여부를 확인합니다.

단계 8 저장을 클릭합니다.

다음에 수행할 작업

자동 등록용 CSS(발신 검색 공간) 구성, 403 페이지

자동 등록용 CSS(발신 검색 공간) 구성

CSS(발신 검색 공간)을 특히 자동 등록용으로 구성하여 자동 등록된 전화기를 내부 통화로만 제한합니다.

시작하기 전에

자동 등록에 대한 파티션 구성, 402 페이지

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.통화 라우팅 > 제어 클래스 > 발신 검색 공간.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 이름 필드에 이름을 입력합니다.

각 발신 검색 공간 이름은 시스템에 고유해야 합니다. 이 이름은 최대 50자의 영숫자로 구성되고 공백, 마침표(.), 하이픈(-) 및 밑줄(_) 조합이 포함될 수 있습니다.

단계 **4** 설명 필드에 설명을 입력합니다.

설명에는 언어와 관계없이 최대 50자가 포함될 수 있지만 큰따옴표("), 퍼센트 기호(%), 앰퍼샌드(&), 백슬래시(\) 또는 꺾쇠 괄호(<>)는 사용할 수 없습니다.

단계 **5** 사용 가능한 파티션 드롭다운 목록에서 다음 단계 중 하나를 수행합니다.

- 단일 파티션의 경우 해당 파티션을 선택합니다.
- 여러 파티션의 경우 컨트롤**(CTRL)** 키를 누른 상태에서 해당 파티션을 선택합니다.

단계 **6** 상자 사이에서 아래쪽 화살표를 선택하여 선택한 파티션 필드로 파티션을 이동합니다.

단계 **7** (선택 사항) 선택한 파티션 상자 오른쪽의 화살표 키를 사용하여 선택한 파티션의 우선 순위를 변경합니다.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

자동 등록을 위한 디바이스 풀 구성, 404 페이지

관련 항목

CoS(서비스 종별), 184 페이지

자동 등록을 위한 디바이스 풀 구성

자동 등록을 위한 기본 디바이스 풀을 사용하거나 자동 등록을 위해 사용할 SIP 및 SCCP 디바이스에 대한 별도의 디바이스 풀을 구성할 수 있습니다.

자동 등록을 위한 기본 디바이스 풀을 구성하려면, 기본 Cisco Unified Communications Manager 그룹과 자동 등록 CSS(발신 검색 공간)을 기본 디바이스 풀에 할당합니다. SIP 및 SCCP 디바이스에 대해 별도의 기본 디바이스 풀을 구성하도록 선택한 경우, 기본 디바이스 풀 값을 사용합니다.

시작하기 전에

자동 등록용 CSS(발신 검색 공간) 구성, 403 페이지

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 디바이스 풀을 선택합니다.

단계 **2** 자동 등록을 위한 기본 디바이스 풀을 수정하려면 다음 작업을 수행합니다.

a) 찾기를 클릭한 다음 디바이스 풀 목록에서 기본값을 선택합니다.

b) 디바이스 풀 구성 창에서, 자동 등록에 대한 **CSS(**발신 검색 공간**)** 필드에서 자동 등록에 사용할 CSS를 선택한 다음 저장을 클릭합니다.

단계 **3** 자동 등록을 위한 새 디바이스 풀을 생성하려면 다음 작업을 수행합니다.

a) 새로 추가를 클릭합니다.

b) 디바이스 풀 구성 창에 디바이스 풀의 고유 이름을 입력합니다.

최대 50자까지 입력할 수 있으며, 영숫자, 마침표(.), 하이픈(-), 밑줄(_) 및 공백을 포함할 수 있습니다.

c) 기본 디바이스 풀과 일치하도록 다음 필드를 설정합니다. 필드 설명은 온라인 도움말을 참조하십시오.

- **Cisco Unified Communications Manager** 그룹에서 기본값을 선택합니다.
- 날짜/시간 그룹에서 **CMLocal**을 선택합니다.
- 지역에서 기본값을 선택합니다.

d) 자동 등록에 대한 **CSS(**발신 검색 공간**)** 필드에서 자동 등록에 사용할 CSS를 선택한 다음 저장을 클릭합니다.

다음에 수행할 작업

자동 등록을 위한 디바이스 프로토콜 유형 설정, 405 페이지

자동 등록을 위한 디바이스 프로토콜 유형 설정

SIP 및 SCCP 디바이스를 자동 등록하려는 경우, 먼저 자동 등록 전화기 프로토콜 매개변수를 SCCP로 설정하고 SCCP를 실행하는 모든 디바이스를 설치해야 합니다. 그런 다음 자동 등록 전화기 프로토콜 매개변수를 SIP로 변경하고 SIP를 실행하는 모든 디바이스를 자동으로 등록합니다.

시작하기 전에

자동 등록을 위한 디바이스 풀 구성, 404 페이지

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > 엔터프라이즈 매개변수를 선택합니다.

단계 **2** 엔터프라이즈 매개변수 설정 창에서 자동 등록 전화기 프로토콜 드롭다운 목록의 **SCCP** 또는 **SIP**를 선택하고 저장을 클릭합니다.

다음에 수행할 작업

자동 등록 활성화, 406 페이지

자동 등록 활성화

자동 등록을 활성화하면, 네트워크에 연결될 때 새로운 엔드포인트에 할당되는 여러 디렉터리 번호를 지정해야만 합니다. 각각의 새로운 엔드포인트가 연결될면, 다음 사용 가능한 디렉터리 번호가 할당됩니다. 모든 사용 가능한 자동 등록 디렉터리 번호가 모두 소진된 후에는, 더 이상 엔드포인트를 자동 등록할 수 없습니다.

새로운 엔드포인트가 자동 등록 **Cisco Unified Communications Manager** 그룹 설정이 활성화된 그룹의 첫 번째 Unified Communications Manager 노드에 자동 등록됩니다. 그런 다음 해당 노드는 각각의 자동 등록된 엔드포인트를 디바이스 유형에 따라 기본 디바이스 풀에 자동으로 할당합니다.

시작하기 전에

자동 등록을 위한 디바이스 프로토콜 유형 설정, 405 페이지

- 자동 등록 중인 디바이스 액세스를 제한하는 디바이스 풀, CSS(발신 검색 공간) 및 라우트 파티션을 생성하여 인터컴 전화만 허용합니다.
- 자동 등록 범위 내에서 디렉터리 번호를 사용할 수 있는지 확인하십시오.
- 새 전화기를 등록할 수 있는 충분한 라이센스 지점을 사용할 수 있는지 확인하십시오.
- 디바이스 기본값 구성 창에 SIP 및 SCCP의 올바른 전화기 이미지 이름이 표시되는지 확인하십시오. TFTP 서버에서 대부분의 공통 디바이스 구성 파일을 사용할 수 있어야 합니다. 그럼에도 디바이스에 대한 해당 구성 파일이 서버에 있는지 확인하십시오.
- Cisco TFTP 서버가 완전히 제대로 실행 중이고 TFTP의 DHCP 옵션에 올바른 서버가 지정되어 있는지 확인하십시오.

프로시저

단계 **1** Cisco 통합 커뮤니케이션 매니저 관리에서 시스템 > **Cisco** 통합 **CM**을 선택한 다음, **Cisco Unified Communications Managers** 찾기 및 나열 창에서 찾기를 클릭합니다.

단계 **2** 클러스터에서 Cisco Unified Communications Manager를 선택하여 자동 등록을 위해 사용합니다.

나타납니다.

단계 **3** **Cisco Unified CM Configuration** 창에서, 자동 등록 정보 섹션에서 노드에 대한 자동 등록 매개변수를 구성한 다음, 저장을 클릭합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

a) 드롭다운 목록에서 자동 등록에 사용할 범용 디바이스 템플릿을 선택합니다.

자동 등록을 위해 어떤 범용 디바이스 템플릿도 만들지 않은 경우, 기본 범용 디바이스 템플릿을 선택할 수 있습니다. 선택한 템플릿에서 사용자 관리 > 사용자/전화기 추가 > 범용 디바이스 템플릿에서 자동 등록에 사용할 디바이스 풀을 지정하고 있는지 확인하십시오.

b) 드롭다운 목록에서 자동 등록에 사용할 범용 회선 템플릿을 선택합니다.

자동 등록을 위해 어떤 범용 회선 템플릿도 만들지 않은 경우, 기본 범용 회선 템플릿을 선택할 수 있습니다. 선택한 템플릿에서 사용자 관리 > 사용자/전화기 추가 > 범용 회선 템플릿에서 자동 등록에 사용할 CSS(발신 검색 공간) 및 라우트 파티션을 지정하고 있는지 확인하십시오.

c) 시작 디렉터리 번호 및 종료 디렉터리 번호 필드에 시작 및 종료 디렉터리 번호를 입력합니다.

시작 디렉터리 번호와 종료 디렉터리 번호를 동일한 값으로 설정하면 자동 등록이 비활성화됩니다.

d) 이 **Cisco Unified Communications Manager**에서 자동 등록 비활성화를 선택 취소하여 이 노드에 대한 자동 등록을 활성화합니다.

항상 선택된 Unified Communications Manager 노드에서만 자동 등록을 활성화하거나 비활성화합니다. 자동 등록 기능을 클러스터에 포함된 다른 노드로 옮길 경우, Unified Communications Manager 노드, 기본 Unified Communications Manager 그룹, 그리고 사용한 기본 디바이스 풀을 다시 구성해야만 합니다.

단계 **4** 시스템 > **Cisco Unified CM** 그룹을 선택한 다음, 찾기를 **Cisco Unified Communications Manager** 그룹 찾기 및 나열 창에서 클릭합니다.

단계 **5** Unified Communications Manager 그룹을 선택하여 자동 등록을 위해 활성화합니다.

대부분 경우, 이 그룹의 이름이 기본값입니다. 다른 Cisco Unified Communications Manager 그룹을 선택할 수 있습니다. 그룹에는 하나 이상의 노드가 선택되어 있어야 합니다.

단계 **6** 해당 그룹에 대한 **Cisco Unified CM** 구성 창에서, 자동 등록 **Cisco Unified Communications Manager** 그룹을 선택하여 그룹에 대한 자동 등록을 활성화한 다음, 저장을 클릭합니다.

팁 선택한 **Cisco Unified Communications Manager** 목록에 자동 등록을 위해 구성한 노드가 포함되어 있는지 확인하십시오. 화살표를 사용하여 목록에 표시할 노드를 이동 합니다. Unified Communications Manager 노드가 나열되는 순서대로 선택됩니다. 변경 내용을 저장합니다.

단계 **7** 자동 등록하려는 디바이스를 설치합니다.

참고 계속해서 자동 등록된 디바이스를 다시 구성하고 영구 디바이스 풀에 할당할 수 있습니다. 전화기 위치를 변경해도 전화기에 할당된 디렉터리 번호는 변경되지 않습니다.

참고 다른 유형의 전화기를 등록하려면, 디바이스 프로토콜 유형을 변경하고 해당 디바이스를 설치한 후에 자동 등록를 비활성화합니다.

자동 등록 비활성화

새 디바이스의 등록을 완료하자마자 노드에 대한 자동 등록을 비활성화합니다.

시작하기 전에

자동 등록 활성화, 406 페이지

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > **Cisco** 통합 **CM**을 선택한 다음, **Cisco** 통합 **CM** 찾기 및 나열 창에서 찾기를 클릭합니다.

단계 **2** 노드목록에서 **Cisco Unified Communications Manager**를 선택합니다.

단계 **3** 선택한 노드에 대한 **Cisco Unified CM** 구성 창에서, 이 **Cisco Unified Communications Manager**에서 자동 등록 비활성화됨 확인란에 체크 표시하여 이 노드에 대한 자동 등록을 비활성화한 다음, 저장을 클릭합니다.

팁 시작 디렉터리 번호와 끝 디렉터리 번호 필드를 같은 값으로 설정하면 자동 등록이 비활성화됩니다.

다음에 수행할 작업

(선택 사항) 자동 등록된 디바이스의 디렉터리 번호를 수동으로 변경하는 경우 또는 해당 디바이스를 데이터베이스에서 삭제한 경우, 디렉터리 번호를 재사용할 수 있습니다. 자세한 내용은 자동 등록 번호 재사용, 408 페이지를 참조하십시오.

자동 등록 번호 재사용

네트워크에 새 디바이스를 연결하면, 시스템에서 다음으로 사용 가능한 자동 등록 디렉터리 번호를 해당 디바이스에 할당합니다. 자동 등록된 디바이스의 디렉터리 번호를 수동으로 변경하는 경우 또는 해당 디바이스를 데이터베이스에서 삭제하는 경우, 해당 디바이스의 자동 등록 디렉터리 번호를 재사용할 수 있습니다.

디바이스에서 자동 등록을 시도하면, 시스템에서 지정한 자동 등록 번호의 범위를 검색하고 다음으로 사용 가능한 디렉터리 번호를 찾아 디바이스에 할당하려고 합니다. 먼저 순서가 마지막으로 할당된 디렉터리 번호 이후인 다음 디렉터리 번호를 검색합니다. 해당 범위의 종료 디렉터리 번호에 도달하는 경우, 시스템에서 범위의 시작 디렉터리 번호에서부터 계속해서 검색합니다.

자동 등록 디렉터리 번호의 범위를 재설정하고 시스템에서 범위의 시작 번호에서부터 검색하도록 만들 수 있습니다.

프로시저

단계 **1** Cisco Unified Communications Manager 관리에서 시스템 > **Cisco Unified ommunications Manager**를 선택합니다.

단계 **2** Cisco Unified Communications Manager를 선택하여 자동 등록을 위해 재설정합니다.

단계 **3** 시작 디렉터리 번호 및 종료 디렉터리 번호 필드에 현재 설정을 적어 둡니다.

단계 **4** 이 **Cisco Unified Communications Manager**에서 자동 등록 비활성화됨을 클릭한 다음, 저장을 클릭합니다.

자동 등록이 비활성화되어 있으면 새 전화기를 자동 등록할 수 없습니다.

단계 **5** 시작 디렉터리 번호 및 종료 디렉터리 번호 필드를 이전 값으로 설정한 다음, 저장을 클릭합니다.

팁 해당 필드를 새 값으로 설정할 수 있습니다.

36 장

셀프 프로비저닝 구성

셀프 프로비저닝 개요

셀프 프로비저닝 기능을 사용하면 엔드 유저에게 관리자에게 문의하지 않은 상태로 자신의 전화기를 프로비저닝할 수 있는 능력을 부여하여 네트워크에 대한 전화기를 프로비저닝하는 것을 지원할 수 있습니다. 시스템이 셀프 프로비저닝을 위해 구성되고 개별 엔드 유저가 셀프 프로비저닝을 위해 활성화된 경우, 엔드 유저는 전화기를 네트워크에 연결하고 지정된 몇 개의 프롬프트를 따라 새 전화기를 프로비저닝할 수 있습니다. Cisco Unified Communications Manager에서 사전에 구성된 템플릿을 적용하여 전화기와 전화 회선을 구성합니다.

셀프 프로비저닝은 관리자가 엔드 유저를 대신하여 전화기를 프로비저닝하기 위해 사용될 수 있거나, 엔드 유저는 셀프 프로비저닝을 사용하여 자체 전화기를 프로비저닝할 수 있습니다.

클러스터 보안 설정이 비보안 모드 또는 혼합 모드 여부에 관계 없이 셀프 프로비저닝은 지원됩니다.

보안 모드

다음 두 가지 모드 중 하나로 셀프 프로비저닝을 구성할 수 있습니다.

- 보안 모드—보안 모드에서는 사용자 또는 관리자를 인증해야만 셀프 프로비저닝에 액세스하는 것이 가능합니다. 엔드 유저는 암호나 PIN에 대해 인증할 수 있습니다. 관리자는 사전에 구성된 인증 코드를 입력할 수 있습니다.
- 비보안 모드—비보안 모드에서 사용자 또는 관리자는 사용자 ID 또는 셀프 프로비저닝 ID를 입력하여 사용자 어카운트에 전화기를 연결할 수 있습니다. 비보안 모드는 일상적 사용에는 사용하지 않는 것이 좋습니다.

범용 회선 및 디바이스 템플릿을 통한 구성

셀프 프로비저닝에서 범용 회선 템플릿 및 범용 디바이스 템플릿 구성을 사용하여 엔드 유저에 대해 프로비저닝된 전화기와 전화 회선을 구성합니다. 사용자가 자신의 전화기를 프로비저닝하는 경우,

시스템에서는 해당 사용자의 사용자 프로파일을 참조하 고, 연결된 범용 회선 템플릿을 프로비저닝된 전화기 회선에, 범용 디바이스 템플릿을 프로비저닝된 전화기에 적용합니다.

전화기 셀프 프로비저닝

기능이 구성된 경우, 다음을 수행하여 전화기를 프로비저닝할 수 있습니다.

- 전화기를 네트워크에 연결합니다.
- 셀프 프로비저닝 IVR 내선 번호로 전화를 겁니다.
- 프롬프트에 따라 전화기를 구성하고 전화기를 엔드 유저와 연결합니다. 셀프 프로비저닝을 구성한 방법에 따라 엔드 유저는 사용자 암호, PIN 또는 관리 인증 코드를 입력할 수 있습니다.

팁 엔드 유저를 대신하여 많은 수의 전화기를 프로비저닝하는 경우, 셀프 프로비저닝 IVR 내선 번호로 전달되는 범용 디바이스 템플릿에서 단축 다이얼을 구성합니다.

아날로그 **FXS** 포트 셀프 프로비저닝

사용자가 셀프 프로비저닝 IVR에 전화를 걸고 해당 DN을 해당 아날로그 포트에 할당 수 있도록, 아날로그 FXS 포트에 대한 셀프 프로비저닝을 활성화할 수 있습니다. 또한 프로비저닝된 전화기의 경우, 사용자는 아날로그 음성 게이트웨이 포트와 연결된 DN을 할당 해제하고 이를 다른 사용자에게 할당할 수 있습니다.

절차

1. 게이트웨이의 FXS 음성 포트에 아날로그 전화기를 연결합니다. 포트가 자동 등록되거나 (수동으로) 사전에 구성되기 때문에 전화기가 자동 등록된 풀이나 할당된 DN에서 DN을 자동으로 가져옵니다.
2. 자동 등록된 아날로그 디바이스에서 셀프 프로비저닝 IVR로 전화를 겁니다.
3. 셀프 서비스 ID 및 PIN을 입력합니다.

참고 확인되는 즉시 엔드 유저의 기본 내선 번호를 사용하여 아날로그 디바이스가 프로비저닝됩니다. 자동 등록된 DN이 풀로 릴리스됩니다.

셀프 프로비저닝 사전 요건

엔드 유저가 셀프 프로비저닝을 사용하려면 먼저 엔드 유저가 다음과 같은 항목을 구성해야 합니다.

- 엔드 유저에게 기본 내선 번호가 있어야 합니다.

- 엔드 유저가 범용 회선 템플릿, 범용 디바이스 템플릿 등을 포함하는 사용자 프로파일 또는 기능 그룹 템플릿에 연결되어 있어야 합니다. 셀프 프로비저닝에 대한 사용자 프로파일이 활성화되어 있어야 합니다.

셀프 프로비저닝 구성 작업 플로우

프로시저

	명령 또는 동작	목적
단계 **1**	셀프 프로비저닝 서비스 활성화, 413 페이지	Cisoc Unified Serviceability에서 셀프 프로비저닝 **IVR** 및 **CTI Manager** 서비스를 활성화합니다.
단계 **2**	셀프 프로비저닝을 위한 자동 등록 활성화, 414 페이지	셀프 프로비저닝에 대한 자동 등록 매개변수 활성화
단계 **3**	CTI 라우트 포인트 구성, 414 페이지	CTI 라우트 포인트를 구성하여 셀프 프로비저닝 IVR 서비스를 처리합니다.
단계 **4**	CTI 라우트 포인트에 디렉터리 번호 할당, 415 페이지	사용자가 전화하려는 내선 번호를 구성하여 셀프 프로비저닝 IVR에 액세스하고 해당 내선 전화를 CTI 라우트 포인트에 연결합니다.
단계 **5**	셀프 프로비저닝을 위한 애플리케이션 사용자 구성, 415 페이지	셀프 프로비저닝 IVR을 위한 애플리케이션 사용자를 구성합니다. CTI 라우트 포인트를 애플리케이션 사용자와 연결합니다.
단계 **6**	셀프 프로비저닝을 위한 시스템 구성, 416 페이지	애플리케이션 사용자 및 CTI 라우트 포인트를 셀프 프로비저닝 IVR에 연결하는 것을 포함하여 시스템에 대한 셀프 프로비저닝 설정을 구성합니다.
단계 **7**	사용자 프로파일에서 셀프 프로비저닝 활성화, 417 페이지	사용자가 할당된 사용자 프로파일에서 전화기를 셀프 프로비저닝할 수 있습니다.

셀프 프로비저닝 서비스 활성화

이 절차를 사용하여 셀프 프로비저닝 기능을 지원하는 서비스를 활성화합니다. 셀프 프로비저닝 IVR과 Cisco CTI 관리자 서비스가 모두 실행되고 있는지 확인하십시오.

프로시저

단계 **1** Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.

단계 **2** 서버 드롭다운 목록에서 퍼블리셔 노드를 선택하고 이동을 클릭합니다.

단계 **3** **CM** 서비스에서 **Cisco CTI** 관리자를 확인합니다.

단계 **4** **CTI** 서비스 아래에서 셀프 프로비저닝 **IVR**을 확인합니다.

단계 **5** 저장을 클릭합니다.

셀프 프로비저닝을 위한 자동 등록 활성화

셀프 프로비저닝을 위해 이 절차를 사용하여 퍼블리셔에서 자동 등록 매개변수를 구성해야만 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **Cisco Unified CM**을 선택합니다.

단계 **2** 퍼블리셔 노드를 클릭합니다.

단계 **3** 프로비저닝된 전화기에 적용하려는 범용 디바이스 템플릿을 선택합니다.

단계 **4** 프로비저닝된 전화기에 대한 전화 회선에 적용하려는 범용 회선 템플릿을 선택합니다.

단계 **5** 시작 디렉터리 번호 및 종료 디렉터리 번호 필드를 사용하여 프로비저닝된 전화기에 적용할 디렉터리 번호의 범위를 입력합니다.

단계 **6** 이 **Cisco Unified Communications Manager**에서 자동 등록 비활성화됨 확인란을 선택 취소합니다.

단계 **7** SIP 등록에 사용될 포트를 확인합니다. 대부분의 경우 기본 설정에서 포트를 변경할 필요가 없습니다.

단계 **8** 저장을 클릭합니다.

CTI 라우트 포인트 구성

이 절차를 사용하여 셀프 프로비저닝 IVR에 대한 CTI 라우트 포인트를 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.

단계 **2** 다음 단계 중 하나를 완료합니다.

a) 찾기를 클릭하고 기존 CTI 라우트 포인트를 선택합니다.

b) 새로 추가 를 클릭하여 새 CTI 라우트 포인트를 만듭니다.

단계 **3** 디바이스 이름 필드에 라우트 포인트를 식별하는 고유 이름을 입력합니다.

단계 **4** 디바이스 풀 드롭다운 목록에서 이 디바이스에 대한 속성을 지정하는 디바이스 풀을 선택합니다.

단계 **5** 위치 드롭다운 목록에서 이 CTI 라우트 포인트에 대한 해당 위치를 선택합니다.

단계 **6** **TRP(Trusted Relay Point)** 사용 드롭다운 목록에서 Unified Communications Manager에서 이 미디어 엔드포인트로 TRP 디바이스에 삽입하도록 설정할 것인지 여부를 선택합니다. 기본 설정은이 디바이스와 연결된 일반 디바이스 구성 설정을 사용하는 것입니다.

단계 **7** **CTI** 라우트 포인트 구성 창에서 나머지 필드를 완료합니다. 필드와 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

CTI 라우트 포인트에 디렉터리 번호 할당

이 절차를 사용하여 사용자가 셀프 프로비저닝 IVR에 액세스하기 위해 전화를 거는 내선 번호를 설정합니다. 셀프 프로비저닝을 위해 사용하려는 CTI 라우트 포인트에이 이 내선 번호를 연결해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > **CTI** 라우트 포인트를 선택합니다.

단계 **2** 찾기를 클릭하고 셀프 프로비저닝을 위해 설정한 CTI 라우트 포인트를 선택합니다.

단계 **3** 연결에서 회선 **[1]** - 새 **DN** 추가를 클릭합니다.
디렉터리 번호 구성 창이 표시됩니다.

단계 **4** 디렉터리 번호 필드에 사용자가 셀프 프로비저닝 IVR 서비스에 액세스하기 위해 전화를 걸려고 하는 내선 번호를 입력합니다.

단계 **5** 저장을 클릭합니다.

단계 **6** 디렉터리 번호 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

셀프 프로비저닝을 위한 애플리케이션 사용자 구성

셀프 프로비저닝 IVR에 대한 애플리케이션 사용자를 설정하고 생성 한 CTI 라우트 포인트를 애플리케이션 사용자에 연결해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 > 애플리케이션 사용자를 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

a) 기존 애플리케이션 사용자를 선택 하려면 찾기를 클릭하고 애플리케이션 사용자를 선택합니다.

b) 새 애플리케이션 사용자를 만들려면 새로 추가를 클릭합니다.

단계 **3** 사용자 **ID** 텍스트 상자에 애플리케이션 사용자의 고유 ID를 입력합니다.

단계 **4** 애플리케이션 사용자에 대한 **BLF** 프리젠스 그룹을 선택합니다.

단계 **5** 다음 단계를 수행하여 생성한 CTI 라우트 포인트를 애플리케이션 사용자에 연결합니다.

a) 생성한 CTI 라운트 포인트가 사용 가능한 디바이스 목록 상자에 나타나지 않는 경우, 추가 라우트 포인트 찾기]를 클릭합니다.
생성한 CTI 라우트 포인트는 사용 가능한 디바이스로 표시됩니다.

b) 사용 가능한 디바이스 목록에서 셀프 프로비저닝을 위해 생성한 CTI 라우트 포인트를 선택하고 아래쪽 화살표를 클릭합니다.
제어된 디바이스 목록에 CTI 라우트 포인트가 표시됩니다.

단계 **6** 애플리케이션 사용자 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

셀프 프로비저닝을 위한 시스템 구성

이 절차를 사용하여 셀프 프로비저닝을 위해 시스템을 구성합니다. 셀프 프로비저닝을 통해 네트워크 사용자는 관리자에게 연락하지 않고서도 IVR 시스템을 통해 자신의 데스크폰을 추가할 수 있습니다.

참고 셀프 프로비저닝 기능을 사용하려면 엔드 유저가 사용자 프로파일에서도 기능을 활성화해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 셀프 프로비저닝을 선택합니다.

단계 **2** 다음 라디오 버튼 중 하나를 클릭하여 셀프 프로비저닝 IVR에서 엔드 유저를 인증할 것인지 여부를 구성합니다.

- 인증 필요—셀프 프로비저닝 IVR을 사용하려면 엔드 유저가 암호, PIN 또는 시스템 인증 코드를 입력해야 합니다.
- 인증 필요 없음—엔드 유저가 인증 없이 셀프 프로비저닝 IVR에 액세스할 수 있습니다.

단계 **3** 셀프 프로비저닝 IVR이 인증을 요구하도록 구성된 경우, 다음 라디오 버튼 중 하나를 클릭하여 IVR에서 엔드 유저를 인증하는 방법을 구성합니다.

- 엔드 유저에게만 인증 허용—엔드 유저가 암호나 PIN을 입력해야 합니다.
- 사용자**(**암호**/PIN** 사용**)** 및 관리자**(**인증 코드 사용**)**에 대한 인증 허용—엔드 유저가 인증 코드를 입력해야 합니다. 이 옵션을 선택하는 경우, 인증 코드 텍스트 상자에 0 ~ 20 사이의 정수를 입력하여 인증 코드를 구성합니다.

단계 **4** **IVR** 설정 목록 상자에서 화살표를 사용하여 IVR 프롬프트에 사용할 언어를 선택합니다. 사용 가능한 언어 목록은 시스템에 설치된 언어 팩에 따라 달라집니다. 추가 언어 팩을 다운로드하려면 cisco.com의 다운로드 섹션을 참조하십시오.

단계 **5** **CTI** 라우트 포인트 드롭다운 목록에서 셀프 프로비저닝 IVR에 대해 구성한 CTI 라우트 포인트를 선택합니다.

단계 **6** 애플리케이션 사용자 드롭다운 목록에서 셀프 프로비저닝을 위해 구성한 애플리케이션 사용자를 선택합니다.

단계 **7** 저장을 클릭합니다.

사용자 프로파일에서 셀프 프로비저닝 활성화

사용자가 전화기를 셀프 프로비저닝할 수 있으려면, 기능이 할당된 사용자 프로파일에서 기능을 활성화해야 합니다.

참고 사용자가 사용 중인 사용자 프로파일을 모르는 경우 최종 사용자 구성 창에서 사용자 설정을 열고 사용자 프로파일 필드를 확인하여 올바른 프로파일을 가져올 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 사용자 프로파일을 선택합니다.

단계 **2** 사용자가 할당된 사용자 프로파일 찾기 및 선택을 클릭합니다.

단계 **3** 사용자 프로파일에 범용 회선 템플릿 및 범용 디바이스 템플릿을 할당합니다.

단계 **4** 셀프 프로비저닝을 위한 사용자 설정 구성:

- 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.
- 사용자가 프로비저닝할 수 있는 전화기 수에 대한 제한을 입력합니다. 기본값은 10입니다.
- 사용자가 셀프 프로비저닝을 사용하여 이전에 할당된 전화기를 다시 할당하려는 경우, 이전 디바이스의 최종 사용자와 연결된 사용자 프로파일 페이지에서 다른 최종 사용자에 이미 할당된 전화기의 프로비저닝 허용 설정을 선택합니다. 이전 디바이스에 연결된 사용자 프로파일에서이 확인란이 활성화 된 경우에만 사용자가 이전에 할당 된 전화기를 다시 할당할 수 있습니다.

단계 **5** 저장을 클릭합니다.

VI 부

참조 정보

37 장

Cisco Unified Communications Manager TCP 및 UDP 포트 사용

Cisco Unified Communications Manager TCP 및 UDP 포트 사용 개요

Cisco Unified Communications Manager TCP 및 UDP 포트는 다음 범주로 구성 됩니다.

- Cisco Unified Communications Manager 간 클러스터 간 포트
- 공통 서비스 포트
- Cisco Unified Communications Manager와 LDAP 디렉터리 간 보안 포트
- CCMAdmin 또는 CCMUser에서 Cisco Unified Communications Manager로 웹 요청
- Cisco Unified Communications Manager에서 전화기로 웹 요청
- 전화기와 Cisco Unified Communications Manager 간 신호, 미디어 및 기타 통신
- 게이트웨이와 Cisco Unified Communications Manager 간 신호, 미디어 및 기타 통신
- 애플리케이션과 Cisco Unified Communications Manager 간 통신
- CTL 클라이언트와 방화벽 간 통신
- HP 서버에 대한 특별 포트

위의 각 범주에서 포트 세부 정보는 “포트 설명”을 참조하십시오.

참고 Cisco는 이러한 포트에 대해 가능한 모든 구성 시나리오를 확인하지 않았습니다. 이 목록을 사용하여 구성 문제가 있는 경우 Cisco 기술 지원부에 지원을 요청하십시오.

포트 참조는 Cisco Unified Communications Manager에만 적용됩니다. 일부 포트는 릴리스마다 변경되며 이후 릴리스에서는 새로운 포트가 도입될 수 있습니다. 따라서 설치된 Cisco Unified Communications Manager 버전에 이 문서의 올바른 버전을 사용하고 있는지 확인하십시오.

거의 모든 프로토콜이 양방향이지만 세션 생성자 관점에서의 방향성이 가정됩니다. 경우에 따라 관리자가 수동으로 기본 포트 번호를 변경할 수 있지만 Cisco에서는 이를 권장하지 않습니다. 따라서 Cisco Unified Communications Manager는 여러 포트를 내부용으로만 엽니다.

Cisco Unified Communications Manager 소프트웨어를 설치하면 서비스 가용성을 위해 다음과 같은 네트워크 서비스가 자동으로 설치되고 기본적으로 활성화됩니다. 자세한 내용은 "Cisco Unified Communications Manager 간 클러스터 간 포트"를 참조하십시오.

- Cisco 로그 파티션 모니터링(일반 파티션을 모니터링하고 제거합니다. 사용자 지정 공통 포트를 사용하지 않습니다.)
- Cisco 추적 수집 서비스(TCTS 포트 사용)
- Cisco RIS 데이터 컬렉터(RIS 서버 포트 사용)
- Cisco AMC 서비스(AMC 포트 사용)

방화벽, ACL 또는 QoS의 구성은 토폴로지, 전화 통신 디바이스의 배치 및 전화 보안 디바이스의 배치와 관련한 서비스 및 사용 중인 애플리케이션 및 전화 통신 확장 기능에 따라 다릅니다. 또한 ACL의 형식은 디바이스와 버전에 따라 다양합니다.

참고 Cisco Unified Communications Manager에서 멀티캐스트 대기 중 음악(MOH) 포트를 구성할 수도 있습니다. 관리자가 실제 포트 값을 지정하기 때문에 멀티캐스트 MOH의 포트 값은 제공되지 않습니다.

참고 시스템의 임시 포트 범위는 32768 ~ 61000이며 전화 등록을 유지하려면 포트를 열어야합니다. 자세한 정보는 http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html를 참조하십시오.

참고 포트 22에 대한 연결이 열려 있고 스로틀되지 않도록 방화벽을 구성해야 합니다. IM and Presence 가입자 노드를 설치하는 동안 Cisco Unified Communications Manager 게시자 노드에 대한 여러 연결이 빠르게 연속적으로 열립니다. 이러한 연결을 조절하면 설치가 실패할 수 있습니다.

포트 설명

Cisco Unified Communications Manager 간 클러스터 간 포트

표 ***29: Cisco Unified Communications Manager*** 간 클러스터 간 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	Unified Communications Manager	514 / UDP	시스템 로깅 서비
Unified Communications Manager	Unified Communications Manager	443 / TCP	이 포트는 가입자 COP 파일을 설치 입자와 게시자 간 용됩니다.
Unified Communications Manager	RTMT	1090, 1099 / TCP	RTMT 성능 모니 집, 로깅 및 경고 서비스
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1500, 1501 / TCP	데이터베이스 연 TCP 는 보조 연결
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1510 / TCP	CAR IDS DB. CA 은 클라이언트의 기다리면서 수신
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1511 / TCP	CAR IDS DB. 업 는 동안 CAR IDS 인스턴스를 표시 되는 대체 포트입
Unified Communications Manager(DB)	Unified Communications Manager(DB)	1515 / TCP	설치 중 노드 간 데 복제
Cisco 확장 기능(QRT)	Unified Communications Manager(DB)	2552 / TCP	가입자가 Cisco U Communications M 터베이스 변경 알 수 있습니다.
Unified Communications Manager	Unified Communications Manager	2551 / TCP	활성/백업 결정을 확장 서비스 간의 통신
Unified Communications Manager(RIS)	Unified Communications Manager(RIS)	2555 / TCP	실시간 정보 서비 터베이스 서버

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager(RTMT/AMC/SOAP)	Unified Communications Manager(RIS)	2556 / TCP	Cisco RIS용 실시간 스(RIS) 데이터베이 언트
Unified Communications Manager(DRS)	Unified Communications Manager(DRS)	4040 / TCP	DRS 주 에이전트
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5001/TCP	이 포트는 실시간모 비스를 위해 SOAP 서 사용됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5002/TCP	이 포트는 성능 모니 를 위해 SOAP 모니 용됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5003/TCP	이 포트는 제어 센터 위해 SOAP 모니터 됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5004/TCP	이 포트는 로그 수집 위해 SOAP 모니터 됩니다.
표준 CCM 관리 사용자 / 관리자	Unified Communications Manager	5005 / TCP	이 포트는 SOAP CDROnDemand2 서 사용됩니다.
Unified Communications Manager(Tomcat)	Unified Communications Manager(SOAP)	5007 / TCP	SOAP 모니터
Unified Communications Manager(RTMT)	Unified Communications Manager(TCTS)	임시 / TCP	Cisco 추적 수집 서비 - RTMT 추적 및 Log Central(TLC)에 대한 서비스
Unified Communications Manager(Tomcat)	Unified Communications Manager(TCTS)	7000, 7001, 7002 / TCP	이 포트는 Cisco 추적 구 서비스와 Cisco 추 서블릿 간의 통신에 다.
Unified Communications Manager(DB)	Unified Communications Manager(CDLM)	8001 / TCP	클라이언트 데이터 경 알림
Unified Communications Manager(SDL)	Unified Communications Manager(SDL)	8002 / TCP	클러스터 간 통신 서

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager(SDL)	Unified Communications Manager(SDL)	8003 / TCP	클러스터 간 통신 측)
Unified Communications Manager	CMI 관리자	8004 / TCP	Cisco Unified Co Manager와 CMI M 러스터 간 통신
Unified Communications Manager(Tomcat)	Unified Communications Manager(Tomcat)	8005 / TCP	Tomcat 종료 스크 용하는 내부 수신
Unified Communications Manager(Tomcat)	Unified Communications Manager(Tomcat)	8080 / TCP	진단 테스트에 사 간 통신
게이트웨이	Unified Communications Manager	8090	게이트웨이 레코 한 CuCM 및 GW(페이스) 간의 통신 HTTP 포트.
Unified Communications Manager	게이트웨이		
Unified Communications Manager(IPSec)	Unified Communications Manager(IPSec)	8500 / TCP 및 UDP	IPSec Cluster Ma 시스템 데이터의 복제
Unified Communications Manager(RIS)	Unified Communications Manager(RIS)	8888 - 8889 / TCP	RIS 서비스 관리 및 응답
위치 대역폭 관리자(LBM)	위치 대역폭 관리자(LBM)	9004 / TCP	LBM 간 클러스터
Unified Communications Manager 게시자	Unified Communications Manager 가입자	22 / TCP	Cisco SFTP 서비 가입자를 설치할 열어야 합니다.
Unified Communications Manager	Unified Communications Manager	8443 / TCP	노드 간에 제어 신 네트워크 서비스 허용합니다.

공통 서비스 포트

표 ***30:*** 공통 서비스 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	Unified Communications Manager	7	인터넷 제어 메시지 프로토콜(ICMP). 이 프로토콜 번호는 에코 관련 트래픽을 전달합니다. 열 머리글에 표시된 대로 포트를 구성하지 않습니다.
Unified Communications Manager	엔드포인트		
Unified Communications Manager(DRS, 통화 세부 정보 기록)	SFTP 서버	22 / TCP	SFTP 서버에 백업 데이터를 전송합니다. (DRS 로컬 에이전트) 통화 세부 정보 기록 데이터를 SFTP 서버로 전송합니다.
엔드포인트	Unified Communications Manager(DHCP 서버)	67 / UDP	DHCP 서버 역할을 하는 Cisco Unified Communications Manager 참고 Cisco Unified Communications Manager에서 DHCP 서버를 실행하지 않는 것이 좋습니다.
Unified Communications Manager	DHCP 서버	68 / UDP	DHCP 클라이언트 역할을 하는 Cisco Unified Communications Manager 참고 Cisco Unified Communications Manager에서 DHCP 클라이언트를 실행하지 않는 것이 좋습니다. Configure Cisco Unified Communications Manager는 정적 IP 주소를 사용)
엔드포인트 또는 게이트웨이	Unified Communications Manager	69 6969, 그런 다음 임시 / UDP	전화기 및 게이트웨이에 대한 TFTP 서비스

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트 또는 게이트웨이	Unified Communications Manager	6970 / TCP	기본 서버와 프록시 서버 간 TFTP. TFTP 서버에서 전화기 및 게이트웨이로의 HTTP 서비스
Unified Communications Manager	NTP 서버	123 / UDP	NTP(Network Time Protocol)
SNMP 서버	Unified Communications Manager	161 / UDP	SNMP 서비스 응답(관리 애플리케이션에서 요청)
CUCM 서버 SNMP 주 에이전트 애플리케이션	SNMP 트랩 대상	162 / UDP	SNMP 트랩
SNMP 서버	Unified Communications Manager	199 / TCP	SMUX 지원용 기본 제공 SNMP 에이전트 수신 대기 포트
Unified Communications Manager	DHCP 서버	546 / UDP	DHCPv6. IPv6용 DHCP 포트입니다.
Unified Communications Manager 서비스 가용성	위치 대역폭 관리자(LBM)	5546 / TCP	고급 위치 기반 CAC 서비스 가용성
Unified Communications Manager	위치 대역폭 관리자(LBM)	5547 / TCP	통화 허용 요청 및 대역폭 공제
Unified Communications Manager	Unified Communications Manager	6161 / UDP	기본 에이전트 MIB 요청을 처리하기 위해 주 에이전트와 기본 에이전트 간의 통신에 사용
Unified Communications Manager	Unified Communications Manager	6162 / UDP	기본 에이전트에서 생성된 알림을 전달하기 위해 주 에이전트와 기본 에이전트 간의 통신에 사용
중앙 집중식 TFTP	대체 TFTP	6970 / TCP	중앙 집중식 TFTP 파일 로케이터 서비스
Unified Communications Manager	Unified Communications Manager	7161 / TCP	SNMP 주 에이전트와 하위 에이전트 간의 통신에 사용
SNMP 서버	Unified Communications Manager	7999 / TCP	Cisco Discovery Protocol(CDP) 에이전트가 CDP 실행 파일과 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	Unified Communications Manager	443, 8443 / TCP	Cisco 사용자 데이터 서비스(UDS) 요청에 사용
Unified Communications Manager	Unified Communications Manager	9050 / TCP	Cisco Unified Communications Manager에 있는 TAPS를 통해 서비스 CRS 요청
Unified Communications Manager	Unified Communications Manager	61441 / UDP	Cisco Unified Communications Manager 애플리케이션은 UDP를 통해 이 포트에 경보를 전송합니다. Cisco Unified Communications Manager MIB 에이전트는 이 포트를 수신하고 Cisco Unified Communications Manager MIB 정의에 따라 SNMP 트랩을 생성합니다.
Unified Communications Manager	Unified Communications Manager	5060, 5061 / TCP	트렁크 기반 SIP 서비스를 제공
Unified Communications Manager	Unified Communications Manager	7501	인증서 기반 인증을 위해 ILS(Intercluster Lookup Service)에서 사용됩니다.
Unified Communications Manager	Unified Communications Manager	7502	암호 기반 인증을 위해 ILS에서 사용됩니다.
Unified Communications Manager	Unified Communications Manager	9966	Cisco 푸시 알림 서비스는 방화벽이 활성화되어 있을 때 클러스터 노드 간 통신을 위해 이를 사용합니다.
Unified Communications Manager	Unified Communications Manager	9560	로컬 푸시 알림 서비스(LPNS)에서 사용됩니다.
--	--	8000-48200	ASR 및 ISR G3 플랫폼 기본 포트 범위입니다.
		16384-32766	ISR G2 플랫폼 기본 포트 범위입니다.

Cisco Unified Communications Manager와 LDAP 디렉터리 간 보안 포트

표 *31: Cisco Unified Communications Manager*와 *LDAP* 디렉터리 간 보안 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager	외부 디렉터리	389, 636, 3268, 3269 / TCP	외부 디렉터리(Netscape Directory Active Directory)에 LDAP(Lightweight Directory Access Protocol) 쿼리
외부 디렉터리	Unified Communications Manager	임시	

CCMAdmin 또는 CCMUser에서 Cisco Unified Communications Manager로 웹 요청

표 *32: CCMAdmin* 또는 *CCMUser*에서 *Cisco Unified Communications Manager*로 웹 요청

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
브라우저	Unified Communications Manager	80, 8080 / TCP	HTTP(Hypertext Protocol)
브라우저	Unified Communications Manager	443, 8443 / TCP	HTTPS(Hypertex Protocol over SSL
브라우저	Unified Communications Manager	9463 / TCP	SSL(HTTPS)를 통 스트 전송 프로토 TLS1.3만 허용합

Cisco Unified Communications Manager에서 전화기로 웹 요청

표 *33: Cisco Unified Communications Manager*에서 전화기로 웹 요청

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager • QRT • RTMT • 전화기 찾기 및 나열 페이지 • 전화기 구성 페이지	전화기	80 / TCP	HTTP(Hypertext Protocol)

전화기와 **Cisco Unified Communications Manager** 간 신호, 미디어 및 기타 통신

표 ***34:*** 전화기와 ***Cisco Unified Communications Manager*** 간 신호, 미디어 및 기타 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
전화기	DNS 서버	53 / TCP	SIP(Session Initiation Protocol) 전화기는 DNS(Domain Name System)를 사용하여 FQDN(정규화된 도메인 이름)을 확인합니다. 참고 기본적으로 일부 무선 액세스 지점은 TCP 53 포트를 차단하므로 FQDN을 사용하여 CUCM을 구성할 때 무선 SIP 전화기가 등록되지 않습니다.
전화기	Unified Communications Manager(TFTP)	69, 그런 다음 임시 / UDP	펌웨어 및 구성 파일을 다운로드하는 데 사용되는 TFTP(Trivial File Transfer Protocol)
전화기	Unified Communications Manager	2000 / TCP	SCCP(Skinny Client Control Protocol)
전화기	Unified Communications Manager	2443 / TCP	SCCPS(Secure Skinny Client Control Protocol)
전화기	Unified Communications Manager	2445 / TCP	엔드포인트에 신뢰 검증 서비스를 제공합니다.
전화기	Unified Communications Manager(CAPF)	3804 / TCP	IP Phone에 로컬 서명 인증서(LSC)를 발행하는 CAPF(Certificate Authority Proxy Function) 수신 포트
전화기	Unified Communications Manager	5060 / TCP 및 UDP	SIP(Session Initiation Protocol) 전화기
Unified Communications Manager	전화기		

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
전화기	Unified Communications Manager	TCP 5061	SIPS(Secure Session Initiation Protocol) 전화기
Unified Communications Manager	전화기		
전화기	Unified Communications Manager(TFTP)	6970 TCP	펌웨어 및 구성 파일의 HTTP 기반 다운로드
전화기	Unified Communications Manager(TFTP)	6971, 6972 / TCP	TFTP에 대한 HTTPS 인터페이스입니다. 전화기는 이 포트를 사용하여 TFTP에서 보안 구성 파일을 다운로드합니다.
전화기	Unified Communications Manager	8080 / TCP	XML 애플리케이션, 인증, 디렉터리, 서비스 등을 위한 전화기 URL 이러한 포트는 서비스 별로 구성할 수 있습니다.
전화기	Unified Communications Manager	9443 / TCP	전화기 인증된 연락처 검색에 이 포트를 사용합니다.
전화기	Unified Communications Manager	9444	전화기는 이 포트 번호를 사용하여 헤드셋 관리 기능을 사용합니다.
iPhone/iPad(Webex 앱)	Unified Communications Manager	9560/보안 WebSocket	Webex 앱은 LPNS 기능에 이 포트 번호를 사용합니다.
IP VMS	전화기	16384 - 32767 / UDP	RTP(Real-Time Protocol), SRTP(Secure Real-Time Protocol) 참고 다른 디바이스들은 전체 범위를 사용하지만Cisco Unified Communications Manager는 24576-32767만 사용합니다.
전화기	IP VMS		

게이트웨이와 **Cisco Unified Communications Manager** 간 신호, 미디어 및 기타 통신

표 ***35:*** 게이트웨이와 ***Cisco Unified Communications Manager*** 간 신호, 미디어 및 기타 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
게이트웨이	Unified Communications Manager	47, 50, 51	GRE(Generic Routin Encapsulation), ESP(Encapsulating S Payload), AH(Auther Header). 이러한 프로 호는 암호화된 IPSec 을 전달합니다. 열 머 표시된 대로 포트를 않습니다.
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	500 / UDP	IP 보안 프로토콜(IP 을 위한 IKE(인터넷
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager(TFTP)	69, 그런 다음 임시 / UDP	TFTP(Trivial File Tra Protocol)
Cisco Intercompany Media Engine(CIME) 트렁크를 사용하는 Unified Communications Manager	CIME ASA	1024-65535 / TCP	포트 매핑 서비스입 CIME 경로 이탈 구 서만 사용됩니다.
Gatekeeper	Unified Communications Manager	1719 / UDP	게이트키퍼(H.225)
게이트웨이	Unified Communications Manager	1720 / TCP	H.323 게이트웨이 및 터클러스터 트렁크) H.225 신호 서비스
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	임시 / TCP	게이트키퍼 제어 트 한 H.225 신호 서비
Unified Communications Manager	게이트웨이		

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
게이트웨이	Unified Communications Manager	임시 / TCP	음성, 비디오 및 을 위한 H.245 신 참고 원격 사용 포트 이 유 다릅 IOS 의 경 트 범 ~ 655
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	2000 / TCP	SCCP(Skinny Cli Protocol)
게이트웨이	Unified Communications Manager	2001 / TCP	Cisco Unified Co Manager 구축을 6608 게이트웨이 업그레이드
게이트웨이	Unified Communications Manager	2002 / TCP	Cisco Unified Co Manager 구축을 6624 게이트웨이 업그레이드
게이트웨이	Unified Communications Manager	2427 / UDP	MGCP(Media Ga Protocol) 게이트
게이트웨이	Unified Communications Manager	2428 / TCP	MGCP(Media Ga Protocol) 백홀
--	--	4000 - 4005 / TCP	이러한 포트는 C Communications 러한 미디어에 대 을 때 오디오, 비 터 채널에 대해 RTP(Real-Time T Protocol) 및 RTC Transport Control 트로 사용됩니다
게이트웨이	Unified Communications Manager	5060 / TCP 및 UDP	SIP(Session Initia 게이트웨이 및 IC 스터 트렁크)
Unified Communications Manager	게이트웨이		

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
게이트웨이	Unified Communications Manager	5061 / TCP	SIPS(Secure Session Protocol) 게이트웨이 ICT(인터클러스터 트
Unified Communications Manager	게이트웨이		
게이트웨이	Unified Communications Manager	16384 - 32767 / UDP	RTP(Real-Time Proto SRTP(Secure Real-Ti Protocol) 참고 다른 디 은 전체 사용하지 Unified Commun Manager 24576-32 용합니다
Unified Communications Manager	게이트웨이		

애플리케이션과 **Cisco Unified Communications Manager** 간 통신

표 ***36:*** 애플리케이션과 ***Cisco Unified Communications Manager*** 간 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
CTL 클라이언트	Unified Communications Manager CTL 공급자	2444 / TCP	Cisco Unified Commu Manager의 인증서 신 (CTL) 공급자 수신 서
Cisco Unified Communications 앱	Unified Communications Manager	2748 / TCP	CTI 애플리케이션 서
Cisco Unified Communications 앱	Unified Communications Manager	2749 / TCP	CTI 애플리케이션(JT 및 CTIManager 간 T
Cisco Unified Communications 앱	Unified Communications Manager	2789 / TCP	JTAPI 애플리케이션
Unified Communications Manager Assistant 콘솔	Unified Communications Manager	2912 / TCP	Cisco Unified Commu Manager Assistant 서 에는 IPMA)
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	1103 -1129 / TCP	Cisco Unified Commu Manager Attendant 콘 JAVA RMI 레지스트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	1101 / TCP	RMI 서버는 RMI 를 이 포트의 클라 송합니다.
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	1102 / TCP	어텐던트 콘솔(A 바인드 포트 - RM 러한 포트에서 R 전송합니다.
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	3223 / UDP	Cisco Unified Co Manager AC(Atte Console) 서버 회 는 어텐던트 콘솔 및 등록 메시지를 선 상태를 어텐던 로 보냅니다.
Unified Communications Manager Attendant 콘솔	Unified Communications Manager	3224 / UDP	Cisco Unified Co Manager Attendan Console(AC) 클라 선 및 디바이스 상 위해 AC 서버에
Unified Communications ManagerAttendant 콘솔	Unified Communications Manager	4321 / UDP	Cisco Unified Co Manager Attendan Console(AC) 클라 화 제어를 위해 A 록합니다.
Unified Communications Manager(SAF/CCD 포함)	SAF 이미지를 실행하는 IOS 라우터	5050 / TCP	EIGRP/SAF 프로 하는 다중 서비스
Unified Communications Manager	Cisco Intercompany Media Engine(IME) 서버	5620 / TCP Cisco는 이 포트에 5620 값을 권장하지만 Cisco IME 서버에서 add ime vapserver 또는 ime vapserver port CLI 명령을 실행하여 값을 변경할 수 있습니다.	Cisco Intercompa Engine 서버와 통 용되는 VAP 프로

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
Cisco Unified Communications 앱	Unified Communications Manager	8443 / TCP	결제 또는 전화 통신 플리케이션과 같은 사용하는 프로그래 Cisco Unified Commu Manager 데이터베이 또는 쓰기용 AXL / S 입니다.

CTL 클라이언트와 방화벽 간 통신

표 *37: CTL* 클라이언트와 방화벽 간 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
CTL 클라이언트	TLS 프록시 서버	2444 / TCP	ASA 방화벽에서 인 목록(CTL) 공급자 스

Cisco 스마트 라이센스 서비스와 Cisco Smart Software Manager 간의 통신

Unified Communications Manager의 Cisco 스마트 라이센스 서비스는 통화 홈을 통해 Cisco Smart Software Manager와 직접 통신을 설정합니다.

표 *38: Cisco* 스마트 라이센스 서비스와 *Cisco Smart Software Manager* 간의 통신

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
통합 커뮤니케이션 관리자(Cisco 스마트 라이센스 서비스)	CSSM(Cisco Smart Software Manager)	443 / HTTPS	스마트 라이센스 서비스는 라이선스 사용량을 CSSM에 전송하여 Unified CM의 불만 사항 여부를 확인합니다.

HP 서버에 대한 특별 포트

표 *39: HP* 서버에 대한 특별 포트

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	HP SIM	2301 / TCP	HP 에이전트측 HTT
엔드포인트	HP SIM	2381 / TCP	HP 에이전트측 HTT

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트	Compaq 관리 에이전트	25375, 25376, 25393 / UDP	COMPAQ 관리 에 번호(cmaX)
엔드포인트	HP SIM	50000 - 50004 / TCP	HP SIM측 HTTP

포트 참조

방화벽 애플리케이션 검사 설명서

ASA 시리즈 참조 정보

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/tsd-products-support-series-home.html

PIX 애플리케이션 검사 구성 설명서

http://www.cisco.com/c/en/us/support/security/pix-firewall-software/products-installation-and-configuration-guides-list.html

FWSM 3.1 애플리케이션 검사 구성 설명서

http://www-author.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/inspct_f.html

IETF UDP/TCP 포트 할당 목록

IANA(Internet Assigned Numbers Authority) IETF 할당 포트 목록

http://www.iana.org/assignments/port-numbers

IP 전화 통신 구성 및 포트 활용 설명서

Cisco CRS 4.0(IP IVR and IPCC Express) 포트 활용 설명서

http://www.cisco.com/en/US/products/sw/custcosw/ps1846/products_installation_and_configuration_guides_list.html

Cisco ICM/IPCC Enterprise 및 Hosted Editions용 포트 활용 설명서

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Cisco Unified Communications Manager Express 보안 설명서(모범 사례)

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e30.html

Cisco Unity Express 보안 설명서(모범 사례)

http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns391/networking_solutions_design_guidance09186a00801f8e31.html#wp41149

VMware 포트 할당 목록

vCenter 서버, ESX 호스트 및 기타 네트워크 구성 요소 관리 액세스를 위한 TCP 및 UDP 포트

38 장

IM and Presence 서비스를 위한 포트 사용 정보

IM and Presence 서비스 포트 사용 개요

이 문서는 IM and Presence 서비스가 클러스터 내 연결 및 외부 애플리케이션 또는 디바이스와의 통신에 사용하는 TCP 및 UDP 포트 목록을 제공합니다. 또한 IP Communications 솔루션이 구현될 때 네트워크의 방화벽 구성, 액세스 제어 목록(ACL) 및 서비스 품질(QoS)에 대한 중요한 정보를 제공합니다.

참고 Cisco는 이러한 포트에 대해 가능한 모든 구성 시나리오를 확인하지 않았습니다. 이 목록을 사용하여 구성 문제가 있는 경우 Cisco 기술 지원부에 지원을 요청하십시오.

거의 모든 프로토콜이 양방향이지만 이 문서에서는 세션 생성자 관점에서의 방향성을 제공합니다. 경우에 따라 관리자가 수동으로 기본 포트 번호를 변경할 수 있지만 Cisco에서는 이를 권장하지 않습니다. IM and Presence 서비스는 여러 포트를 내부용으로만 엽니다.

이 문서의 포트는 특히 IM and Presence 서비스에 적용됩니다. 일부 포트는 릴리스마다 변경되며 이후 릴리스에서는 새로운 포트가 도입될 수 있습니다. 따라서 설치된 IM and Presence 서비스 버전에 이 문서의 올바른 버전을 사용하고 있는지 확인하십시오.

방화벽, ACL 또는 QoS의 구성은 토폴로지, 디바이스의 배치 및 전화 보안 디바이스의 배치와 관련한 서비스 및 사용 중인 애플리케이션 및 전화 통신 확장 기능에 따라 다릅니다. 또한 ACL의 형식은 디바이스와 버전에 따라 다양합니다.

표에 정리된 정보

이 표는 이 문서의 각 표에 정리된 정보를 정의합니다.

표 ***40:*** 표 정보 정의

표 제목	설명
보낸 사람	이 포트에 요청을 전송하는 클라이언트
끝	이 포트에 대한 요청을 수신하는 클라이언트
역할	클라이언트 또는 서버 애플리케이션 또는 프로세스
프로토콜	통신 설정 및 종료에 사용되는 세션 계층 프로토콜 또는 요청 및 응답 트랜잭션에 사용되는 애플리케이션 계층 프로토콜
전송 프로토콜	연결 지향형(TCP) 또는 비연결(UDP)인 전송 계층 프로토콜
대상/리스너	요청 수신에 사용되는 포트
소스/전송자	요청을 전송하는 데 사용되는 포트

IM and Presence 서비스 포트 목록

다음 표에서는 IM and Presence 서비스가 클러스터 내 및 클러스터 간 트래픽에 사용하는 포트를 보여줍니다.

표 ***41: IM and Presence*** 서비스 포트 **-** ***SIP*** 프록시 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
SIP Gateway --- IM and Presence	IM and Presence --- SIP Gateway	SIP	TCP/UDP	5060	임시	기본 SIP 프록시 UDP 및 TCP 리스너
SIP Gateway	IM and Presence	SIP	TLS	5061	임시	TLS 서버 인증 리스너 포트
IM and Presence	IM and Presence	SIP	TLS	5062	임시	TLS 상호 인증 리스너 포트

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	SIP	UDP / TCP	5049	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다.
IM and Presence	IM and Presence	HTTP	TCP	8081	임시	구성 변경을 나타내기 위해 구성 에이전트의 HTTP 요청에 사용됩니다.
타사 클라이언트	IM and Presence	HTTP	TCP	8082	임시	기본 IM and Presence HTTP 리스너. 타사 클라이언트를 연결하는 데 사용
타사 클라이언트	IM and Presence	HTTPS	TLS / TCP	8083	임시	기본 IM and Presence HTTPS 리스너. 타사 클라이언트를 연결하는 데 사용

표 ***42: IM and Presence*** 서비스 포트 **-** 프레즌스 엔진 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence (프레즌스 엔진)	SIP	UDP / TCP	5080	임시	기본 SIP UDP/TCP 리스너 포트
IM and Presence (프레즌스 엔진)	IM and Presence (프레즌스 엔진)	Livebus	UDP	50000	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. LiveBus 메시징 포트입니다. IM and Presence 서비스는 이 포트를 클러스터 통신에 사용합니다.

표 ***43: IM and Presence*** 서비스 포트 ***- Cisco Tomcat WebRequests***

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
브라우저	IM and Presence	HTTPS	TCP	8080	임시	웹 액세스에 사용

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
브라우저	IM and Presence	AXL / HTTPS	TLS / TCP	8443	임시	SOAP를 통해 데이터베이스 및 서비스 가용성을 제공합니다.
브라우저	IM and Presence	HTTPS	TLS / TCP	8443	임시	웹 관리에 대한 액세스를 제공합니다.
브라우저	IM and Presence	HTTPS	TLS / TCP	8443	임시	사용자 옵션 페이지에 대한 액세스를 제공합니다.
브라우저	IM and Presence	SOAP	TLS / TCP	8443	임시	SOAP를 통해 Cisco Unified Personal Communicator, Cisco Unified Mobility Advantage 및 타사 API 클라이언트에 대한 액세스를 제공합니다.
브라우저	IM and Presence	HTTPS	TCP	9463	임시	SSL(HTTPS)를 통한 하이퍼텍스트 전송 프로토콜은 v6의 TLS1.3만 허용합니다.

표 ***44: IM and Presence*** 서비스 포트 **-** 외부 회사 디렉터리 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence --- 외부 회사 디렉터리	외부 회사 디렉터리 --- IM and Presence	LDAP	TCP	389 / 3268	임시	디렉터리 프로토콜은 외부 회사 디렉터리와 통합하는 것을 허용합니다. LDAP 포트는 회사 디렉토리에 따라 다릅니다(기본값은 389). Netscape Directory의 경우 고객은 LDAP 트래픽을 수용할 수 있도록 다른 포트를 구성 할 수 있습니다. LDAP가 인증을 위해 IM&P와 LDAP 서버 간에 통신을 허용합니다.

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	외부 회사 디렉터리	LDAPS	TCP	636	임시	디렉터리 프로토콜은 외부 회사 디렉터리와 통합하는 것을 허용합니다. LDAP 포트는 회사 디렉토리에 따라 다릅니다(기본값은 636).

표 ***45: IM and Presence*** 서비스 포트 - 구성 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (구성 에이전트)	IM and Presence (구성 에이전트)	TCP	TCP	8600	임시	구성 에이전트 하트비트 포트

표 ***46: IM and Presence*** 서비스 포트 - 인증서 관리자 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	Certificate Manager	TCP	TCP	7070	임시	내부 포트 - Localhost 트래픽 전용

표 ***47: IM and Presence*** 서비스 포트 - ***IDS*** 데이터베이스 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (데이터베이스)	IM and Presence (데이터베이스)	TCP	TCP	1500	임시	데이터베이스 클라이언트를 위한 내부 IDS 포트입니다. 로컬 호스트 트래픽 전용입니다.
IM and Presence (데이터베이스)	IM and Presence (데이터베이스)	TCP	TCP	1501	임시	내부 포트 - 업그레이드하는 동안 IDS의 두 번째 인스턴스를 표시하는 데 사용됩니다. 로컬 호스트 트래픽 전용입니다.
IM and Presence (데이터베이스)	IM and Presence (데이터베이스)	XML	TCP	1515	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. DB 복제 포트

표 ***48: IM and Presence*** 서비스 포트 - ***IPSec*** 관리자 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (IPSec)	IM and Presence (IPSec)	Proprietary	UDP/TCP	8500	8500	내부 포트 - 플랫폼 데이터(호스트) 인증서의 클러스터 복제를 위해 ipsec_mgr 데몬에서 사용하는 클러스터 관리자 포트

표 ***49: IM and Presence*** 서비스 포트 - ***DRF*** 마스터 에이전트 서버 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (DRF)	IM and Presence (DRF)	TCP	TCP	4040	임시	로컬 에이전트, GUI 및 CLI에서 연결을 허용하는 DRF 마스터 에이전트 서버 포트

표 ***50: IM and Presence*** 서비스 포트 - ***RISDC*** 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	2555	임시	실시간 정보 서비스(RIS) 데이터베이스 서버. 클러스터의 다른 RISDC 서비스에 연결하여 클러스터 전체의 실시간 정보를 제공
IM and Presence (RTMT/AMC/ SOAP)	IM and Presence (RIS)	TCP	TCP	2556	임시	Cisco RIS용 실시간 정보 서비스(RIS) 데이터베이스클라이언트. RIS 클라이언트 연결을 통해 실시간 정보를 검색 가능
IM and Presence (RIS)	IM and Presence (RIS)	TCP	TCP	8889	8888	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. RISDC(시스템 액세스)에서 서비스 상태 요청 및 응답을 위해 TCP를 통해 servM에 연결하는 데 사용

표 51: IM and Presence 서비스 포트 - SNMP 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
SNMP 서버	IM and Presence	SNMP	UDP	161, 8161	임시	SNMP 기반 관리 애플리케이션에 대한 서비스를 제공
IM and Presence	IM and Presence	SNMP	UDP	6162	임시	SNMP 마스터 에이전트가 전달한 요청을 수신하는 기본 SNMP 에이전트
IM and Presence	IM and Presence	SNMP	UDP	6161	임시	기본 SNMP 에이전트에서 트랩을 수신하고 관리 애플리케이션으로 전달하는 마스터 에이전트
SNMP 서버	IM and Presence	TCP	TCP	7999	임시	cdp 에이전트가 cdp 바이너리와 통신하기 위한 소켓으로 사용
IM and Presence	IM and Presence	TCP	TCP	7161	임시	SNMP 마스터 에이전트와 하위 에이전트 간의 통신에 사용
IM and Presence	SNMP 트랩 모니터	SNMP	UDP	162	임시	SNMP 트랩을 관리 애플리케이션으로 전송
IM and Presence	IM and Presence	SNMP	UDP	가능 설정	61441	내부 SNMP 트랩 수신기

표 52: IM and Presence 서비스 포트 - Racoon 서버 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
게이트웨이 --- IM and Presence	IM and Presence --- 게이트웨이	Ipsec	UDP	500	임시	Internet Security Association and the Key Management 프로토콜 활성화

표 *53: IM and Presence* 서비스 포트 - 시스템 서비스 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (RIS)	IM and Presence (RIS)	XML	TCP	8888 및 8889	임시	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. RIS Service Manager(servM)와 통신하는 클라이언트를 수신하는 데 사용됩니다.

표 *54: IM and Presence Service* 포트 - *DNS* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	DNS Server(DNS 서버)	DNS	UDP	53	임시	DNS 서버가 IM and Presence DNS 쿼리를 수신하는 포트입니다. 수신: DNS 서버 | 발신: IM and Presence

표 *55: IM and Presence* 서비스 포트 - *SSH/SFTP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	엔드포인트	SSH / SFTP	TCP	22	임시	많은 애플리케이션에서 서버에 대한 명령줄 액세스에 사용됩니다. 또한 인증서와 기타 파일 교환을 위해 노드간에 사용됩니다(sftp).

표 *56: IM and Presence* 서비스 포트 - *ICMP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence --- Cisco Unified Communications Manager	Cisco Unified Communications Manager --- IM and Presence	ICMP	IP	해당 없음	임시	ICMP(Internet Control Message Protocol). Cisco Unified Communications Manager 서버와 통신하는 데 사용

표 *57: IM and Presence* 서비스 포트 *- NTP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	NTP 서버	NTP	UDP	123	임시	Cisco Unified Communications Manager는 작동 중인 NTP 서버입니다. 게시자 노드와 시간을 동기화하기 위해 구독자 노드에서 사용됩니다.

표 *58: IM and Presence* 서비스 포트 *- Microsoft Exchange* 알림 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
Microsoft Exchange	IM and Presence	HTTP (HTTPu)	) WebDAV - HTTP /UDP/IP 알림 2) EWS - HTTP/TCP /IP SOAP 알림	IM and Presence 서버 포트(기본값 50020)	임시	Microsoft Exchange는 이 포트를 사용하여 달력 이벤트의 특정 구독 식별자가 변경되었음을 알리는 알림(알림 메시지 사용)을 보냅니다. 네트워크 구성에서 Exchange 서버와 통합하는 데 사용됩니다. 두 개의 포트가 생성됩니다. 전송되는 메시지의 종류는 구성된 일정 프레즌스 백엔드 게이트웨이의 유형에 따라 다릅니다.

표 *59: IM and Presence* 서비스 포트 *- SOAP* 요청 서비스

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (Tomcat)	IM and Presence (SOAP)	TCP	TCP	5007	임시	SOAP 모니터 포트

표 *60: IM and Presence* 서비스 포트 - *AMC RMI* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	RTMT	TCP	TCP	1090	임시	AMC RMI 개체 포트입니다. RTMT 성능 모니터, 데이터 수집, 로깅 및 경고용 Cisco AMC 서비스
IM and Presence	RTMT	TCP	TCP	1099	임시	AMC RMI 레지스트리 포트입니다. RTMT 성능 모니터, 데이터 수집, 로깅 및 경고용 Cisco AMC 서비스

표 *61: IM and Presence* 서비스 포트 - *XCP* 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
XMPP 클라이언트	IM and Presence	TCP	TCP	5222	임시	클라이언트 액세스 포트
IM and Presence	IM and Presence	TCP	TCP	5269	임시	서버 간 연결(S2S) 포트
타사 BOSH 클라이언트	IM and Presence	TCP	TCP	7335	임시	BOSH 타사 API 연결을 위해 XCP 웹 연결 관리자에서 사용하는 HTTP 수신 대기 포트
IM and Presence (XCP 서비스)	IM and Presence (XCP 라우터	TCP	TCP	7400	임시	XCP 라우터 마스터 수락 포트입니다. 개방 포트 구성(예: XCP 인증 구성 요소 서비스)에서 라우터에 연결하는 XCP 서비스는 일반적으로 이 포트에 연결합니다.
IM and Presence (XCP 라우터	IM and Presence (XCP 라우터	UDP	UDP	5353	임시	MDNS 포트입니다. 클러스터의 XCP 라우터는 이 포트를 사용하여 서로를 찾습니다.

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (XCP 라우터	IM and Presence (XCP 라우터	TCP	TCP	7336	HTTPS	MFT 파일 전송(온-프레미스에만 해당).

표 ***62: IM and Presence*** 서비스 포트 - 외부 데이터베이스 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	PostgreSQL 데이터베이스	TCP	TCP	5432[1]	임시	PostgreSQL 데이터베이스 수신 대기 포트
IM and Presence	Oracle 데이터베이스	TCP	TCP	1521	임시	Oracle 데이터베이스 수신 대기 포트
IM and Presence	MSSQL 데이터베이스	TCP	TCP	1433	임시	MSSQL 데이터베이스 수신 대기 포트

[1] 이것은 기본 포트이지만 모든 포트에서 수신 대기하도록 PostgreSQL 데이터베이스를 구성할 수 있습니다.

표 ***63: IM and Presence*** 서비스 포트 - 고가용성 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (서버 복구 매니저)	IM and Presence (서버 복구 매니저)	TCP	TCP	20075	임시	Cisco 서버 복구 매니저가 admin rpc 요청을 제공하는 데 사용하는 포트입니다.
IM and Presence (서버 복구 매니저)	IM and Presence (서버 복구 매니저)	UDP	UDP	21999	임시	Cisco 서버 복구 매니저가 피어와 통신하는 데 사용하는 포트입니다.

표 ***64: IM and Presence*** 서비스 포트 - 인 메모리 데이터베이스 복제 메시지

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6603*	임시	Cisco Presence 데이터 저장소

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6604*	임시	Cisco 로그인 데이터 저장소
IM and Presence	IM and Presence	Proprietary	TCP	6605*	임시	Cisco SIP 등록 데이터 저장소
IM and Presence	IM and Presence	Proprietary	TCP	9003	임시	Cisco 프레즌스 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence	IM and Presence	Proprietary	TCP	9004	임시	Cisco 로그인 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence	IM and Presence	Proprietary	TCP	9005	임시	Cisco SIP 등록 데이터 저장소 이중 노드 하위 클러스터 복제.

* 관리 CLI 진단 유틸리티를 실행하려면 `utils imdb_replication status` 명령을 사용하여 이러한 포트가 클러스터의 IM 및 프레즌스 서비스 노드 사이에 설정된 모든 방화벽에서 열려 있어야 합니다. 정상적인 작동에는 이 설정이 필요하지 않습니다.

표 ***65: IM and Presence*** 서비스 포트 - 인메모리 데이터베이스 ***SQL*** 메시지

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6603	임시	Cisco Presence 데이터 저장소 SQL 쿼리.
IM and Presence	IM and Presence	Proprietary	TCP	6604	임시	Cisco 로그인 데이터 저장소 SQL 쿼리.
IM and Presence	IM and Presence	Proprietary	TCP	6605	임시	Cisco SIP 등록 데이터 저장소 SQL 쿼리.
IM and Presence	IM and Presence	Proprietary	TCP	6606	임시	Cisco 라우트 데이터 저장소 SQL 쿼리.

표 *66: IM and Presence* 서비스 포트 - 인메모리 데이터베이스 알림 메시지

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence	IM and Presence	Proprietary	TCP	6607	임시	Cisco Presence 데이터 저장소 XML 기반 변경 알림.
IM and Presence	IM and Presence	Proprietary	TCP	6608	임시	Cisco 로그인 데이터 저장소 XML 기반 변경 알림.
IM and Presence	IM and Presence	Proprietary	TCP	6609	임시	Cisco SIP 등록 데이터 저장소 XML 기반 변경 알림.
IM and Presence	IM and Presence	Proprietary	TCP	6610	임시	Cisco 라우트 데이터 저장소 XML 기반 변경 알림.

표 *67: IM and Presence* 서비스 포트 - 강제 수동 동기화*/X.509* 인증서 업데이트 요청

보낸 사람(전송자)	받는 사람(리스너)	프로토콜	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence (Intercluster 동기화 에이전트)	IM and Presence (Intercluster 동기화 에이전트)	TCP	TCP	37239	임시	Cisco 클러스터 간 동기화 에이전트 서비스는 이 포트를 사용하여 명령을 처리하기 위한 소켓 연결을 설정합니다.

표 *68: IM and Presence* 서비스 포트 - *ICMP* 요청

보낸 사람(전송자)	받는 사람(리스너)	대상 포트	목적
엔드포인트/IM and Presence	IM and Presence	7	인터넷 제어 메시 (ICMP). 이 프로 에코 관련 트래픽 다. 열 머리글에 포트를 구성하지
IM and Presence	엔드포인트/IM and Presence		

표 *69: IM and Presence*에 사용되는 포트 - *Cisco Unified CM* 통신 및 *IM and Presence* 게시자 - 가입자 통신

보낸사람(전송자)	받는사람(리스너)	전송 프로토콜	대상/리스너	소스/전송자	참고
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	1500	양방향	데이터베이스 클라이언트를 위한 내부 ID 포트입니다. 로컬 호스트 트래픽 전용입니다.
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	8443	양방향	웹 관리에 대한 액세스를 제공합니다.
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	1090	양방향	AMC RMI 개체 포트입니다. RTMT 성능 모니터, 데이터 수집, 로깅 및 경고용 Cisco AMC 서비스
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	2555	양방향	양방향 실시간 정보 서비스(RIS) 데이터베이스 서버. 클러스터의 다른 RISDC 서비스에 연결하여 클러스터 전체의 실시간 정보를 제공
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	8500	양방향	내부 포트 - 플랫폼 데이터(호스트) 인증서의 클러스터 복제를 위해 ipsec_mgr 데몬에서 사용하는 클러스터 관리자 포트
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	8600	양방향	구성 에이전트 하트비트 포트
Cisco Unified Communications Manager	IM and Presence 게시자	UDP	123	양방향	시간 동기화에 사용되는 NTP(Network Time Protocol)
IM and Presence 게시자	IM and Presence 가입자	UDP	50000	양방향	내부 포트입니다. 로컬 호스트 트래픽 전용입니다. LiveBus 메시징 포트입니다. IM and Presence 서비스는 이 포트를 클러스터 통신에 사용합니다.

보낸사람(전송자)	받는사람(리스너)	전송 프로토콜	대상/리스너	소스/전송자	참고
IM and Presence 게시자	IM and Presence 가입자	UDP	21999	양방향	Cisco 서버 복구 매니저가 피어와 통신하는 데 사용하는 포트입니다.
IM and Presence 게시자	Cisco Unified Communications Manager	TCP	4040	양방향	로컬 에이전트, GUI 및 CLI에서 연결을 허용하는 DRF 마스터 에이전트 서버 포트
IM and Presence 게시자	Cisco Unified Communications Manager	TCP	8001	양방향	영구 채팅을 구성하는 중에 사용됩니다.
IM and Presence 게시자	Cisco Unified Communications Manager	TCP	6379	양방향	관리형 파일 전송(MFT)을 구성하는 동안 사용됩니다.
IM and Presence 게시자	IM and Presence 가입자	TCP	7	양방향	외부 데이터베이스(MSSQL)를 구성하는 중에 사용됩니다.
IM and Presence 게시자	IM and Presence 가입자	TCP	20075	양방향	Cisco 서버 복구 매니저가 admin RPC 요청을 제공하는 데 사용하는 포트입니다.
IM and Presence 게시자	IM and Presence 가입자	TCP	8600	양방향	구성 에이전트 하트비트 포트
IM and Presence 가입자	IM and Presence 게시자	TCP	9005	양방향	Cisco SIP 등록 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence 가입자	IM and Presence 게시자	TCP	9003	양방향	Cisco 프레즌스 데이터 저장소 이중 노드 하위 클러스터 복제.
IM and Presence 가입자	IM and Presence 게시자	TCP	20075	양방향	Cisco 서버 복구 매니저가 admin RPC 요청을 제공하는 데 사용하는 포트입니다.
IM and Presence 가입자	IM and Presence 게시자	TCP	9004	양방향	Cisco 로그인 데이터 저장소 이중 노드 하위 클러스터 복제.

보낸사람(전송자)	받는사람(리스너)	전송프로토콜	대상/리스너	소스/전송자	참고
Cisco Unified Communications Manager	IM and Presence 게시자	TCP	5070	양방향	통화 구성에 사용됨
IM and Presence 게시자	IM and Presence 가입자	TCP	44000	양방향	통화 구성에 사용됨

표 ***70: On-a-call_Presence***

보낸사람(전송자)	받는사람(리스너)	소스 포트	대상 포트	프로토콜	참고
Cisco Unified Communications Manager	IM and Presence 게시자	[37240 – 61000]	5070	TCP	
IM and Presence 게시자	XMPP 클라이언트(Jabber)	5222	64846	TCP	클라이언트 액세스 포트
IM and Presence 게시자	XMPP 클라이언트(Jabber)	5222	56361	TCP	클라이언트 액세스 포트

표 ***71: MS-SQL DB*** 구성

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	데이터베이스	[37240 – 61000]	7	TCP

표 ***72: MS-SQL*** 영구 채팅 구성

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	데이터베이스	37240 – 61000	1433	TCP

표 ***73:*** 관리형 파일 전송***(MFT)*** 구성

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	외부 파일 서버	37240 – 61000	7	TCP

보낸 사람(전송자)	받는 사람(리스너)	소스 포트	대상 포트	프로토콜
IM and Presence 게시자	외부 파일 서버	37240 – 61000	22	TCP
IM and Presence 게시자	외부 파일 서버	37240 – 61000	5432	TCP
IM and Presence 게시자	데이터베이스	54288 - 54292	5432	TCP

SNMP에 대한 자세한 내용은 *Cisco Unified Serviceability* 관리 설명서를 참조하십시오.