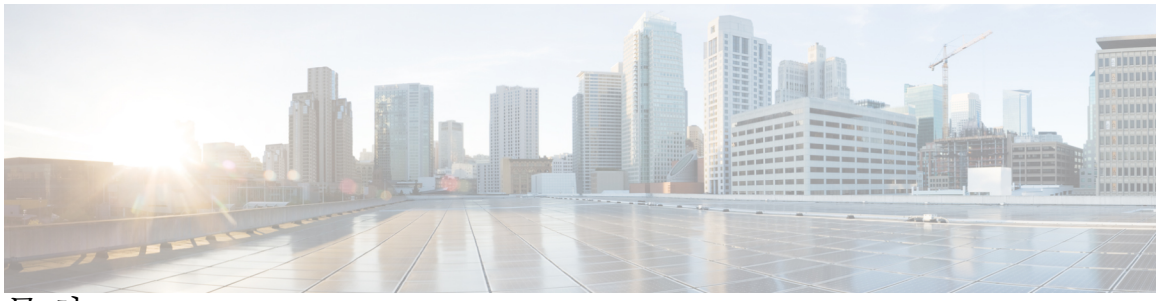
Cisco Jabber 14.1용 계획 설명서

초판: 2022년 2월 24일

최종 변경: 2024년 4월 2일

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



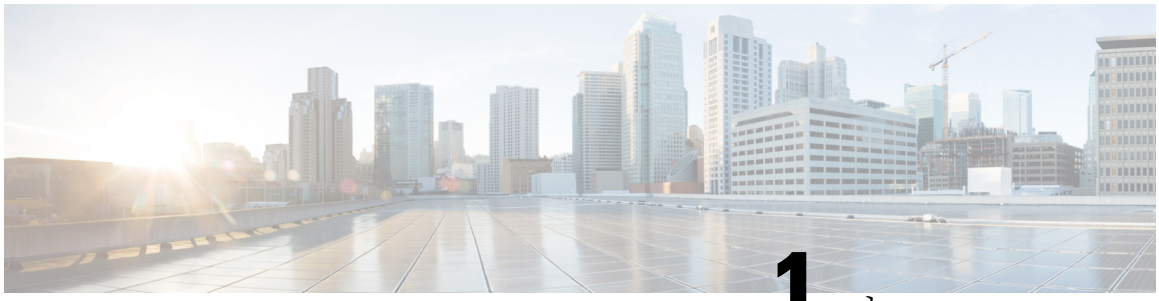
목 차

신규 및 변경된 정보

신규 및 변경된 정보

날짜	설명	위치
2023년 7월	VDI(가상 데스크톱 인프라) 환경에 배포하기 위한 로컬 및 로밍 프로필 폴더 요구 사항이 업데이트되었습니다.	가상 환경에 구축
2022년 7월	iPhone 요구 사항이 업데이트되었습니다.	iPhone 및 iPad용 Cisco Jabber의 하드웨어 요구 사항
2022년 6월	전체 UC 배포에서 비 DNS SRV 레코드 방법을 변경했습니다.	권장 연결 방법
	14.1.3은 Android 8.1 이전 버전을 지원하는 마지막 버전입니다.	Android용 Cisco Jabber의 운영 체제
2022년 2월	최초 게시	
	Android용 Jabber에 대한 최소 요구 사항 및 지원되는 장치가 업데이트되었습니다.	Android용 Cisco Jabber 하드웨어 요구 사항
	iPhone 및 iPad용 Jabber에 대한 최소 요구 사항 및 지원되는 장치가 업데이트되었습니다.	iPhone 및 iPad용 Cisco Jabber의 하드웨어 요구 사항
	Windows 11에 대한 지원 추가	Windows용 Cisco Jabber의 운영 체제

신규 및 변경된 정보



1 장

Jabber 요구 사항

서버 요구 사항

다음 소프트웨어 요구 사항은 이 릴리스의 모든 Cisco Jabber 클라이언트에 공통으로 적용됩니다.

서비스	소프트웨어 요구 사항	지원되는 버전
IM and Presence	Cisco Unified Communications Manager IM and Presence Service	10.5(2) 이상(최소) 11.5(1) SU2 이상(권장)
	Webex Messenger	
텔레포니	Cisco Unified Communications Manager	10.5(2) 이상(최소) 11.5(1) SU3 이상(권장)
	Cisco Unified Survivable Remote Site Telephony	통합 SIP SRST 12.8 이상
연락처 검색	LDAP 디렉토리	LDAP v3 준수 디렉터리(예: Microsoft Active directory 2008 R2 및 Open LDAP 2.4 이상)
음성 메일	Cisco Unity Connection	10.5 이상
복수 회선	Cisco Unified Contact Center Express	11.6

서비스	소프트웨어 요구 사항	지원되는 버전
전화회의	Cisco Meeting Server	2.2 이상
	Cisco TelePresence Server	3.1 이상
	Cisco TelePresence MCU	4.3 이상
	Cisco ISR PVDM3	Cisco Unified Communications Manager 9.x 이상
	클라우드 CMR	Webex Meetings 협업 회의실이 있는 서버
	Webex Meetings 서버	2.8 MR1 이상
	Webex Meetings Center	WBS33 이상
Remote Access	Cisco Adaptive Security Appliance Android용 Cisco Jabber에만 적용됩니다.	8.4(1) 이상
	Cisco AnyConnect Secure Mobility Client Android용 Cisco Jabber 및 iPhone 및 iPad용 Cisco Jabber 클라이언트만 해당합니다.	플랫폼별
	Cisco Expressway C	X8.10.1 이상
	Cisco Expressway E	X8.10.1 이상

Cisco Jabber는 시작 중에 DNS(domain name system) 서버를 사용합니다. DNS 서버는 Cisco Jabber 설정에 반드시 필요합니다.

운영 체제 요구 사항

Windows용 Cisco Jabber의 운영 체제

다음 운영 체제에 Windows용 Cisco Jabber를 설치할 수 있습니다.

- Microsoft Windows 10(데스크탑 모드)
- Microsoft Windows 8.1(데스크탑 모드)
- Microsoft Windows 8(데스크탑 모드)

Windows용 Cisco Jabber에는 Microsoft .NET Framework 또는 모든 Java 모듈이 필요하지 않습니다.

Windows 10 서비스 옵션

Windows용 Cisco Jabber는 다음 Windows 10 서비스 옵션을 지원합니다.

- 현재 브랜치(CB)
- 현재 비즈니스 브랜치(CBB)
- LTSB(장기 서비스 브랜치) - 이 옵션을 사용하면 관련 서비스 업데이트를 구축해야 할 책임이 있습니다.

Windows 10 서비스 옵션에 대한 자세한 내용은 다음 Microsoft 설명서를 참조하십시오.
https://technet.microsoft.com/en-us/library/mt598226(v=vs.85).aspx

참고 Cisco Jabber는 기본적으로 다음 디렉터리에 필요한 파일을 설치합니다.

- %temp%\Cisco Systems\Cisco Jabber-Bootstrap.properties file and installation log
- %LOCALAPPDATA%\Cisco\Unified Communications-Logs and temporary telemetry data
- %APPDATA%\Cisco\Unified Communications-Cached configurations and account credentials
- %ProgramFiles%\Cisco Systems\Cisco Jabber-Installation files for x86 Windows
- %ProgramFiles(x86)%\Cisco Systems\Cisco Jabber-Installation files for x64 Windows

Mac용 Cisco Jabber의 운영 체제

다음 운영 체제에 Mac용 Cisco Jabber를 설치할 수 있습니다.

- macOS Monterey
- macOC Big Sur
- macOS Catalina 10.15 이상
- macOS Mojave 10.14 이상
- macOS High Sierra 10.13(이상)
- macOS Sierra 10.12(이상)

Android용 Cisco Jabber의 운영 체제

지원되는 최신 운영 체제 버전 정보에 대해서는 Play Store를 참조하십시오.

중요 Jabber 14.1.3은 Android OS 6.x, 7.x 및 8.0을 지원하는 마지막 릴리스입니다. 보안상의 이유로 다음 Jabber 릴리스에는 최소 Android OS 8.1이 포함됩니다.

참고 Android용 Cisco Jabber는 32비트 앱과 64비트 앱으로 사용할 수 있습니다. Android 장치에 64비트 OS가 있는 경우 64비트 Jabber 클라이언트를 실행하여 더 빠르고 풍부한 경험을 얻을 수 있습니다.

32비트 OS에는 64비트 앱을 설치할 수 없습니다. 대부분의 64비트 플랫폼에서 32비트 앱을 사용하는 경우 64비트 앱으로 업그레이드하 라는 알림을 받게 됩니다.

참고 Android 6.0 Marshmallow OS 이상에 Cisco Jabber가 설치되어 있고 유휴 상태로 유지되는 경우:

- Cisco Jabber에 대한 네트워크 연결이 비활성화됩니다.
- 사용자는 통화 또는 메시지를 수신하지 않습니다.

설정 변경을 누르고 배터리 최적화를 무시하여 통화 및 메시지를 수신합니다.

Android 5.x를 지원하는 마지막 **Jabber** 릴리스

Cisco Jabber 12.8은 Android 5.x를 실행하는 장치를 지원하는 마지막 릴리스입니다.

Jabber 12.9는 Android 6.x로 업그레이드할 수 없는 모든 장치에 대한 지원을 종료합니다.

iPhone 및 iPad용 Cisco Jabber의 운영 체제

지원되는 최신 운영 체제 버전 정보에 대해서는 App Store를 참조하십시오.

중요 Cisco는 iPhone 및 iPad용 Cisco Jabber의 현재 App Store 버전만 지원합니다. iPhone 및 iPad용 Cisco Jabber 릴리스에서 발견된 결함은 현재 버전에 대해 평가됩니다.

하드웨어 요구 사항

데스크톱 클라이언트의 하드웨어 요구 사항

요구 사항	**Windows**용 **Cisco Jabber**	**Mac**용 **Cisco Jabber**
설치된 RAM	2GB RAM	2GB RAM

요구 사항	**Windows**용 **Cisco Jabber**	**Mac**용 **Cisco Jabber**
가용 실제 메모리	128 MB	1 GB
여유 디스크 공간	256 MB	300MB
CPU 속도 및 종류	AMD Mobile Sempron 프로세서 3600+ 2GHz Intel Core 2 Duo 프로세서 T7400 @ 2. 16 GHz	다음 Apple 하드웨어에 Intel Core 2 Duo 이상 프로세서 장착: • iMac Pro • MacBook Pro(Retina Display 모델 포함) • MacBook • MacBook Air • iMac • Mac Mini
I/O 포트	USB 카메라 및 오디오 장치용 USB 2.0	USB 카메라 및 오디오 장치용 USB 2.0

CTI 지원 장치

통합 커뮤니케이션 관리자에 대해 지원되는 CTI(컴퓨터 전화 통신 통합) 장치 목록을 보려면 다음을 수행합니다.

1. **Cisco** 통합 보고 페이지의 시스템 보고서 메뉴에서 **Unified CM** 전화 기능 목록을 선택합니다.
2. 보고서를 연 후 기능 드롭다운 목록에서 **CTI** 제어를 선택합니다.

Android용 Cisco Jabber 하드웨어 요구 사항

Android 장치에 대한 최소 요구 사항:

Android 운영 체제	**CPU**	디스플레이
6.0 이상	1.5GHz 듀얼 코어 권장: 1.2GHz 쿼드 코어 이상	양방향 비디오: 480p x 800p 이상 IM 전용: 320p x 480p 이상.

Android용 Cisco Jabber는 OS 버전을 사용하는 장치에서 전체 UC 모드를 지원합니다.

표 *1:* 지원되는 ***Android*** 장치

장치	모델	최소 **Android OS** 버전	참고
BlackBerry	Priv	6.0.1	최근에 본 앱 목록에서 Jabber를 제거하고 얼마 동안 장치가 유휴 상태로 유지되는 경우 Jabber가 비활성화됩니다.
Fujitsu	Arrows M357	6.0.1	

장치	모델	최소 Android OS 버전	참고
Google	Nexus 5	6.0	
	Nexus 5X	6.0	
	Nexus 6	6.0	
	Nexus 6P	6.0	Android OS 버전 6.x 또는 7.0이 설치된 Google Nexus 6P의 경우 관리자가 Jabber 전화 서비스를 보안 전화 서비스로 설정해야 합니다. 그렇지 않으면 장치가 응답하지 않을 수도 있습니다. Android OS 버전이 7.1 이상인 경우 이러한 조치는 필요하지 않습니다.
	Nexus 7	6.0	
	Nexus 9	6.0	
	Pixel	7.0	
	Pixel C	6.0	
	Pixel XL	7.0	
	Pixel 2	8.0	Jabber call 중에 사용자가 모바일 장치에서 헤드셋으로 오디오를 전환하면 오디오가 일시 정지되는 문제가 발생할 수 있습니다.
	Pixel 2 XL	8.0	Jabber call 중에 사용자가 모바일 장치에서 헤드셋으로 오디오를 전환하면 오디오가 일시 정지되는 문제가 발생할 수 있습니다.
	Pixel 3	8.0	연결된 헤드셋을 전화기와 함께 사용하는 경우 몇 초 동안 오디오에 몇 가지 문제가 발생할 수 있습니다.
	Pixel 3 XL	8.0	연결된 헤드셋을 전화기와 함께 사용하는 경우 몇 초 동안 오디오에 몇 가지 문제가 발생할 수 있습니다.
	Pixel 4	10.0	
	Pixel 4 XL	10.0	
	Pixel 4a 5G	10.0	

장치	모델	최소 **Android OS** 버전	참고
Honeywell Dolphin	CT50	6.0	
	CT40	7.1.1	
	CT60	7.1.1 및 8.1	Android OS 7.1.1 및 8.1을 사용하는 CT60만 지원합니다.
HTC	10	6.0	
	A9	6.0	
	M8	6.0	
	M9	6.0	
	X9	6.0	
Huawei [1]	Honor 7	6.0	
	Mate 8	6.0	
	Mate 9	6.0	
	Nova	7.0	
	Mate 10	8.0	
	Mate 10 Pro	8.0	
	P8	6.0	
	P9	6.0	
	P10	7.0	
	P10 Plus	7.0	
	P20	8.0	
	P20 Pro	8.0	
	Mate20	8.0	
	Mate20 Pro	8.0	
	P30	9.0	
	P30 Pro	9.0	

장치	모델	최소 Android OS 버전	참고
LG	G3	6.0	
	G4	6.0	
	G5	6.0	
	G6	7.0	
	V10	6.0	
	V30	8.0	
Motorola	Moto G4	6.0	
	Moto G5	7.0	
	Moto G6	8.0	
	Moto Z Droid	6.0	
Nokia	6.1	8.0	
	8.1	8.1	
OnePlus	1	6.0	
	5	8.0	
	5T	8.0	
	6	9.0	
	6T	9.0	
	7T	10.0	
	8	11.0	
	8 Pro	11.0	
	8T	11.0	

장치	모델	최소 **Android OS** 버전	참고
삼성	모두	6.0	• Android OS 6. x 이상으로 업그레이드할 수 없는 장치는 더 이상 지원되지 않습니다. • Jabber에 대한 자동 실행 옵션을 활성화합니다. Android OS 6.x 이상의 경우, **App Smart Manager**에서 자동 실행 옵션을 찾을 수 있습니다. • 캐나다의 Samsung Galaxy Tab Pro 8.4(모델 T320UEU1AOC1)에서는 Jabber의 수신 전화 알림 팝업이 지연됩니다. • Jabber는 Wi-Fi 연결이 끊어지면 Samsung Xcover 3에서 네트워크에 다시 연결하는 것을 지연합니다. • Exynos 7580 칩셋이 장착된 Samsung 장치에 오디오 품질 문제가 있습니다. 장치 화면이 꺼지면 오디오가 선명하지 않게 됩니다. 다음은 장치 목록입니다. • Samsung Galaxy A3 2016 • Samsung Galaxy A5 2016 • Samsung Galaxy A7 2016 • Samsung Galaxy S5 Neo • Samsung Galaxy J7 • Samsung Galaxy View
Seuic	Cruise 1	9.0	
Sonim	XP8	7.1.1	

장치	모델	최소 **Android OS** 버전	참고
Sony Xperia	XZ	7.0	
	XZ1	8.0	
	XZ2	8.0	
	XZ3	9.0	
	Z2	6.0	
	Z2 태블릿	6.0	
	Z3	6.0	Android OS 5.0.2가 설치된 Sony Xperia Z3(모델 SO-01G)은 Jabber call 시 오디오 품질이 좋지 않습니다.
	Z3 Tablet Compact	6.0	
	Z3+/Z4	6.0	Sony Z3+/Z4에서 영상 통화가 불안정합니다. 영상 통화에 대해 셀프 비디오를 비활성화해 보십시오. 그렇지 않으면 음성 통화로만 전화를 거십시오.
	Z4 TAB	6.0	
	Z5 Premium 및 Z5	6.0	
	Xperia 5 Mark II	11.0	

장치	모델	최소 Android OS 버전	참고
Xiaomi	4C	6.0	이러한 장치에서는 32비트 버전만 실행됩니다.
	MAX	6.0	
	Mi 4	6.0	
	Mi 5	6.0	
	Mi 5s	7.0	
	Mi 6	7.0	
	Mi 8	8.0	
	Mi 9	9.0	
	Mi 10	10.0	
	Mi 10 Ultra	10.0	
	Pocophone	8.0	
	Mi Note	6.0	이러한 장치에서는 32비트 버전만 실행됩니다.
	Mi Note 2	7.0	
	Mi MIX 2	8.0	
	Mi A1	8.0	
	Redmi Note 3	6.0	
	Redmi Note 4X	6.0.1	
	Redmi Note 5	8.0	
	Redmi Note 6 Pro	8.1	
Zebra	TC75X	6.0	
	TC51	6.0	

[1] EMUI 10의 변경 사항으로 인해, 장치가 잠겨 있을 때 수신 전화 알림이 나타나지 않을 수 있습니다. Jabber에서 설정 > 알림으로 이동하여 배너를 선택합니다.

Samsung Knox에 대한 Jabber 지원

Android용 Cisco Jabber는 다음과 같이 Samsung Knox를 지원합니다.

Knox 버전	Samsung 장치
2.6	Note 4 Note 5 Note Edge S5 S6 S6 Edge S6 Edge Plus S7 S7 Edge Note 10.1(2014 버전)
2.7.1	Galaxy Note5
3.1	Galaxy A5(2017)
3.2	Galaxy On5(2016)
3.3	Galaxy S10

참고 Samsung에서 Android용 Cisco Jabber를 실행하는 경우, Samsung Knox의 보안 설계에서 먼저 Knox의 잠금을 해제해야 합니다. 사용자는 Knox의 잠금을 해제할 때까지 Jabber를 사용하여 통화를 응답하거나 거부할 수 없습니다.

Jabber에서 Samsung Dex 지원

Android용 Cisco Jabber는 Samsung S8, S8 Plus 및 Note 8에서 Samsung Dex를 지원합니다.

Cisco Jabber의 이전 Android 버전에 대한 지원 정책

Android 커널 문제로 인해 Cisco Jabber는 일부 Android 장치에서 Cisco Unified Communications Manager에 등록할 수 없습니다. 이 문제를 해결하려면 다음과 같이 해보십시오.

Android 커널을 3.10 이상 버전으로 업그레이드합니다.

Cisco Unified Communications Manager를 혼합 모드 보안을 사용하고, SIP 통화 신호 처리를 활성화하고, 포트 5061을 사용하도록 설정합니다. Cisco CTL Client에 혼합 모드를 구성하는 방법에 대해서는 해당 릴리스에 대한 *Cisco Unified Communications Manager* 보안 설명서를 참조하십시오. Cisco Unified Communications Manager Maintain and Operate Guides에서 보안 안내서를 찾을 수 있습니다. 이 솔루션은 다음의 지원 장치에 적용됩니다.

장치 모델	운영 체제
HTC M8	Android OS 6.0 이상
HTC M9	Android OS 6.0 이상
Sony Xperia Z2	Android OS 6.0 이상 및 3.10.49 이전 커널 버전 장치의 Android OS가 6.0 이상이고 커널 버전이 3.10.49 이상이면 장치가 비보안 모드를 지원할 수 있습니다.
Sony Xperia Z2 태블릿	
Sony Xperia Z3	
Sony Xperia Z3 태블릿 콤팩트	
Xiaomi Mi4	Android OS 6.0 이상
Xiaomi Mi Note	Android OS 6.0 이상
Honeywell Dolphin CT50	Android OS 6.0 이상

지원되는 블루투스 장치

Bluetooth 장치	종속성
Cisco 561	
Cisco 562	
Plantronics Voyager Legend	
Plantronics Voyager Legend UC	
Plantronics Voyager edge UC	
Plantronics Voyager edge	
Plantronics PLT focus	
Plantronics BackBeat 903+	Samsung Galaxy S4를 사용하는 경우 이러한 장치 간의 호환성 문제로 인해 문제가 발생할 수 있습니다.
Jabra Motion	Jabra Motion 블루투스 헤드셋을 펌웨어 버전 3.72 이상으로 업그레이드합니다. 펌웨어 버전 3.72 이상인 Jabra Motion 블루투스 헤드셋은 Cisco Jabber call 제어를 지원합니다.
Jabra Wave+	
Jabra Biz 2400	
Jabra Easygo	

Bluetooth 장치	종속성
Jabra PRO 9470	
Jabra Speak 510	
Jabra Supreme UC	
Jabra Stealth	
Jabra Evolve 65 UC Stereo	
Cisco 블루투스 헤드셋용 Jawbone ICON	Samsung Galaxy S4를 사용하는 경우 이러한 장치 간의 호환성 문제로 인해 문제가 발생할 수 있습니다.

블루투스 제한 사항**:**

- Samsung Galaxy SIII에서 블루투스 장치를 사용하면 벨소리 및 통화 오디오가 왜곡될 수 있습니다.
- 사용자가 Jabber call 도중 블루투스 헤드셋의 연결을 끊었다가 다시 연결하면 사용자가 오디오를 들을 수 없습니다. 이 제한 사항은 Android 5.0 OS 이전 버전의 스마트폰에 적용됩니다.
- Sony Z4/LG G4/장치에서 OS Android 6.0을 사용하는 경우 Jabber call을 시작한 후 블루투스 헤드셋으로 전환할 때 오디오 손실이 발생할 수 있습니다. 해결 방법은 오디오 출력을 스피커로 전환한 다음 다시 블루투스로 전환하는 것입니다. 또는 Cisco Jabber 전화를 걸기 전에 블루투스 헤드셋을 연결하십시오.

지원되는 **Android Wear**

Cisco Jabber는 Android OS 5.0 이상 및 Google 서비스 8.3 이상이 설치된 모든 Android Wear 장치에서 실행됩니다. Cisco Jabber는 다음 Android Wear 장치에서 테스트합니다.

- Fossil Gen 3 SmartWatch
- Huawei watch
- LG G Watch R
- LG Watch Urbane
- Moto 360
- Moto 360(2세대)
- Samsung Gear Live
- Sony SmartWatch 3

참고 Android Wear 장치용 Cisco Jabber 설치 관리자는 기본 Jabber APK 파일과 분리되어 있습니다. 사용자가 Wear 장치를 모바일 장치와 페어링하면 Google Play store에서 Android Wear 설치 관리자를 받습니다.

지원되는 **Chromebook** 모델

Chromebook에 Chrome OS 버전 53 이상이 있어야 합니다. Google Play 스토어에서 Android용 Cisco Jabber를 다운로드할 수 있습니다.

- HP Chromebook 13 G1 노트북 PC
- Google Chromebook Pixel
- Google Chromebook Pixelbook
- Samsung Chromebook Pro
- Asus C302

iPhone 및 iPad용 Cisco Jabber의 하드웨어 요구 사항

Jabber는 다음 Apple 장치를 지원합니다. iPhone 및 iPad의 최소 요구 사항은 iOS 15.x 및 iPadOS입니다. 이러한 버전으로 업그레이드되지 않은 장치는 지원하지 않습니다.

Apple 기기	버전
iPad	5, 6 및 7세대
iPad Air	Air 2 및 Air 3
iPad Pro	9.7 및 10.5 인치 12.9 인치, 1, 2 및 3세대
iPad mini	Mini 4 및 mini 5
iPhone	8, 8 Plus, X, Xs, Xs Max, 11, 11 Pro, 11 Pro Max, XR 및 SE, 12, 13
iPod touch	6세대
Apple Watch	Apple Watch 및 Apple Watch 2, 3 및 4에서 실행되는 WatchOS 5.

iPhone 및 iPad에서 지원되는 블루투스 헤드셋은 다음과 같습니다.

제조업체	모델
Apple	AirPod

제조업체	모델
Cisco	561, 562
Jabra	BIZ 2400, Easygo, Evolve 65 UC Stereo, EXTREME 2, Motion[2], PRO 9470, Cisco용 Speak 450, Speak 510, Stealth Supreme UC, Wave +에서만 지원됩니다.
Jawbone	Cisco 블루투스 헤드셋용 ICON
Plantronics	Voyager Edge, Voyager Edge UC, Voyager Legend, Voyager Legend UC
Sony Eriksson	MW-600

[2] 은 Cisco Jabber call을 위한 Bluetooth 제어를 지원합니다. 이 기능은 펌웨어 버전 3.72.

네트워크 요구 사항

기업 Wi-Fi 네트워크에서 Cisco Jabber를 사용할 때 다음을 수행할 것을 권장합니다.

- 엘리베이터, 계단 및 외부 복도 등의 영역을 포함하여 최대한의 범위에서 갭을 없앨 수 있도록 Wi-Fi 네트워크를 설계합니다.
- 모든 액세스 포인트에서 모바일 기기에 같은 IP 주소를 할당했는지 확인합니다. 통화 중에 IP 주소가 바뀌면 통화가 끊깁니다.
- 모든 액세스 포인트가 같은 SSID(Service Set Identifier)인지 확인합니다. SSID가 일치하지 않으면 핸드오프가 훨씬 느려질 수 있습니다.
- 모든 액세스 포인트가 SSID를 브로드캐스트하는지 확인합니다. 액세스 포인트가 SSID를 브로드캐스트하지 않으면, 모바일 기기에서 사용자에게 또 다른 Wi-Fi 네트워크로 연결하도록 표시되며 통화가 중단됩니다.
- 엔터프라이즈 방화벽이 STUN(Session Traversal Utilities for NAT) 패킷의 통로를 허용하도록 구성되어 있는지 확인합니다.

음성 품질에 영향을 줄 수 있는 네트워크 문제를 최소화하기 위해 철저한 사이트 설문조사를 시행합니다. 다음을 수행하는 것이 좋습니다.

- 채널 구성 중복 여부, 액세스 포인트 범위, 필수 데이터 및 트래픽 속도를 확인합니다.
- 비인증 액세스 포인트를 제거합니다.
- 가능한 간섭 소스 가능성을 식별하여 최소화합니다.

자세한 내용은 다음 문서를 참조하십시오.

- 기업 모빌리티 설계 가이드의 “VoWLAN 설계 추천” 섹션.
- *Cisco Unified* 무선 *IP* 전화기 *7925G* 구축 가이드.

- *IEEE 802.11g*의 용량 범위 및 고려사항 백서.
- Cisco Unified Communications Manager 릴리스용 *Solutions Reference Network Design (SRND)*.

IPv6 요구 사항

Cisco Jabber는 IPv6를 완벽하게 지원하며, 순수 IPv6 및 하이브리드 네트워크에서는 이 섹션에 나열된 제한 사항이 있지만 정상적으로 작동합니다. Cisco Collaboration 솔루션은 현재 IPv6를 완벽하게 지원하지 않습니다. 예를 들어, 모바일 및 Remote Access용 Cisco VCS Expressway는 순수 IPv6 네트워크에서 NAT64/DNS64를 이동 통신사 네트워크에 구축해야 하는 제한 사항이 있습니다. Cisco Unified Communications Manager 및 Cisco Unified Communications Manager IM and Presence는 현재 순수 IPv6 네트워크에서 HTTPS를 지원하지 않습니다.

Jabber의 이 기능은 IP_Mode 매개 변수를 사용하여 프로토콜을 IPv4, IPv6 또는 이중 스택으로 설정합니다. 이중 스택이 기본 설정입니다. IP_Mode 매개 변수는 Jabber 클라이언트 구성(*Cisco Jabber*용 매개 변수 참조 설명서의 최신 버전 참조), Windows용 부트스트랩 및 Mac 및 모바일 클라이언트용 URL 구성에 포함될 수 있습니다.

Jabber가 서비스에 연결할 때 사용하는 네트워크 IP 프로토콜은 다음 요소에 의해 결정됩니다.

- Jabber 클라이언트 구성 IP_Mode 매개 변수.
- 클라이언트 운영 체제 IP 기능.
- 서버 운영 체제 IP 기능.
- IPv4 및 IPv6에 대한 DNS 레코드 가용성.
- IPv4, IPv6 또는 둘 모두의 소프트폰 장치 구성을 위한 Cisco Unified Communications Manager SIP 설정. 소프트폰 장치의 SIP 연결 설정은 Jabber IP_Mode 매개 변수 설정과 일치해야 성공적으로 연결할 수 있습니다.
- 기본 네트워크 IP 기능.

Cisco Unified Communications Manager에서 IP 기능은 일반 서버 설정 및 장치별 설정에 의해 결정됩니다. 다음 표에는 다양한 설정에서 예상되는 Jabber 연결이 나열되어 있습니다. 이 목록에서는 IPv4 및 IPv6에 대한 DNS 레코드가 모두 구성되어 있다고 가정합니다.

클라이언트 OS, 서버 OS 및 Jabber IP_Mode 매개 변수가 2개의 스택으로 설정되면 Jabber는 RFC6555에 따라 서버와의 연결에 IPv4 또는 IPv6 주소를 사용합니다.

클라이언트 **OS**	서버 **OS**	**Jabber IP_Mode** 매개 변수	**Jabber** 연결 결과
IPv4 전용	IPv4 전용	IPv4 전용	IPv4 연결
		IPv6 전용	연결 실패
		두 개의 스택	IPv4 연결

클라이언트 **OS**	서버 **OS**	**Jabber IP_Mode** 매개 변수	**Jabber** 연결 결과
IPv4 전용	IPv6 전용	IPv4 전용	연결 실패
		IPv6 전용	연결 실패
		두 개의 스택	연결 실패
IPv6 전용	IPv4 전용	IPv4 전용	연결 실패
		IPv6 전용	연결 실패
		두 개의 스택	연결 실패
IPv6 전용	IPv6 전용	IPv4 전용	연결 실패
		IPv6 전용	IPv6 연결
		두 개의 스택	IPv6 연결
IPv4 전용	두 개의 스택	IPv4 전용	IPv4 연결
		IPv6 전용	연결 실패
		두 개의 스택	IPv4 연결
IPv6 전용	두 개의 스택	IPv4 전용	연결 실패
		IPv6 전용	IPv6 연결
		두 개의 스택	IPv6 연결
두 개의 스택	IPv4 전용	IPv4 전용	IPv4 연결
		IPv6 전용	연결 실패
		두 개의 스택	IPv4 연결
두 개의 스택	IPv6 전용	IPv4 전용	연결 실패
		IPv6 전용	IPv6 연결
		두 개의 스택	IPv6 연결
두 개의 스택	두 개의 스택	IPv4 전용	IPv4 연결
		IPv6 전용	IPv6 연결
		두 개의 스택	IPv6 연결

Jabber를 IPv6 전용 모드로 사용하는 경우, NAT64/DNS64가 Webex Messenger 서비스, Cisco VCS 모바일 및 Remote Access용 ExpresswayCisco Webex 플랫폼 서비스 같은 IPv4 인프라에 연결되어야 합니다.

데스크톱 장치 지원은 IPv6 전용 온프레미스 구축에 사용할 수 있습니다. 모든 Jabber 모바일 장치는 두 개의 스택으로 구성되어야 합니다.

IPv6 구축에 대한 자세한 내용은 IPv6 Deployment Guide for Cisco Collaboration Systems 릴리스 12.0을 참조하십시오.

제한 사항

- HTTPS 연결
  - 온프레미스 구축에서 Cisco Jabber는 IPv4 전용 및 두 개의 스택 모드를 지원하여 Cisco Unified Communications Manager 및 Cisco Unified Communications Manager IM and Presence Service에 연결합니다. 이러한 서버는 현재 IPv6 HTTPS 연결을 지원하지 않습니다.

    Cisco Jabber는 IPv6 전용 모드를 사용하여 음성 메일에 대한 Cisco Unity Connection에 HTTPS를 사용하여 연결할 수 있습니다.

- Webex Messenger 제한
  - Webex Messenger IPv6에서는 지원되지 않습니다.

- 전화 통신 제한
  - Cisco Unified Communications Manager의 사용자 장치를 두 개의 스택 또는 IPv6 전용으로 업그레이드하는 경우 해당 Jabber 클라이언트를 11.6 이상으로 업그레이드해야 합니다.
  - 설치에 IPv4 엔드포인트 및 IPv6 엔드포인트가 포함된 경우 하드웨어 MTP를 사용하여 이러한 장치 간의 오디오 및 비디오를 브리지로 연결하는 것이 좋습니다. 이는 Cisco IOS 버전 15.5를 사용하는 하드웨어 MTP에서 지원됩니다. 예를 들어, Cisco 3945 라우터는 T-train 빌드 c3900e-universalk9-mz.SPA.155-2.T2.bin을 실행해야 합니다.
  - 현재는 Jabber를 포함하여 Cisco 엔드포인트에서 동시에 IPv4 및 IPv6을 지원하기 위한 솔루션 로드맵을 가지고 있지 않습니다. Cisco Unified Communications Manager는 IPv4 전용 및 IPv6 전용의 최신 기능을 지원합니다. IPv4 전용 및 IPv6 전용 엔드포인트 또는 IPv4 전용 또는 IPv6 전용 게이트웨이 간의 통화를 지원하려면 MTP가 필요합니다.
  - Jabber간 통화는 IPv6에서 지원되지 않습니다.

- 파일 전송 제한
  - 고급 파일 전송 - 클라이언트가 두 개의 스택으로 구성되고 Cisco Unified Communications Manager IM and Presence Service에 두 개의 스택이 활성화된 경우, 고급 파일 전송은 다음 Cisco Unified Communications Manager IM and Presence Service 버전에서 지원됩니다.
    - 10.5.2 SU2
    - 11.0.1 SU2

- 11.5

- 사용자간 파일 전송 - IPv4 및 IPv6 클라이언트 사이의 개인 간 파일 전송에 대한 온프레미스 구축의 경우에는 지원되지 않습니다. IPv4 및 IPv6 클라이언트를 모두 사용하는 네트워크 구성이 있는 경우 고급 파일 전송을 구성하는 것이 좋습니다.

- 모바일 및 Remote Access 제한
  - 모바일 및 Remote Access용 Cisco VCS Expressway는 IPv6을 지원하지 않습니다.
  - Cisco Unified Communications Manager가 IPv6 SIP 연결에 대해 구성된 경우 Cisco VCS 모바일 및 Remote Access용 Expressway를 사용하여 전화 통신 서비스를 사용하는 Cisco Unified Communications Manager에 연결할 수 없습니다.

Android에서 IPv6을 지원하기 위한 요구 사항

Android OS 요구 사항

Android 5.0 이상

네트워크 요구 사항

- IPv4 전용 모드(Android는 IPv4 주소만 허용)
- SLAAC가 포함된 듀얼 스택(Android는 IPv4 및 IPv6 주소를 모두 허용)
- NAT64 또는 DNS64(서버에서 IPv4 주소를 사용하고 클라이언트는 IPv6 주소 사용)

제한 사항

- DHCPv6 제한 사항
  - Android 장치에서는 DHCPv6이 지원되지 않습니다.

- Android OS 제한 사항
  - Android OS는 IPv6 전용 네트워크를 지원하지 않습니다. 이 제한 사항에 대한 자세한 내용은 Android 개발자 링크를 참조하십시오.

포트 및 프로토콜

클라이언트는 다음 표에 기재된 포트와 프로토콜을 사용합니다. 클라이언트와 서버 사이에 방화벽을 배치할 계획이라면 이러한 포트와 프로토콜을 허용하도록 방화벽을 구성합니다.

	Port(포트)	애플리케이션 계층 프로토콜	전송 레이어 프로토콜	설명
컨피그레이션				
	6970	HTTP	TCP	클라이언트 설정 파일을 다운로드하려면 TFTP 서버에 연결하십시오.
	6972	HTTPS	TCP	Cisco Unified Communications Manager 릴리스 11.0 이상에 대하여 안전하게 클라이언트 설정 파일을 다운로드하려면 TFTP 서버로 연결하십시오.
	53	DNS	UDP	호스트네임 해상도.
	3804	CAPF	TCP	IP 전화에 Locally Significant Certificates(LSC)를 발행합니다. 이 포트는 Cisco Unified Communications Manager Certificate Authority Proxy Function(인증센터 프록시 기능, CAPF) 등록을 위한 리스닝 포트입니다.
	8443	HTTPS		Cisco Unified Communications Manager와 Cisco Unified Communications Manager IM and Presence Service에 대한 트래픽
	8191	SOAP	TCP	Simple Object Access Protocol(SOAP) 웹 서비스를 제공할 수 있도록 로컬 포트로 연결합니다.
디렉터리 통합—LDAP 연락처 확인을 위해 LDAP 설정을 기준으로 이러한 포트 중 하나를 사용하게 됩니다.				
	389	LDAP	TCP	LDAP TCP (UDP)는 LDAP 디렉터리 서비스로 연결됩니다.
	3268	LDAP	TCP	연락처 검색을 위해 Global Catalog 서버로 연결됩니다.
	636	LDAPS	TCP	LDAPS TCP는 안전하게 LDAP 디렉터리 서비스로 연결됩니다.
	3269	LDAPS	TCP	LDAPS TCP는 Global Catalog 서버로 안전하게 연결됩니다.
인스턴트 메시징 및 프레즌스				

	Port(포트)	애플리케이션 계층 프로토콜	전송 레이어 프로토콜	설명
	443	XMPP	TCP	Webex Messenger 서비스에 대한 XMPP 트래픽. 클라이언트는 클라우드 기반 구축에서만 이 포트를 통해 XMPP를 전송합니다. 포트 443이 차단된 경우 클라이언트는 포트 5222로 대체됩니다.
	5222	XMPP	TCP	인스턴스 메시지와 프레즌스를 위해 Cisco Unified Communications Manager IM and Presence Service로 연결됩니다.
	37200	SOCKS5 바이트 스트림	TCP	P2P 파일 전송, 온프레미스 구축에서 클라이언트는 화면 캡처 전송에도 이 포트를 사용합니다.
	7336	HTTPS	TCP	MFT 파일 전송(온-프레미스에만 해당).
Communication Manager 시그널링				
	2748	CTI	TCP	회사 전화기 제어에 사용되는 CTI(Computer Telephony Interface)
	5060	SIP	TCP	SIP(Session Initiation Protocol) 통화 시그널링을 제공합니다.
	5061	TLS를 통한 SIP	TCP	TCP를 통한 SIP는 안전한 SIP 콜 시그널링을 제공합니다. (장치에 안전한 SIP가 활성화되는 경우에 사용됨)
	3000-3999	FECC	UDP	FECC(Far End Camera Control).
	5070-6070	BFCP	UDP	영상 화면 공유 기능을 위한 Binary Floor Control Protocol(BFCP).
음성 또는 영상 미디어 교환				
	16384-32766	RTP/SRTP	UDP	Cisco Unified Communications Manager 미디어 포트 범위는 오디오, 비디오, 및 BFCP 비디오 데스크톱 공유에 사용됩니다.
	33434-33598	RTP/SRTP	UDP	Cisco Hybrid Services(Jabber간 통화) 미디어 포트 범위는 오디오 및 비디오에 사용됩니다.
	8000	RTP/SRTP	TCP	Jabber 데스크폰 비디오 인터페이스에서 사용됩니다. 이 인터페이스를 사용하면 Jabber 클라이언트를 통해 데스크폰으로 전송되는 비디오를 수신할 수 있습니다.
Unity Connection				

	Port(포트)	애플리케이션 계층 프로토콜	전송 레이어 프로토콜	설명
	7080	HTTP	TCP	음성 메시지 알림을 수신하기 위한 Cisco Unity Connection(신규 메시지, 메시지 업데이트 및 메시지 삭제)에 사용됩니다.
	7443	HTTPS	TCP	음성 메시지 알림을 안전하게 수신하기 위한 Cisco Unity Connection(신규 메시지, 메시지 업데이트 및 메시지 삭제)에 사용됩니다.
	8443	HTTPS	TCP	구성을 위해 Cisco Unity Connection에 연결합니다.
	443	HTTPS	TCP	음성 메일을 위해 Cisco Unity Connection에 연결합니다.
Webex Meetings				
	80	HTTP	TCP	미팅을 위해 Webex Meetings에 연결합니다.
	443	HTTPS	TCP	미팅을 위해 Webex Meetings에 연결합니다.
	8443	HTTPS	TCP	Cisco Unified Communications Manager의 웹 액세스로 다음에 대한 연결을 포함합니다: • 할당된 장치용 Cisco Unified Communications Manager IP 전화기(CCMCIP) 서버. • 연락처 확인을 위한 사용자 데이터 서비스(UDS)
액세서리 관리자				
	8001		TCP	Windows 및 Mac용 Cisco Jabber에서 Sennheiser 플러그인은 통화 제어를 위해 Localhost 트래픽에 이 포트를 사용합니다.

다른 서비스 및 프로토콜용 포트

이 섹션에 나열된 포트 외에 구축 환경의 모든 프로토콜 및 서비스에 필요한 포트를 검토합니다. 다음 문서에서 여러 서버에 대한 포트 및 프로토콜 요구 사항을 확인할 수 있습니다.

- Cisco Unified Communications Manager, Cisco Unified Communications Manager IM and Presence Service에 대해서는 *TCP* 및 *UDP* 포트 사용 설명서를 참조하십시오.
- Cisco Unity Connection의 경우 시스템 관리 설명서를 참조하십시오.
- Webex Meetings 서버의 경우 관리 설명서를 참조하십시오.
- Cisco Meeting Server의 경우 *Cisco Meeting Server* 릴리스 *2.6* 및 *2.7:* 단일 결합 *Meeting Server* 구축을 참조하십시오.
- Webex 서비스의 경우 관리 설명서를 참조하십시오.

- 모바일 및 Remote Access용 Expressway의 경우 방화벽 트리 순회를 위한 *Cisco Expressway IP* 포트 사용을 참조하십시오.
- 파일 전송 포트 사용에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스 구성 및 관리를 참조하십시오.

지원되는 코덱

유형	코덱	코덱 유형	Android용 Cisco Jabber	iPhone 및 iPad용 Cisco Jabber	Mac용 Cisco Jabber	Windows용 Cisco Jabber
오디오	G.711	A-law	예 표준 모드를 지원합니다.		예	예
		µ-law/Mu-law	예 표준 모드를 지원합니다.		예	예
	G.722		예		예	예
	G.722.1	24kb/s 및 32kb/s	예 표준 모드를 지원합니다.		예	예
	G.729		G.729를 사용하는 시각적 음성 메일은 지원하지 않습니다. 그러나 G.729 및 통화 음성 메일 기능을 사용하여 음성 메시지에 액세스할 수 있습니다.		아니요	아니요
	G.729a		예 낮은 대역폭 가용성에 대한 최소 요구 사항. 낮은 대역폭 모드를 지원하는 코덱에만 해당됩니다. 표준 모드를 지원합니다.		예	예
	Opus		예		예	예
영상	H.264/AVC	기준선 프로파일	예		예	예
		높은 프로파일	아니요		예	예

유형	코덱	코덱 유형	Android용 Cisco Jabber	iPhone 및 iPad용 Cisco Jabber	Mac용 Cisco Jabber	Windows용 Cisco Jabber
음성 메일	G.711	A-law	예		예	예
		μ-law / Mu-law(기본값)	예		예	예
	PCM linear		예		예	예

Android용 Cisco Jabber 또는 iPhone 및 iPad용 Cisco Jabber 사용 시 음성 품질에 문제가 있는 경우, 사용자는 클라이언트 설정에서 낮은 대역폭 모드를 켜거나 끌 수 있습니다.

가상 환경 요구 사항

소프트웨어 요구 사항

가상 환경에서 Windows용 Cisco Jabber을 구축하려면 지원되는 다음 소프트웨어 버전 중에서 선택합니다.

소프트웨어	지원되는 버전
Citrix XenDesktop	7.9, 7.8, 7.6, 7.5, 7.1
Citrix XenApp	7.9 게시된 앱 및 데스크톱 7.8 게시된 앱 및 데스크톱 7.6 게시된 앱 및 데스크톱 7.5 게시된 데스크톱 6.5 게시된 데스크톱
VMware Horizon View	6.x ~ 8.x

소프트폰 요구 사항

소프트폰 통화의 경우 VDI용 Cisco Jabber Softphone을 사용하십시오. 자세한 내용은 **VDI용 Cisco Jabber Softphone** 릴리스 **12.9** 릴리스 노트를 참조하십시오.

오디오 및 비디오 성능 참조

주의 다음 데이터는 랩 환경에서의 테스트에 기반을 둔 것입니다. 이 데이터는 대역폭 사용량 측면에서 예상할 수 있는 요소에 대한 아이디어를 제공하기 위한 것입니다. 이 항목의 내용은 완전하거나 모든 내용을 반영하기 위한 것이 아닙니다. 대역폭 사용량에 영향을 줄 수 있는 미디어 시나리오

미디어 보장

모든 네트워크 유형에서 실시간 미디어의 품질을 보장하여 미흡한 미디어 품질로 인해 회의가 중단되지 않도록 합니다. Media Assure는 패킷 손실을 25%까지 줄일 수 있습니다.

Media Assure는 Cisco Unified Communications Manager 릴리스 10.x 이상의 비디오, Cisco Unified Communications Manager 릴리스 11.5 이상의 오디오 및 비디오에서 지원됩니다.

Expressway for Mobile 및 Remote Access 구축의 경우 Media Assure는 Cisco Expressway Release 8.8.1 이상이 필요합니다.

사소하거나 심각한 네트워크 조건의 경우 Jabber에서 다음과 같이 처리할 수 있습니다.

- 스트림의 대역폭을 일시적으로 제한합니다.
- 비디오를 다시 동기화합니다.
- 불필요한 혼잡 기반 버스트 손실을 방지하기 위해 패킷 속도를 조절합니다.
- 첫 번째 미디어 패킷에서 고급 SDP 신호 처리를 사용하여 복원력 메커니즘을 제공합니다.
- 패킷 손실을 보호합니다.
- 미디어의 생산 초과로 인한 혼잡 기반 손실을 방지합니다.
- 낮은 프레임 속도/낮은 비트 전송률 스트림의 보호를 개선합니다.
- 인증 및 암호화된 FEC를 지원합니다.

Fast Lane 지원

Fast Lane 지원 기능을 사용하면 트래픽이 많을 때에도 네트워크에서 비즈니스 크리티컬 애플리케이션을 우선 처리합니다. Jabber는 음성 및 비디오 트래픽에 대해 Fast Lane을 지원합니다. iOS 10의 경우 액세스 포인트(AP) Fast Lane 기능을 사용하면 Cisco Unified Communications Manager에 구성된 DSCP 값을 더 이상 사용하지 않습니다. Fast Lane 기능을 지원 하지 않는 iOS 11의 경우, Jabber는 Cisco Unified Communications Manager에 구성된 DSCP 값을 계속 사용합니다.

Cisco Unified Communications Manager의 DSCP 구성과 관계 없이, 무선 AP가 Fast Lane 기능을 지원하는 경우 Jabber는 자동으로 다음과 같은 DSCP 및 사용자 우선 순위(UP) 값을 설정합니다.

- 오디오 통화 또는 영상 통화의 오디오 부분에 대해서는 DSCP가 0x2e로 설정되고 UP이 6으로 설정됩니다.
- 영상 통화의 비디오 부분에 대해서는 DSCP가 0x22로 설정되고 UP은 5로 설정됩니다.
- AP가 Fast Lane을 지원하지 않거나 사용하지 않는 경우 DSCP 값은 자동으로 Cisco Unified Communications Manager에 의해 지정된 값으로 설정됩니다.

필수 조건:

- AireOS 8.3 이상을 실행하는 WLC
- AP1600/2600 시리즈 액세스 포인트, AP1700/2700 시리즈 액세스 포인트, AP3500 시리즈 액세스 포인트, AP3600 시리즈 액세스 포인트 + 11ac 모듈, WSM, Hyperlocation 모듈, 3602P, AP3700 시리즈 액세스 포인트 + WSM, 3702P, OEAP600 시리즈 OfficeExtend 액세스 포인트, AP700 시리즈 액세스 포인트, AP700W 시리즈 액세스 포인트, AP1530 시리즈 액세스 포인트, AP1550 시리즈 액세스 포인트, AP1570 시리즈 액세스 포인트 및 AP1040/1140/1260 시리즈 액세스 포인트
- iOS 11 이상을 실행 중인 iOS 장치.

Cisco Jabber 데스크톱 클라이언트를 위한 오디오 비트 전송률

다음 오디오 비트 전송률은 Windows용 Cisco Jabber 및 Mac용 Cisco Jabber에 적용됩니다.

코덱	**RTP(kbits/**초**)**	실제 비트 전송률**(kbits/**초**)**	참고
G.722.1	24/32	54/62	고품질 압축
G.711	64	80	표준 비압축
G.729a	8	38	저품질 압축

Cisco Jabber 모바일 클라이언트를 위한 오디오 비트 전송률

다음 오디오 비트 전송률을 iPhone 및 iPad용 Cisco Jabber와 Android용 Cisco Jabber에 적용합니다.

코덱	코덱 비트 전송률**(kbits/**초**)**	사용되는 네트워크 대역폭**(kbits/**초**)**
g.711	64	80
g.722.1	32	48
g.722.1	24	40
g.729a	8	24

Cisco Jabber 데스크톱 클라이언트를 위한 비디오 비트 전송률

다음 비디오 비트 전송률(g.711 오디오 포함)는 Windows용 Cisco Jabber 및 Mac용 Cisco Jabber에 적용됩니다. 이 표에서는 가능한 모든 해상도를 나열하지는 않습니다.

해결책	픽셀	**g.711** 오디오 사용 시 측정된 비트 전송률**(**초당 **kbits)**
w144p	256 x 144	156
w288p 이는 Cisco Jabber용 비디오 렌더링 창의 기본 크기입니다.	512 x 288	320
w448p	768 x 448	570
w576p	1024 x 576	890
720p	1280 x 720	1300
1080p	1920 x 1080	2500-4000

참고 측정된 비트 전송률은 사용되는 실제 대역폭(RTP 페이로드 + IP 패킷 오버헤드)입니다.

Android용 Cisco Jabber를 위한 비디오 비트 전송률

영상	해결책	대역폭
HD	1280 x 720	1024
VGA	640 x 360	512
CIF	488x211	310

참고 통화 중에 HD 비디오를 전송 및 수신하려면:

- Cisco Unified Communications Manager에서 1024 kbps 보다 큰 영상 통화에 대한 최대 비트 전송률을 구성합니다.
- 라우터의 DSCP를 활성화하여 우선 순위가 높은 비디오 RTP 패키지를 전송합니다.

iPhone 및 iPad용 Cisco Jabber를 위한 비디오 비트 전송률

클라이언트가 20 fps로 캡처 및 전송됩니다.

해결책	픽셀	**g.711** 오디오 사용 시 비트 전송률**(kbits/**초**)**
w144p	256 x 144	290
w288p	512 x 288	340
w360p	640 x 360	415
w720p	1280 x 720	1024

프레젠테이션 비디오 비트 전송률

Cisco Jabber는 8fps로 캡처되고 2 ~ 8fps로 전송됩니다.

이 테이블의 값은 오디오를 포함하지 않습니다.

픽셀	**2fps**에서 예상 회선 비트 전송률**(**초당 **kbits)**	**8fps**에서 예상 회선 비트 전송률**(**초당 **kbits)**
720 x 480	41	164
704 x 576	47	188
1024 x 768	80	320
1280 x 720	91	364
1280 x 800	100	400
1920 x 1080	150-300	500-1000

릴리스 12.5에서는 총 비디오 대역폭이 300kb 미만인 경우 기본 비디오 품질을 개선하도록 비트 전송률 할당을 변경했습니다. 그러나 이 변경 사항으로 기본 비디오의 최대 비트 전송률은 450 킬로비트/초로 설정됩니다.

전체 비디오 대역폭을 높이면 기본 비디오에서 이전 릴리스와 비교할 때 해상도가 낮게 표시될 수 있습니다.

최대 협상된 비트 전송률

지역 구성 창에서 Cisco Unified Communications Manager의 최대 페이로드 비트 전송률을 지정합니다. 이 최대 페이로드 비트 전송률에는 패킷 오버헤드가 포함되지 않으므로 사용된 실제 비트 전송률은 사용자가 지정하는 최대 페이로드 비트 전송률보다 높습니다.

다음 표에서는 Cisco Jabber가 최대 페이로드 비트 전송률을 할당하는 방식에 대해 설명합니다.

데스크톱 공유 세션	오디오	대화형 비디오(기본 비디오)	프레젠테이션 비디오 (데스크톱 공유 비디오)
아니요	Cisco Jabber는 최대 오디오 비트 전송률을 사용합니다.	Cisco Jabber는 다음과 같이 나머지 비트 전송률을 할당합니다. 최대 비디오 통화 비트 전송률에서 오디오 비트 전송률을 뺀 값입니다.	—
예	Cisco Jabber는 최대 오디오 비트 전송률을 사용합니다.	Cisco Jabber는 오디오 비트 전송률을 빼고 나머지 대역폭의 절반을 할당합니다.	Cisco Jabber는 오디오 비트 전송률을 빼고 나머지 대역폭의 절반을 할당합니다.

오디오	대화형 비디오(기본 비디오)
Cisco Jabber는 최대 오디오 비트 전송률을 사용합니다.	Cisco Jabber는 다음과 같이 나머지 비트 전송률을 할당합니다. 최대 비디오 통화 비트 전송률에서 오디오 비트 전송률을 뺀 값입니다.

대역폭

Cisco Unified Communications Manager의 지역 구성에서 클라이언트에 사용할 수 있는 대역폭을 제한할 수 있습니다.

지역을 사용하면 음성 및 영상 통화에 대한 전송 독립적 최대 비트 레이트를 지정하여 지역 내와 기존 지역 간의 음성 및 영상 통화에 사용되는 대역폭을 제한할 수 있습니다. 지역 구성에 대한 자세한 내용은 해당 릴리스용 Cisco Unified Communications Manager 문서를 참조하십시오.

Cisco Jabber 데스크톱 클라이언트에 대한 대역폭 성능 예상

Mac용 Cisco Jabber는 오디오에 대한 비트 전송률을 분리한 후 나머지 대역폭을 대화형 비디오와 프레젠테이션 비디오 간에 동일하게 나눕니다. 다음 표에서는 대역폭 당 달성할 수 있어야 하는 성능을 이해하는 데 도움이 되는 정보를 제공합니다.

업로드 속도	오디오	오디오 + 대화형 비디오 (기본 비디오)
VPN의 125kbps	g.711을 위한 대역폭 임계값. g.729a 및 g.722.1의 경우 충분한 대역폭.	비디오의 경우 대역폭 부족.
VPN의 384kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w288p(512 x 288)

업로드 속도	오디오	오디오 + 대화형 비디오 (기본 비디오)
엔터프라이즈 네트워크의 384kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w288p(512 x 288)
1000kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w576p(1024 x 576)
2000kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w720p30(1280 x 720)

Windows용 Cisco Jabber는 오디오에 대한 비트 전송률을 분리한 후 나머지 대역폭을 대화형 비디오와 프레젠테이션 비디오 간에 동일하게 나눕니다. 다음 표에서는 대역폭 당 달성할 수 있어야 하는 성능을 이해하는 데 도움이 되는 정보를 제공합니다.

업로드 속도	오디오	오디오 + 대화형 비디오 (기본 비디오)	오디오 + 프레젠테이션 비디오(데스크톱 공유 비디오)	오디오 + 대화형 비디오 + 프레젠테이션 비디오
VPN의 125kbps	g.711을 위한 대역폭 임계값. g.729a 및 g.722.1의 경우 충분한 대역폭 .	비디오의 경우 대역폭 부족.	비디오의 경우 대역폭 부족.	비디오의 경우 대역폭 부족.
VPN의 384kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w288p(512 x 288)	2+ fps에서 1280 x 800	30fps에서 w144p (256 x 144) + 2+ fps에서 1280 x 720
엔터프라이즈 네트워크의 384kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w288p(512 x 288)	2+ fps에서 1280 x 800	30fps에서 w144p (256 x 144) + 2+ fps에서 1280 x 800
1000kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w576p(1024 x 576)	8fps에서 1280 x 800	30 fps에서 w288p(512 x 288) + 8 fps에서 1280 x 800
2000kbps	모든 오디오 코덱의 경우 충분한 대역폭	30fps에서 w720p30(1280 x 720)	8fps에서 1280 x 800	30fps에서 w288p(1024 x 576) + 8fps에서 1280 x 800

VPN이 페이로드의 크기를 증가시키며 대역폭 소비가 증가합니다.

Android용 Cisco Jabber에 대한 대역폭 성능 예상

VPN이 페이로드의 크기를 증가시키며 대역폭 소비가 증가합니다.

업로드 속도	오디오	오디오 + 대화형 비디오(기본 비디오)
VPN의 125kbps	g.711을 위한 대역폭 임계값. 비디오의 경우 대역폭 부족. g.729a 및 g.722.1의 경우 충분한 대역폭.	비디오의 경우 대역폭 부족.
256kbps	모든 오디오 코덱의 경우 충분한 대역폭	전송 속도(Tx) — 256 x 144(15fps) 수신 속도(Rx) — 256 x 144(30fps)
VPN의 384kbps	모든 오디오 코덱의 경우 충분한 대역폭	Tx — 15 fps에서 640 x 360 Rx — 30fps에서 640 x 360
엔터프라이즈 네트워크의 384kbps	모든 오디오 코덱의 경우 충분한 대역폭	Tx — 15 fps에서 640 x 360 Rx — 30fps에서 640 x 360

참고 장치 제한 사항으로 인해, Samsung Galaxy SII 및 Samsung Galaxy SIII 장치는 이 표에 나열된 최대 해상도를 달성할 수 없습니다.

iPhone 및 iPad용 Cisco Jabber에 대한 대역폭 성능 예상

클라이언트는 오디오에 대한 비트 전송률을 분리한 후 나머지 대역폭을 대화형 비디오와 프레젠테이션 비디오 간에 동일하게 나눕니다. 다음 표에서는 대역폭 당 달성할 수 있어야 하는 성능을 이해하는 데 도움이 되는 정보를 제공합니다.

VPN이 페이로드의 크기를 증가시키며 대역폭 소비가 증가합니다.

업로드 속도	오디오	오디오 + 대화형 비디오(기본 비디오)
VPN의 125kbps	g.711을 위한 대역폭 임계값. 비디오의 경우 대역폭 부족. g.729a 및 g.722.1의 경우 충분한 대역폭.	비디오의 경우 대역폭 부족.
290kbps	모든 오디오 코덱의 경우 충분한 대역폭	20fps에서 256 x144
415kbps	모든 오디오 코덱의 경우 충분한 대역폭	25fps에서 640 x 360
1024kbps	모든 오디오 코덱의 경우 충분한 대역폭	20fps에서 1280 x 720

비디오 속도 적응

Cisco Jabber는 비디오 속도 적응을 사용하여 최적의 비디오 품질을 결정합니다. 비디오 속도 적응은 비디오 비트 전송률 처리량을 동적으로 증가 또는 감소하여 사용 가능한 IP 경로 대역폭에 대한 실시간 변형을 처리 합니다.

Cisco Jabber 사용자는 짧은 시간 동안 비디오 통화가 더 낮은 해상도에서 시작하고 더 높은 해상도로 확장될 것을 기대해야 합니다. Cisco Jabber는 기록도 저장하므로 후속 영상 통화가 최적의 해상도에서 시작되도록 합니다.

대역폭에 미치는 H/264 프로파일 영향

이전 릴리스에서는 H.264 기본 프로필만 지원했습니다. 릴리스 12.8에서는 데스크톱 클라이언트용으로 H.264 높음 프로파일에 대한 지원을 추가했습니다. VDI 또는 모바일 클라이언트에는 높음 프로파일을 사용할 수 없습니다.

높음 프로파일은 최대 10% 이하의 대역폭을 사용하여 동일한 비디오 품질을 제공할 수 있습니다. 또는, 동일한 대역폭을 사용하여 더 나은 비디오 품질을 실현할 수 있습니다.

Jabber는 기본적으로 H.264 기본 프로파일을 사용합니다. 높음 프로파일을 활성화하려면 H264HighProfileEnable 매개 변수를 사용합니다.

통화 관리 기록

통화가 종료되면 Jabber는 Cisco Unified Communications Manager에게 통화 품질 및 성능 정보를 보냅니다. Cisco Unified Communications Manager는 이러한 메트릭을 사용하여 Cisco Unified Communications Manager CMR(통화 관리 레코드)을 채웁니다. Cisco Jabber는 오디오 및 영상 통화에 대해 다음 정보를 보냅니다.

- 보내고 받은 패킷 수.
- 보내고 받은 옥텟 수.
- 손실된 패킷 수입니다.
- 평균 지터.

또한 클라이언트는 다음과 같은 비디오 관련 정보를 보냅니다.

- 주고 받은 코덱.
- 주고 받은 해상도.
- 주고 받은 프레임 속도.
- 평균 왕복 시간(RTT)

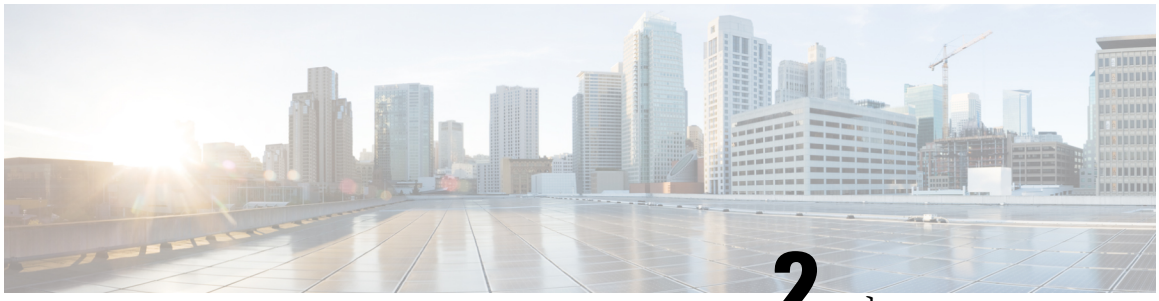
클라이언트는 다음과 같은 오디오 관련 정보를 보냅니다.

- 숨김(초).

- 엄격한 숨김(초).

메트릭은 Cisco Unified Communications Manager CMR 레코드 출력에 일반 텍스트 형식으로 표시됩니다. 이 데이터는 원격 측정 또는 분석 애플리케이션에서 직접 읽거나 소비할 수 있습니다.

Cisco Unified Communications Manager CMR 레코드 구성에 대한 자세한 내용은 Cisco Unified Communications Manager 릴리스의 통화 세부 정보 레코드 관리 설명서에서 통화 관리 레코드 장을 참조하십시오.



2 장

배포 시나리오

온프레미스 구축

온프레미스 구축은 회사 네트워크에서 모든 서비스를 설정, 관리 및 유지 관리하는 것입니다.

다음 모드에서 Cisco Jabber를 구축할 수 있습니다.

- 전체 **UC** - 전체 UC 모드를 구축하려면 인스턴트 메시징 및 프레즌스 상태 기능을 활성화하고, 음성 메일 및 전화회의 기능을 프로비저닝하고, 오디오 및 비디오용 장치와 사용자를 프로비저닝합니다.
- **IM** 전용 - IM 전용 모드를 구축하려면 인스턴트 메시징 및 프레즌스 상태 기능을 활성화합니다. 장치를 사용하여 사용자를 프로비저닝하지 마십시오.
- 전화기 전용 모드 - 전화기 전용 모드에서 사용자의 기본 인증은 Cisco Unified Communications Manager입니다. 전화기 전용 모드를 구축하려면 사용자에게 오디오 및 비디오 기능이 있는 장치를 프로비저닝합니다. 음성 메일 등의 추가 서비스를 사용하여 사용자를 프로비저닝할 수도 있습니다.

기본 제품 모드는 사용자의 기본 인증이 IM and Presence 서버가 되도록 하는 것입니다.

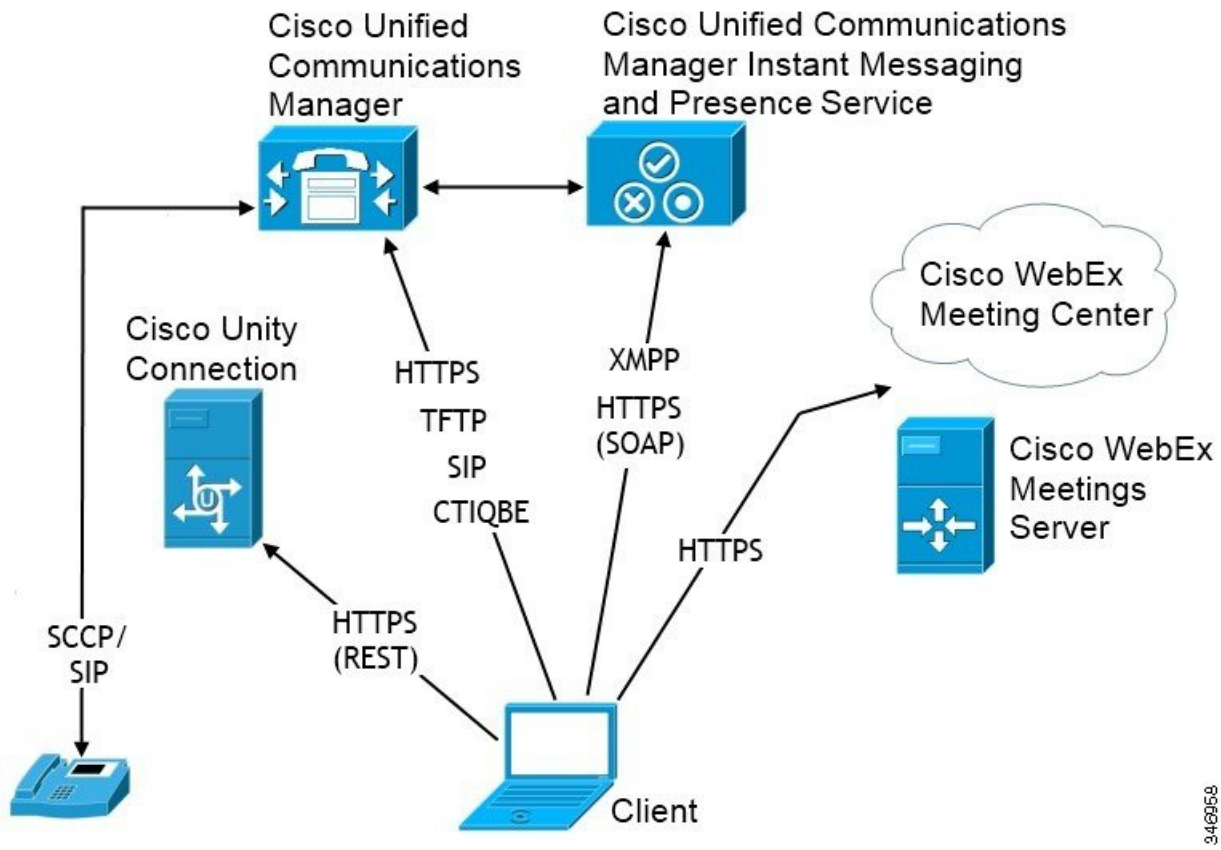
Cisco Unified Communications Manager IM and Presence Service를 사용한 온프레미스 구축

다음 서비스는 Cisco Unified Communications Manager IM and Presence Service와 함께 온프레미스 구축에서 사용할 수 있습니다.

- 프레즌스 - 가용성을 게시하고 Cisco Unified Communications Manager IM and Presence Service를 통해 다른 사용자의 가용성을 구독합니다.
- **IM** - Cisco Unified Communications Manager IM and Presence Service를 통해 IM을 보내고 받습니다.
- 파일 전송 - Cisco Unified Communications Manager IM and Presence Service를 통해 파일 및 스크린샷을 보내고 받습니다.
- 음성 통화 - Cisco Unified Communications Manager를 통해 사무실 전화기 또는 컴퓨터에서 오디오 전용 통화를 합니다.
- 비디오 - Cisco Unified Communications Manager를 통해 영상 통화를 합니다.
- 음성 메일 - Cisco Unity Connection를 통해 음성 메시지를 전송 및 수신합니다.
- 전화회의 - 다음 중 하나와 통합합니다.
  - Webex Meetings 센터 - 호스팅된 미팅 기능을 제공합니다.
  - Webex Meetings 서버 - 온프레미스 미팅 기능을 제공합니다.

다음 그림은 Cisco Unified Communications Manager IM and Presence Service를 사용한 온프레미스 구축의 아키텍처를 보여줍니다.

그림 *1:* 온프레미스 구축 ***Cisco Unified Communications Manager IM and Presence Service***



Computer Telephony Integration의 약어입니다.

Mac용 Windows용 Cisco Jabber 및 Mac용 Cisco Jabber는 타사 애플리케이션에서 Cisco Jabber의 CTI를 지원합니다.

CTI(컴퓨터 전화 통신 통합)를 사용하여 전화 통화를 걸고 받고 관리하는 중에 컴퓨터 처리 기능을 사용할 수 있습니다. CTI 애플리케이션을 사용하면 발신자 ID가 제공하는 정보를 기준으로 데이터베이스에서 고객 정보를 검색하고 IVR(대화형 음성 응답) 시스템이 캡처하는 정보를 사용할 수 있습니다.

CTI에 대한 자세한 내용은 *Cisco Unified Communications Manager* 시스템 설명서의 해당 릴리스의 CTI 섹션을 참조하십시오. 또는 Cisco 개발자 네트워크에서 Cisco Unified Communications Manager API를 통해 CTI 제어를 위한 애플리케이션을 만드는 방법에 대한 정보를 볼 수 있습니다.

- Cisco TAPI: https://developer.cisco.com/site/jtapi/overview/
- Cisco JTAPI: https://developer.cisco.com/site/jtapi/overview/

전화기 모드에서 온프레미스 구축

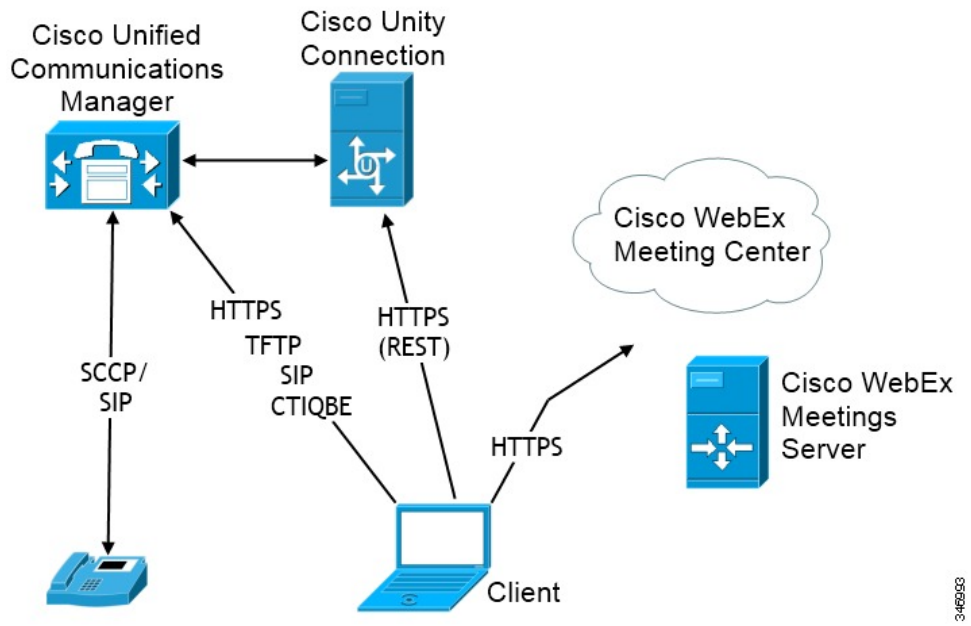
다음 서비스는 전화기 모드 구축에서 사용할 수 있습니다.

- 연락처 - 이는 모바일 클라이언트에만 해당됩니다. Cisco Jabber는 전화기의 연락처 주소록에서 연락처 정보를 업데이트합니다.
- 음성 통화 - Cisco Unified Communications Manager를 통해 사무실 전화기 또는 컴퓨터에서 오디오 전용 통화를 합니다.
- 비디오 - Cisco Unity Connection를 통해 영상 통화를 합니다.
- 음성 메일 - Cisco Unity Connection를 통해 음성 메시지를 전송 및 수신합니다.
- 전화회의 - 다음 중 하나와 통합합니다.
  - **Webex Meetings**센터 - 호스팅된 미팅 기능을 제공합니다.
  - **Webex Meetings**서버 - 온프레미스 미팅 기능을 제공합니다.

참고 Android용 Cisco Jabber 및 iPhone 및 iPad용 Cisco Jabber에서는 전화기 모드에서 전화회의를 지원하지 않습니다.

다음 그림은 전화기 모드에서 온프레미스 구축의 아키텍처를 보여줍니다.

그림 *2:* 전화기 모드에서 온프레미스 구축



소프트폰

소프트폰 모드는 TFTP 서버에서 구성 파일을 다운로드하고 SIP 등록 엔드포인트로 작동합니다. 클라이언트는 CCMCIP 또는 UDS 서비스를 사용하여 Cisco Unified Communications Manager에 등록할 장치 이름을 가져옵니다.

유선 전화

데스크폰 모드는 IP 전화기를 제어하기 위해 Cisco Unified Communications Manager를 사용하여 CTI 연결을 생성합니다. 클라이언트는 CCMCIP를 사용하여 사용자와 연결된 장치에 대한 정보를 수집하고 클라이언트가 제어하는 데 사용할 수 있는 IP 전화기 목록을 생성합니다.

데스크폰 모드의 Mac용 Cisco Jabber는 데스크폰 비디오를 지원하지 않습니다.

확장 및 연결

Cisco Unified Communications Manager 확장 및 연결 기능을 사용하면 PSTN(Public Switched Telephone Network) 전화기 및 PBX(Private Branch Exchange) 장치 같은 장치에서 통화를 제어할 수 있습니다. 자세한 내용은 Cisco Unified Communications Manager 릴리스를 위한 확장 및 연결 기능을 참조하십시오.

Cisco Unified Communications Manager 9.1(1) 이상과 함께 확장 및 연결 기능을 사용하는 것이 좋습니다.

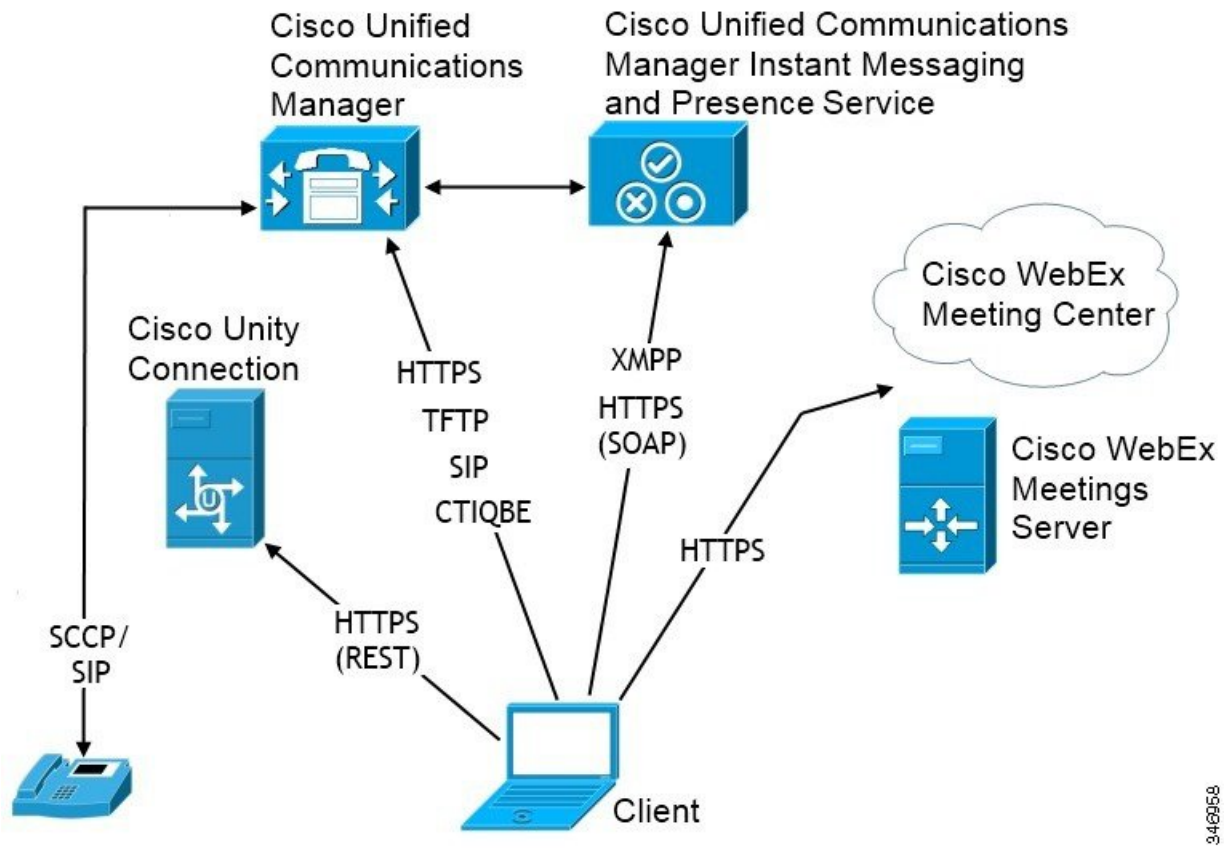
연락처 포함 전화기 모드 구축

다음 서비스는 연락처 포함 전화기 모드 구축에서 사용할 수 있습니다.

- 연락처 - Cisco Unified Communications Manager IM and Presence Service를 통한 연락처 정보
- 프레즌스 - 가용성을 게시하고 Cisco Unified Communications Manager IM and Presence Service를 통해 다른 사용자의 가용성을 구독합니다.
- 음성 통화 - Cisco Unified Communications Manager를 통해 사무실 전화기 또는 컴퓨터에서 오디오 전용 통화를 합니다.
- 비디오 - Cisco Unified Communications Manager를 통해 영상 통화를 합니다.
- 음성 메일 - Cisco Unity Connection를 통해 음성 메시지를 전송 및 수신합니다.
- 전화회의 - 다음 중 하나와 통합합니다.
    - Webex Meetings 센터 - 호스팅된 미팅 기능을 제공합니다.
    - Webex Meetings 서버 - 온프레미스 미팅 기능을 제공합니다.

다음 그림은 Cisco Unified Communications Manager IM and Presence Service를 사용한 온프레미스 구축의 아키텍처를 보여줍니다.

그림 *3:* 연락처 포함 전화기 모드 구축



클라우드 기반 구축

클라우드 기반 구축은 Webex를 사용하여 서비스를 호스트합니다.

Cisco Webex Messenger를 사용한 클라우드 및 하이브리드 구축 모델의 경우, Webex 관리 도구를 사용하여 클라우드 기반 구축을 관리하고 모니터링합니다. 사용자에 대한 서비스 프로파일을 설정할 필요는 없습니다.

Cisco Webex 플랫폼 서비스를 사용한 클라우드 및 하이브리드 구축의 경우 Cisco 제어 허브를 사용하여 구축을 관리하고 모니터링합니다.

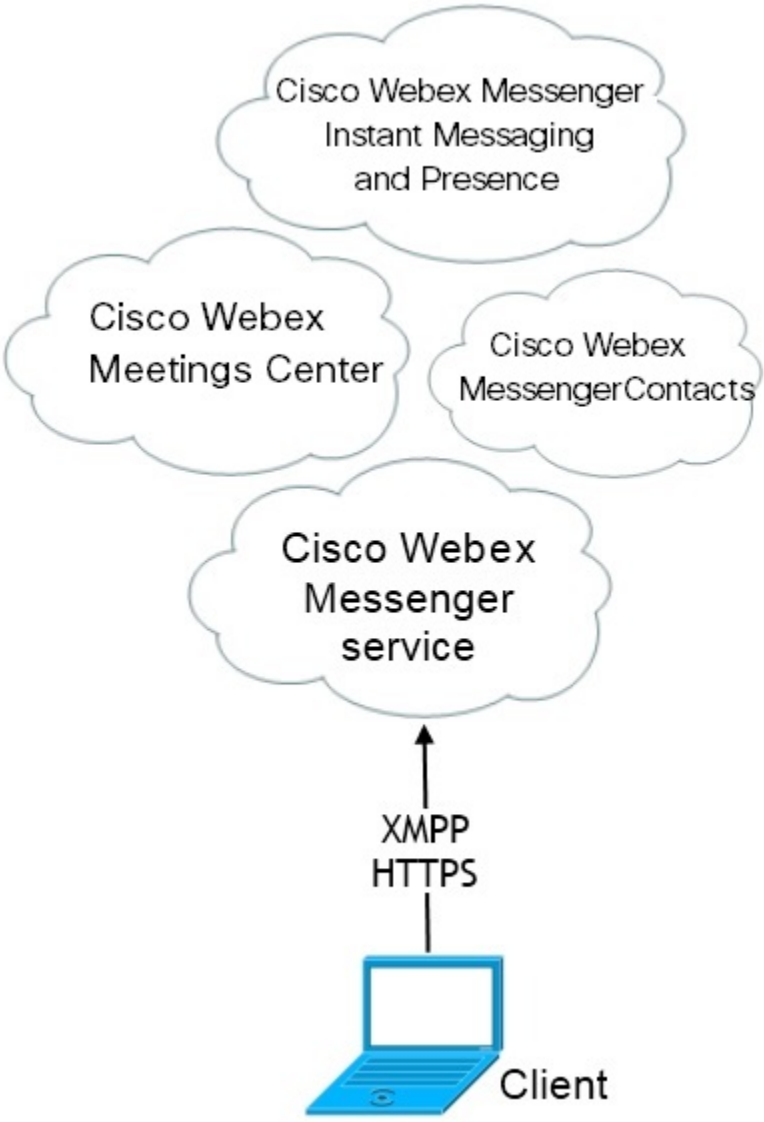
Cisco Webex Messenger를 통한 클라우드 기반 구축

다음 서비스는 Webex Messenger를 사용하는 클라우드 기반 구축에서 사용할 수 있습니다.

- 연락처 소스—Webex Messenger 연락처 확인을 제공합니다.
- 프레즌스 —Webex Messenger에서 사용자가 가용성을 표시하고 다른 사용자의 가용성을 볼 수 있습니다.

- 인스턴트 메시징—Webex Messenger에서 사용자가 인스턴트 메시지를 보내고 받을 수 있습니다.
- 전화회의 — Webex Meetings 센터는 호스팅된 미팅 기능을 제공합니다.

다음 그림은 클라우드 기반 구축의 아키텍처를 보여줍니다.



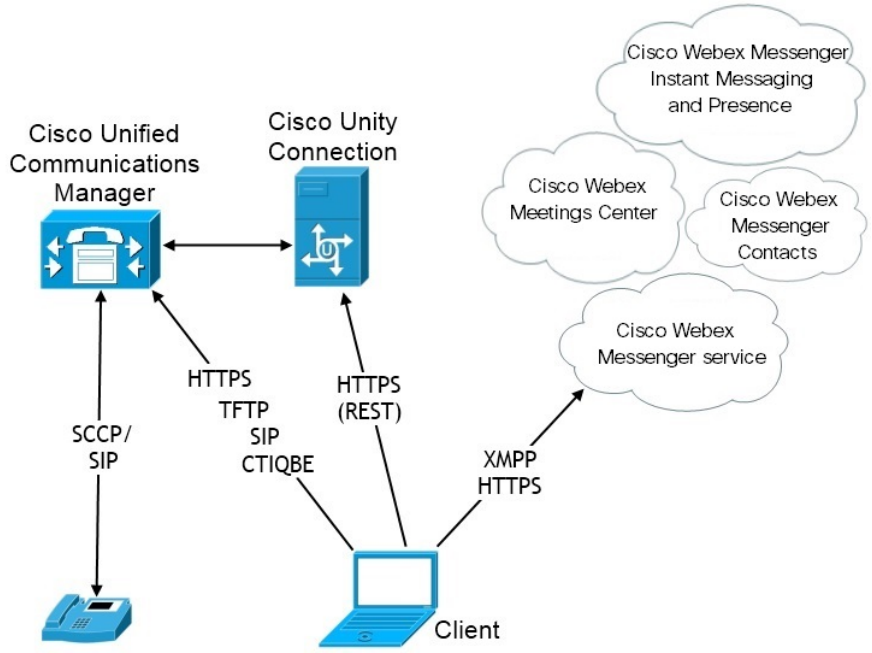
Cisco Webex Messenger 서비스를 통한 하이브리드 클라우드 기반 구축

다음 서비스는 Webex Messenger 서비스를 사용하는 하이브리드 클라우드 기반 구축에서 사용할 수 있습니다.

- 연락처 소스 - Webex Messenger 서비스는 연락처 확인을 제공합니다.

- 프레즌스 - Webex Messenger 서비스를 통해 사용자가 가용성을 게시하고 다른 사용자의 가용성을 구독할 수 있습니다.
- 인스턴트 메시징 - Webex Messenger 서비스를 통해 사용자가 인스턴트 메시지를 보내고 받을 수 있습니다.
- 오디오 - Cisco Unified Communications Manager를 통해 사무실 전화기 또는 컴퓨터에서 오디오 전용 통화를 합니다.
- 비디오 - Cisco Unified Communications Manager를 통해 영상 통화를 합니다.
- 전화회의 — Webex Meetings 센터는 호스팅된 미팅 기능을 제공합니다.
- 음성 메일 - Cisco Unity Connection를 통해 음성 메시지를 전송 및 수신합니다.

다음 그림은 하이브리드 클라우드 기반 구축의 아키텍처를 보여줍니다.



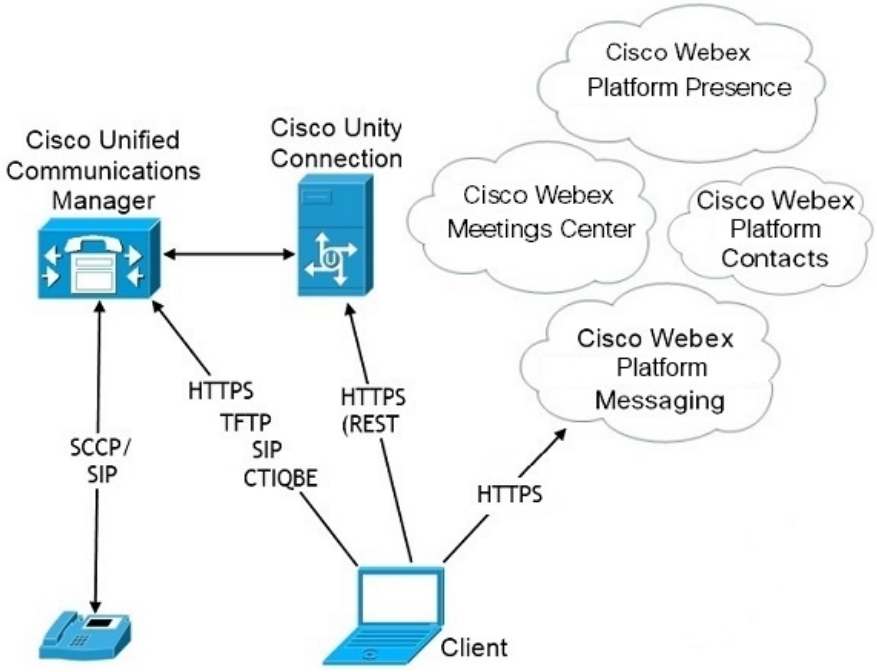
하이브리드 클라우드 기반 구축 **Cisco Webex** 플랫폼 서비스

다음 Jabber 팀 메시징 모드 서비스는 Cisco Webex 플랫폼 서비스을 포함하는 Jabber 하이브리드 클라우드 기반 구축에서 사용할 수 있습니다.

- 연락처 소스 - Cisco Webex 플랫폼 서비스이 연락처를 제공합니다.
- 프레즌스 - Cisco Webex 플랫폼 서비스을 사용하면 사용자의 사용 가능성을 게시하고 다른 사용자의 사용 가능성을 볼 수 있습니다.
- 메시징 - Cisco Webex 플랫폼 서비스을 사용하면 메시지를 보내고 받을 수 있습니다.

- 오디오 - Cisco UC Manager를 사용하여 사무실 전화기 장치 또는 컴퓨터를 통해 음성 전화를 걸 수 있습니다.
- 비디오 - Cisco UC Manager를 사용하여 영상 통화를 할 수 있습니다.
- 전화 회의 - Webex Meetings Center는 호스팅된 미팅 기능을 제공합니다.
- 음성 메일 - Cisco Unity Connection를 통해 음성 메시지를 주고 받습니다.

다음 그림은 Cisco Webex 플랫폼 서비스에서 Jabber 하이브리드 클라우드 기반 구축의 아키텍처를 보여줍니다.



Jabber 팀 메시징 모드의 연락처

로그인 흐름

Webex Control Hub에서 팀 메시징 모드를 활성화하는 동안 사용자의 연락처를 마이그레이션해야 합니다.

이 로그인 흐름은 사용자의 연락처를 마이그레이션하는 과정을 요약합니다. 이 흐름은 현재 Jabber 구축에 로그인하는 사용자로 시작합니다. Jabber 팀 메시징 모드를 활성화한 다음 해당 연락처를 마이그레이션합니다.

1. 사용자는 현재 Jabber 구축에 로그인되어 있으며, 이 구축은 Cisco UC Manager IM&P 또는 Cisco Webex Messenger에 연결됩니다.
2. 관리자는 Webex Control Hub의 구성을 변경하여 Jabber 팀 메시징 모드, 선택적으로 연락처 마이그레이션 및 Jabber call을 활성화합니다.

3. 다음 날에 사용자는 최신 Jabber 구축에 로그인합니다. 5분 내에 Jabber는 서비스 검색 프로세스를 수행하여 해당 사용자에 대한 Cisco Webex 플랫폼 서비스 구축이 있음을 감지합니다.
4. Jabber는 사용자에게 메시지를 사용하여 Jabber에서 로그아웃하도록 지시하고 "구성 변경 사항이 감지되었음"을 알립니다.
5. 사용자가 다시 로그인할 수 있으며, 이 번에는 Cisco Webex 플랫폼 서비스에 인증합니다.
6. 연락처 마이그레이션을 활성화한 경우 사용자에게 Jabber 연락처를 표시하라는 메시지가 표시됩니다. 확인을 클릭하면, Jabber는 연락처 목록 캐시를 가져와서 Cisco Webex 플랫폼 서비스에 업로드합니다. 사용자가 취소를 선택하면 Jabber에서 연락처 목록을 마이그레이션하지 않습니다. 나중에 연락처를 개별적으로 검색하여 추가할 수 있습니다.

   연결을 마이그레이션하는 동안 Jabber는 Cisco Webex 플랫폼 서비스에 대해 활성화 된 연락처만 마이그레이션합니다. Jabber는 사용자 지정 연락처를 Cisco Webex 플랫폼 서비스에 저장하지 않으며 사용자의 연락처 목록에 추가할 수 없습니다.
7. Jabber가 Cisco Webex 플랫폼 서비스에 연결되고 나면 서비스 프로파일을 다운로드하기 위해 Cisco UC Manager에 연결됩니다. SSO가 Cisco Webex 플랫폼 서비스 및 서로 다른 IdPs를 사용하는 UC 관리자에서 활성화되어 있거나 SSO가 한 번만 활성화된 경우에는 사용자에게 자격 증명을 입력하라는 메시지가 표시됩니다. 그러나 SSO가 동일한 IdP에 모두 있는 경우에는 로그인이 필요하지 않습니다.

Jabber 팀 메시지 모드 및 연락처 마이그레이션에 대한 구축 고려 사항

조직 Cisco Webex 플랫폼 서비스에 서비스 도메인과 동일한 도메인이 있어야 합니다. 도메인이 서로 다른 경우에는 사용자에게 연락처 마이그레이션을 사용할 수 없습니다.

가상 환경에 구축

가상 환경에서 Windows용 Cisco Jabber를 구축할 수 있습니다.

가상 환경에서는 다음 기능을 지원합니다.

- 다른 Cisco Jabber 클라이언트와의 인스턴트 메시징 및 프레즌스
- 사무실 전화기 제어
- 음성 메일
- Microsoft Outlook 2007, 2010 및 2013과의 프레즌스 통합
- 모바일 및 Remote Access(MRA)

가상 환경 및 로밍 프로파일

가상 환경에서는 사용자가 항상 동일한 가상 데스크톱에 액세스하지 않습니다. 일관된 사용자 경험을 보장하기 위해서는 클라이언트가 시작될 때마다 이러한 파일에 액세스할 수 있어야 합니다. Cisco Jabber는 사용자 데이터를 다음 위치에 저장합니다.

- `C:\Users\username\AppData\Local\Cisco\Unified Communications\Jabber\CSF`

- 연락처 - 연락처 캐시 파일
- 기록 - 통화 및 채팅 기록
- 사진 캐시 - 디렉터리 사진을 로컬로 캐시

- `C:\Users\username\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF`
  - 구성 - 사용자 구성 파일을 유지 관리하고 구성 저장소 캐시를 저장
  - 자격 증명 - 암호화된 사용자 이름 및 암호 파일을 저장

파일 암호화 및 암호 해독이 Windows 사용자 프로파일에 연결되어 있으므로 다음 폴더에 액세스할 수 있는지 확인하십시오.

- `C:\Users\username\AppData\Roaming\Microsoft\Credentials`
- `C:\Users\username\AppData\Roaming\Microsoft\Crypto`
- `C:\Users\username\AppData\Roaming\Microsoft\Protect`
- `C:\Users\username\AppData\Roaming\Microsoft\SystemCertificates`
- `C:\Users\username\AppData\Local\Microsoft\Credentials`
- `C:\Users\username\AppData\Local\Microsoft\identitycache`

참고 비 영구적인 VDI(가상 구축 인프라) 모드에서 Cisco Jabber를 사용하는 경우에는 Cisco Jabber 자격 증명 캐싱이 지원되지 않습니다.

필요한 경우 파일 및 폴더를 제외 목록에 추가하여 동기화에서 제외할 수 있습니다. 제외된 폴더에 있는 하위 폴더를 동기화하려면 포함 목록에 하위 폴더를 추가합니다.

개인 사용자 설정을 보존하려면 다음을 수행하십시오.

- 다음 디렉터리를 제외하지 마십시오.
  - `AppData\Local\Cisco`
  - `AppData\Local\JabberWerxCPP`
  - `AppData\Roaming\Cisco`
  - `AppData\Roaming\JabberWerxCPP`
- 다음 전용 프로파일 관리 솔루션을 사용합니다.
  - **Citrix** 프로파일 관리 - Citrix 환경에 대한 프로파일 솔루션을 제공합니다. 임의 호스팅된 가상 데스크톱 할당을 사용한 구축에서는 Citrix 프로파일 관리에서 각 사용자의 전체 프로파일을 설치된 시스템 간에 동기화하고 사용자를 저장합니다.

- **VMware View** 개인 관리 - 사용자 프로파일을 보존하고 원격 프로파일 리포지토리와 동적으로 동기화합니다. VMware View 개인 관리에는 Windows 로밍 프로파일 구성이 필요하지 않으며 VMware Horizon View 사용자 프로파일 관리에서 Windows Active Directory를 우회할 수 있습니다. 개인 관리는 기존 로밍 프로파일의 기능을 향상시킵니다.

VDI용 Jabber Softphone 구축

통화 기능이 있는 가상 환경에 Jabber를 구축하려면 가상 데스크톱 인프라에 대해 Jabber Softphone을 구축해야 합니다.

VDI용 Jabber Softphone을 구축하기 위한 워크플로는 온프레미스 또는 하이브리드 환경에서 구축하는 경우에 따라 다르며, 애플리케이션 설치 전까지 Jabber 구축 워크플로를 준수해야 합니다. 이 경우에는 VDI용 Jabber Softphone 구축 및 을 설치 워크플로를 따라야 합니다.

VDI 용 Jabber Softphone에 대한 온프레미스 구축 워크플로를 얻으려면 Cisco Jabber의 온프레미스 구축의 구축 및 설치 워크플로에서 전체 *UC* 구축으을 참조하십시오.

VDI용 Jabber Softphone에 대한 하이브리드 구축 워크플로를 가져오려면 Cisco Jabber용 클라우드 및 하이브리드 구축의 클라우드 및 하이브리드 구축의 워크플로 섹션에서 the *Webex Messenger*를 사용한 하이브리드 구축 워크플로를 참조하십시오.

Enterprise Mobility Management 구축

Jabber는 EMM(엔터프라이즈 이동성 관리) 구축을 위해 두 개의 SDK 기반 클라이언트를 지원합니다.

- Intune용 Cisco Jabber
- BlackBerry용 Cisco Jabber

조직에서 이러한 클라이언트를 구축하여 "BYOD(Bring Your Own Device)"를 허용하는 구축에서 모바일 장치에서 Jabber를 사용하는 정책을 시행할 수 있습니다. 예를 들어, 이러한 정책은 다음 작업을 수행할 수 있습니다.

- 안전하지 않은 장치를 사용하지 못하도록 합니다.
- 최소 OS 및 앱 버전을 시행합니다.
- 사용자가 Jabber에서 데이터를 복사하여 다른 앱에 붙여 넣지 못하도록 합니다.

새 EMMType 매개 변수를 사용하여 사용자가 로그인할 수 있는 Jabber 클라이언트를 제어합니다.

기억 이러한 클라이언트는 지연된 릴리스 주기를 따릅니다. 클라이언트는 Android용 Jabber 및 iPhone과 iPad용 Jabber의 해당 릴리스 이후 버전을 릴리스합니다.

Intune용 Jabber가 포함된 EMM

구축에서 Intune용 Jabber 클라이언트를 사용하는 경우 관리자가 Microsoft Azure에서 관리 정책을 구성합니다. 사용자는 App Store 또는 Google Play Store에서 새 클라이언트를 다운로드합니다. 사용자가 새 클라이언트를 실행하면 관리자가 만든 정책과 동기화합니다.

참고 Android 장치의 경우 먼저 사용자가 Intune 회사 포털을 설치합니다. 그런 다음 포털을 통해 클라이언트를 실행합니다.

Intune용 Jabber 설정에 대한 일반 절차는 다음과 같습니다.

1. 새 Azure AD 테넌트를 만듭니다.
2. 새 AD 사용자를 만들거나 온프레미스 AD 사용자를 동기화합니다.
3. Office 365 그룹 또는 보안 그룹을 만들고 사용자를 추가합니다.
4. Intune용 Jabber 클라이언트를 Microsoft Intune에 추가합니다.
5. Microsoft Intune에서 정책을 만들고 구축합니다.
6. 사용자는 사용자의 정책을 수신하도록 클라이언트에 로그인하고 동기화합니다.

이러한 단계에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

이 표에는 Cisco Jabber를 위한 앱 보호 정책에서 지원하는 Microsoft Intune 제한 사항이 나열되어 있습니다.

제한 사항	**Android**	**iPhone** 및 **iPad**
다른 앱으로 데이터 전송	예	예
조직의 데이터 사본 저장	예	예
잘라내기, 복사 및 다른 앱으로 붙여넣기	예	예
화면 캡처	예	해당 없음
최대 PIN 시도 횟수	예	예
오프라인 유예 기간	예	예
최소 앱 버전	예	예
탈옥 또는 루팅된 장치에서 사용	예	예
최소 장치 OS 버전	예	예
최소 패치 버전	예	해당 없음
액세스를 위한 직장 (또는 학교) 계정 자격 증명	예	예

제한 사항	Android	iPhone 및 iPad
액세스 요구 사항 다시 확인	예	예

Blackberry용 Jabber가 포함된 EMM

구축에서 BlackBerry용 Jabber 클라이언트를 사용하는 경우 관리자는 해당 UEM(BlackBerry 통합 엔드포인트 관리)에서 관리 정책을 구성합니다. 사용자는 App Store 또는 Google Play Store에서 새 클라이언트를 다운로드합니다. BlackBerry용 Jabber는 BlackBerry 인증 중이며 아직 BlackBerry Marketplace에서 사용할 수 없습니다.

중요 클라이언트가 BlackBerry 인증을 진행 중이기 때문에 조직에 대한 액세스 권한을 부여해야 합니다. 액세스 권한을 받으려면 당사(jabber-mobile-mam@cisco.com)에 문의하고 해당 BlackBerry UEM 서버에서 고객의 조직 ID를 제공하십시오.

새 클라이언트는 BlackBerry Dynamics SDK를 통합했으며, BlackBerry UEM에서 정책을 직접 가져올 수 있습니다. 클라이언트는 연결 및 저장소에 대한 BlackBerry Dynamics를 우회합니다. FIPS 설정은 BlackBerry Dynamics SDK를 통해 지원되지 않습니다.

채팅, 음성 및 비디오 트래픽은 BlackBerry 인프라를 우회합니다. 클라이언트가 온-프레미스 상태가 아니면 모든 트래픽에 대해 Cisco Expressway를 통한 모바일 및 Remote Access가 필요합니다.

참고 Android의 BlackBerry용 Jabber에는 Android 6.0 이상이 필요합니다.

iOS의 BlackBerry용 Jabber에는 iOS 11.0 이상이 필요합니다.

BlackBerry Dynamics의 경우 관리자가 BlackBerry용 Jabber 클라이언트의 사용을 제어하기 위해 정책을 설정합니다.

BlackBerry용 Jabber를 설정하는 일반적인 프로세스는 다음과 같습니다.

1. UEM에 서버를 만듭니다.
2. Blackberry용 Jabber 클라이언트를 BlackBerry Dynamics에 추가합니다.
3. BlackBerry Dynamics에서 사용자를 만들거나 가져옵니다.

참고 Android 사용자의 경우 필요에 따라 BlackBerry Dynamics에서 선택적으로 액세스 키를 생성할 수 있습니다.

4. UEM에서 정책을 만들고 구축합니다. 다음은 BlackBerry용 Jabber 앱 구성에 대한 이러한 설정의 동작입니다.
   - 선택적 DLP 정책을 활성화하는 경우 BlackBerry에서 다음을 수행해야 합니다.

- BlackBerry 작업을 사용하여 이메일을 전송합니다.
- iOS 장치에서 SSO 인증에 BlackBerry 액세스를 사용합니다. Expressway 및 통합 커뮤니케이션 관리자에서 iOS용 기본 브라우저 사용을 활성화합니다. 그런 다음 **ciscojabber** 체계를 BlackBerry UEM의 BlackBerry 액세스 정책에 추가합니다.

- 이 목록에는 BlackBerry용 Jabber 구축에서 앱 구성을 통해 설정하는 데 유용한 Jabber 매개 변수가 표시됩니다. 이러한 매개 변수에 대한 자세한 내용은 구축 설명서의 *Android, IPhone* 및 *iPad*용 *Cisco Jabber*에 대한 *URL* 구성 섹션을 참조하십시오.

필드	**iOS**에서 지원됨	**Android**에서 지원됨
Webex Meetings 크로스 실행 비활성화 [3]	예	예
서비스 도메인	예	예
음성 서비스 도메인	예	예
서비스 검색 제외 서비스	예	예
서비스 도메인 SSO 이메일 프롬프트	예	예
잘못된 인증서 동작	예	예
전화 통신 활성화	예	예
URL 프로비저닝 허용	예	예
IP 모드	예	예

[3] Webex Meetings의 크로스 실행을 활성화하면 비 동적 앱을 허용하지 않는 BlackBerry 동적 컨테이너에서 예외로 실행될 수 있습니다.

5. 사용자가 클라이언트에 로그인합니다.

이러한 단계에 대한 자세한 내용은 BlackBerry 설명서를 참조하십시오.

이 표에는 Cisco Jabber를 위한 앱 보호 정책에서 지원하는 Microsoft Intune 제한 사항이 나열되어 있습니다.

그룹	기능	**Android**	**iPhone** 및 **iPad**
IT 정책	네트워크 연결이 없는 장치를 지웁니다.	예	예
Activation	허용되는 버전	예	예

그룹	기능	Android	iPhone 및 iPad
BlackBerry Dynamics	암호	예	예
	데이터 누출 방지 - BlackBerry Dynamics 앱의 데이터를 비 BlackBerry Dynamics 앱으로 복사를 허용 안 함	예	예
	데이터 누출 방지 - 비 BlackBerry Dynamics 앱의 데이터를 BlackBerry Dynamics 앱으로 복사를 허용 안 함	예	예
	데이터 누출 방지 - Android 및 Windows 10+ 장치에서 화면 캡처를 허용 안 함	예	해당 없음
	데이터 누출 방지 - iOS 장치에서 화면 녹화 및 공유를 허용 안 함	해당 없음	예
	데이터 누출 방지 - iOS 장치에서 사용자 지정 키보드 허용 안 함	해당 없음	예
엔터프라이즈 관리 에이전트 프로파일	개인 앱 모음 허용	예	예
준수 프로파일	루트 OS 또는 실패한 증명	예	예
	제한된 OS 버전이 설치됨	예	예
	필수 보안 패치 수준이 설치되어 있지 않음	예	해당 없음

BlackBerry용 Jabber의 IdP 연결

Android 및 iPhone 및 iPad용 Jabber 구축의 경우 클라이언트는 DMZ의 IdP(Id 공급자) 프록시에 연결됩니다. 그런 다음 프록시는 내부 방화벽 뒤에 IdP 서버에 요청을 전달합니다.

BlackBerry용 Jabber에는 대체 경로를 사용할 수 있습니다. BlackBerry UEM에서 DLP 정책을 활성화하는 경우 iOS 장치의 클라이언트는 IdP 서버에 직접 안전하 게 터널링될 수 있습니다. 이 설치 프로그램을 사용하려면 다음과 같이 구축을 구성하십시오.

- Expressway 및 Unified CM에서 iOS용 기본 브라우저 사용을 활성화합니다.
- Blackberry UEM의 BlackBerry 액세스 정책에 **`ciscojabber`** 체계를 추가합니다.

Android OS의 BlackBerry용 Jabber는 항상 SSO에 대한 IdP 프록시에 연결합니다.

구축에 iOS에서 실행되는 장치만 포함되어 있는 경우에는 DMZ에 IdP 프록시가 필요하지 않습니다. 그러나, 구축에 Android OS에서 실행 중인 장치가 포함되어 있는 경우 IdP 프록시가 필요합니다.

iOS의 앱 전송 보안

iOS에는 ATS(App Transport Security) 기능이 포함되어 있습니다. ATS를 사용하려면 BlackBerry용 Jabber 및 Intune용 Jabber에서 신뢰할 수 있는 인증서와 암호화 기능을 갖춘 TLS를 통해 보안 네트워크 연결을 수행해야 합니다. ATS는 x.509 디지털 인증서가 없는 서버에 대한 연결을 차단합니다. 인증서는 다음 검사를 통과해야 합니다.

- 디지털 서명 유지
- 유효한 만료일
- 서버의 DNS 이름과 일치하는 이름
- CA의 신뢰할 수 있는 앵커 인증서에 대한 유효한 인증서 체인

참고 IOS의 일부인 신뢰할 수 있는 앵커 인증서에 대한 자세한 내용은 https://support.apple.com/en-us/HT204132의 *iOS*에서 사용 가능한 신뢰할 수 있는 루트 인증서 목록을 참조하십시오. 시스템 관리자 또는 사용자는 동일한 요구 사항을 충족하는 경우에도 신뢰할 수 있는 앵커 인증서를 설치할 수 있습니다.

ATS에 대한 자세한 내용은 https://developer.apple.com/documentation/security/preventing_insecure_network_connections의 비 보안 네트워크 연결 금지를 참조하십시오.

Remote Access

사용자는 회사 네트워크 외부에 있는 위치에서 자신의 작업에 액세스해야 할 수 있습니다. Remote Access용 Cisco 제품 중 하나를 사용하여 작업에 대한 액세스 권한을 제공할 수 있습니다.

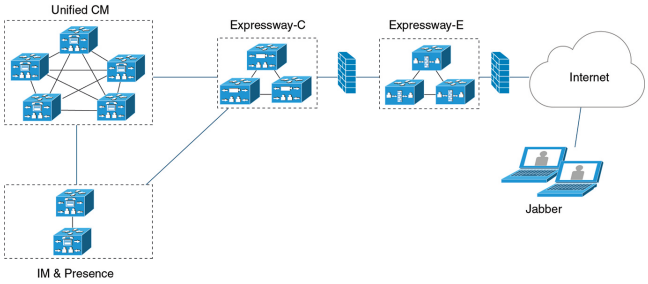
Jabber는 타사 VPN 클라이언트에서 테스트되거나 확인되지 않았습니다.

모바일 및 Remote Access용 Expressway

Cisco Unified Communications Manager에 대해 모바일 및 Remote Access용 Expressway를 사용하면 사용자는 VPN(가상 사설망)을 사용하지 않고 회사 방화벽 외부에서 협업 도구에 액세스할 수 있습니다. Cisco 협업 게이트웨이를 사용하면 클라이언트가 공용 Wi-Fi 네트워크나 모바일 데이터 네트워크와 같은 외부 위치에서 회사 네트워크에 안전하게 연결할 수 있습니다.

그림 *4:* 클라이언트가 모바일 및 *Remote Access*용 *Expressway*에 연결하는 방법

다음 다이어그램은 모바일 및 Remote Access용 Expressway 환경의 아키텍처를 보여줍니다.



모바일 및 Remote Access용 Expressway를 사용하여 Jabber에 처음 로그인

Cisco Jabber 모바일 클라이언트에 적용됩니다.

사용자는 회사 방화벽 외부에서 서비스에 연결하기 위해 모바일 및 Remote Access용 Expressway를 사용하여 처음으로 클라이언트에 로그인할 수 있습니다. 그러나 다음 경우에는 처음에 회사 네트워크에 있는 동안 로그인합니다.

- 음성 서비스 도메인이 다른 서비스 도메인과 다른 경우 `jabber-config.xml` 파일에서 올바른 음성 서비스 도메인을 가져오려면 사용자가 회사 네트워크 내에 있어야 합니다. 하이브리드 구축의 경우 관리자가 VoiceServicesDomain 매개 변수를 구성할 수 있습니다. *Cisco Jabber*에 대한 매개 변수 참조 설명서의 최신 버전을 참조하십시오. 이 경우 사용자는 회사 네트워크 내에서 로그인할 필요가 없습니다.
- Cisco Jabber가 보안 또는 혼합 모드 클러스터를 사용할 때 필요한 CAPF 등록 프로세스를 완료해야 합니다.

사용자가 모바일 및 Remote Access용 Expressway 환경을 통해 보안 전화기를 사용하는 경우에는 공용 네트워크에서 첫 번째 로그인을 지원하지 않습니다. 암호화된 TFTP를 사용하는 보안 프로파일에 대한 구성인 경우 CAPF 등록을 허용하려면 첫 번째 로그인이 온프레미스에 있어야 합니다. 공용 네트워크의 첫 번째 로그인은 Cisco Unified Communications Manager, 모바일 및 Remote Access용 Expressway, Cisco Jabber 향상 기능을 사용하지 않고는 지원될 수 없습니다. 그러나 다음을 지원합니다.

- 온프레미스를 통한 첫 번째 로그인을 사용하는 암호화된 TFTP
- 모바일 및 Remote Access용 Expressway 또는 또는 온프레미스를 통한 첫 번째 로그인의 암호화되지 않은 TFTP

지원되는 서비스

다음 표에는 클라이언트가 모바일 및 Remote Access용 Expressway를 사용하여 원격으로 Cisco Unified Communications Manager에 연결할 때 지원되는 서비스 및 기능이 요약되어 있습니다.

표 *2:* 모바일 및 ***Remote Access***용 ***Expressway***를 위해 지원되는 서비스 요약

서비스	지원됨	지원되지 않음
디렉터리		
UDS 디렉터리 검색	X	
LDAP 디렉터리 검색		X
디렉터리 사진 해상도	X * Cisco Expressway-C에서 HTTP 화이트 리스트 사용	
도메인 내 페더레이션	X * 연락처 검색 지원은 연락처 ID의 형식에 따라 달라집니다. 자세한 내용은 아래 참고를 참조하십시오.	
도메인 간 페더레이션	X	
인스턴트 메시징 및 프레즌스		
온-프레미스	X	
클라우드	X	
채팅	X	
그룹 채팅	X	
영구 채팅	X	
고가용성: 온프레미스 구축	X	
파일 전송: 온프레미스 구축	X Cisco Unified Communications Manager IM and Presence Service 10.5(2) 이상을 사용하 여 파일을 전송할 때 사용할 수 있는 고급 옵션은 아래 참고 사항을 참조하십시오.	
파일 전송: 클라우드 구축	X	

서비스	지원됨	지원되지 않음
영상 화면 공유 - BFCP	X(모바일 클라이언트용 Cisco Jabber는 BFCP 수신만 지원합니다.)	
IM 전용 화면 공유		x
오디오 및 비디오		
오디오 및 비디오 전화	X * Cisco Unified Communications Manager 9.1(2) 이상	
CTI(데스크폰 제어 모드) (데스크톱 클라이언트만 해당)		X
확장 및 연결(데스크톱 클라이언트만 해당)		X
원격 데스크톱 제어(데스크톱 클라이언트만 해당)		X
무성 모니터링 및 녹음		X
DVO(Dial via Office) - 역방향(모바일 클라이언트만 해당)	X	
세션 지속성		X
Early media		X
셀프 케어 포털 액세스		X
정상적인 등록	X * Android용 Cisco Jabber에 적용됩니다. Android용 Jabber는 Cisco Unified Communications Manager 릴리스 10.5.(2) 10000-1에서 모바일 및 Remote Access용 Expressway를 통한 정상적인 등록을 지원합니다.	

서비스	지원됨	지원되지 않음
공유 회선	X 필수 조건: • Cisco Expressway를 X8.9.1 이상으로 • Cisco Unified Communications Manager를 11.5 SU(2) 이상으로	
음성 메일		
Visual VoiceMail	X * Cisco Expressway-C에서 HTTP 화이트 리스트 사용	
Webex Meetings		
온-프레미스		X * Jabber 11.6 이후부터 온-프레미스 Cisco Webex 미팅 서버를 제외하고는 지원되지 않습니다.
클라우드	X	
Webex 화면 공유(데스크톱 클라이언트만 해당)	X	
설치(데스크톱 클라이언트)		
설치 관리자 업데이트	X * Cisco Expressway-C에서 HTTP 화이트 리스트 사용	X Mac용 Cisco Jabber에서 지원되지 않음
맞춤 설정		
사용자 정의 HTML 탭		X

서비스	지원됨	지원되지 않음
Enhanced911 프롬프트	X * 회사 네트워크 외부에서 작동하는 모든 Jabber 클라이언트에 대해 웹 페이지가 올바르게 렌더링되도록 하려면 E911NotificationURL 매개 변수에서 스크립트 및 링크 태그를 지원하지 않으므로 웹 페이지는 정적 HTML 페이지여야 합니다. 자세한 내용은 최신 *Cisco Jabber*용 매개 변수 참조 설명서를 참조하십시오.	
보안		
미디어용 ICE 프로토콜	X	
CAPF 등록		X
SSO(Single Sign-On)	X	
Advanced Encryption Standard(AES) 256 및 TLS1.2	X * Android용 Cisco Jabber에 적용됩니다. 고급 암호화는 회사 Wi-Fi에서만 지원됩니다.	
문제 해결(데스크톱 클라이언트만 해당)		
문제 보고서 생성	X	
문제 보고서 업로드		X
고가용성**(**페일오버**)**		
오디오 및 비디오 서비스		X
음성 메일 서비스		X
IM and Presence 서비스	X	
연락처 검색	X	
연락처 확인	X	
컨피그레이션 관리		
빠른 로그인	X	

서비스	지원됨	지원되지 않음
인증		
SSO Jabber 사용자에 대한 O-Auth 지원	X	

디렉토리

클라이언트가 모바일 및 Remote Access용 Expressway를 사용 하 여 서비스에 연결 하는 경우에는 다음과 같은 제한 사항이 있는 디렉터리 통합을 지원합니다.

- LDAP 연락처 확인 - 클라이언트가 회사 방화벽 외부에 있을 때 연락처 확인에 LDAP를 사용할 수 없습니다. 대신, 클라이언트에서 UDS를 사용하여 연락처를 확인해야 합니다.

  사용자가 회사 방화벽 내부에 있는 경우 클라이언트는 UDS 또는 LDAP를 사용하여 연락처를 확인할 수 있습니다. 회사 방화벽 내에서 LDAP를 구축하는 경우 LDAP 디렉터리 서버를 Cisco Unified Communications Manager와 동기화하여 사용자가 회사 방화벽 외부에 있을 때 클라이언트가 UDS에 연결할 수 있도록 하는 것이 좋습니다.

- 디렉터리 사진 해상도 - 클라이언트가 연락처 사진을 다운로드할 수 있도록 하려면 연락처 사진을 호스팅하는 서버를 Cisco Expressway-C 서버의 화이트 리스트에 추가해야 합니다. Cisco Expressway-C 화이트 리스트에 서버를 추가하려면 **HTTP** 서버 허용 설정을 사용하십시오. 자세한 내용은 관련 Cisco Expressway 설명서를 참조하십시오.
- 도메인 내 페더레이션 - 도메인 내 페더레이션을 구축하고 클라이언트가 방화벽 외부에서 모바일 및 Remote Access용 Expressway와 연결되면 연락처 ID가 다음 형식 중 하나를 사용하는 경우에만 연락처 검색이 지원됩니다.
  - sAMAccountName@domain
  - UserPrincipleName(UPN)@domain
  - EmailAddress@domain
  - employeeNumber@domain
  - telephoneNumber@domain
- XMPP를 사용하는 도메인 간 페더레이션 - 모바일 및 Remote Access용 Expressway는 XMPP 도메인 간 페더레이션 자체를 활성화하지 않습니다. 모바일 및 Remote Access용 Expressway를 통해 연결하는 Cisco Jabber 클라이언트는 Cisco Unified Communications Manager IM and Presence에서 활성화된 경우 XMPP 도메인 간 페더레이션을 사용할 수 있습니다.

인스턴트 메시징 및 프레즌스

모바일 및 Remote Access용 Expressway를 사용하여 서비스에 연결하는 경우에는 다음과 같은 제한 사항이 있는 인스턴트 메시징 및 프레즌스를 지원합니다.

파일 전송에는 데스크톱 및 모바일 클라이언트에 대한 다음과 같은 제한 사항이 있습니다.

- Webex 클라우드 구축의 경우 파일 전송이 지원됩니다.

- Cisco Unified Communication IM and Presence Service 10.5(2) 이상의 온프레미스 구축의 경우 관리되는 파일 전송 선택이 지원되지만 피어 투 피어 옵션은 지원되지 않습니다.
- Cisco Unified Communications Manager IM and Presence Service 10.0(1) 또는 이전 구축을 사용하는 온프레미스 구축의 경우 파일 전송은 지원되지 않습니다.
- 무제한 Cisco Unified Communications Manager IM and Presence 서버를 사용하는 모바일 및 Remote Access용 Expressway 구축의 경우 관리되는 파일 전송이 지원되지 않습니다.

오디오 및 영상 통화

클라이언트가 모바일 및 Remote Access용 Expressway를 사용 하 여 서비스에 연결 하는 경우에는 다음과 같은 제한 사항이 있는 오디오 및 영상 통화를 지원합니다.

- Cisco Unified Communications Manager - 모바일 및 Remote Access용 Expressway는 Cisco Unified Communications Manager 버전 9.1.2 이상에서 오디오 및 영상 통화를 지원합니다.
- CTI(데스크폰 제어 모드) (데스크톱 클라이언트만 해당) - 클라이언트는 내선 이동을 포함한 CTI(데스크폰 제어 모드)를 지원하지 않습니다.
- 확장 및 연결(데스크톱 클라이언트만 해당) - 클라이언트를 사용하여 다음 작업을 수행할 수 없습니다.
  - 사무실에 있는 Cisco IP 전화기로 전화를 걸고 받습니다.
  - 집 전화, 호텔 전화 또는 사무실에 있는 Cisco IP 전화기에서 보류 및 재시작 같은 통화 중 제어를 수행합니다.
- 세션 지속성 - 네트워크 전환이 발생하면 클라이언트가 오디오 및 영상 통화를 복구할 수 없습니다. 예를 들어, 사용자가 사무실 내에서 Cisco Jabber call을 시작한 다음 건물 외부로 이동하여 Wi-Fi 연결이 끊기는 경우 클라이언트가 모바일 및 Remote Access용 Expressway를 사용하도록 전환할 때 통화가 끊어집니다.
- Early Media - Early Media를 사용하면 연결이 설정되기 전에 클라이언트가 엔드포인트 간에 데이터를 교환할 수 있습니다. 예를 들어, 사용자가 동일한 조직에 속하지 않은 상대방에게 전화를 걸고 다른 상대방이 통화를 거부하거나 응답하지 않는 경우 Early Media를 사용하면 사용자가 통화 중 신호음을 듣게 되거나 음성 메일로 전송됩니다.

  모바일 및 Remote Access용 Expressway를 사용하는 경우 다른 상대방이 통화를 거부하거나 응답하지 않으면 통화 중 신호음이 들리지 않습니다. 대신, 통화가 종료되기까지 약 1분 동안 아무 소리도 들리지 않습니다.
- 셀프 서비스 포털 액세스(데스크톱 클라이언트만 해당) - 사용자가 방화벽 밖에 있을 때 Cisco Unified Communications Manager 셀프 서비스 포털에 액세스할 수 없습니다. Cisco Unified Communications Manager 사용자 페이지는 외부에서 액세스할 수 없습니다.

  Cisco Expressway-E는 방화벽 내에서 클라이언트와 통합 커뮤니케이션 서비스 간의 모든 통신을 프록시합니다. 그러나 Cisco Expressway-E는 Cisco Jabber 애플리케이션에 속하지 않는 브라우저에서 액세스하는 프록시 서비스는 지원하지 않습니다.

음성 메일

음성 메일 서비스는 클라이언트가 모바일 및 Remote Access용 Expressway를 사용하여 서비스에 연결하는 경우 지원됩니다.

참고 클라이언트에서 음성 메일 서비스에 액세스할 수 있도록 하려면 Cisco Expressway 서버의 화이트 리스트에 음성 메일 서버를 추가해야 합니다. Cisco Expressway-C 화이트 리스트에 서버를 추가하려면 **HTTP** 서버 허용 설정을 사용하십시오. 자세한 내용은 관련 Cisco Expressway 설명서를 참조하십시오.

설치

Mac용 Cisco Jabber - 클라이언트가 모바일 및 Remote Access용 Expressway를 사용하여 서비스에 연결할 때 설치 관리자 업데이트를 지원하지 않습니다.

Windows용 Cisco Jabber - 클라이언트가 모바일 및 Remote Access용 Expressway를 사용하여 서비스에 연결할 때 설치 관리자 업데이트를 지원합니다.

참고 클라이언트에서 설치 관리자 업데이트를 다운로드할 수 있도록 하려면 설치 관리자 업데이트를 호스트하는 서버를 Cisco Expressway 서버의 화이트 리스트에 추가해야 합니다. Cisco Expressway-C 화이트 리스트에 서버를 추가하려면 **HTTP** 서버 허용 설정을 사용하십시오. 자세한 내용은 관련 Cisco Expressway 설명서를 참조하십시오.

보안

클라이언트가 모바일 및 Remote Access용 Expressway를 사용하여 서비스에 연결하는 경우에는 다음과 같은 제한 사항이 있는 대부분의 보안 기능을 지원합니다.

- 초기 CAPF 등록 - CAPF(Certificate Authority Proxy Function) 등록은 Cisco Jabber(또는 다른 클라이언트)에 인증서를 발행하는 Cisco Unified Communications Manager 게시자에서 실행되는 보안 서비스입니다. CAPF를 성공적으로 등록하려면 클라이언트가 방화벽 내부에서 또는 VPN을 사용하여 연결해야 합니다.
- 엔드 투 엔드 암호화 - 사용자가 모바일 및 Remote Access용 Expressway를 통해 연결하고 통화에 참가하는 경우:
  - 미디어는 모바일 및 Remote Access용 Expressway를 사용하여 Cisco Unified Communications Manager에 등록된 장치와 Cisco Expressway-C 간의 통화 경로에서 항상 암호화됩니다.
  - Cisco Jabber 또는 내부 장치 중 하나가 암호화된 보안 모드로 구성되지 않은 경우, Cisco Unified Communications Manager에 로컬로 등록된 장치와 Cisco Expressway-C 간의 통화 경로에서 미디어가 암호화되지 않습니다.
  - Cisco Jabber 및 내부 장치 모두 암호화된 보안 모드로 구성된 경우, Cisco Unified Communications Manager에 로컬로 등록된 장치와 Cisco Expressway-C 간의 통화 경로에서 미디어가 암호화됩니다.

- Cisco Jabber 클라이언트가 모바일 및 Remote Access용 Expressway를 통해 항상 연결되는 경우에는 엔드 투 엔드 암호화를 달성하기 위해 CAPF 등록이 필요하지 않습니다. 그러나 Cisco Jabber 장치는 여전히 암호화된 보안 모드를 사용하여 구성해야 하며 혼합 모드를 지원하려면 Cisco Unified Communications Manager를 활성화해야 합니다.
- Expressway-C 또는 Expressway-E 서버에서 ICE 통과 지원을 구성하여 Jabber를 통해 전송된 미디어가 회사 네트워크 외부에 있을 때 암호화되도록 할 수 있습니다. 이를 설정하는 방법에 대한 자세한 내용은 구축 설명서의 *Cisco Expressway*를 통한 모바일 및 *Remote Access*를 참조하십시오.

문제 해결

Windows용 Cisco Jabber만 해당. 문제 보고서 업로드 - 데스크톱 클라이언트가 모바일 및 Remote Access용 Expressway를 사용하여 서비스에 연결하는 경우 클라이언트에서 지정된 내부 서버로 HTTPS를 통해 문제 보고서를 업로드하므로 문제 보고서를 전송할 수 없습니다.

이 문제를 해결하기 위해 사용자는 보고서를 로컬로 저장하고 다른 방법으로 보고서를 전송할 수 있습니다.

고가용성(페일오버)

고가용성은 클라이언트가 기본 서버에 연결하는 데 실패하는 경우 서비스에 대한 중단이 거의 없거나 중단 없는 보조 서버로 페일오버하는 것을 의미합니다. 모바일 및 Remote Access용 Expressway에서 지원되는 고가용성과 관련해서 고가용성은 특정 서비스에 대한 서버를 보조 서버(예: 인스턴트 메시징 및 프레즌스)로 페일오버하는 것을 의미합니다.

일부 서비스는 고가용성을 위해 지원되지 않는 모바일 및 Remote Access용 Expressway에서 사용할 수 있습니다. 이는 사용자가 회사 네트워크 외부에서 클라이언트에 연결되고 인스턴트 메시징 및 프레즌스 서버가 페얼오버됨을 의미하는 경우 서비스는 정상적으로 계속 작동합니다. 그러나 오디오 및 비디오 서버 또는 음성 메일 서버가 페일오버되는 경우 관련 서버가 고가용성을 지원하지 않으므로 이러한 서비스가 작동하지 않습니다.

Cisco AnyConnect 구축

Cisco AnyConnect는 클라이언트가 Wi-Fi 네트워크 또는 모바일 데이터 네트워크와 같은 원격 위치에서 회사 네트워크에 안전하게 연결할 수 있도록 하는 서버 클라이언트 인프라를 나타냅니다.

Cisco AnyConnect 환경에는 다음 구성 요소가 포함되어 있습니다.

- Cisco 적응 보안 어플라이언스 — Remote Access를 보호하는 서비스를 제공합니다.
- Cisco AnyConnect Secure Mobility Client - 사용자의 장치에서 Cisco 적응 보안 어플라이언스에 대한 보안 연결을 설정합니다.

이 섹션에서는 Cisco AnyConnect Secure Mobility Client를 사용하여 Cisco Adaptive Security Appliance (ASA)를 구축할 때 고려해야 하는 정보를 제공합니다. Cisco AnyConnect는 Android용 Cisco Jabber 및 iPhone 및 iPad용 Cisco Jabber에 지원되는 VPN입니다. 지원되지 않는 VPN 클라이언트를 사용하는 경우 관련 타사 설명서를 사용하여 VPN 클라이언트를 설치하고 구성해야 합니다.

Android OS 4.4.x를 실행하는 삼성 장치의 경우 Samsung AnyConnect 버전 4.0.01128 이상을 사용합니다. 5.0 이상의 Android OS 버전의 경우 4.0.01287 이후의 Cisco AnyConnect 소프트웨어 버전을 사용해야 합니다.

Cisco AnyConnect는 원격 사용자에게 Cisco 5500 시리즈 ASA에 대해 보안 IPsec (IKEv2) 또는 SSL VPN 연결을 제공합니다. Cisco AnyConnect는 ASA에서 또는 엔터프라이즈 소프트웨어 구축 시스템을 사용하여 원격 사용자에게 구축할 수 있습니다. ASA에서 구축될 때 원격 사용자는 SSL VPN 연결을 수락하도록 구성된 ASA의 브라우저에 IP 주소 또는 DNS 이름을 입력하여 ASA에 대한 초기 SSL 연결을 설정합니다. 그런 다음, 사용자가 로그인 및 인증을 충족하는 경우에는 ASA가 브라우저 창에 로그인 화면을 표시하고 컴퓨터 운영 체제와 일치하는 클라이언트를 다운로드합니다. 다운로드 후 클라이언트는 스스로 설치 및 구성하며 IPsec(IKEv2) 또는 ASA에 대한 SSL 연결을 설정합니다.

Cisco 적응 보안 어플라이언스 및 Cisco AnyConnect Secure Mobility Client의 요구 사항에 대한 자세한 내용은 소프트웨어 요구 사항 항목을 참조하십시오.

관련 항목

Cisco ASA Series 문서 탐색
Cisco AnyConnect Secure Mobility Client

싱글 사인온을 통한 구축

SAML(Security Assertion Markup Language) SSO(Single Sign-On)를 사용하여 서비스를 활성화할 수 있습니다. SAML SSO는 온프레미스, 클라우드 또는 하이브리드 구축에서 사용할 수 있습니다.

다음 단계에서는 사용자가 Cisco Jabber 클라이언트를 시작한 후 SAML SSO에 대한 로그인 흐름에 대해 설명합니다.

1. 사용자가 Cisco Jabber 클라이언트를 시작합니다. 사용자가 웹 양식을 사용하여 로그인하라는 메시지를 표시하도록 IdP(ID 공급자)를 구성하는 경우 양식이 클라이언트 내에 표시됩니다.
2. Cisco Jabber 클라이언트는 연결 중인 서비스(예: Webex Messenger 서비스, Cisco Unified Communications Manager 또는 Cisco Unity Connection)에 인증 요청을 보냅니다.
3. 이 서비스는 IdP에서 인증을 요청하도록 클라이언트를 재전송합니다.
4. IdP가 자격 증명을 요청합니다. 다음 방법 중 하나를 통해 자격 증명을 제공할 수 있습니다.
   - 사용자 이름 및 암호 필드를 포함하는 양식 기반 인증
   - IWA(Windows 통합 인증)용 Kerberos(Windows만 해당)
   - 스마트 카드 인증(Windows만 해당)
   - 클라이언트에서 HTTP 요청을 할 때 사용자 이름과 암호를 제공하는 기본 HTTP 인증 방법입니다.
5. IdP는 브라우저 또는 다른 인증 방법에 쿠키를 제공합니다. IdP는 SAML를 사용하여 ID를 인증하며, 이를 통해 서비스에서 클라이언트에 토큰을 제공할 수 있습니다.
6. 클라이언트는 인증을 위해 토큰을 사용하여 서비스에 로그인합니다.

인증 방법

인증 메커니즘은 사용자가 로그인하는 방식에 영향을 미칩니다. 예를 들어, Kerberos를 사용하는 경우 사용자가 이미 데스크톱에 액세스할 수 있는 인증을 제공했기 때문에 클라이언트가 사용자에게 자격 증명을 요구하지 않습니다.

사용자 세션

사용자는 세션에 로그인하여 Cisco Jabber 서비스를 사용하기 위해 미리 정의된 기간을 제공합니다. 세션이 지속되는 기간을 제어하려면 쿠키 및 토큰 시간 초과 매개 변수를 구성합니다.

사용자에게 로그인하라는 메시지가 표시되지 않도록 적절한 시간을 사용하여 IdP 시간 초과 매개 변수를 구성합니다. 예를 들어, Jabber 사용자가 외부 Wi-Fi로 전환되는 경우, 로밍, 노트북 컴퓨터 최대 절전 모드 또는 해당 노트북 컴퓨터는 사용자 비활성 상태로 인해 절전 상태가 됩니다. IdP 세션이 여전히 활성 상태인 경우에는 사용자가 연결을 다시 시작한 후 로그인할 필요가 없습니다.

세션이 만료되고 Jabber가 자동으로 갱신할 수 없는 경우 사용자 입력이 필요하므로 사용자에게 재인증을 요청하는 메시지가 표시됩니다. 이 문제는 인증 쿠키가 더 이상 유효하지 않을 때 발생할 수 있습니다.

Kerberos 또는 스마트 카드를 사용하는 경우 스마트 카드에 PIN이 필요하지 않으면 다시 인증하는 데 조치가 필요 하지 않습니다. 음성 메일, 수신 통화 또는 인스턴트 메시징과 같은 서비스가 중단될 위험은 없습니다.

싱글 사인온 요구 사항

SAML 2.0

Cisco Unified Communications Manager 서비스를 사용하여 Cisco Jabber 클라이언트에 대해 SSO(싱글 사인온)를 활성화하려면 SAML 2.0을 사용합니다. SAML 2.0은 SAML 1.1과 호환되지 않습니다. SAML 2.0 표준을 사용하는 IdP를 선택합니다. 지원되는 ID 공급자는 SAML 2.0을 준수하므로 SSO를 구현하는 데 사용할 수 있습니다.

지원되는 **ID** 공급자

Cisco에서는 SAML(Security Assertion Markup Language)을 준수하는 IdP를 지원합니다. 다음과 같은 ID 공급자를 테스트했습니다.

- Ping Federate 6.10.0.4
- Microsoft Active Directory 페더레이션 서비스(ADFS) 2.0
- Open Access Manager(OpenAM) 10.1

참고 OpenAM에 사용할 전역 영구 쿠키를 구성해야 합니다.

IdP를 구성하면 구성된 설정이 클라이언트에 로그인하는 방법에 영향을 미칩니다. 쿠키 유형(영구 또는 세션) 또는 인증 메커니즘(Kerberos 또는 Web form)과 같은 매개 변수는 인증해야 하는 빈도를 결정합니다.

쿠키

브라우저에서 쿠키 공유를 활성화하려면 영구 쿠키를 사용하고 세션 쿠키는 사용하지 마십시오. 영구 쿠키는 클라이언트에서 한 번 또는 Internet Explorer를 사용하는 다른 데스크톱 애플리케이션에 자격 증명을 입력하라는 메시지를 표시합니다. 세션 쿠키를 사용하려면 클라이언트를 시작할 때마다 사용자가 인증서를 입력해야 합니다. 영구 쿠키를 IdP 설정으로 구성합니다. Open Access Manager를 IdP로 사용하는 경우 전역 영구 쿠키(영역 특정 영구 쿠키가 아님)를 구성합니다.

사용자가 SSO 자격 증명을 사용하여 iPhone 및 iPad용 Cisco Jabber에 성공적으로 로그인하면 쿠키는 기본적으로 iOS 키체인에 저장됩니다. 쿠키가 iOS 키체인에 있는 경우 로그인할 때 쿠키가 만료되지 않으면 사용자는 다음 로그인에 로그인 시 자격 증명을 입력할 필요가 없습니다. 다음과 같은 시나리오에서 iOS 키체인에서 쿠키가 삭제됩니다.

- Cisco Jabber에서 수동으로 로그아웃
- Cisco Jabber 재설정
- iOS 장치 재부팅 후
- Cisco Jabber가 수동으로 종료됨

참고 임베디드 Safari 브라우저를 사용하는 경우 Jabber는 Safari에서 제어하는 쿠키를 제어할 수 없습니다. Jabber에서 이러한 쿠키를 지울 수 없으므로, Jabber는 이 경우 SSO 토큰만 지울 수 있습니다. Safari에서 영구 쿠키에 사용자 인증서가 있는 경우 Jabber가 SSO 토큰을 지울 때 쿠키를 사용하여 사용자가 인증서를 다시 입력하지 않도록 합니다.

iOS 시스템이 iPhone 및 iPad용 Cisco Jabber를 백그라운드에서 중지하는 경우 Jabber에서 사용자가 암호를 입력하지 않고 자동으로 로그인 할 수 있습니다.

필수 브라우저

브라우저와 클라이언트 간에 IdP에 의해 발행된 인증 쿠키를 공유하려면 다음 브라우저 중 하나를 기본 브라우저로 지정합니다.

제품	필수 브라우저
Windows용 Cisco Jabber	Internet Explorer
Mac용 Cisco Jabber	Safari
iPhone 및 iPad용 Cisco Jabber	Safari
Android용 Cisco Jabber	Chrome 또는 Internet Explorer

참고 내장 브라우저는 Android용 Cisco Jabber에서 SSO를 사용할 때 쿠키를 외부 브라우저와 공유할 수 없습니다.

싱글 사인온 및 **Remote Access**

모바일 및 Remote Access용 Expressway를 사용하여 회사 방화벽 외부에서 자격 증명을 제공하는 사용자의 경우 단일 로그인에는 다음과 같은 제한 사항이 있습니다.

- SSO(싱글 사인온)는 Cisco Expressway 8.5 및 Cisco Unified Communications Manager 릴리스 10.5.2 이상에서 사용할 수 있습니다. 두 가지 모두에서 SSO를 활성화하거나 비활성화해야 합니다.
- 보안 전화기에서 모바일 및 Remote Access용 Expressway를 통해 SSO를 사용할 수 없습니다.
- 사용 된 ID 공급자에는 동일한 내부 및 외부 URL이 있어야 합니다. URL이 다른 경우 회사 방화벽 내부와 외부 사이에서 변경할 때 사용자에게 다시 로그인하라는 메시지가 표시될 수 있습니다.

Location awareness for Enhanced 911 (Nomadic E911) support

To comply with the Ray Baum's Act in the United States, Jabber must report location information for emergency calls after January 6, 2022. *Nomadic E911* is the ability to report your actual location as you move. If you operate in the United States, almost all enterprises must enable this feature.

Wireless on-premises network

We already report wireless location when it's over on-premises network through Cisco Emergency Responder (CER) to your local Public Safety Answering Point (PSAP).

Other networks

We now support nomadic E911 as follows:

- **Mobile phones (Android and iPhone)**—Jabber always launches the native phone app to place the emergency call.
- **Desktop client and tablets**—If you oeprate in the United States, install the RedSky MyE911 app. Use MyE911 to report location information to your local PSAP.

Note You must create a RedSky account.

Server requirement

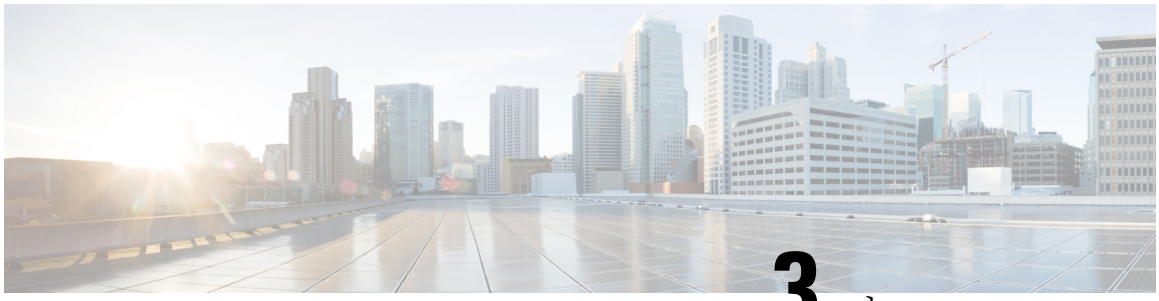
To pick up the routing logic change, update Cisco Emergency Responder (CER) to Release 12.5 SU6 or Release 14 SU2.

Note If you want the change before updating CER, you'll need to install a COP file for CER.

More information

See the following resources:

- "Wireless Location Monitoring Service" in the Feature Configuration for Cisco Jabber
- Cisco Emergency Responder Administration Guide
- RedSky E911 for Cisco



3 장

사용자 관리

Jabber ID

Cisco Jabber는 Jabber ID를 사용하여 연락처 소스에서 연락처 정보를 식별합니다.

기본 Jabber ID는 사용자 ID 및 프레즌스 도메인을 사용하여 생성됩니다.

예를 들어, Adam McKenzie의 사용자 ID가 `amckenzie`이고 해당 도메인이 `example.com`이며 Jabber ID가 `amckenzie@example.com`입니다.

Cisco Jabber 사용자 ID 또는 이메일 주소에서 다음 문자가 지원됩니다.

- 밑줄 문자(A ~ Z)
- 소문자(a ~ z)
- 숫자(0-9)
- 마침표(.)
- 하이픈(-)
- 밑줄(_)
- 물결표(~)
- 해시태그(#)

연락처 목록을 채울 때 클라이언트는 Jabber ID를 사용하여 연락처 소스를 검색하여 연락처를 확인하고 이름, 성 및 기타 연락처 정보를 표시합니다.

IM 주소 체계

Cisco Jabber 10.6 이상에서는 도메인이 동일한 프레즌스 아키텍처에 있는 경우(예: example-us.com 및 example-uk.com 사용자) 온프레미스 구축에 대한 다중 프레즌스 도메인 아키텍처 모델을 지원합니다. Cisco Jabber는 Cisco Unified Communications Manager IM and Presence 10.x 이상을 사용하여 유연한 IM 주소 체계를 지원합니다. IM 주소 체계는 Cisco Jabber 사용자를 식별하는 Jabber ID입니다.

다중 도메인 모델을 지원하려면 구축의 모든 구성 요소에 다음 버전이 필요합니다.

- Cisco Unified Communications IM and Presence 서버 노드 및 통화 제어 노드 버전 10.x 이상.
- Windows, Mac, IOS 및 Android 버전 10.6 이상을 실행 중인 모든 클라이언트.

다음과 같은 시나리오에서 여러 도메인 아키텍처를 사용하는 Cisco Jabber만 구축합니다.

- Cisco Jabber 10.6 이상 버전은 모든 플랫폼(Windows, Mac, IOS 및 Android(DX 시리즈와 같은 Android 기반 IP 전화기 포함))에서 조직의 모든 사용자에게 새 설치로 구축됩니다.
- 프레즌스 서버에서 도메인 또는 IM 주소를 변경하기 전에 Cisco Jabber는 모든 플랫폼(Windows, Mac, IOS 및 Android(DX 시리즈와 같은 Android 기반 IP 전화기 포함))에서 모든 사용자에 대해 버전 10.6 이상으로 업그레이드됩니다.

고급 프레즌스 설정에서 사용 가능한 IM 주소 체계는 다음과 같습니다.

- UserID@[기본 도메인]
- 디렉토리 URI

UserID@[기본 도메인**]**

사용자 ID 필드는 LDAP 필드에 매핑됩니다. 이는 기본 IM 주소 체계입니다.

예를 들어, 사용자 Anita Perez에 계정 이름 aperez가 있고 사용자 ID 필드는 sAMAccountName LDAP 필드에 매핑됩니다. 사용된 주소 체계는 aperez@example.com입니다.

디렉토리 **URI**

디렉터리 URI가 메일 또는 **msrtcsip-primaryuseraddress** LDAP 필드에 매핑됩니다. 이 옵션은 인증을 위해 사용자 ID와 관계 없는 체계를 제공합니다.

예를 들어, 사용자 Anita Perez에 계정 이름 aperez가 있고, 메일 필드가 Anita.Perez@domain.com이며 사용되는 주소 체계가 Anita.Perez@domain.com입니다.

Jabber ID를 사용한 서비스 검색

서비스 검색은 `[userid]@[domain.com]` 형식으로 입력한 Jabber ID를 사용하 고 기본적으로 Jabber ID의 `domain.com` 부분을 추출하여 사용 가능한 서비스를 검색합니다. 프레즌스 도메인이 서비스 검색 도메인과 동일하지 않은 구축의 경우, 다음과 같이 설치 중에 서비스 검색 도메인 정보를 포함할 수 있습니다.

- Windows용 Cisco Jabber에서는 이 작업이 `SERVICES_DOMAIN` 명령줄 인수를 사용하여 수행됩니다.
- Mac용 Cisco Jabber, Android용 Cisco Jabber 또는 iPhone 및 iPad용 Cisco Jabber의 경우 URL 구성에 사용된 `ServicesDomain` 매개 변수를 사용하여 서비스 검색 도메인을 설정할 수 있습니다.

.

SIP URI

SIP URI는 각 사용자와 연결됩니다. SIP URI는 이메일 주소, IMAddress 또는 UPN일 수 있습니다.

SIP URI는 Cisco Unified Communications Manager의 디렉터리 URI 필드를 사용하여 구성됩니다. 사용 가능한 옵션은 다음과 같습니다.

- mail
- msRTCSIP-primaryuseraddress

사용자는 SIP URI를 입력하여 연락처를 검색하고 연락처에 전화를 걸 수 있습니다.

LDAP 사용자 ID

디렉터리 소스에서 Cisco Unified Communications Manager로 동기화되면 디렉터리에 있는 속성에서 사용자 ID가 채워집니다. 사용자 ID를 보유하는 기본 속성은 `sAMAccountName`입니다.

페더레이션에 대한 사용자 ID 계획

페더레이션을 위해 Cisco Jabber는 연락처 검색 중에 각 사용자의 연락처 ID 또는 사용자 ID가 연락처를 확인하도록 요구합니다.

SipUri 매개 변수의 사용자 ID에 대한 속성을 설정합니다. 기본값은 `msRTCSIP-PrimaryUserAddress`입니다. 사용자 ID에서 제거할 접두사가 있는 경우 UriPrefix 매개 변수에 값을 설정할 수 있습니다. *Cisco Jabber*에 대한 매개 변수 참조 설명서의 최신 버전을 참조하십시오.

사용자 연락처 사진에 대한 프록시 주소

Cisco Jabber는 사진 서버에 액세스하여 연락처 사진을 검색합니다. 네트워크 구성에 웹 프록시가 포함되어 있는 경우에는 Cisco Jabber가 사진 서버에 액세스할 수 있는지 확인해야 합니다.

인증

Cisco Unified Communications Manager LDAP 인증

디렉터리 서버를 인증하도록 Cisco Unified Communications Manager에 LDAP 인증이 구성되어 있습니다.

사용자가 클라이언트에 로그인하면 프레즌스 서버가 해당 인증을 Cisco Unified Communications Manager로 라우팅합니다. 그런 다음 Cisco Unified Communications Manager는 디렉터리 서버에 대한 인증을 프록시합니다.

Webex Messenger 로그인 인증

Webex Messenger 인증은 Webex 관리 도구를 사용하여 구성됩니다.

사용자가 클라이언트에 로그인하면 정보가 Webex Messenger로 전송되고 인증 토큰이 클라이언트로 다시 전송됩니다.

SSO(Single Sign-On) 인증

단일 로그인 인증은 ID 제공자(IdP) 및 서비스를 사용하여 구성됩니다.

사용자가 클라이언트에 로그인하면 정보가 IdP로 전송되고 자격 증명이 승인되면 인증 토큰이 Cisco Jabber로 다시 전송됩니다.

iPhone 및 iPad용 Cisco Jabber에 대한 인증서 기반 인증

Cisco Jabber는 클라이언트 인증서를 통해 IdP 서버에서 인증합니다. 이 인증서 인증을 사용하면 사용자 자격 증명을 입력하지 않고도 서버에 로그인할 수 있습니다. 클라이언트는 Safari 프레임워크를 사용하여 이 기능을 구현합니다.

필요조건

- Cisco Unified Communications Manager 11.5, IM and Presence 서비스 11.5, Cisco Unity Connection 11.5 이상.
- 모바일 및 Remote Access용 Expressway 8.9 이상
- 통합 커뮤니케이션 인프라에 활성화된 SSO.

- 모든 서버 인증서는 Cisco Unified Communications Manager, IM and Presence 서비스, Cisco Unity Connection 및 IdP 서버를 포함하여 CA 서명됩니다. iOS 장치에서 OS의 신뢰할 수 있는 인증 기관을 사용하는 경우 Cisco Jabber 앱을 설치하기 전에 CA 인증서를 설치합니다.
- Cisco Unified Communications Manager의 SSO에 대한 기본 브라우저(임베디드 Safari)를 구성합니다. 자세한 내용은 *Cisco Jabber*의 온프레미스 구축에서 인증서 기반 SSO 인증에 대한 섹션을 참조하십시오.
- 모바일 및 Remote Access용 Expressway 서버의 SSO에 대한 기본 브라우저(임베디드 Safari)를 구성합니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html의 Cisco Expressway 설치 설명서를 참고하십시오.

EMM 솔루션을 통해 iOS 장치에 Cisco 인증서를 구축할 수 있습니다.

권장 사항 - Cisco는 iOS 장치에 인증서를 구축하는 데 EMM 솔루션을 사용할 것을 권장합니다.

Android용 Cisco Jabber에 대한 인증서 기반 인증

Cisco Jabber는 클라이언트 인증서를 사용하여 싱글 사인온 서버(Webex Messenger 및 온프레미스)에 로그인합니다.

요구 사항

- Android OS 5.0 이상
- SSO(Single Sign-On)가 활성화됨
- Jabber 클라이언트는 MRA(Mobile and Remote Access) 및 비 MRA 구축 모드를 통해 지원됩니다.
- Jabber는 Android 7.0 이상에서 잘못된 인증서에 대한 알림을 Android OS에 설치된 사용자 정의 CA 서명 인증서에 대해서만 표시합니다. Android 7.0을 대상으로 하는 앱은 시스템에서 제공하는 인증서만 신뢰하고 더 이상 사용자 추가 인증 기관을 신뢰하지 않습니다.

인증서 구축

Cisco는 Android 장치에 인증서를 구축하는 데 EMM 솔루션을 사용하는 것을 권장합니다.

음성 메일 인증

사용자가 Cisco Unity Connection에 있어야 합니다. Cisco Unity Connection은 다중 인증 유형을 지원합니다. Cisco Unified Communications Manager 및 Cisco Unity Connection이 동일한 인증을 사용하는 경우, 동일한 자격 증명을 사용하도록 Cisco Jabber를 구성하는 것이 좋습니다.

OAuth

Cisco Jabber에서 OAuth 프로토콜을 사용하여 서비스에 대한 사용자 액세스 권한을 인증하도록 설정할 수 있습니다. 사용자가 OAuth 사용 환경에 로그인하면 로그인할 때마다 자격 증명을 입력할 필요

가 없습니다. 그러나 서버가 OAuth를 지원하지 않는 경우 Jabber가 적절하게 작동하지 않을 수 있습니다.

Cisco Unified Communication Manager 12.5 이상을 사용하는 경우 SIP OAuth를 활성화할 수도 있습니다. Jabber가 SIP에 대한 권한을 부여하여 Jabber가 TLS를 통해 SIP 서비스에 연결할 수 있도록 합니다. 또한 Jabber에서 보안 연결(sRTP)을 통해 미디어를 전송할 수 있습니다. SIP OAuth는 보안 SIP 및 미디어를 활성화하는 데 CAPF 등록이 더 이상 필요하지 않음을 의미합니다.

필수 조건:

- 작동하도록 구축된 경우 이러한 모든 구성 요소에 대해 OAuth 새로 고침 토큰이 설정되어 있어야 합니다.
- Cisco Unified Communication Manager, Cisco Unified Communication Manager Instant Messaging and Presence 및 Cisco Unity Connection은 버전 11.5(SU3) 또는 12.0 이어야 합니다.
- 모바일 및 Remote Access용 Cisco Expressway 버전 X 8.10 이상
- SIP OAuth의 경우: Cisco Unified Communication Manager 12.5 이상, 모바일 및 Remote Access용 Cisco Expresswayversion X12.5 이상.

OAuth를 구성하기 전에 다음에 해당하는 구축 유형을 확인하십시오.

- 로컬 인증 구축을 사용하는 경우 IdP 서버가 필요하지 않으며 Cisco Unified Communication Manager가 인증을 담당합니다.
- OAuth를 구성하거나 구성하지 않은 상태로 OAuth를 설정할 수 있습니다. SSO를 사용하는 경우 모든 서비스에 대해 이 기능이 활성화되어 있는지 확인합니다. SSO가 활성화된 구축을 사용하는 경우 IdP 서버를 구축하고 IdP 서버가 인증을 담당합니다.

사용자를 위해 다음 서비스에서 OAuth를 활성화할 수 있습니다.

- Cisco Unified Communications Manager
- Cisco Expressway
- Cisco Unity Connection

이러한 서버에서 OAuth는 기본적으로 비활성화되어 있습니다. 이러한 서버에서 OAuth를 활성화하려면 다음을 수행합니다.

- Cisco Unified Communications Manager 및 Cisco Unity Connection 서버의 경우 엔터프라이즈 매개변수 구성 > 새로 고침 로그인 흐름을 사용한 **OAuth**로 이동합니다.
- Cisco Expressway-C의 경우 구성 통합 커뮤니케이션 > 구성 새로 고침을 사용하여 **OAuth** 토큰으로 인증으로 이동합니다.

이러한 서버에서 OAuth가 활성화 또는 비활성화되면 Jabber가 구성 다시 가져오기 간격 동안 이를 식별하고 사용자가 Jabber에서 로그아웃했다가 로그인하도록 합니다.

로그아웃하는 동안 Jabber는 캐시에 저장된 사용자 자격 증명을 삭제한 다음 사용자가 일반 로그인 흐름으로 로그인한 다음, Jabber가 모든 구성 정보를 먼저 가져온 다음 사용자가 Jabber 서비스에 액세스할 수 있도록 합니다.

Cisco Unified Communication Manager에서 OAuth를 구성하려면:

1. **Cisco Unified Communication Manager Admin** > 시스템 > 엔터프라이즈 매개 변수 > **SSO** 구성으로 이동합니다.
2. **O-Auth** 액세스 토큰 만료 타이머**(**분**)**를 원하는 값으로 설정합니다.
3. **O-Auth** 새로 고침 토큰 만료 타이머**(**일**)**를 원하는 값으로 설정합니다.
4. 저장 버튼을 클릭합니다.

Cisco Expressway에서 OAuth를 구성하려면:

1. 구성 > 통합 커뮤니케이션 > 구성 > **MRA** 액세스 제어로 이동합니다.
2. **O-Auth** 로컬 인증을 켜기로 설정합니다.

Cisco Unity에서 OAuth를 구성하려면:

1. **AuthZ** 서버로 이동하고 새로 추가를 선택합니다.
2. 모든 필드에 세부 정보를 입력하 고 인증서 오류 무시를 선택합니다.
3. 저장을 클릭합니다.

제한 사항

Jabber가 자동 침입 방지를 트리거합니다**.**

조건:

- 모바일 및 Remote Access용 Expressway 구축은 OAuth 토큰(새로 고침 토큰 포함 또는 제외)으로 인증되도록 구성됩니다.
- Jabber 사용자 액세스 토큰이 만료되었습니다.

Jabber는 다음 중 하나를 수행합니다.

- 데스크톱 최대 절전 모드에서 재시작
- 네트워크 연결 복구
- 몇 시간 동안 로그아웃한 후 빠른 로그인 시도

동작(Behavior):

- 일부 Jabber 모듈은 만료된 액세스 토큰을 사용하여 Expressway-E에서 인증을 시도합니다.
- Expressway-E는 (올바르게) 이러한 요청을 거부합니다.
- 특정 Jabber 클라이언트에서 이러한 요청이 6개 이상 있는 경우 Expressway-E는 10분(기본적으로) 동안 해당 IP 주소를 차단합니다.

증상:

영향을 받는 Jabber 클라이언트의 IP 주소는 HTTP 프록시 인증 실패 범주에 있는 Expressway-E의 차단된 주소 목록에 추가됩니다. 이 내용은 시스템 > 보호 > 자동 탐지 > 차단된 주소에서 확인할 수 있습니다.

대체 방법:

두 가지 방법으로 이 문제를 해결할 수 있습니다. 특정 범주에 대한 탐색 임계값을 늘리거나 영향을 받는 클라이언트에 대한 예외를 만들 수 있습니다. 여기서는 사용자 환경에서 예외가 실용적이 지 않을 수 있으므로 임계값 옵션에 대해 설명합니다.

1. 시스템 > 보호 > 자동 탐지 > 구성으로 이동합니다.
2. **HTTP** 프록시 인증 실패를 클릭합니다.
3. 트리거 수준을 5에서 10으로 변경합니다. 10은 만료된 토큰을 제공하는 Jabber 모듈을 허용하기에 충분해야 합니다.
4. 구성을 저장하여 즉시 적용합니다.
5. 영향을 받는 클라이언트의 차단을 해제합니다.

여러 리소스 로그인

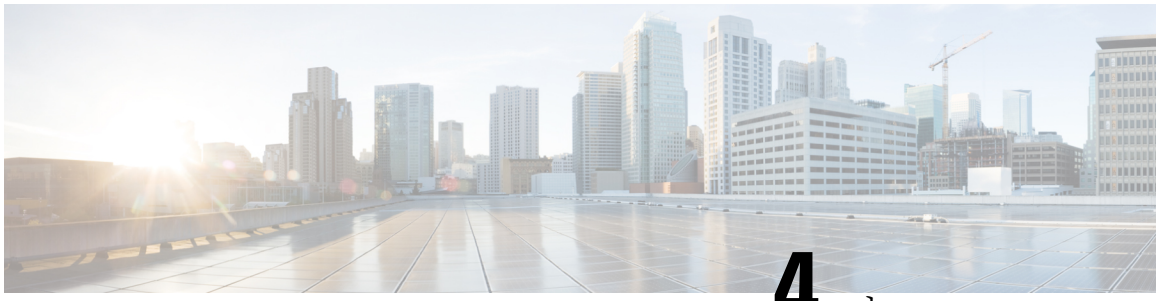
모든 Cisco Jabber 클라이언트는 사용자가 시스템에 로그인할 때 다음 중앙 IM and Presence 서비스 노드 중 하나에 등록됩니다. 이 노드는 IM and Presence 서비스 환경의 가용성, 연락처 목록 및 기타 측면을 추적합니다.

- 온프레미스 구축: Cisco Unified Communications Manager IM and Presence Service
- 클라우드 구축: Webex.

이 IM and Presence 서비스 노드는 각 고유 네트워크 사용자와 연결된 등록된 모든 클라이언트를 다음 순서로 추적합니다.

1. 두 사용자 간에 새 IM 세션이 시작되면, 첫 번째 들어오는 메시지는 수신 사용자의 등록된 모든 클라이언트로 브로드 캐스팅됩니다.
2. 그런 다음 IM and Presence 서비스 노드는 등록된 클라이언트 중 하나의 첫 번째 응답을 기다립니다.
3. 응답하는 첫 번째 클라이언트는 사용자가 다른 등록된 클라이언트를 사용하여 응답을 시작할 때까지 나머지 수신 메시지를 수신합니다.
4. 그런 다음 노드는 후속 메시지를 이 새 클라이언트로 재 라우팅합니다.

참고 사용자가 여러 장치에 로그인되어 있을 때 활성 리소스가 없는 경우 우선 순위가 가장 높은 클라이언트에게 우선 순위가 부여됩니다. 모든 장치에서 프레즌스 상태 우선 순위가 동일하면 사용자가 로그인한 최신 클라이언트에게 우선 순위가 부여됩니다.



4 장

서비스 검색

클라이언트가 서비스에 연결하는 방법

서비스에 연결하기 위해 Cisco Jabber에는 다음 정보가 필요합니다.

- 사용자가 클라이언트에 로그인할 수 있게 해주는 인증 소스.
- 서비스 위치.

다음 방법을 사용하여 해당 정보를 클라이언트에 제공할 수 있습니다.

URL 구성

사용자에게 관리자의 이메일이 전송됩니다. 이메일에는 서비스 검색에 필요한 도메인을 구성하는 URL이 포함되어 있습니다.

서비스 검색

클라이언트가 자동으로 서비스를 찾아 연결합니다.

수동 연결 설정

사용자는 클라이언트 사용자 인터페이스에 연결 설정을 수동으로 입력합니다.

Cisco Webex 플랫폼 서비스 검색

Cisco Jabber는 사용자가 팀 메시징 모드에 대해 활성화되었는지 여부를 확인하기 위해 HTTPS 요청을 Cisco Webex 플랫폼 서비스에 전송합니다. 사용자가 팀 메시징을 활성화한 경우 Jabber는 계속해서 사용 가능한 온프레미스 서비스를 확인합니다.

Cisco Webex Messenger 서비스 검색

Cisco Jabber는 Webex Messenger 서비스의 CAS URL로 클라우드 HTTP 요청을 전송합니다. Cisco Jabber는 Webex Messenger 서비스를 사용하여 사용자를 인증하고 사용 가능한 서비스에 연결합니다.

서비스는 Webex 관리 도구에 구성되어 있습니다.

Cisco 클러스터 간 조회 서비스

여러 Cisco Unified Communications Manager 클러스터가 있는 환경에서는 ILS(Intercluster Lookup Service)를 구성합니다. ILS를 사용하면 클라이언트가 사용자 홈 클러스터를 찾고 서비스를 검색할 수 있습니다.

모바일 및 Remote Access용 Expressway 서비스 검색

모바일 및 Remote Access용 Expressway는 원격 사용자 액세스 서비스를 활성화합니다.

클라이언트는 SRV 레코드에 대해 이름 서버를 쿼리합니다. `_collab-edge` SRV 레코드를 사용하여 클라이언트가 모바일 및 Remote Access용 Expressway를 통해 내부 네트워크에 연결을 시도하고 서비스를 검색합니다.

이름 서버는 `_collab-edge` SRV 레코드를 반환하고 클라이언트는 Cisco Expressway-E 서버의 위치를 가져옵니다. 그런 다음 Cisco Expressway-E 서버는 내부 이름 서버에 대한 쿼리 결과를 클라이언트에 제공합니다. 이것은 `_cisco-uds` SRV 레코드를 포함해야 하며, 클라이언트는 Cisco Unified Communication Manager에서 서비스 프로파일을 검색합니다.

참고 음성 서비스 도메인이 로그인 도메인과 동일한 경우 MRA에 대해 voiceservicesdomain을 구성하지 마십시오. 도메인이 다른 경우에만 voiceservicesdomain을 구성하십시오.

권장 연결 방법

서비스에 연결하는 데 필요한 정보를 클라이언트에 제공하기 위해 사용해야 하는 방법은 구축 유형, 서버 버전 및 제품 모드에 따라 달라집니다. 다음 표에서는 다양한 구축 방법과 클라이언트에 필요한 정보를 제공하는 방법을 중점적으로 설명합니다.

표 *3:* 온프레미스 구축 ***Windows***용 ***Cisco Jabber***

제품 모드	서버 버전	검색 방법	비 **DNS SRV** 레코드 방법
전체 UC(기본 모드)	릴리스 9.1.2 이상: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	_cisco-uds에 대한 DNS SRV 요청.<domain>	다음과 같은 설치 프로그램 스위치 및 값을 사용합니다. • AUTHENTICATOR=CUCM • TFTP=<tftp_server_address>
IM 전용(기본 모드)	릴리스 9 이상: Cisco Unified Communications Manager IM and Presence Service	_cisco-uds에 대한 DNS SRV 요청.<domain>	다음과 같은 설치 프로그램 스위치 및 값을 사용합니다. • AUTHENTICATOR=CUP • CUP_ADDRESS=<presence_server_address>
전화기 모드	릴리스 9 이상: Cisco Unified Communications Manager	_cisco-uds에 대한 DNS SRV 요청.<domain>	다음과 같은 설치 프로그램 스위치 및 값을 사용합니다. • AUTHENTICATOR=CUCM • TFTP=<CUCM_address> • CCMCIP=<CUCM_address> • PRODUCT_MODE=phone_mode 이 구축 방법을 사용하는 경우 고가용성이 지원되지 않습니다.

Cisco Unified Communications Manager 9.x 이전 릴리스 - Cisco Extension Mobility을 활성화하는 경우, CCMCIP에 사용되는 Cisco Unified Communications Manager 노드에서 `Cisco Extension Mobility` 서비스를 활성화해야 합니다. Cisco Extension Mobility에 대한 자세한 내용은 Cisco Unified Communications Manager 릴리스의 기능 및 서비스 설명서를 참조하십시오.

참고 Cisco Jabber 릴리스 9.6 이상에서는 `_cuplogin` DNS SRV 요청을 사용하여 전체 통합 커뮤니케이션 및 IM 전용 서비스를 검색할 수 있지만 `_cisco-uds` 요청이 있는 경우 우선 적용됩니다.

사용자가 새 설치의 처음 로그인 중에 이메일 화면을 무시하도록 하려면 SERVICES_DOMAIN 설치 관리자 스위치를 사용하여 DNS 레코드가 있는 도메인의 값을 지정합니다.

표 *4:* 온프레미스 구축 ***Mac***용 ***Cisco Jabber***

제품 모드	서버 버전	검색 방법
전체 UC(기본 모드)	릴리스 9 이상: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	_cisco-uds에 대한 DNS SRV 요청.<domain>

표 *5:* ***Android***용 ***Cisco Jabber*** 및 ***iPhone*** 및 ***iPad***용 ***Cisco Jabber***용 온프레미스 구축

제품 모드	서버 버전	검색 방법
전체 UC(기본 모드)	릴리스 9 이상: • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service	_cisco-uds.<domain> 및 _cuplogin.<domain>에 대한 DNS SRV 요청
IM 전용(기본 모드)	릴리스 9 이상: Cisco Unified Communications Manager IM and Presence Service	_cisco-uds.<domain> 및 _cuplogin.<domain>에 대한 DNS SRV 요청
전화기 모드	릴리스 9 이상: Cisco Unified Communications Manager	_cisco-uds에 대한 DNS SRV 요청.<domain>

참고 Cisco Unified Communications Manager 버전 9 이상에서는 _cuplogin DNS SRV 요청을 사용하여 전체 통합 커뮤니케이션 및 IM 전용 서비스를 검색할 수 있지만 _cisco-uds 요청이 있는 경우 우선 적용됩니다.

표 *6:* 하이브리드 클라우드 기반 구축

서버 버전	연결 방법
Webex Messenger	https://loginp.webexconnect.com/cas/FederatedSSO?org=<domain>에 대한 HTTPS 요청
Cisco Webex 플랫폼 서비스	atlas-a.wbx2.com에 대한 HTTPS 요청

표 *7:* 클라우드 기반 구축

구축 유형	연결 방법
SSO(Single Sign-On) 활성화	Webex 관리 도구 SSO_ORG_DOMAIN 인수를 설정하는 부트스트랩 파일.
SSO 활성화되지 않음	Webex 관리 도구

인증 소스

인증 소스 또는 인증자를 사용하여 사용자가 클라이언트에 로그인할 수 있습니다.

인증의 세 가지 가능한 소스는 다음과 같습니다.

- Cisco Unified Communications Manager IM and Presence - 전체 UC 또는 IM 전용에서 온프레미스 구축.
- Cisco Unified Communications Manager - 전화기 모드에서 온프레미스 구축
- Webex Messenger 서비스 - 클라우드 기반 또는 하이브리드 클라우드 기반 구축.
- Cisco Webex 플랫폼 서비스— 클라우드 기반 또는 하이브리드 클라우드 기반 구축.

클라이언트가 서비스를 찾는 방법

다음 단계에서는 클라이언트가 SRV 레코드를 사용하여 서비스를 찾는 방법을 설명합니다.

1. 클라이언트의 호스트 컴퓨터 또는 장치에서 네트워크 연결을 가져옵니다.

   클라이언트의 호스트 컴퓨터가 네트워크 연결을 사용할 때 DHCP 설정에서 DNS(Domain Name System) 이름 서버의 주소도 가져옵니다.

2. 사용자는 첫 번째 로그인 중에 서비스를 검색하기 위해 다음 방법 중 하나를 사용합니다.
   - 수동 - 사용자가 Cisco Jabber를 시작하고 시작 화면에서 이메일 유사 주소를 입력합니다.
   - URL 구성 - URL 구성을 사용하면 사용자가 이메일을 수동으로 입력하지 않고 링크를 클릭하여 Cisco Jabber를 교차 실행할 수 있습니다.
   - EMM(Enterprise Mobility Management)을 사용한 모바일 구성 - URL 구성 대신 Android용 Cisco Jabber의 Android for Work 및 iPhone 및 iPad용 Cisco Jabber의 Apple Managed App 구성으로 EMM(Enterprise Mobility Management)을 사용하여 Cisco Jabber를 구성할 수 있습니다. URL 구성 링크를 만드는 데 사용되는 동일한 매개 변수를 EMM 콘솔에서 구성해야 합니다.

   URL 구성 링크를 만들려면 다음을 포함해야 합니다.

   - ServicesDomain - Cisco Jabber가 서비스 검색에 사용하는 도메인입니다.

- VoiceServicesDomain - 하이브리드 구축의 경우 Cisco Jabber가 DNS SRV 레코드를 검색하는 데 사용하는 도메인은 Cisco Jabber 도메인을 검색하는 데 사용되는 ServicesDomain 도메인과 다를 수 있습니다.
- ServiceDiscoveryExcludedServices - 특정 구축 시나리오에서는 서비스 검색 프로세스에서 서비스를 제외할 수 있습니다. 이러한 값은 다음을 조합하여 사용할 수 있습니다.
  - WEBEX
  - CUCM

참고 세 매개 변수가 모두 포함된 경우에는 서비스 검색이 발생하지 않으며 사용자에게 연결 설정을 수동으로 입력하 라는 메시지가 표시됩니다.

다음 형식으로 링크를 생성합니다.

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
```

예:

- `ciscojabber://provision?servicesdomain=example.com`
- `ciscojabber://provision?servicesdomain=example.com &VoiceServicesDomain=VoiceServices.example.com`
- `ciscojabber://provision?servicesdomain=example.com &ServiceDiscoveryExcludedServices=WEBEX,CUCM`

이메일 또는 웹 사이트를 사용하여 사용자에 대한 링크를 제공합니다.

참고 조직에서 교차 시작 전용 프로토콜이나 사용자 정의 링크를 지원하는 메일 애플리케이션을 사용하는 경우 이메일을 사용하여 사용자에게 링크를 제공할 수 있습니다. 그렇지 않으면 웹 사이트를 사용하는 사용자에게 링크를 제공합니다.

3. 클라이언트는 DHCP 설정에서 DNS 이름 서버의 주소를 가져옵니다.
4. 클라이언트는 HTTP 쿼리를 Webex Messenger 서비스의 CAS(중앙 인증 서비스) URL로 발급합니다.

   이 쿼리를 사용하면 클라이언트가 유효한 Webex 도메인인지 여부를 확인할 수 있습니다.
5. 클라이언트는 우선 순위 순으로 다음 SRV 레코드에 대한 이름 서버를 쿼리합니다.
   - `_cisco-uds`
   - `_collab-edge`

참고 클라이언트는 후속 시작 시 로드되는 DNS 쿼리 결과를 캐시합니다.

참고 클라이언트는 후속 시작 시 로드되는 DNS 쿼리 결과를 캐시합니다.

다음은 SRV 레코드 입력의 예입니다.

```
_cisco_uds._tcp.DOMAIN SRV service location:
 priority = 0
 weight = 0
 port = 8443
 svr hostname=192.168.0.26
```

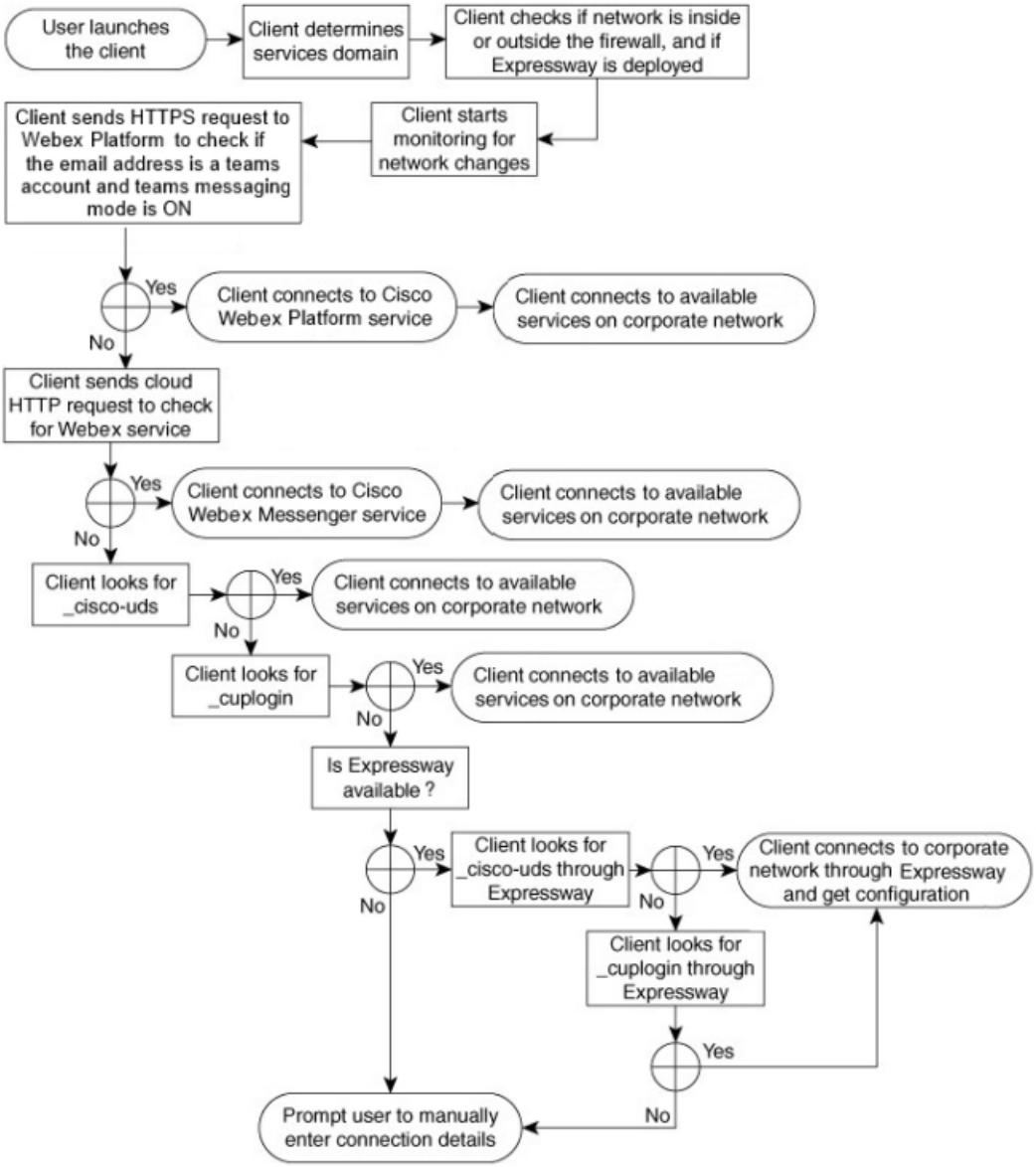
방법 1: 서비스 검색

Cisco Jabber에서 사용자에게 제공되는 서비스 및 기능을 검색하는 방법에 이 방법을 사용하는 것이 좋습니다. 서비스를 검색하면 클라이언트가 DNS 서비스(SRV) 레코드를 사용하여 클라이언트에서 사용할 수 있는 서비스를 결정하는 것을 의미합니다.

클라이언트에서 사용 가능한 서비스를 검색하는 방법

다음 그림은 클라이언트가 서비스에 연결하는 데 사용하는 흐름을 보여줍니다.

그림 *5:* 서비스 검색을 위한 로그인 흐름



클라이언트는 사용 가능한 서비스를 검색하기 위해 다음 작업을 수행합니다.

1. 네트워크가 방화벽 내부 또는 외부에 있고, 모바일 및 Remote Access용 Expressway가 구축되었는지 확인합니다. 클라이언트가 이름 서버에 쿼리를 전송하여 SRV(DNS 서비스) 레코드를 얻습니다.
2. 네트워크 변경 사항에 대한 모니터링을 시작합니다.

   모바일 및 Remote Access용 Expressway를 구축할 때 클라이언트는 네트워크를 모니터링하여 네트워크가 방화벽 내부 또는 외부에서 변경될 경우 다시 연결할 수 있는지 확인합니다.

3. Jabber가 팀 메시징 모드로 전환되는지 여부를 결정하기 위해 Cisco Webex 플랫폼 서비스에 여러 HTTPS 요청을 발행합니다. 이 요청은 사용자의 이메일 주소를 확인하여 사용자가 Webex Control Hub에서 팀 메시징을 위해 활성화되었는지 여부를 확인합니다.
4. Webex Messenger 서비스의 CAS URL에 대한 HTTP 쿼리를 발행합니다.

   이 쿼리를 사용하면 클라이언트가 유효한 Webex 도메인인지 여부를 확인할 수 있습니다.

   모바일 및 Remote Access용 Expressway를 구축하는 경우 클라이언트가 Webex Messenger 서비스에 연결하고 모바일 및 Remote Access용 Expressway를 사용하여 Cisco Unified Communications Manager에 연결합니다. 클라이언트가 처음 시작될 때 전화 서비스 연결 오류가 표시되고 클라이언트 옵션 화면에 자격 증명을 입력해야 하며, 이후 시작 시에는 캐시된 정보가 사용됩니다.
5. 이전 쿼리의 캐시에 레코드가 없는 경우, SRV(DNS 서비스) 레코드를 가져오기 위해 이름 서버에 쿼리합니다.

   이 쿼리를 사용하면 클라이언트에서 다음 작업을 수행할 수 있습니다.

   - 사용할 수 있는 서비스를 확인합니다.
   - 모바일 및 Remote Access용 Expressway를 통해 회사 네트워크에 연결할 수 있는지 확인합니다.

클라이언트가 **Cisco Webex Messenger** 서비스에 대한 **HTTP** 쿼리 발행

SRV 레코드에 대한 이름 서버를 쿼리하여 사용 가능한 서비스를 찾을 수 있을뿐만 아니라, Cisco Jabber에서 Webex Messenger 서비스에 대한 HTTP 쿼리를 CAS URL로 전송합니다. 이 요청을 통해 클라이언트에서 클라우드 기반 구축을 결정하고 Webex Messenger 서비스에 대한 사용자를 인증할 수 있습니다.

클라이언트가 사용자로부터 서비스 도메인을 가져오는 경우 다음 HTTP 쿼리에 해당 도메인을 추가합니다.

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=
```

예를 들어, 클라이언트가 사용자의 서비스 도메인으로 `example.com`을 가져오면 다음 쿼리를 발행합니다.

```
https://loginp.webexconnect.com/cas/FederatedSSO?org=example.com
```

이 쿼리는 클라이언트에서 서비스 도메인이 유효한 Webex 도메인인지 확인하는 데 사용하는 XML 응답을 반환합니다.

클라이언트에서 서비스 도메인이 유효한 Webex 도메인인지 확인하면 사용자에게 Webex 자격 증명을 입력하라는 메시지가 표시됩니다. 그러면 클라이언트가 Webex Messenger 서비스에 인증되고 Webex 조직 관리자에 구성된 UC 서비스와 구성을 검색합니다.

클라이언트에서 서비스 도메인이 유효한 Webex 도메인이 아닌 것으로 판단하면 쿼리 결과를 이름 서버에 사용하여 사용 가능한 서비스를 찾습니다.

클라이언트가 HTTP 요청을 CAS URL로 보낼 때 구성된 시스템 프록시를 사용합니다.

자세한 내용은 *Cisco Jabber* 구축 및 설치 설명서의 프록시 설정 구성 섹션을 참조하십시오.

클라이언트가 이름 서버 쿼리

클라이언트가 이름 서버에 쿼리하면 SRV 레코드에 대한 별도의 동시 요청이 이름 서버에 전송됩니다.

클라이언트는 다음 SRV 레코드를 다음 순서로 요청합니다.

- `_cisco-uds`
- `_collab-edge`

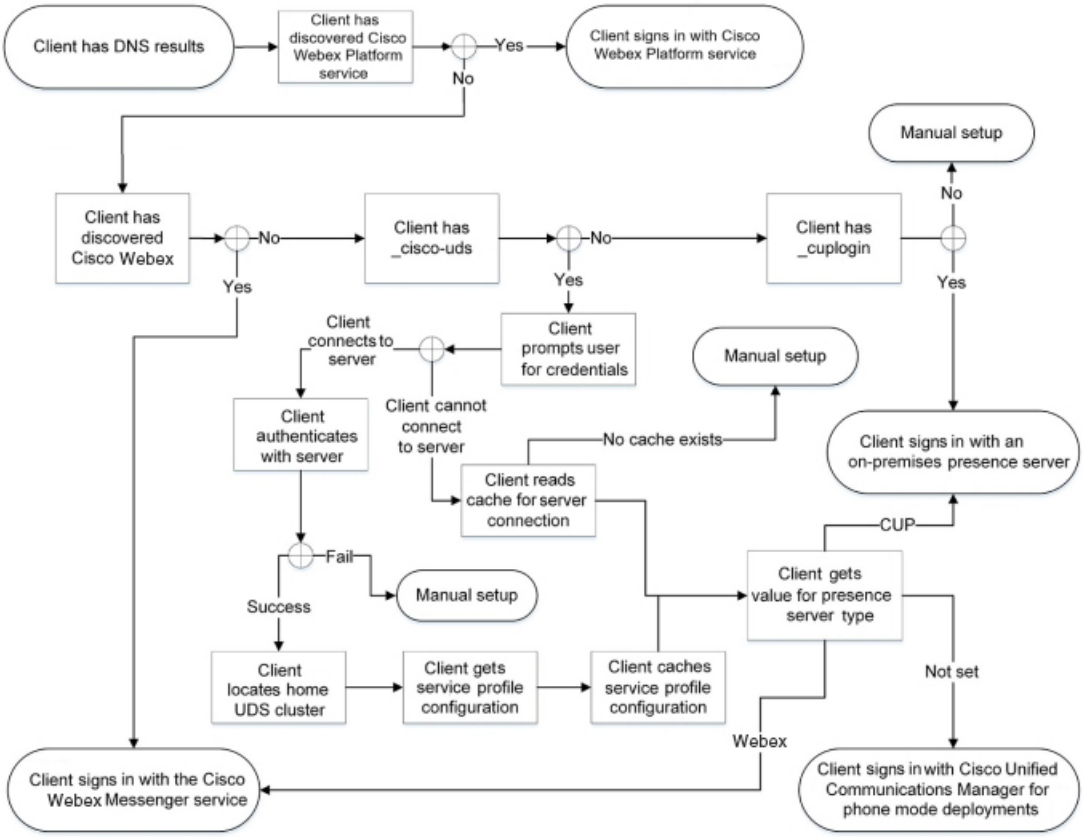
이름 서버가 다음을 반환하는 경우:

- `_cisco-uds` - 클라이언트가 회사 네트워크 내에 있고 Cisco Unified Communications Manager에 연결하는 것을 감지합니다.
- `_collab-edge` - 클라이언트가 모바일 및 Remote Access용 Expressway를 통해 내부 네트워크에 연결을 시도하고 서비스를 검색합니다.
- SRV 레코드가 없음 - 클라이언트에서 사용자에게 설정 및 로그인 세부 정보를 수동으로 입력하라는 메시지를 표시합니다.

클라이언트가 내부 서비스에 연결

다음 그림은 클라이언트가 내부 서비스에 연결하는 방법을 보여줍니다.

그림 *6:* 내부 서비스에 연결하는 클라이언트



내부 서비스에 연결할 때의 목표는 인증자를 결정하고, 사용자가 로그인하고, 사용 가능한 서비스에 연결하는 것입니다.

로그인 화면에서 사용자는 다음 서비스 중 하나를 사용하여 인증합니다.

- Cisco Webex 플랫폼 서비스—클라우드 또는 하이브리드 구축.
- Webex Messenger 서비스 — 클라우드 또는 하이브리드 구축.
- Cisco Unified Communications Manager—전화기 모드에서 온프레미스 구축.

클라이언트는 검색하는 모든 서비스에 연결하며, 이는 구축에 따라 달라집니다.

1. 클라이언트에서 사용자가 팀 메시징 모드에 대해 활성화된 것을 감지하면 클라이언트는 다음 작업을 수행합니다.
    1. Cisco Webex 플랫폼 서비스이 인증의 기본 소스인지 결정합니다.
    2. Cisco Webex 플랫폼 서비스에 자동으로 연결합니다.
    3. 사용자에게 자격 증명을 묻는 메시지를 표시합니다.
2. 클라이언트에서 CAS URL 조회 결과 Webex 사용자를 나타내는 것을 감지하면 클라이언트는 다음 작업을 수행합니다.

1. Webex Messenger 서비스가 인증의 기본 소스인지 확인합니다.
2. Webex Messenger 서비스에 자동으로 연결합니다.
3. 사용자에게 자격 증명을 묻는 메시지를 표시합니다.
4. 클라이언트 및 서비스 구성을 검색합니다.

3. 클라이언트가 `_cisco uds` SRV 레코드를 검색하는 경우 클라이언트는 다음 작업을 수행합니다.

   Cisco Unified Communications Manager 인증을 위해 사용자에게 자격 증명을 묻는 메시지를 표시합니다.

   1. 사용자의 홈 클러스터를 찾습니다.

      홈 클러스터를 찾으면 클라이언트가 자동으로 사용자의 장치 목록을 가져와서 Cisco Unified Communications Manager에 등록할 수 있습니다.

      여러 Cisco Unified Communications Manager 클러스터가 있는 환경에서는 ILS(Intercluster Lookup Service)를 구성해야 합니다. ILS를 사용하면 클라이언트가 사용자 홈 클러스터를 찾을 수 있습니다.

      중요 ILS를 구성하는 방법은 *Cisco Unified Communications Manager* 기능 및 서비스 설명서의 해당 버전을 참조하십시오.

   2. 서비스 프로파일을 검색합니다.

      서비스 프로파일은 클라이언트에 인증자뿐만 아니라 클라이언트 및 UC 서비스 구성도 제공합니다.

      클라이언트는 다음과 같이 IM and presence 프로파일의 제품 유형 필드 값에서 인증자를 결정합니다.

      - Cisco Unified Communications Manager— Cisco Unified Presence 또는 Cisco Unified Communications Manager IM and Presence Service가 인증자입니다.
      - Webex(IM and presence)Webex Messenger -서비스가 인증자입니다.

      참고 이 릴리스와 마찬가지로 클라이언트는 SRV 레코드에 대한 쿼리 외에도 HTTP 쿼리를 발행합니다. HTTP 쿼리를 사용하면 클라이언트가 Webex Messenger 서비스를 인증해야 하는지 여부를 결정할 수 있습니다.

      HTTP 쿼리의 결과로 클라이언트가 클라우드 기반 구축의 Webex Messenger 서비스에 연결합니다. 클라이언트가 CAS 조회를 사용하여 Webex 서비스를 이미 검색한 경우 제품 유형 필드의 값을 Webex로 설정할 수 없습니다.

      - 설정 안 됨 - 서비스 프로파일에 IM and presence 서비스 구성이 포함되어 있지 않으면 인증자는 Cisco Unified Communications Manager입니다.

3. 인증자에 로그인합니다.

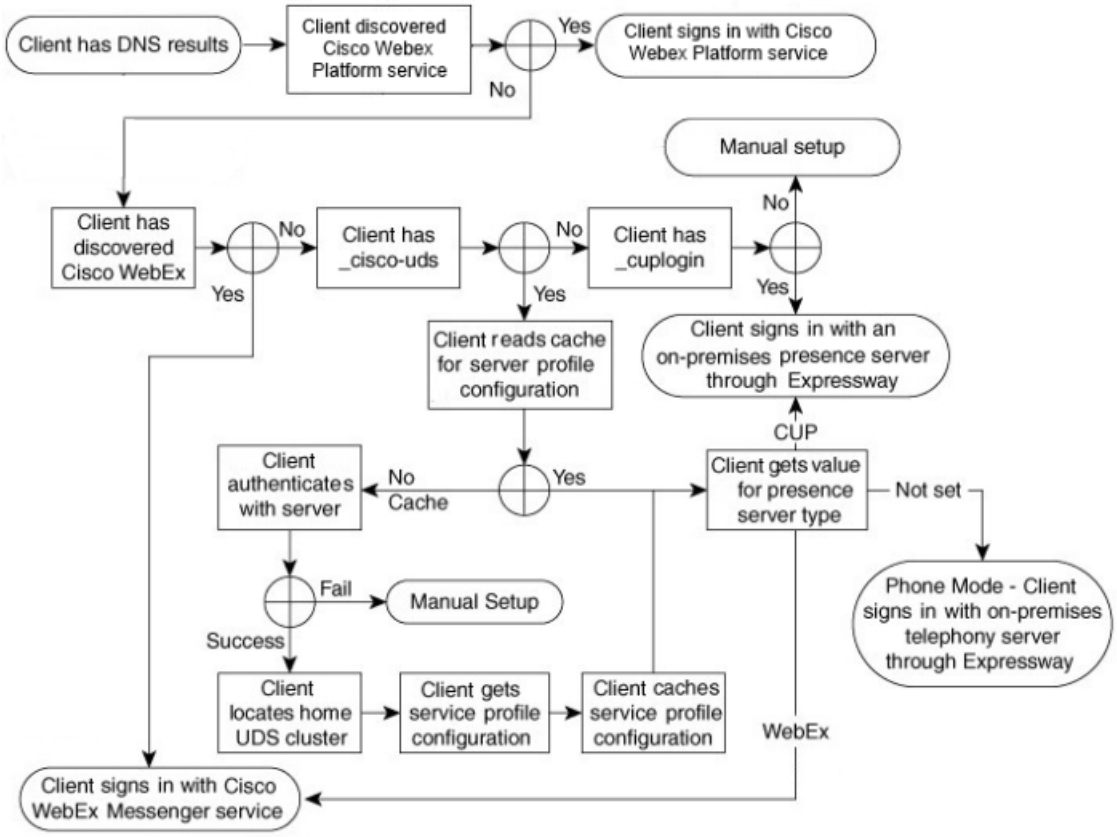
   클라이언트가 로그인한 후에는 제품 모드를 결정할 수 있습니다.

클라이언트가 모바일 및 **Remote Access**용 **Expressway**를 통해 연결

이름 서버가 `_collab-edge` SRV 레코드를 반환하는 경우 클라이언트는 모바일 및 Remote Access용 Expressway를 통해 내부 서버에 연결을 시도합니다.

다음 그림은 클라이언트가 모바일 및 Remote Access용 Expressway를 통해 네트워크에 연결된 경우 클라이언트가 내부 서비스에 연결하는 방법을 보여줍니다.

그림 ***7:*** 클라이언트가 모바일 및 ***Remote Access***용 ***Expressway***를 통해 연결



이름 서버가 `_collab-edge` SRV 레코드를 반환하면 클라이언트는 Cisco Expressway-E 서버의 위치를 가져옵니다. 그런 다음 Cisco Expressway-E 서버는 내부 이름 서버에 대한 쿼리 결과를 클라이언트에 제공합니다.

참고 Cisco Expressway-C 서버는 내부 SRV 레코드를 조회하고 해당 레코드를 Cisco Expressway-E 서버에 제공합니다.

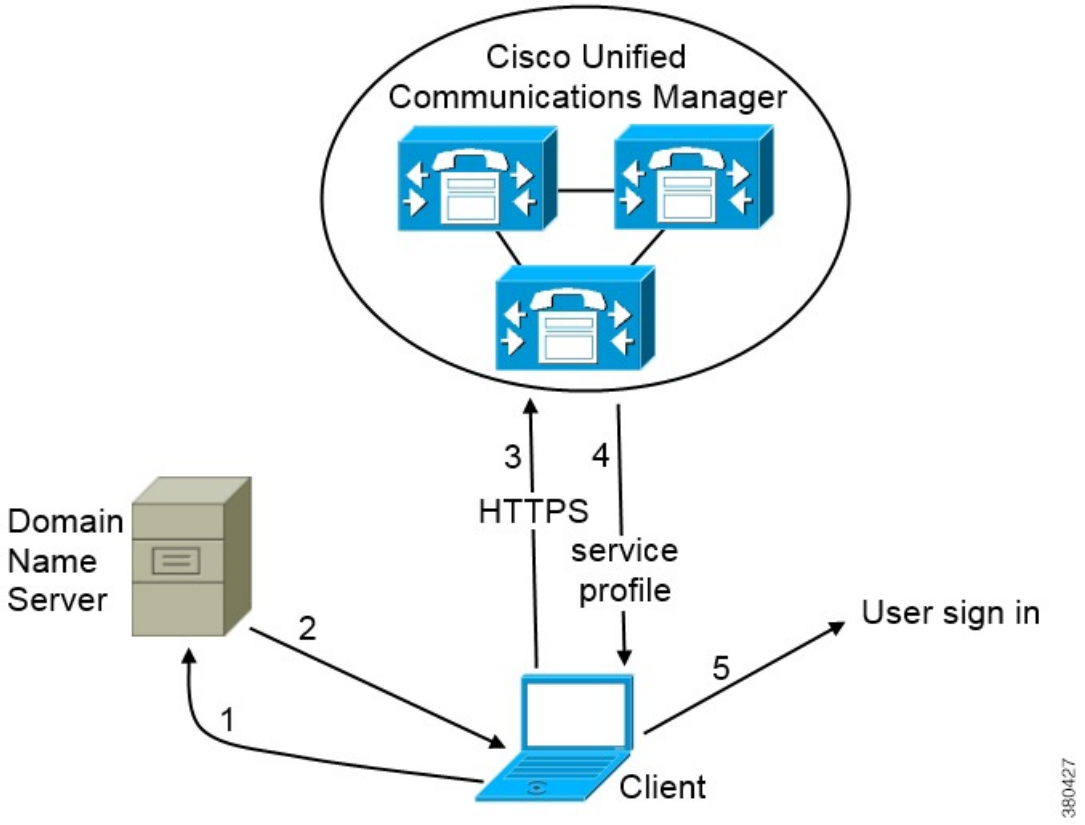
클라이언트가 _cisco-uds SRV 레코드를 포함해야 하는 내부 SRV 레코드를 가져온 후에는 Cisco Unified Communications Manager에서 서비스 프로파일을 검색합니다. 그런 다음 서비스 프로파일은 클라이언트에게 사용자의 홈 클러스터, 인증의 기본 소스 및 구성을 제공합니다.

Cisco UDS SRV 레코드

Cisco Unified Communications Manager 버전 9 이상 구축에서는 클라이언트가 _cisco-uds SRV 레코드를 사용하여 서비스 및 구성을 자동으로 검색할 수 있습니다.

다음 그림은 클라이언트가 _cisco-uds SRV 레코드를 사용하는 방법을 보여줍니다.

그림 ***8: UDS SRV*** 레코드 로그인 흐름



1. 클라이언트는 도메인 이름 서버에 SRV 레코드를 쿼리합니다.
2. 도메인 이름 서버는 _cisco-uds SRV 레코드를 반환합니다.
3. 클라이언트는 사용자의 홈 클러스터를 찾습니다.

   그 결과, 클라이언트는 사용자에 대한 장치 구성을 검색하고 전화 통신 서비스를 자동으로 등록할 수 있습니다.

중요 여러 Cisco Unified Communications Manager 클러스터가 있는 환경에서는 ILS(Intercluster Lookup Service)를 구성할 수 있습니다. ILS를 사용하면 클라이언트가 사용자 홈 클러스터를 찾고 서비스를 검색할 수 있습니다.

ILS를 구성하지 않으면 EMCC(Extension Mobility Cross Cluster) 원격 클러스터 설치와 유사한 원격 클러스터 정보를 수동으로 구성해야 합니다. 원격 클러스터 구성에 대한 자세한 정보는 *Cisco Unified Communications Manager* 기능 및 서비스 설명서를 참조하십시오.

4. 클라이언트는 사용자의 서비스 프로파일을 검색합니다.

   사용자의 서비스 프로파일에는 UC 서비스 및 클라이언트 구성에 대한 주소와 설정이 포함되어 있습니다.

   클라이언트는 서비스 프로파일에서 인증자를 결정합니다.

5. 클라이언트는 사용자를 인증자에게 로그인합니다.

다음은 `_cisco-uds` SRV 레코드의 예입니다.

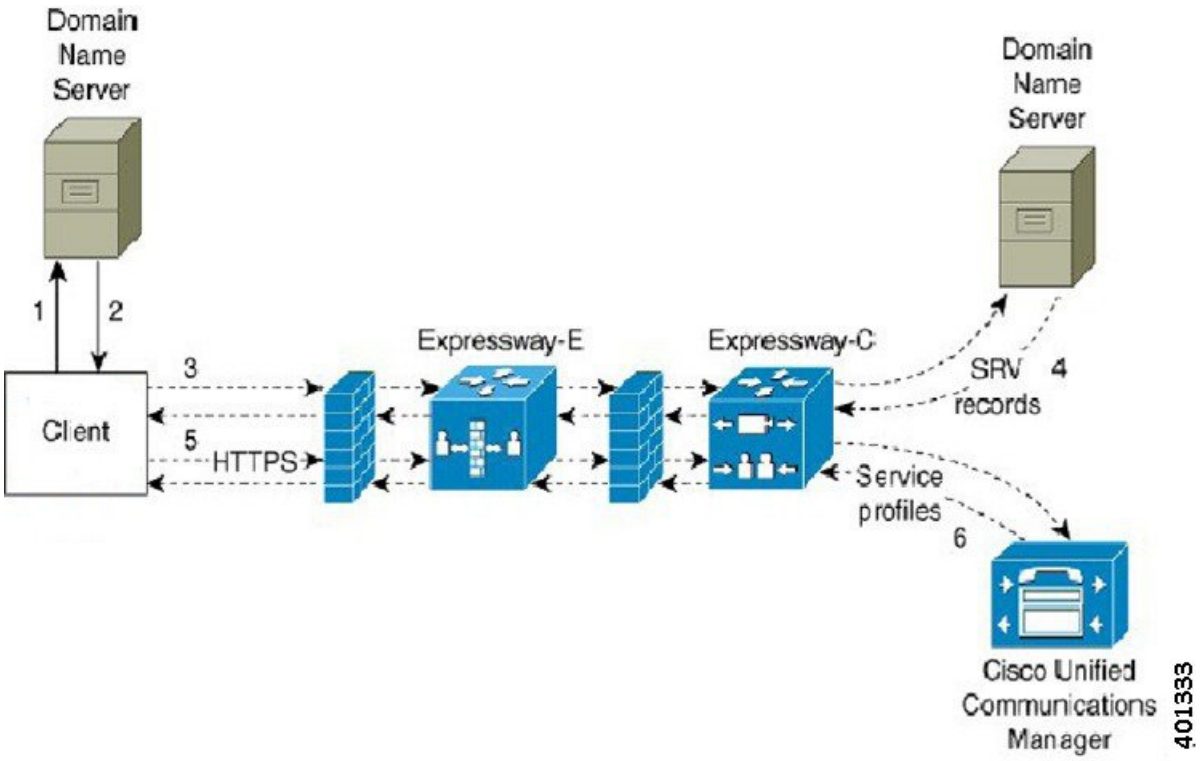
```
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 6
          weight         = 30
          port           = 8443
          svr hostname   = cucm3.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 2
          weight         = 20
          port           = 8443
          svr hostname   = cucm2.example.com
_cisco-uds._tcp.example.com     SRV service location:
          priority       = 1
          weight         = 5
          port           = 8443
          svr hostname   = cucm1.example.com
```

Collaboration Edge SRV 레코드

Cisco Jabber는 모바일 및 Remote Access용 Expressway를 통해 내부 서버에 연결을 시도하여 다음 `_collab-edge` SRV 레코드를 사용하여 서비스를 검색할 수 있습니다.

다음 그림은 클라이언트가 `_collab-edge` SRV 레코드를 사용하는 방법을 보여줍니다.

그림 *9: Collaboration Edge* 레코드 로그인 흐름



1. 클라이언트는 외부 도메인 이름 서버에 SRV 레코드를 쿼리합니다.
2. 이름 서버는 `_collab-edge` SRV 레코드를 반환하고 `_cuplogin` 또는 `_cisco uds` SRV 레코드를 반환하지 않습니다.

   그 결과, Cisco Jabber는 Cisco Expressway-E 서버를 찾을 수 있습니다.
3. 클라이언트는 내부 도메인 이름 서버에서 Expressway를 통해 내부 SRV 레코드를 요청합니다.

   이러한 SRV 레코드에는 `_cisco-uds` SRV 레코드가 포함되어야 합니다.
4. 클라이언트는 Expressway를 통해 내부 SRV 레코드를 얻습니다.

   그 결과 클라이언트에서 Cisco Unified Communications Manager 서버를 찾을 수 있습니다.
5. 클라이언트는 Cisco Unified Communications Manager에서 Expressway를 통해 서비스 프로파일을 요청합니다.
6. 클라이언트는 Cisco Unified Communications Manager에서 Expressway를 통해 서비스 프로파일을 검색합니다.

   서비스 프로파일에는 사용자의 홈 클러스터, 인증의 기본 소스 및 클라이언트 구성이 포함됩니다.

DNS 컨피그레이션

클라이언트에서 DNS를 사용하는 방법

Cisco Jabber 도메인 이름 서버를 사용하여 다음을 수행합니다.

- 클라이언트가 회사 네트워크 내부 또는 외부에 있는지 확인합니다.
- 회사 네트워크 내에서 온프레미스 서버를 자동으로 검색합니다.
- 공용 인터넷에서 모바일 및 Remote Access용 Expressway에 대한 액세스 지점을 찾습니다.

참고 Android OS 제한 사항: DNS 서비스를 사용하는 Android OS 4.4.2 및 5.0은 도메인 이름만 확인할 수 있고 호스트 이름은 확인할 수 없습니다.

자세한 내용은 Android 개발자 링크를 참조하십시오.

클라이언트가 이름 서버를 찾는 방법

Cisco Jabber다음에서 DNS 레코드를 찾습니다.

- 회사 네트워크 내부의 내부 이름 서버.
- 공용 인터넷의 외부 이름 서버.

클라이언트의 호스트 컴퓨터 또는 장치에서 네트워크 연결을 사용할 때 호스트 컴퓨터나 장치는 DHCP 설정에서 DNS 이름 서버의 주소를 가져옵니다. 네트워크 연결에 따라, 해당 이름 서버가 회사 네트워크 내부 또는 외부에 있을 수 있습니다.

Cisco Jabber 호스트 컴퓨터 또는 장치가 DHCP 설정에서 가져오는 이름 서버를 쿼리합니다.

클라이언트가 서비스 도메인을 가져오는 방법

서비스 도메인은 클라이언트에서 다양한 방식으로 검색됩니다.

새로운 설치:

- 클라이언트 사용자 인터페이스에 `username@example.com` 형식으로 주소를 입력합니다.
- 서비스 도메인을 포함하는 구성 URL을 클릭합니다. 이 옵션은 다음 클라이언트 버전에서만 사용할 수 있습니다.
  - Android용 Cisco Jabber 릴리스 9.6 이상
  - Mac용 Cisco Jabber 릴리스 9.6 이상
  - iPhone 및 iPad용 Cisco Jabber 릴리스 9.6.1 이상
- 클라이언트는 부트스트랩 파일에 설치 스위치를 사용합니다. 이 옵션은 다음 클라이언트 버전에서만 사용할 수 있습니다.

- Windows용 Cisco Jabber 릴리스 9.6 이상

기존 설치:

- 클라이언트는 캐시된 구성을 사용합니다.
- 수동으로 클라이언트 사용자 인터페이스에 주소를 입력합니다.

하이브리드 구축에서 CAS(중앙 인증 서비스) 조회를 통해 Webex 도메인을 검색하는 데 필요한 도메인이 DNS 레코드가 구축되는 도메인과 다를 수 있습니다. 이 시나리오에서는 ServicesDomain을 Webex을 검색하는 데 사용되는 도메인으로 설정하고 VoiceServicesDomain을 DNS 레코드가 구축되는 도메인으로 설정합니다. 음성 서비스 도메인은 다음과 같이 구성됩니다.

- 클라이언트는 구성 파일에서 VoiceServicesDomain 매개 변수를 사용합니다. 이 옵션은 `jabber-config` 파일을 지원하는 클라이언트에서 사용할 수 있습니다.
- VoiceServicesDomain을 포함하는 구성 URL을 클릭합니다. 이 옵션은 다음 클라이언트에서 사용할 수 있습니다.
  - Android용 Cisco Jabber 릴리스 9.6 이상
  - Mac용 Cisco Jabber 릴리스 9.6 이상
  - iPhone 및 iPad용 Cisco Jabber 릴리스 9.6.1 이상
- 클라이언트는 부트스트랩 파일에서 Voice_Services_Domain 설치 스위치를 사용합니다. 이 옵션은 다음 클라이언트 버전에서만 사용할 수 있습니다.
  - Windows용 Cisco Jabber 릴리스 9.6 이상

Cisco Jabber가 서비스 도메인을 가져오면 클라이언트 컴퓨터 또는 장치로 구성된 이름 서버를 쿼리합니다.

도메인 이름 시스템 디자인

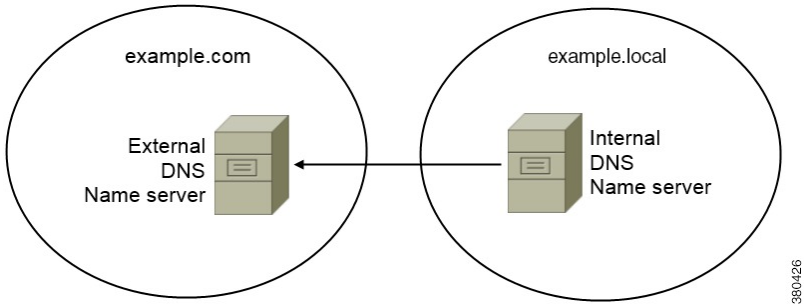
SRV(DNS 서비스) 레코드를 구축하는 위치는 DNS 네임스페이스의 설계에 따라 달라 집니다. 일반적으로 두 가지 DNS 디자인이 있습니다.

- 회사 네트워크 외부 및 내부에 있는 도메인 이름을 구분합니다.
- 회사 네트워크 외부 및 내부의 동일한 도메인 이름

별도의 도메인 설계

다음 그림은 별도의 도메인 설계를 보여줍니다.

그림 ***10:*** 별도의 도메인 설계



별도의 도메인 설계의 예는 조직에서 인터넷 이름 기관을 사용하여 외부 도메인으로 `example.com`을 등록하는 경우입니다.

회사는 다음 중 하나인 내부 도메인도 사용합니다.

- 외부 도메인의 하위 도메인(예: `example.local`).
- 외부 도메인에 다른 도메인(예: `exampledomain.com`).

별도의 도메인 설계는 다음과 같은 특징이 있습니다.

- 내부 이름 서버에는 내부 도메인에 대한 리소스 레코드를 포함하는 영역이 있습니다. 내부 이름 서버는 내부 도메인에 대해 권한이 있습니다.
- 내부 이름 서버는 DNS 클라이언트가 외부 도메인에 대해 쿼리하는 경우 요청을 외부 이름 서버로 전달합니다.
- 외부 이름 서버에는 조직의 외부 도메인에 대한 리소스 레코드를 포함하는 영역이 있습니다. 외부 이름 서버는 해당 도메인에 대해 권한이 있습니다.
- 외부 이름 서버는 요청을 다른 외부 이름 서버로 전달할 수 있습니다. 그러나 외부 이름 서버는 내부 이름 서버에 요청을 전달할 수 없습니다.

별도의 도메인 구조에 *SRV* 레코드 구축

별도의 이름 설계에는 내부 도메인과 외부 도메인이라는 두 개의 도메인이 있습니다. 클라이언트는 서비스 도메인의 SRV 레코드를 쿼리합니다. 내부 이름 서버는 서비스 도메인에 대한 레코드를 제공해야 합니다. 그러나 별도의 이름 설계에서는 서비스 도메인에 대한 영역이 내부 이름 서버에 존재하지 않을 수 있습니다.

서비스 도메인이 현재 내부 이름 서버에서 제공되지 않는 경우 다음을 수행할 수 있습니다.

- 서비스 도메인에 대한 내부 영역 내에 레코드를 구축합니다.
- 내부 이름 서버의 정확히 하위 도메인 영역 내에 레코드를 구축합니다.

서비스 도메인에 내부 영역 사용

내부 이름 서버에 서비스 도메인에 대한 영역이 아직 없는 경우에는 하나를 만들 수 있습니다. 이 방법을 사용하면 서비스 도메인에 대해 내부 이름 서버를 사용할 수 있습니다. 내부 이름 서버는 신뢰할 수 있으므로 다른 이름 서버로 쿼리를 전달하지 않습니다.

이 방법은 전체 도메인에 대한 전달 관계를 변경하며 내부 DNS 구조를 방해할 가능성이 있습니다. 서비스 도메인에 대한 내부 영역을 만들 수 없는 경우 내부 이름 서버에서 정확히 하위 도메인 영역을 만들 수 있습니다.

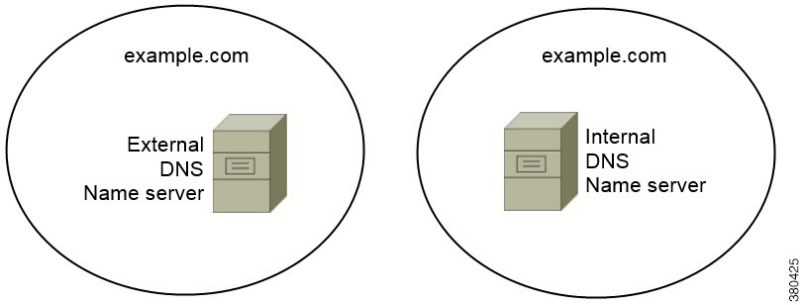
동일한 도메인 설계

동일한 도메인 설계의 예는 조직이 인터넷 이름 기관을 사용하여 외부 도메인으로 `example.com`을 등록하는 것입니다. 조직에서는 내부 도메인의 이름으로 `example.com`도 사용합니다.

단일 도메인, 스플릿 브레인

다음 그림은 스플릿 브레인 도메인 설계의 단일 도메인을 보여줍니다.

그림 ***11:*** 단일 도메인, 스플릿 브레인



두 DNS 영역은 단일 도메인을 나타냅니다. 하나는 내부 이름 서버에 있는 DNS 영역이고 다른 하나는 외부 이름 서버에 있는 DNS 영역입니다.

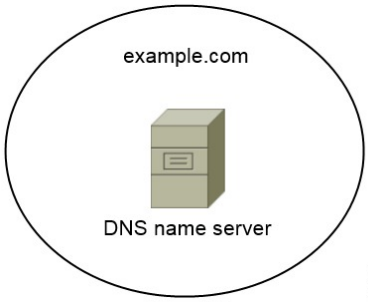
내부 이름 서버와 외부 이름 서버는 모두 단일 도메인에 대해 권한이 있지만 호스트의 다른 커뮤니티를 지원합니다.

- 회사 네트워크 내에 있는 호스트는 내부 이름 서버에만 액세스합니다.
- 공용 인터넷의 호스트는 외부 이름 서버에만 액세스합니다.
- 회사 네트워크와 공용 인터넷 간에 이동하는 호스트는 서로 다른 시간에 다른 이름 서버에 액세스합니다.

단일 도메인, 비 스플릿 브레인

다음 그림은 스플릿 브레인 도메인 설계가 없는 단일 도메인을 보여줍니다.

그림 12: 단일 도메인, 비 스플릿 브레인



단일 도메인에서 비 스플릿 설계, 내부 및 외부 호스트는 하나의 이름 서버 집합에 의해 제공되며 동일한 DNS 정보에 액세스할 수 있습니다.

중요 이 설계는 내부 네트워크에 대한 추가 정보를 잠재적 공격자에게 노출하기 때문에 일반적이지 않습니다.

방법 2: 사용자 정의

설치 매개변수, URL 구성 또는 EMM(Enterprise Mobility Management)을 사용하여 서비스 검색을 사용자 정의할 수 있습니다.

서비스 검색 맞춤 설정

Windows용 Cisco Jabber 사용자 정의 설치

Windows용 Cisco Jabber는 다음과 같은 방법으로 사용할 수 있는 MSI 설치 패키지를 제공합니다.

- 명령줄 사용 - 명령줄 창에서 인수를 지정하여 설치 속성을 설정할 수 있습니다.

  여러 인스턴스를 설치할 계획인 경우 이 옵션을 선택합니다.

- MSI를 수동으로 실행 - 클라이언트 워크스테이션의 파일 시스템에서 수동으로 MSI를 실행한 다음 클라이언트를 시작할 때 연결 속성을 지정합니다.

  테스트 또는 평가 목적으로 단일 인스턴스를 설치할 계획인 경우 이 옵션을 선택합니다.

- 사용자 정의 설치 관리자 만들기 - 기본 설치 패키지를 열고 필수 설치 속성을 지정한 다음 사용자 정의 설치 패키지를 저장합니다.

  동일한 설치 속성을 사용하여 설치 패키지를 배포하려는 경우 이 옵션을 선택합니다.

- 그룹 정책과 함께 구축 - 동일한 도메인에 있는 여러 컴퓨터에 클라이언트를 설치합니다.

설치 프로그램 스위치

부트스트랩 파일은 서비스 검색이 구축되지 않았고 사용자가 수동으로 연결 설정을 지정하기를 원하지 않는 상황에서 서비스 검색을 위한 폴백 메커니즘을 제공합니다.

클라이언트는 초기 실행에서 부트스트랩 파일만 읽습니다. 초기 실행 후 클라이언트는 서버 주소 및 구성을 캐시한 다음, 후속 실행 시 캐시에서 로드합니다.

Webex 앱(Unified CM)에서 통화 구축에 대해서는 부트스트랩 파일 대신에 서비스 검색을 사용하는 것이 좋습니다.

Mac용, iPhone 및 iPad용 및 Android용 Cisco Jabber 사용자 정의 설치

URL 구성을 사용하여 Mac용 Cisco Jabber 또는 모바일 클라이언트에 대한 사용자 정의 설치를 생성할 수 있습니다. 모바일 클라이언트의 경우에는 EMM(Enterprise Mobility Management)을 사용할 수도 있습니다. 이러한 사용자 정의 설치는 서비스를 활성화하는 설치 매개 변수에 따라 달라집니다.

URL 구성

사용자가 수동으로 서비스 검색 정보를 입력하지 않고 Cisco Jabber를 시작할 수 있게 하려면 사용자에게 클라이언트를 설치할 구성 URL 링크를 제공합니다.

사용자에게 구성 URL 링크를 이메일로 바로 전송하거나, 링크를 웹사이트에 게시합니다.

EMM(Enterprise Mobility Management)을 사용한 모바일 구성

Android용 Cisco Jabber 및 iPhone 및 iPad용 Cisco Jabber에서 EMM(Enterprise Mobility Management)을 사용하여 Cisco Jabber를 구성할 수 있습니다. EMM 설정에 대한 자세한 내용은 EMM 제공자가 제공하는 관리자용 지침을 참조하십시오.

관리되는 장치에서만 Jabber가 실행되게 하려면 인증서 기반 인증을 구축하고 EMM을 통해 클라이언트 인증서를 등록하면 됩니다.

EMM을 구축하는 방법에 대한 자세한 내용은 *Cisco Jabber*의 온프레미스 구축 또는 *Cisco Jabber* ○의 클라우드 및 하이브리드 구축에서 *Cisco Jabber* 애플리케이션 구축 섹션을 참조하십시오.

방법 3: 수동 설치

고급 옵션으로, 사용자는 로그인 화면에서 서비스에 수동으로 연결할 수 있습니다.

고가용성

인스턴트 메시징 및 프레즌스에 대한 고가용성

고가용성은 인스턴트 메시징 및 프레즌스 서비스에 대한 페일오버 기능을 제공하기 위해 하위 클러스터에 여러 노드가 있는 환경을 말합니다. 하위 클러스터의 한 노드를 사용할 수 없게 되면 해당 노드의 인스턴트 메시징 및 프레즌스 서비스는 하위 클러스터의 다른 노드로 페일오버됩니다. 이러한

방식으로 고가용성은 Cisco Jabber에 대한 인스턴트 메시징 및 프레즌스 서비스의 안정적인 연속성을 보장합니다.

LDAP의 경우 고가용성은 지원되지 않습니다. UDS 연락처 소스를 사용하는 경우 고가용성이 지원되지 않습니다.

Cisco Jabber는 다음 서버에서 고가용성을 지원합니다.

Cisco Unified Communications Manager IM and Presence Service 릴리스 **9.0** 이상

고가용성에 대한 자세한 내용은 다음 Cisco Unified Communications Manager IM and Presence Service 설명서를 참조하십시오.

Cisco Unified Communications Manager의 **IM and Presence** 서비스 구성 및 관리

고가용성 클라이언트 로그인 프로파일

고가용성 문제 해결

페일오버 중 활성 통화 보류

Cisco Unified Communications Manager의 주 인스턴스에서 보조 인스턴스로 페일오버가 발생하는 경우 활성 통화를 보류 상태로 전환할 수 없습니다.

클라이언트에서 고가용성

페일오버 중 클라이언트 동작

서버에 고가용성이 구성되어 있는 경우 기본 서버가 보조 서버로 페일오버되면 클라이언트는 최대 1분 동안 프레즌스 상태를 일시적으로 상실합니다. 다시 로그인 매개 변수를 구성하여 클라이언트가 서버에 다시 로그인을 시도하기 전에 대기하는 시간을 정의합니다.

로그인 매개 변수 구성

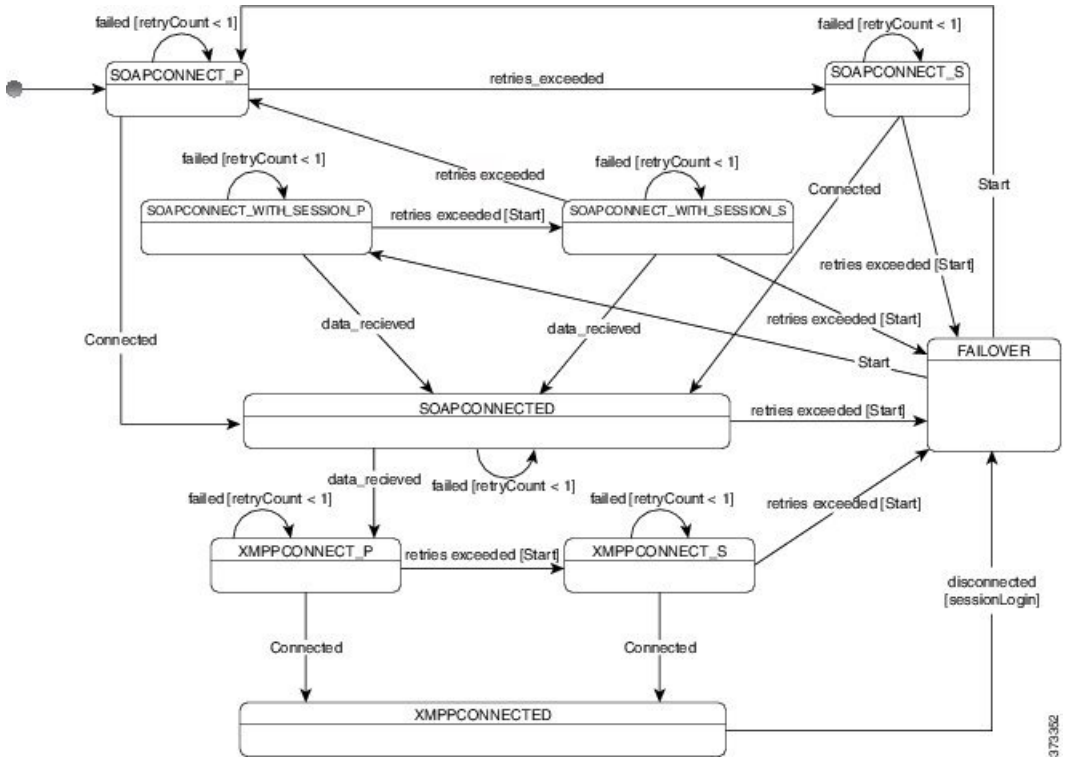
Cisco Unified Communications Manager IM and Presence Service에서 서버에 다시 로그인을 시도하기 전에 Cisco Jabber가 대기하는 최대 및 최소 시간(초)을 구성할 수 있습니다. 서버에서 다음 필드에 다시 로그인 매개 변수를 지정합니다.

- 클라이언트 다시 로그인 하한값
- 클라이언트 다시 로그인 상한값

페일오버 중 클라이언트 동작

다음 그림은 페일오버 중에 Cisco Unified Communications Manager IM and Presence Service를 사용할 때 클라이언트의 동작을 보여줍니다.

그림 ***13:*** 페일오버 중 클라이언트 동작



1. 클라이언트가 활성 서버에서 연결이 끊기면 클라이언트가 XMPPCONNECTED 상태에서 FAILOVER 상태로 전환됩니다.
2. FAILOVER 상태에서 클라이언트는 SOAPCONNECT_SESSION_P(기본 서버)를 시도하여 SOAPCONNECTED 상태를 얻으려고 시도하고, 실패할 경우 SOAPCONNECT_SESSION_S(보조 서버)를 얻으려고 시도합니다.
   - SOAPCONNECT_SESSION_P 또는 SOAPCONNECT_SESSION_S를 얻을 수 없는 경우 클라이언트가 FAILOVER 상태로 다시 전환됩니다.
   - FAILOVER 상태에서 클라이언트는 SOAPCONNECT_P 상태를 얻으려고 시도하고, 실패할 경우 SOAPCONNECT_S 상태에 도달하려고 시도합니다.
   - 클라이언트가 SOAPCONNECT_P 또는 SOAPCONNECT_S 상태에 도달할 수 없는 경우 클라이언트는 사용자가 로그인 시도를 시작할 때까지 IM&P 서버에 대한 추가 자동 연결을 시도하지 않습니다.
3. SOAPCONNECT_SESSION_P, SOAPCONNECT_SESSION_S, SOAPCONNECT_P 또는 SOAPCONNECT_S 상태에서 클라이언트는 현재 기본 보조 XMPP 서버 주소를 검색합니다. 이 주소는 페일오버 중 변경됩니다.
4. SOAPCONNECTED 상태에서 클라이언트는 XMPPCONNECT_P 상태에 연결을 시도하여 XMPPCONNECTED 상태를 얻으려고 시도하며, 실패할 경우 XMPPCONNECT_S 상태를 시도합니다.

- 클라이언트가 XMPPCONNECT_P 또는 XMPPCONNECT_S 상태에 도달할 수 없는 경우 클라이언트는 사용자가 로그인 시도를 시작할 때까지 IM&P 서버에 대한 추가 자동 연결을 시도하지 않습니다.

5. 클라이언트가 XMPPCONNECTED 상태가 된 후에는 클라이언트가 IM&P 기능을 사용할 수 있습니다.

음성 및 영상의 고가용성

하위 클러스터의 한 노드를 사용할 수 없게 되면 하위 클러스터의 다른 노드로 음성 및 비디오가 페일오버됩니다.

기본적으로 소프트웨어 전화기 또는 데스크폰이 다른 노드에 등록하는 데는 120초까지 걸릴 수 있습니다. 이 시간 초과 기간이 너무 길면 노드에 대한 SIP Station 킵 얼라이브 간격(SIP Station KeepAlive Interval) 서비스 매개 변수의 값을 조정합니다. SIP Station 킵 얼라이브 간격(SIP Station KeepAlive Interval) 서비스 매개 변수는 Cisco Unified Communications Manager의 모든 전화기를 수정합니다. 간격을 조정 하기 전에 Cisco Unified Communications Manager 서버에 미치는 영향을 분석합니다.

노드에 대한 서비스 매개 변수를 구성하려면 Cisco Unified Communications Manager 관리에서 시스템 > 서비스 매개 변수를 선택합니다.

비 DNS SRV 레코드 방법을 사용하는 전화기 모드 구축의 경우 Cisco Unified Communications Manager 노드가 하나만 지정되어 있으므로 음성 및 비디오에 대한 페일오버를 수행할 수 없습니다.

영구 채팅의 고가용성

영구 채팅을 위해 고가용성이 지원됩니다. 장애 조치 기간 동안 메시지를 보낼 수 없다는 메시지가 사용자에게 표시될 수 있습니다. 노드가 장애 조치되면 사용자는 자동으로 대화방에 다시 참가하고 메시지를 다시 보낼 수 있습니다.

연락처 검색 및 연락처 확인의 고가용성

Cisco Unified Communications Manager UDS(사용자 데이터 서비스)에서 제공하는 연락처 검색 및 연락처 확인에는 고가용성이 지원됩니다. 기본 UDS 서버를 사용할 수 없는 경우 Jabber는 자동으로 두 번째 UDS 서버 또는 세 번째 UDS 서버(구성된 경우)로 페일오버합니다.

음성 메일의 고가용성

보조 음성 메일 서버가 구성되어 있으면 기본 서버를 사용할 수 없거나 연결할 수없는 경우 클라이언트는 자동으로 보조 음성 메일 서버로 장애 조치합니다.

SRST(Survivable Remote Site Telephony)

Windows용 Cisco Jabber 및 Mac용 Cisco Jabber에 적용합니다.

Cisco Unified Communications Manager 애플리케이션에 연결할 수 없거나 WAN이 다운된 경우 Cisco Unified SRST(Survivable Remote Site Telephony)를 사용하여 원격 사용자에 대한 기본 전화 통신 서비스를 유지합니다. 연결이 끊어지면 클라이언트가 원격 사이트의 로컬 라우터로 장애 조치됩니다.

참고 SRST 버전 12.8 이상 버전이 지원됩니다.

SRST는 시스템이 장애 조치에서 시작, 종료, 보류, 재시작, 음소거, 음소거 해제 및 듀얼 신호음 복합 주파수 부호 신호 처리 [DTMF])가 활성화될 때만 기본 통화 제어 기능을 제공합니다.

장애 조치 중에는 다음 서비스를 사용할 수 없습니다.

- 영상
- 통화 중 기능(호 전환, iDivert, 통화 지정 보류, 전화 회의, 휴대폰으로 전송)
- DVO(Dial via Office)
- 임시 전화 회의
- Binary Floor Control Protocol(BFCP) 공유

SRST 구성에 대한 자세한 지침은 *Cisco Unified Communications Manager* 관리 설명서의 해당 릴리스를 참조하십시오.

구성 우선 순위

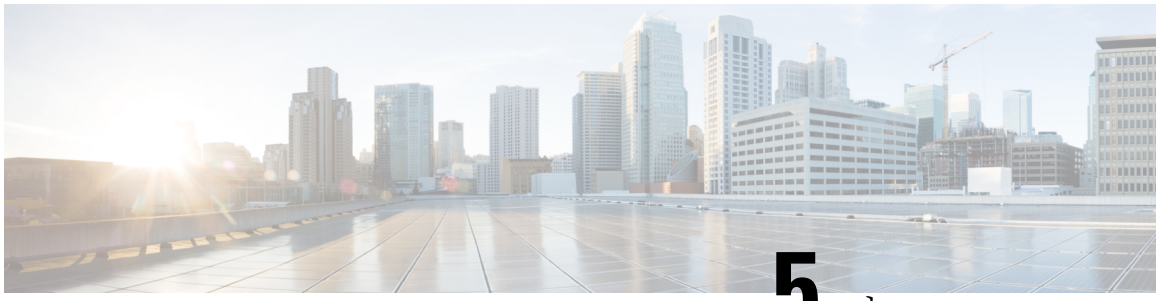
서비스 프로파일과 구성 파일이 모두 있는 경우, 다음 표에서는 어떤 매개변수 값이 우선하는지 설명합니다.

서비스 프로필	컨피그레이션 파일	다른 것에 우선하는 매개변수 값은 무엇입니까**?**
매개변수 값이 설정됨	매개변수 값이 설정됨	서비스 프로필
매개변수 값이 설정됨	매개변수 값이 비어 있음	서비스 프로필
매개변수 값이 비어 있음	매개변수 값이 설정됨	구성 파일
매개변수 값이 비어 있음	매개변수 값이 비어 있음	서비스 프로파일 공백(기본값) 값

Cisco 지원 필드를 사용한 그룹 구성

그룹 구성 파일은 사용자의 하위 집합에 적용됩니다. CSF 장치를 사용하여 사용자를 프로비저닝한 다면, 장치 구성의 **Cisco** 지원 필드 필드에 그룹 구성 파일명을 지정할 수 있습니다. 사용자에게 CSF 장치가 없다면, TFTP_FILE_NAME 인수를 사용하여 설치하는 동안 각 그룹에 고유한 구성 파일명을 설정할 수 있습니다.

그룹 구성은 14122 버전 이후의 COP 파일을 사용하여 TCT 및 BOT에서 지원됩니다.



5 장

연락처 소스

연락처 소스란?

연락처 소스는 사용자에 대한 데이터 모음입니다. 사용자가 Cisco Jabber 클라이언트에서 연락처를 검색하거나 연락처를 추가하는 경우 연락처 정보를 연락처 소스에서 읽습니다.

Cisco Jabber는 연락처 목록을 채우기 위한 정보를 연락처 소스에서 검색하고, 클라이언트의 연락처 카드 및 연락처 정보를 표시하는 기타 영역을 업데이트합니다. 클라이언트가 인스턴트 메시지 또는 음성/영상 통화와 같은 수신 통신을 받을 때 연락처 정보를 확인하는 데 연락처 소스를 사용합니다.

연락처 소스 서버

참고 모든 Jabber 클라이언트는 디렉터리 통합을 위한 LDAPv3 표준을 지원합니다. 이 표준을 지원하는 모든 디렉터리 서버는 이러한 클라이언트와 호환됩니다.

다음 연락처 소스 서버를 Cisco Jabber에 사용할 수 있습니다.

- Windows Server 2012 R2용 Active Directory Domain Services
- Windows Server 2008 R2용 Active Directory Domain Services
- Cisco Unified Communications ManagerUDS (사용자 데이터 서버). Cisco Jabber는 Cisco Unified Communications Manager 버전 10.5 이상을 사용하여 UDS를 지원합니다.
- OpenLDAP
- Active Directory Lightweight Directory Service(AD LDS) 또는 Active Directory Application Mode(ADAM)

연락처 소스가 필요한 이유는 무엇입니까?

Cisco Jabber는 다음과 같은 방법으로 연락처 소스를 사용합니다.

- 사용자가 연락처를 검색하는 경우, 클라이언트는 입력된 정보를 가져와서 연락처 소스에서 검색합니다. 연락처 소스에서 정보가 검색되고 클라이언트에는 연락처와 상호 작용하는 데 사용 가능한 방법이 표시됩니다.
- 클라이언트가 수신 알림을 수신 - 클라이언트는 수신 알림의 정보를 가져와 URI, 번호, JabberID를 연락처 소스의 연락처로 확인합니다. 클라이언트는 경고에 연결 세부 정보를 표시합니다.

연락처 소스 서버를 구성하는 경우

참고 Active Directory 도메인에 등록된 워크스테이션에 Cisco Jabber를 설치합니다. 이 환경에서는 디렉터리에 연결하기 위해 Cisco Jabber를 구성할 필요가 없습니다. 클라이언트는 자동으로 디렉터리를 검색하고 해당 도메인의 글로벌 카탈로그 서버에 연결합니다.

다음 서비스 중 하나를 연락처 소스로 사용할 계획인 경우 디렉터리 서비스에 연결하도록 Cisco Jabber를 구성합니다.

- Active Directory 서비스
- Cisco Unified Communications Manager 사용자 데이터 서비스
- OpenLDAP
- Active Directory Lightweight Directory Service
- Active Directory Application Mode

선택적으로 디렉터리 통합을 다음과 같이 구성할 수 있습니다.

- 기본 특성 매핑을 변경합니다.
- 디렉터리 쿼리 설정을 조정합니다.
- 클라이언트가 연락처 사진을 검색하는 방법을 지정합니다.
- 도메인 내 페더레이션을 수행합니다.

Cisco 디렉터리 통합에 대한 연락처 소스 옵션

온프레미스 구축에서 클라이언트는 다음 연락처 소스 중 하나를 사용하여 사용자 정보에 대한 디렉터리 조회를 확인해야 합니다.

- LDAP(Lightweight Directory Access Protocol) — 회사 디렉터리를 사용하는 경우 다음 LDAP 기반 연락처 소스 옵션을 사용하여 디렉터리를 연락처 소스로 구성할 수 있습니다.
  - CDI(Cisco Directory Integration) - 이 연락처 소스 옵션을 사용하여 모든 클라이언트를 구축합니다.
- Cisco Unified Communications Manager UDS(사용자 데이터 서비스) - 회사 디렉터리가 없거나 구축에 Expressway 모바일 및 Remote Access를 통해 연결되는 사용자가 포함 된 경우 이 옵션을 사용할 수 있습니다.

Lightweight Directory Access Protocol

Cisco 디렉터리 통합이 LDAP와 작동하는 방식

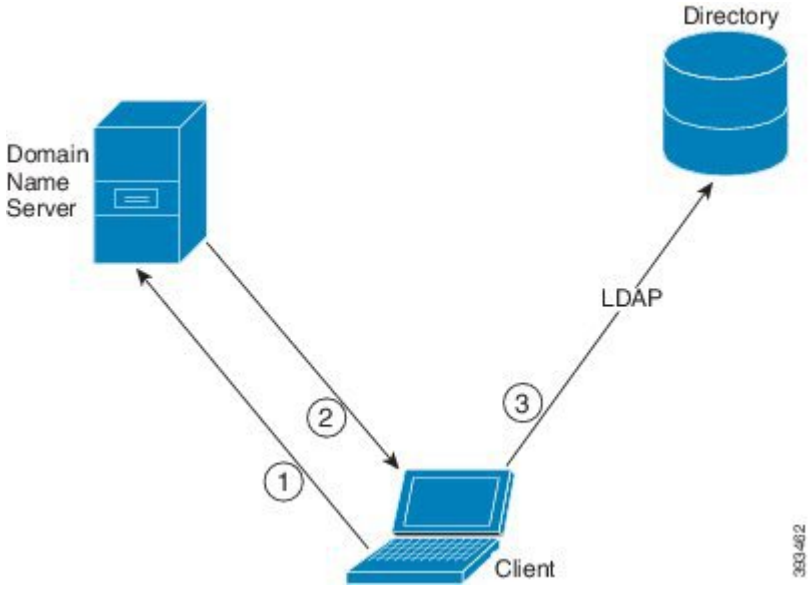
CDI는 서비스 검색을 사용하여 LDAP 서버를 결정합니다.

다음은 CDI를 사용한 온프레미스 구축에 대한 기본 설정입니다.

- Cisco Jabber는 연락처 소스로 Active Directory와 통합됩니다.
- Cisco Jabber는 자동으로 글로벌 카탈로그를 검색하고 연결합니다.

자동 서비스 검색 — 권장

서비스 검색을 사용하여 GC(글로벌 카탈로그) 서버 또는 LDAP 서버를 자동으로 연결하고 인증하는 것이 좋습니다. 구축을 사용자 정의하려는 경우 LDAP 서버 정보를 제공하는 옵션과 사용할 수 있는 인증 옵션을 검토하십시오. Jabber는 먼저 GC 도메인으로 DNS 쿼리를 전송하여 GC 서버를 검색합니다. GC 서버를 검색하지 않으면 Jabber가 LDAP 도메인으로 DNS 쿼리를 전송하여 LDAP 서버를 검색합니다.



사용 가능한 GC가 있는 경우 클라이언트는 다음 작업을 수행합니다.

1. 워크스테이션에서 DNS 도메인을 가져오고 GC에 대한 SRV 레코드를 조회합니다.
2. SRV 레코드에서 GC의 주소를 검색합니다.
3. 로그인한 사용자의 자격 증명을 사용하여 GC에 연결합니다.

글로벌 카탈로그 도메인을 사용하는 검색

Jabber가 DNS SRV 쿼리를 사용하여 GC 서버를 검색하려고 시도합니다. 먼저, Jabber는 GC 도메인을 가져옵니다.

1. 사용 가능한 경우 Jabber는 DNSFORESTNAME 환경 변수를 GC 도메인으로 사용합니다.
2. DNSFORESTNAME을 사용할 수 없는 경우 Jabber는 GC 도메인에 대해 다음을 확인합니다.
   - Windows에서 Jabber는 `DnsForestName`을 받기 위해 Windows `DsGetDcName` API를 호출합니다.
   - 비 Windows 플랫폼에서 Jabber는 `jabber-config.xml`에서 LdapDNSForestDomain을 읽습니다.

Jabber가 GC 도메인을 가져오면 DNS SRV 쿼리를 전송하여 GC 서버 주소를 얻습니다.

- Windows에서 Jabber는 Windows `DsGetSiteName` API를 통해 `SiteName`을 사용할 수 있는지 확인합니다.
  - `SiteName`이 있는 경우 Jabber는 DNS SRV 쿼리 `_gc._tcp.SiteName._sites.GCDomain`을 전송하여 GC 서버 주소를 가져옵니다.
  - `SiteName`이 없거나 `_gc._tcp.SiteName._sites.GCDomain`에 대해 SRV 레코드가 반환되지 않는 경우 Jabber는 DNS SRV 쿼리 `_gc._tcp.GCDomain`을 전송하여 GC 서버 주소를 가져옵니다.

- 비 Windows 플랫폼에서 Jabber는 DNS SRV 쿼리 `_gc._tcp.GCDomain`을 전송하여 GC 서버 주소를 가져옵니다.

LDAP 도메인을 사용하는 검색

Jabber가 GC 서버를 검색할 수 없는 경우 LDAP 도메인을 검색하려고 시도합니다.

1. 사용 가능한 경우 Jabber는 USERDNSDOMAIN 환경 변수를 LDAP 도메인으로 사용합니다.
2. USERDNSDOMAIN을 사용할 수 없는 경우 Jabber는 `jabber-config.xml`에서 LdapUserDomain을 읽습니다.
3. LdapUserDomain을 사용할 수 없는 경우 Jabber는 사용자가 LDAP 도메인으로 로그인한 이메일 도메인을 사용합니다.

Jabber가 LDAP 도메인을 가져오면 DNS SRV 쿼리를 전송하여 LDAP 서버 주소를 얻습니다.

- Windows에서 Jabber는 Windows `DsGetSiteName` API를 통해 `SiteName`을 사용할 수 있는지 확인합니다.
  - `SiteName`이 있는 경우 Jabber는 DNS SRV 쿼리 `_ldap._tcp.SiteName.sites.LdapDomain`을 전송하여 LDAP 서버 주소를 가져옵니다.
  - `SiteName`이 없거나 `_ldap._tcp.SiteName.sites.LdapDomain`에 대해 SRV 레코드가 반환되지 않는 경우 Jabber는 DNS SRV 쿼리 `_ldap._tcp.LdapDomain`을 전송하여 LDAP 서버 주소를 가져옵니다.
- 비 Windows 플랫폼에서 Jabber는 DNS SRV 쿼리 `_ldap._tcp.LdapDomain`을 전송하여 LDAP 서버 주소를 가져옵니다.

Jabber가 LDAP 서버에 연결되면 사용할 인증 메커니즘의 목록과 순서를 지정하는 LDAP 서버의 `SupportedSaslMechanisms` 특성을 읽습니다.

LDAP 서비스에 대한 수동 구성

LDAP 서비스에 대한 수동 구성

1. PrimaryServerName 매개 변수를 구성하여 Jabber가 연결할 특정 LDAP 서버를 정의할 수 있습니다.
2. `jabber-config.xml` 파일에서 LdapSupportedMechanisms 매개 변수를 구성하여 supportedSaslMechanisms 특성의 목록을 재정의할 수 있습니다.

   연락처 서비스와 LDAP 서버는 이러한 각 메커니즘을 지원해야 합니다. 여러 개의 값을 구분하려면 공백을 사용하십시오.

   - GSSAPI – Kerberos v5
   - EXTERNAL – SASL 외부
   - PLAIN(기본값) – 단순 LDAP 바인드, 익명은 단순 바인딩 하위 집합입니다.

예:

```
<LdapSupportedMechanisms>GSSAPI EXTERNAL PLAIN</LdapSupportedMechanisms>
```

3. 필요한 경우, LdapUserDomain 매개 변수를 구성하여 Jabber에서 LDAP 서버를 인증하는 데 사용하는 도메인을 설정합니다. 예:

```
CUCMUsername@LdapUserDomain
```

LDAP 고려 사항

Cisco 디렉토리 통합(CDI) 매개 변수는 기본 디렉토리 통합 (BDI) 및 향상된 디렉터리 통합 (EDI)을 대체합니다 CDI 매개 변수는 모든 클라이언트에 적용됩니다.

Cisco Jabber 구축 시나리오

시나리오 **1: Jabber 11.8**을 처음 사용하는 경우

서비스 검색을 사용하여 LDAP 서버에 자동으로 연결하고 인증하는 것이 좋습니다. 구축을 사용자 정의하려는 경우 LDAP 서버 정보를 제공하는 옵션과 사용할 수 있는 인증 옵션을 검토하십시오.

시나리오 **2: EDI** 구성에서 **11.8**로 업그레이드하는 경우

구성에 EDI 매개 변수만 사용하는 경우 Jabber는 EDI 매개 변수를 읽고 디렉터리 소스 통합에 사용할 수 있도록 합니다. 따라서 EDI 매개 변수를 업그레이드하고 해당하는 CDI 매개 변수로 대체하는 것이 좋습니다.

시나리오 **3: BDI** 구성에서 **11.8**로 업그레이드하는 경우

구성에 BDI 매개 변수만 사용하는 경우에는 BDI 매개 변수를 해당 CDI 매개 변수로 업데이트해야 합니다. 예를 들어 BDIPrimaryServerName의 경우 매개 변수를 PrimaryServerName대체해야 합니다. BDIEnableTLS가 UseSSL 매개 변수로 대체됩니다.

시나리오 **4:** 혼합 **EDI/BDI** 구성에서 **11.8**로 업그레이드 하는 경우

구성에서 EDI 및 BDI를 모두 사용하는 경우, Jabber가 LDAP 서버에 연결할 때 EDI 매개 변수를 사용하므로 BDI에 대한 구성을 검토해야 합니다.

디렉터리 매개 변수

다음 표에는 CDI 매개 변수 이름을 나타내거나 Jabber 11.8 이상에 적용되지 않는 경우 BDI 및 EDI 매개 변수가 나열되어 있습니다.

BDI 매개 변수	**EDI** 매개 변수	**CDI** 매개변수
-	DirectoryServerType	DirectoryServerType
-	ConnectionType	-
BDILDAPServerType	-	-
BDIPresenceDomain	PresenceDomain	PresenceDomain
BDIPrimaryServerName	PrimaryServerName	PrimaryServerName

BDI 매개 변수	**EDI** 매개 변수	**CDI** 매개변수
-	SecondaryServerName	SecondaryServerName
BDIServerPort1	ServerPort1	ServerPort1
-	ServerPort2	ServerPort2
-	UseWindowCredentials	-
BDIUseJabberCredentials	-	-
BDIConnectionUsername	ConnectionUsername	ConnectionUsername
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL
-	UseSecureConnection	-
BDIUseANR	UseANR	UseANR
BDIBaseFilter	BaseFilter	BaseFilter
BDIGroupBaseFilter	GroupBaseFilter	GroupBaseFilter
BDIUseANR	-	-
BDIPredictiveSearchFilter	PredictiveSearchFilter	PredictiveSearchFilter
-	DisableSecondaryNumberLookups	DisableSecondaryNumberLookups
-	SearchTimeout	SearchTimeout
-	UseWildcards	UseWildcards
-	MinimumCharacterQuery	MinimumCharacterQuery
BDISearchBase1	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5
BDIGroupSearchBase1	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5
BDIUseSipUriToResolveContacts	UseSipUriToResolveContacts	UseSipUriToResolveContacts
BDIUriPrefix	UriPrefix	UriPrefix
BDISipUri	SipUri	SipUri
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled

BDI 매개 변수	**EDI** 매개 변수	**CDI** 매개변수
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	PhotoUriSubstitutionToken
BDIPhotoUriWithToken	PhotoUriWithToken	PhotoUriWithToken
BDIPhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName
BDIFirstname	Firstname	Firstname
BDILastname	Lastname	Lastname
BDIEmailAddress	EmailAddress	EmailAddress
BDISipUri	SipUri	SipUri
BDIPhotoSource	PhotoSource	PhotoSource
BDIBusinessPhone	BusinessPhone	BusinessPhone
BDIMobilePhone	MobilePhone	MobilePhone
BDIHomePhone	HomePhone	HomePhone
BDIOtherPhone	OtherPhone	OtherPhone
BDIDirectoryUri	DirectoryUri	DirectoryUri
BDITitle	Title	Title
BDICompanyName	CompanyName	CompanyName
BDIUserAccountName	UserAccountName	UserAccountName
BDIDomainName	DomainName	DomainName
BDICountry	국가	국가
BDILocation	위치	위치
BDINickname	Nickname	Nickname
BDIPostalCode	PostalCode	PostalCode
BDICity	City	City

BDI 매개 변수	EDI 매개 변수	CDI 매개변수
BDIState	상태	상태
BDIStreetAddress	StreetAddress	StreetAddress

Cisco Unified Communications Manager 사용자 데이터 서비스

UDS(사용자 데이터 서비스)는 연락처 확인을 제공하는 Cisco Unified Communications Manager의 REST 인터페이스입니다.

UDS는 다음과 같은 경우 연락처 확인에 사용됩니다.

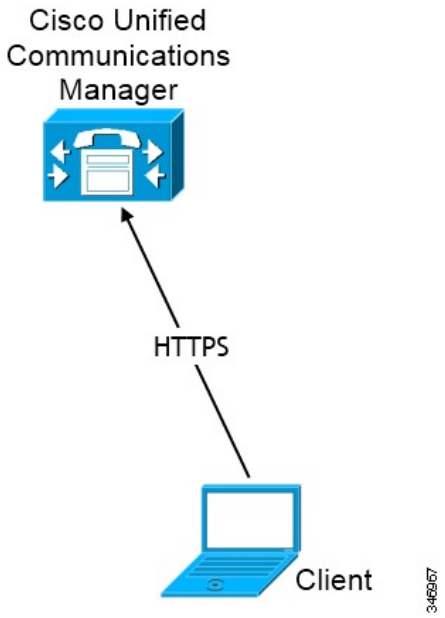
- 클라이언트 구성 파일에서 UDS 값을 사용하도록 DirectoryServerType 매개 변수를 설정하는 경우.

  이 구성을 사용하면 클라이언트가 회사 방화벽 내부 또는 외부에 있을 때 연락처 확인을 위해 UDS를 사용합니다.

- 모바일 및 Remote Access용 Expressway를 구축하는 경우.

  이 구성을 사용하면 클라이언트가 회사 방화벽 외부에 있을 때 연락처 확인을 위해 자동으로 UDS를 사용합니다.

사용자는 디렉터리 서버의 Cisco Unified Communications Manager에 연락처 데이터를 동기화합니다. 그러면 Cisco Jabber가 UDS에서 해당 연락처 데이터를 자동으로 검색합니다.



여러 클러스터를 사용한 연락처 확인

여러 개의 Cisco Unified Communications Manager 클러스터가 있는 연락처 확인의 경우 회사 디렉터리의 모든 사용자를 각 클러스터에 동기화합니다. 해당 클러스터에서 해당 사용자의 하위 집합을 프로비저닝합니다.

예를 들어 조직에 4만 명의 사용자가 있습니다. 2만 명의 사용자는 북미 지역에 있습니다. 2만 명의 사용자는 유럽에 거주합니다. 조직에는 각 위치에 대해 다음과 같은 Cisco Unified Communications Manager 클러스터가 있습니다.

- 북미의 경우 `cucm-cluster-na`
- 유럽의 경우 `cucm-cluster-eu`

이 예에서는 모든 4만 명의 사용자를 두 클러스터에 동기화합니다. `cucm-cluster-na`에서 북미의 2만 사용자를 프로비저닝하고 `cucm-cluster-eu`에서 유럽에 있는 2만 사용자를 프로비저닝합니다.

유럽의 사용자가 북미의 사용자에게 전화를 걸면 Cisco Jabber는 `cucm-cluster-na`에서 유럽의 사용자에 대한 연락처 세부 정보를 검색합니다.

북미의 사용자가 유럽의 사용자에게 전화를 걸면 Cisco Jabber는 `cucm-cluster-eu`에서 북미의 사용자에 대한 연결 세부 정보를 검색합니다.

확장 된 **UDS** 연락처 소스

UDS에서 LDAP 서버로 연락처 검색을 확장합니다. Cisco Unified Communications Manager 11.5(1) 이상에서 Jabber가 LDAP 서버를 검색하는지 여부를 구성할 수 있습니다.

LDAP 필수 조건

Cisco Jabber는 다양한 속성을 사용하여 연락처 소스를 검색하며, 이러한 속성이 모두 기본적으로 인덱싱되지는 않습니다. 효율적인 검색을 위해 Cisco Jabber에서 사용하는 특성이 인덱싱되어야 합니다.

기본 속성 매핑을 사용하는 경우 LDAP 서버에서 다음 속성이 인덱싱되어야 합니다.

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department

- givenName
- telephoneNumber
- otherTelephone
- mobile
- homePhone
- msRTCSIP-PrimaryUserAddress

LDAP 서비스 계정

Unified Communications Manager 릴리스 12.5(1) SU2에서 Unified CM은 서비스 프로파일에서 암호화된 LDAP 자격 증명을 안전하게 전달하기 위한 지원을 추가했습니다. 이 업데이트는 암호가 항상 암호화된 형식으로 저장되고 전송되도록 하여 디렉터리에 대한 액세스를 보호합니다. 이 변경 사항에는 다음 프로세스 중 암호화가 포함됩니다.

- 디렉터리 액세스 인증
- 클라이언트 구성 파일 다운로드
- BAT 가져오기/내보내기
- 업그레이드

자세한 내용은 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스, 릴리스 *12.5(1) SU2*의 릴리스 노트를 참조하십시오.

이 Unified CM 릴리스 이상이 포함된 Jabber 12.8에서는 최종 사용자 인증 후 사용자 프로파일의 일부로 LDAP 자격 증명을 다운로드하여 이 기능을 활용할 수 있습니다.

Jabber를 LDAP 서버에 연결하려면 LDAP가 Jabber 사용자를 인증하는 방법을 정의하십시오.

- 기본 옵션은 Jabber가 Kerberos 또는 클라이언트 인증서(SASL External)를 사용하여 연락처 소스 서버에 자동으로 연결하는 것입니다. 이 옵션은 가장 안전한 것이므로 이 옵션을 권장합니다.
- 서비스 프로파일이나 `jabber-config.xml` 파일에서 자격 증명을 정의하는 경우 항상 기본 옵션보다 우선합니다.
- 일반 값을 사용하여 LdapSupportedMechanisms 매개 변수를 구성하지만, 디렉터리 프로파일 사용자 이름 또는 암호를 구성하지 않을 경우 사용자가 디렉터리 자격 증명을 클라이언트에 직접 입력할 수 있습니다.
- 그렇지 않으면, 서비스 프로파일의 보안 포트에 연결하는 경우 Jabber가 연결 소스 서버에 연결하는 방법을 정의할 수 있습니다. `jabber-config.xml` 파일의 LDAP_UseCredentialsFrom 매개 변수에 Cisco Unified Communications Manager 자격 증명을 지정하여 이를 정의할 수 있습니다.
- 이전 옵션을 사용할 수 없는 경우에는 서비스 프로파일이나 `jabber-config.xml` 파일에서 제공하는 잘 알려진 자격 증명 집합을 사용하십시오. 이 옵션은 보안 수준이 가장 낮은 옵션입니다.

Jabber는 연락처 소스 서버를 인증하는 데 계정을 사용합니다. 이 계정은 디렉터리에 대한 읽기 전용 액세스 권한을 가지며 일반적으로 알려진 공개 자격 증명 집합을 사용하는 것이 좋습니다. 이 경우 모든 Jabber 사용자는 검색에 이러한 자격 증명을 사용합니다.

참고 Cisco Unified Communications Manager 12.0 버전부터는 서비스 프로파일에 사용자 이름과 암호를 구성할 수 없습니다. Jabber 사용자는 디렉터리 서비스를 사용하기 위해 자신을 인증하는 옵션이 있습니다. 처음으로 Jabber에 로그인할 때 이 알림을 받습니다. 자신을 처음에 인증하지 않을 경우 연락처 목록에 액세스하려고할 때 경고가 표시됩니다.

Jabber ID 속성 매핑

사용자 ID의 LDAP 특성은 sAMAccountName입니다. 이것은 기본 속성입니다.

사용자 ID의 속성이 sAMAccountName이 아니고 Cisco Unified Communications Manager IM and Presence Service에서 기본 IM 주소 체계를 사용 중인 경우, 다음과 같이 클라이언트 구성 파일의 매개변수에 대한 값으로 속성을 지정해야 합니다.

CDI 매개 변수는 UserAccountName입니다. <UserAccountName>attribute-name</UserAccountName>

구성에 속성을 지정하지 않고 속성이 sAMAccountName이 아닌 경우, 클라이언트는 디렉터리에서 연락처를 확인할 수 없습니다. 결과적으로 사용자는 프레즌스를 얻지 못하며 인스턴트 메시지를 보내거나 받을 수 없습니다.

Jabber ID 검색

Cisco Jabber는 Jabber ID를 사용하여 디렉터리에서 연락처 정보를 검색합니다. 다음은 디렉터리에서 검색을 최적화하는 몇 가지 옵션입니다.

- 검색 기준 - 기본적으로 클라이언트는 디렉터리 트리의 루트에서 검색을 시작합니다. 검색 기준을 사용하여 다른 검색 시작을 지정하거나 특정 그룹으로 검색을 제한할 수 있습니다. 예를 들어 사용자의 하위 집합에는 인스턴트 메시징 기능만 있습니다. OU에 이러한 사용자를 포함한 다음, 이를 검색 기준으로 지정합니다.
- 기본 필터 - 디렉터리를 쿼리할 때 사용자 개체가 아닌 다른 개체를 검색하려면 디렉터리 하위 키 이름만 지정하십시오.
- 예측 검색 필터 - 쉼표로 구분된 여러 값을 정의하여 검색 쿼리를 필터링할 수 있습니다. 기본값은 ANR(모호한 이름 확인)입니다.

이러한 옵션에 대한 자세한 내용은 *Cisco Jabber*용 매개 변수 참조 설명서에서 디렉터리 통합에 대한 장을 참조하십시오.

로컬 연락처 소스

Cisco Jabber는 로컬 연락처 소스에 액세스하고 검색하는 기능을 갖추고 있습니다. 이러한 로컬 연락처 소스에는 다음이 포함됩니다.

- Microsoft Outlook에 저장된 로컬 연락처는 Windows용 Cisco Jabber에서 액세스합니다.
- IBM Notes에 저장된 로컬 연락처는 Windows용 Cisco Jabber(릴리스 11.1)에서 액세스합니다.
- 로컬 주소록 연락처는 Mac용 Cisco Jabber, Android용 Cisco Jabber 및 iPhone 및 iPad용 Cisco Jabber에서 액세스합니다.

사용자 정의 연락처 소스

모든 클라이언트용 Cisco Jabber는 사용자가 사용자 정의 연락처를 자신의 클라이언트로 가져오는 기능을 제공합니다.

연락처 캐싱

Cisco Jabber는 로컬 캐시를 만듭니다. 다른 여러 항목 중에서 캐시는 사용자의 연락처 목록을 저장합니다. 사용자가 연락처 목록에서 사용자를 검색하는 경우 Jabber는 디렉터리 검색을 시작하기 전에 로컬 캐시에서 일치하는 항목을 검색합니다.

사용자가 연락처 목록에 없는 사용자를 검색하는 경우 Jabber는 먼저 로컬 캐시를 검색한 다음 회사 디렉터리를 검색합니다. 그런 다음 사용자가 채팅을 시작하거나 이 연락처와의 통화를 시작하는 경우 Jabber가 해당 연락처를 로컬 캐시에 추가합니다.

로컬 캐시 정보는 24시간 후에 만료됩니다.

중복 연락처 해결

Jabber의 연락처는 여러 소스에서 올 수 있습니다. Jabber는 여러 연락처 소스에서 동일한 연락처와 일치하는 항목을 찾을 수 있습니다. 이 경우 Jabber는 동일한 사람과 일치하는 레코드를 결정하고 해당 사용자의 모든 데이터를 결합합니다. 연락처 소스 중 하나의 레코드가 연락처와 일치하는지 여부를 결정하기 위해 Jabber는 다음 순서로 이러한 필드를 찾습니다.

1. **Jabber ID(JID)** - 레코드에 JID가 있는 경우 Jabber는 JID를 기준으로 레코드 일치 여부를 확인합니다. Jabber는 메일 또는 전화 번호 필드를 기준으로 더 이상 비교하지 않습니다.
2. 메일 - 레코드에 메일 필드가 있는 경우 Jabber는 메일을 기준으로 레코드 일치 여부를 확인합니다. Jabber는 전화 번호를 기준으로 레코드를 더 이상 비교하지 않습니다.
3. 전화 번호 - 레코드에 전화 번호가 있는 경우 Jabber는 전화 번호를 기준으로 레코드 일치 여부를 확인합니다.

Jabber에서 레코드를 비교하고 동일한 사용자 일치 여부를 확인하면 연락처 데이터를 병합하여 하나의 연락처 레코드를 생성합니다.

다이얼 플랜 매핑

다이얼 플랜 매핑을 구성하여 Cisco Unified Communications Manager의 다이얼 규칙이 디렉터리의 다이얼 규칙과 일치하는지 확인합니다.

애플리케이션 다이얼 규칙

애플리케이션 다이얼 규칙은 사용자가 다이얼하는 전화 번호에 자동으로 번호를 추가하거나 제거합니다. 애플리케이션 다이얼 규칙은 사용자가 클라이언트에서 다이얼하는 번호를 조작합니다.

예를 들면, 7자리 전화 번호 앞에 숫자 9를 자동으로 추가하여 외선 액세스를 제공하는 다이얼 규칙을 구성할 수 있습니다.

디렉토리 조회 다이얼 규칙

디렉터리 조회 다이얼 규칙은 클라이언트가 디렉터리에서 조회할 수 있는 번호로 발신자 ID 번호를 변환합니다. 사용자가 정의하는 각 디렉터리 조회 규칙은 처음 번호와 번호 길이를 기준으로 하여 변환할 번호를 지정합니다.

예를 들면 10자리 전화 번호에서 지역 번호와 2개의 접두사 번호를 자동으로 제거하는 디렉터리 조회 규칙을 만들 수 있습니다. 이 유형의 규칙에 대한 예는 `4089023139`를 `23139`로 변환하는 것입니다.

모바일 및 **Remote Access**용 **Cisco Unified Communication Manager UDS**

Cisco UDS communications Manager는 Cisco Jabber가 모바일 및 Remote Access용 Expressway를 사용하여 연결하는 데 사용되는 연결 소스입니다. 회사 방화벽 내에서 LDAP를 구축하는 경우 LDAP 디렉터리 서버를 Cisco Unified Communications Manager와 동기화하여 사용자가 회사 방화벽 외부에 있을 때 클라이언트가 UDS에 연결할 수 있도록 하는 것이 좋습니다.

클라우드 연락처 소스

Webex 연락처 소스

클라우드 구축의 경우 연락처 데이터가 Webex Messenger 관리 도구나 사용자 업데이트에 구성되어 있습니다. 연락처 정보는 Webex Messenger 관리 도구를 사용하여 가져올 수 있습니다. 자세한 내용은 Webex Messenger 관리 설명서의 사용자 관리 섹션을 참조하십시오.

연락처 사진 형식 및 치수

Cisco Jabber에서 최상의 결과를 얻으려면 연락처 사진에 특정 형식과 치수가 있어야 합니다. 지원되는 형식 및 최적의 치수를 검토합니다. 클라이언트가 연락처 사진에 적용하는 조정에 대해 알아봅니다.

연락처 사진 형식

Cisco Jabber는 디렉터리의 연락처 사진에 대해 다음과 같은 형식을 지원합니다.

- JPG
- PNG
- BMP

중요 Cisco Jabber는 GIF 형식의 연락처 사진에 대한 렌더링을 개선하기 위해 수정 사항을 적용하지 않습니다. 그 결과 GIF 형식의 연락처 사진은 잘못 렌더링되거나 최적 품질보다 떨어질 수 있습니다. 최고 품질을 얻으려면 연락처 사진에 PNG 형식을 사용하십시오.

연락처 사진 크기

팁 연락처 사진의 최적 크기는 가로 세로 비율이 1:1인 128 픽셀 x 128 픽셀입니다.

128 픽셀 x 128 픽셀은 Microsoft Outlook의 로컬 연락처 사진에 대한 최대 크기입니다.

다음 표에서는 Cisco Jabber의 연락처 사진에 대한 다양한 치수를 보여줍니다.

위치	치수
오디오 전용 통화 창	128 픽셀 x 128 픽셀
초대 및 미리 알림, 예: • 착신 통화 창 • 미팅 미리 알림 창	64 픽셀 x 64 픽셀

위치	치수
연락처 목록, 예: • 연락처 목록 • 참가자 등록 명부 • 통화 이력 • 음성 메시지	32 픽셀 x 32 픽셀

연락처 사진 조정

Cisco Jabber는 다음과 같이 연락처 사진을 조정합니다.

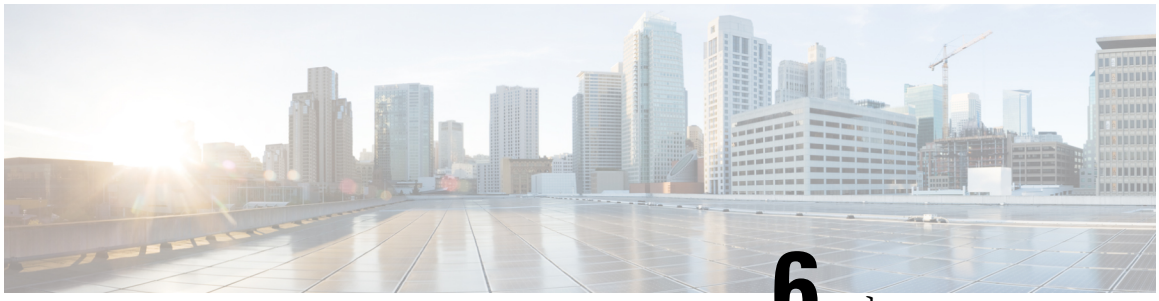
- 크기 조정 - 디렉터리의 연락처 사진이 128 픽셀 x 128 픽셀보다 작거나 큰 경우 클라이언트는 자동으로 사진 크기를 조정합니다. 예를 들어 디렉터리의 연락처 사진은 64 픽셀 x 64 픽셀입니다. Cisco Jabber가 디렉터리에서 연락처 사진을 검색하는 경우 사진 크기를 128 픽셀 x 128 픽셀로 조정 합니다.

  팁 연락처 사진을 크기 조정하면 최적의 해상도가 되지 않을 수 있습니다. 따라서 클라이언트가 크기를 자동으로 조정하지 않도록 128 픽셀 x 128 픽셀인 연락처 사진을 사용하십시오.

- 자르기 - Cisco Jabber는 정사각형이 아닌 연락처 사진을 정사각형 가로 세로 비율 또는 너비가 높이와 동일한 가로 세로 비율 1:1로 자동으로 자릅니다.
- 세로 방향 - 디렉터리의 연락처 사진이 세로 방향인 경우 클라이언트는 상단에서 30%, 하단에서 70%를 잘라냅니다.

  예를 들어 디렉터리의 연락처 사진 너비가 100 픽셀이고 높이가 200 픽셀인 경우 Cisco Jabber는 화면 가로 세로 비율 1:1을 얻기 위해 높이에서 100 픽셀을 잘라야 합니다. 이 경우 클라이언트는 사진 상단에서 30 픽셀을 자르고 사진 하단에서 70 픽셀을 잘라냅니다.
- 가로 방향 - 디렉터리의 연락처 사진이 가로 방향인 경우 클라이언트는 양쪽에서 50%를 잘라냅니다.

  예를 들어 디렉터리의 연락처 사진 너비가 200 픽셀이고 높이가 100 픽셀인 경우 Cisco Jabber는 화면 가로 세로 비율 1:1을 얻기 위해 너비에서 100 픽셀을 잘라야 합니다. 이 경우 클라이언트는 사진 오른쪽에서 50 픽셀을 자르고 사진 왼쪽에서 50 픽셀을 잘라냅니다.



6 장

보안 및 인증서

암호화

파일 전송 및 화면 캡처에 대한 준수 및 정책 제어

Cisco Unified Communications Manager IM and Presence 10.5(2) 이상에서 관리되는 파일 전송 옵션을 사용하여 파일 전송 및 화면 캡처를 전송하는 경우 감사 및 정책 적용을 위해 파일을 준수 서버로 보낼 수 있습니다.

준수에 대한 자세한 내용은 *Cisco Unified Communications Manager*의 *IM and Presence* 서비스에 대한 인스턴트 메시징 준수 설명서를 참조하십시오.

파일 전송 및 화면 캡처 구성에 대한 자세한 내용은 *Cisco Unified Communications Manager IM and Presence* 구축 및 설치 설명서를 참조하십시오.

인스턴트 메시지 암호화

Cisco Jabber는 TLS(Transport Layer Security)를 사용하여 클라이언트와 서버 사이에서 네트워크를 통해 확장 가능한 메시징 및 프레즌스 상태 프로토콜(XMPP) 트래픽을 보호합니다. Cisco Jabber는 포인트간 인스턴트 메시지를 암호화합니다.

온프레미스 암호화

다음 표에는 온프레미스 구축의 인스턴트 메시지 암호화에 대한 세부 정보가 요약되어 있습니다.

연결	프로토콜	협상 인증서	예상 암호화 알고리즘
클라이언트에서 서버로	TLS v1.2를 통한 XMPP	X.509 공개 키 인프라 인증서	AES 256비트

서버 및 클라이언트 협상

다음 서버는 X.509 PKI(공개 키 인프라) 인증서를 사용하여 Cisco Jabber와 TLS 암호화를 협상합니다.

- Cisco Unified Communications Manager IM and Presence
- Cisco Unified Communications Manager

서버 및 클라이언트가 TLS 암호화를 협상하면 클라이언트와 서버 모두 인스턴트 메시징 트래픽을 암호화하기 위해 세션 키를 생성하고 교환합니다.

다음 표는 Cisco Unified Communications Manager IM and Presence Service의 PKI 인증서 키 길이를 나열합니다.

버전	키 길이
Cisco Unified Communications Manager IM and Presence Service 버전 9.0.1 이상	2048비트

XMPP 암호화

Cisco Unified Communications Manager IM and Presence Service는 Cisco Jabber와 프레즌스 서버 간의 인스턴트 메시지 트래픽을 보호하기 위해 AES 알고리즘을 사용하 여 암호화된 256비트 길이 세션 키를 사용합니다.

서버 노드 간 트래픽에 대한 추가 보안이 필요한 경우 Cisco Unified Communications Manager IM and Presence Service에서 XMPP 보안 설정을 구성할 수 있습니다. 보안 설정에 대한 자세한 내용은 다음을 참조하십시오.

- Cisco Unified Communications Manager IM and Presence Service—*IM and Presence*의 보안 구성

인스턴트 메시징 로깅

규정 지침을 준수하기 위해 인스턴트 메시지를 기록하고 보관할 수 있습니다. 인스턴트 메시지를 기록하려면 외부 데이터베이스를 구성하거나 타사 컴플라이언스 서버와 통합합니다. Cisco Unified

Communications Manager IM and Presence Service는 외부 데이터베이스 또는 타사 컴플라이언스 서버에서 로그인하는 인스턴트 메시지를 암호화하지 않습니다. 기록하는 인스턴트 메시지를 보호하려면 외부 데이터베이스 또는 타사 컴플라이언스 서버를 적절하게 구성해야 합니다.

규정 준수에 대한 자세한 내용은 다음을 참조하십시오.

- Cisco Unified Communications Manager IM and Presence Service—*IM and Presence* 서비스를 위한 인스턴트 메시징 규정 준수

대칭 키 알고리즘(예: AES) 또는 공개 키 알고리즘(예: RSA)을 포함하여 암호화 수준 및 암호화 알고리즘에 대한 자세한 내용은 이 링크 https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html의 차세대 암호화를 참조하십시오.

X.509 공개 키 인프라 인증서에 대한 자세한 내용은 이 링크 https://www.ietf.org/rfc/rfc2459.txt의 인터넷 *X.509* 공개 키 인프라 인증서 및 *CRL* 프로파일 문서를 참조하십시오.

클라우드 기반 암호화

다음 표에는 클라우드 기반 구축의 인스턴트 메시지 암호화에 대한 세부 정보가 요약되어 있습니다.

연결	프로토콜	협상 인증서	예상 암호화 알고리즘
클라이언트에서 서버로	TLS 내 XMPP	X.509 공개 키 인프라 인증서	AES 128비트
클라이언트-클라이언트	TLS 내 XMPP	X.509 공개 키 인프라 인증서	AES 256비트

서버 및 클라이언트 협상

다음 서버는 Webex Messenger 서비스가 있는 X.509 PKI(공개 키 인프라) 인증서를 사용하여 Cisco Jabber와 TLS 암호화를 협상합니다.

서버 및 클라이언트가 TLS 암호화를 협상하면 클라이언트와 서버 모두 인스턴트 메시징 트래픽을 암호화하기 위해 세션 키를 생성하고 교환합니다.

XMPP 암호화

Webex Messenger 서비스에서는 AES 알고리즘을 사용하여 암호화된 128비트 세션 키를 사용하여 Cisco Jabber 및 Webex Messenger 서비스 간의 인스턴트 메시지 트래픽을 보호합니다.

선택적으로 256비트 클라이언트-클라이언트 간 AES 암호화를 활성화하여 클라이언트 간의 트래픽을 보호할 수 있습니다.

인스턴트 메시징 로깅

Webex Messenger 서비스는 인스턴트 메시지를 기록할 수 있지만 이러한 인스턴트 메시지를 암호화된 형식으로 보관하지는 않습니다. 그러나 Webex Messenger 서비스는 SAE-16 및 ISO-27001 감사를 포함하여 엄격한 데이터 센터 보안을 사용하여 로그에 기록하는 인스턴트 메시지를 보호합니다.

AES 256비트 클라이언트-클라이언트 간 암호화를 활성화하면 Webex Messenger 서비스에서 인스턴트 메시지를 기록할 수 없습니다.

대칭 키 알고리즘(예: AES) 또는 공개 키 알고리즘(예: RSA)을 포함하여 암호화 수준 및 암호화 알고리즘에 대한 자세한 내용은 이 링크 https://www.cisco.com/c/en/us/about/security-center/next-generation-cryptography.html의 차세대 암호화를 참조하십시오.

X.509 공개 키 인프라 인증서에 대한 자세한 내용은 이 링크 https://www.ietf.org/rfc/rfc2459.txt의 인터넷 *X.509* 공개 키 인프라 인증서 및 *CRL* 프로파일 문서를 참조하십시오.

클라이언트 간 암호화

기본적으로 클라이언트와 Cisco Webex Messenger 서비스 간의 인스턴트 메시징 트래픽은 안전합니다. 선택적으로 Cisco Webex 관리 도구에서 정책을 지정하여 클라이언트 간 인스턴트 메시징 트래픽을 보호할 수 있습니다.

다음 정책은 인스턴트 메시지에 대한 클라이언트 간 암호화를 지정합니다.

- **IM**에 대한 **AES** 인코딩 지원 - 전송 클라이언트는 AES 256비트 알고리즘을 사용 하여 인스턴트 메시지를 암호화합니다. 수신 클라이언트는 인스턴트 메시지의 암호를 해독합니다.
- **IM**에 대한 인코딩 지원 없음 - 클라이언트는 암호화를 지원하지 않는 다른 클라이언트와 인스턴트 메시지를 주고 받을 수 있습니다.

다음 표에서는 이러한 정책으로 설정할 수 있는 다양한 조합에 대해 설명합니다.

정책 조합	클라이언트 간 암호화	원격 클라이언트가 **AES** 암호화를 지원하는 경우	원격 클라이언트가 **AES** 암호화를 지원하지 않는 경우
IM에 대한 **AES** 인코딩 지원 = 거짓 **IM**에 대한 인코딩 지원 안 함 = 참	아니요	Cisco Jabber 암호화되지 않은 인스턴트 메시지를 전송합니다. Cisco Jabber 키 교환을 협상하지 않습니다. 그 결과, 다른 클라이언트는 Cisco Jabber 암호화된 인스턴트 메시지를 전송하지 않습니다.	Cisco Jabber 암호화되지 않은 인스턴트 메시지를 보내고 받습니다.
IM에 대한 **AES** 인코딩 지원 = 참 **IM**에 대한 인코딩 지원 안 함 = 참	예	Cisco Jabber 암호화된 인스턴트 메시지를 보내고 받습니다. Cisco Jabber 인스턴트 메시지가 암호화되었음을 나타내는 아이콘을 표시합니다.	Cisco Jabber 암호화된 인스턴트 메시지를 전송합니다. Cisco Jabber 암호화되지 않은 인스턴트 메시지를 수신합니다.

정책 조합	클라이언트 간 암호화	원격 클라이언트가 **AES** 암호화를 지원하는 경우	원격 클라이언트가 **AES** 암호화를 지원하지 않는 경우
IM에 대한 **AES** 인코딩 지원 = 참 **IM**에 대한 인코딩 지원 안 함 = 거짓	예	Cisco Jabber 암호화된 인스턴트 메시지를 보내고 받습니다. Cisco Jabber 인스턴트 메시지가 암호화되었음을 나타내는 아이콘을 표시합니다.	Cisco Jabber 원격 클라이언트로 인스턴트 메시지를 보내거나 받지 않습니다. Cisco Jabber 사용자가 원격 클라이언트로 인스턴트 메시지를 보내려고 할 때 오류 메시지를 표시합니다.

참고 Cisco Jabber에서는 그룹 채팅을 통한 클라이언트 간 암호화를 지원하지 않습니다.Cisco Jabber는 포인트 간 채팅에 대해서만 클라이언트 간 암호화를 사용합니다.

암호화 및 Cisco Webex 정책에 대한 자세한 내용은 Cisco Webex 설명서의 암호화 수준 정보를 참조하십시오.

암호화 아이콘

클라이언트가 암호화 수준을 표시하기 위해 표시하는 아이콘을 검토합니다.

클라이언트와 서버 간 암호화 잠금 아이콘

온프레미스 및 클라우드 기반 구축에서 Cisco Jabber는 클라이언트가 서버에 암호를 제공하라는 것을 나타내는 다음 아이콘을 표시합니다.

클라이언트 간 암호화 잠금 아이콘

클라우드 기반 구축에서 Cisco Jabber는 클라이언트가 서버에 암호를 제공하라는 것을 나타내는 다음 아이콘을 표시합니다.

로컬 채팅 기록

참가자가 채팅 창을 닫은 후 참가자가 로그아웃할 때까지 채팅 기록이 유지됩니다. 참가자가 채팅 창을 닫은 후 채팅 기록을 유지하지 않으려면 Disable_IM_History 매개 변수를 true로 설정합니다. 이 매개 변수는 IM 전용 사용자를 제외한 모든 클라이언트에서 사용할 수 있습니다.

Mac용 Cisco Jabber의 온프레미스 구축의 경우 Mac용 Cisco Jabber의 채팅 환경설정 창에서 채팅 아카이브를 다음 위치에 저장**:** 옵션을 선택하는 경우 채팅 기록은 Mac 파일 시스템에 로컬로 저장되며 스포트라이트를 사용하여 검색할 수 있습니다.

Cisco Jabber는 로컬 채팅 기록이 활성화되어 있을 때 보관된 인스턴트 메시지를 암호화하지 않습니다.

데스크톱 클라이언트의 경우, 아카이브 저장을 통한 채팅 기록에 대한 액세스를 다음 디렉터리로 제한할 수 있습니다.

- Windows, `%USERPROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\History\uri.db`
- Mac: `~/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/History/uri.db`.

모바일 클라이언트의 경우 채팅 기록 파일에 액세스할 수 없습니다.

음성 및 비디오 암호화

선택적으로 모든 장치에 대 한 보안 전화기 기능을 설정할 수 있습니다. 보안 전화기 기능은 보안 SIP 신호 처리, 보안 미디어 스트림 및 암호화된 장치 구성 파일을 제공합니다.

사용자에 대한 보안 전화기 기능을 활성화한 경우, Cisco Unified Communications Manager에 대한 장치 연결은 안전합니다. 그러나 다른 장치를 사용한 통화는 두 장치에 모두 보안 연결이 있는 경우에만 안전합니다.

보안 미디어에 대한 인증 방법

SIP oAuth를 사용하여 토큰 기반 인증에서 보안 미디어를 활성화합니다. 온프레미스, 클라우드 및 Jabber의 하이브리드 구축의 보안 인증에 대한 CAPF 등록 대신 SIP oAuth를 설정할 수 있습니다.

SIP oAuth
Cisco Unified Communications Manager 설정에서 한 번 수행합니다. 이는 RTP 미디어를 포함하여 SIP 트래픽이 안전하다는 것을 확인합니다.

CAPF 등록
CAPF 등록 활성화에 대한 워크플로는 다음과 같습니다.

- Jabber 장치 만들기 및 구성
- 인증 문자열
- 전화기 보안 프로파일 구성

PIE ASLR 지원

Android, iPhone 및 iPad용 Cisco Jabber는 PIE ASLR(Position Independent Executable Address Space Layout Randomization)을 지원합니다.

Federal Information Processing Standards

FIPS(Federal Information Processing Standard) 140은 암호화 모듈에 대한 보안 요건을 지정하는 미국 정부 표준입니다. 이러한 암호화 모듈에는 승인된 보안 기능을 구현하고 암호화 경계 내에 포함되는 하드웨어, 소프트웨어 및 펌웨어 집합이 포함됩니다.

FIPS를 사용하려면 클라이언트 내에서 사용되는 모든 암호화, 키 교환, 디지털 서명 및 해시 및 난수 생성 기능이 암호화 모듈 보안에 대한 FIPS 140.2 요구 사항을 준수해야 합니다.

FIPS 모드는 클라이언트가 인증서를 더 엄격하게 관리합니다. 서비스에 대한 인증서가 만료되고 해당 자격 증명을 다시 입력하지 않은 경우 FIPS 모드 사용자에게 클라이언트의 인증서 오류가 표시될 수 있습니다. 허브 창에 FIPS 아이콘을 표시하여 클라이언트가 FIPS 모드에서 실행 중임을 나타냅니다.

Windows용 **Cisco Jabber**에 대해 **FIPS** 활성화

Windows용 Cisco Jabber는 FIPS를 활성화하는 두 가지 방법을 지원합니다.

- 운영 체제 활성화됨 - Windows 운영 체제가 FIPS 모드에 있습니다.
- Cisco Jabber 부트스트랩 설정 - FIPS_MODE 설치 관리자 스위치를 구성합니다. Cisco Jabber는 FIPS가 활성화되어 있지 않은 운영 체제의 FIPS 모드에 있을 수 있습니다. 이 시나리오에서는 비 Windows API를 사용한 연결만 FIPS 모드입니다.

표 ***8: FIPS***에 대한 ***Windows***용 ***Cisco Jabber*** 설정

플랫폼 모드	부트스트랩 설정	**Cisco Jabber** 클라이언트 설정
FIPS 활성화	FIPS 활성화	FIPS 활성화 - 부트스트랩 설정입니다.
FIPS 활성화	FIPS 비활성화됨	FIPS 비활성화 - 부트스트랩 설정입니다.
FIPS 활성화	설정 없음	FIPS 활성화 - 플랫폼 설정입니다.
FIPS 비활성화됨	FIPS 활성화	FIPS 활성화 - 부트스트랩 설정입니다.
FIPS 비활성화됨	FIPS 비활성화됨	FIPS 비활성화 - 부트스트랩 설정입니다.
FIPS 비활성화됨	설정 없음	FIPS 비활성화 - 플랫폼 설정입니다.

참고 Jabber 음성 메일 서비스는 SSL 연결 중에 **https://164.62.224.15/vmrest/version with FIPS enabled** HTTPs 요청에 대해서만 TLS 버전 TLS 1.2를 허용합니다.

모바일 클라이언트용 **Cisco Jabber**에 대해 **FIPS** 활성화

모바일 클라이언트용 Cisco Jabber에 대해 FIPS를 활성화하려면 EMM(Enterprise Mobility Management)에서 FIPS_MODE 매개 변수를 TRUE로 설정합니다.

중요
- FIPS를 활성화하면 사용자가 신뢰할 수 없는 인증서를 받을 수 있는 기능이 제거됩니다. 이 경우 일부 서비스를 사용하지 못할 수 있습니다. CTL(인증서 신뢰 목록) 또는 ITL 파일은 여기에 적용되지 않습니다. 서버 인증서가 올바르게 서명되어야 합니다. 그렇지 않으면 클라이언트가 사이드 로딩을 통해 서버 인증서를 신뢰하도록 해야 합니다.
- FIPS는 TLS 1.2를 적용하므로 이전 프로토콜은 비활성화됩니다.
- 모바일 클라이언트용 Cisco Jabber는 플랫폼 모드를 지원하지 않습니다.

공통평가기준

정보 기술 보안 평가에 대한 일반 기준은 IT 제품의 보안 특성을 평가하는 데 사용되는 일련의 국제 표준을 구성합니다. 일반 기준 인증 요구 사항을 준수하는 모드에서 Cisco Jabber를 실행할 수 있습니다. 이렇게 하려면 각 클라이언트에 대해 이 기능을 활성화해야 합니다.

일반 기준으로 활성화된 환경에서 Jabber를 실행하려면 다음을 수행합니다.

- Windows용 Jabber: CC_MODE 설치 인수를 TRUE로 설정합니다.
- Android용 Jabber 및 iPhone 및 iPad용 Jabber: EMM(Enterprise Mobility Management)에서 CC_MODE 매개 변수를 TRUE로 설정합니다.
- RSA 키 길이는 2048비트 이상이어야 합니다. RSA 키 길이를 구성하려면 *Cisco Jabber 12.5* 온프레미스 구축 설명서에서 *Cisco Jabber* 장치를 만들고 구성하는 방법에 대해 읽어 보십시오.

Jabber를 Common Criteria 모드에서 실행하도록 설정하는 방법에 대 한 자세한 내용은 *Cisco Jabber 12.5* 온프레미스 구축 설명서에서 *Cisco Jabber* 애플리케이션 구축 방법을 읽어 보십시오.

보안 **LDAP**

보안 LDAP 통신은 SSL/TLS를 통한 LDAP입니다.

LDAPS는 SSL/TLS 연결을 통해 LDAP 연결을 시작합니다. 그러면 SSL 세션이 열리고 LDAP 프로토콜을 사용하기 시작합니다. 이를 위해서는 별도의 포트, 636 또는 글로벌 카탈로그 포트 3269가 필요합니다.

인증된 UDS 연락처 검색

Cisco Unified Communications Manager에서 UDS 연락처 검색에 대한 인증을 활성화하 고 Cisco Jabber는 연락처 검색을 위해 UDS를 인증하는 자격 증명을 제공합니다.

인증서

인증서 확인

인증서 확인 프로세스

운영 체제 Cisco Jabber는 서비스를 인증할 때 서버 인증서의 유효성을 확인할 때 실행됩니다. 보안 연결을 설정하는 동안에는 서비스가 Cisco Jabber에 인증서를 제공합니다. 운영 체제는 클라이언트 장치의 로컬 인증서 저장소에 있는 것과 비교하여 제시된 인증서의 유효성을 확인합니다. 인증서가 인증서 저장소에 없는 경우 인증서는 신뢰할 수 없는 것으로 간주되고 Cisco Jabber는 사용자에게 인증서를 허용하거나 거부하라는 메시지를 표시합니다.

사용자가 인증서를 수락하면 Cisco Jabber는 서비스에 연결하고 장치의 인증서 저장소나 키 체인에 인증서를 저장합니다. 사용자가 인증서를 거부하는 경우 Cisco Jabber는 서비스에 연결하지 않고 인증서가 장치의 인증서 저장소나 키 체인에 저장되지 않습니다.

인증서가 장치의 로컬 인증서 저장소에 있는 경우 인증서를 Cisco Jabber는 인증서를 신뢰합니다. Cisco Jabber는 사용자에게 인증서를 수락 또는 거절할지 묻지 않고 서비스에 연결합니다.

Cisco Jabber 조직에 구축된 항목에 따라 여러 서비스를 인증할 수 있습니다. 각 서비스에 대해 CSR(인증서 서명 요청)을 생성해야 합니다. 일부 공개 인증 기관은 FQDN(Fully Qualified Domain Name) 당 두 개 이상의 CSR을 허용하지 않습니다. 이는 각 서비스의 CSR을 별도의 공개 인증 기관에 보내야 할 수 있음을 의미합니다.

IP 주소 또는 호스트 이름 대신 각 서비스에 대한 서비스 프로파일에 FQDN을 지정했는지 확인하십시오.

서명된 인증서

인증서는 자체 서명 인증서일 수도 있고 CA(인증 기관)에서 서명한 인증서일 수도 있습니다.

- CA 서명 인증서(권장) - 장치에 인증서를 설치하고 있으므로 사용자에게 프롬프트가 표시되지 않습니다. CA 서명 인증서는 사설 CA 또는 공용 CA에서 서명할 수 있습니다. 공용 CA가 서명한 많은 인증서는 장치의 인증서 저장소 또는 키 체인에 저장됩니다. Android 7.0 이상을 사용하는 장치는 CA 서명 인증서만 인식합니다.

- 자체 서명 인증서 - 인증서를 제공하는 서비스에 의해 인증서가 서명되며, 사용자에게 인증서를 허용 또는 거부할 것인지 묻는 메시지가 항상 표시됩니다.

인증서 확인 옵션

인증서 확인을 설정하기 전에 인증서의 유효성을 확인할 방법을 결정해야 합니다.

- 온프레미스 또는 클라우드 기반 구축에 대한 인증서를 구축하는지 여부.
- 인증서에 서명하는 데 사용하는 방법.
- CA 서명 인증서를 구축하는 경우에는 공개 CA 또는 비공개 CA를 사용할지 여부.
- 인증서를 얻는 데 필요한 서비스.

온프레미스 서버에 필요한 인증서

온프레미스 서버는 다음 인증서를 제공하여 Cisco Jabber와의 보안 연결을 설정합니다.

서버	인증서
Cisco Unified Communications Manager IM and Presence Service	HTTP(Tomcat) XMPP
Cisco Unified Communications Manager	HTTP(Tomcat) 및 CallManager 인증서(보안 전화기에 대한 보안 SIP 통화 신호 처리)
Cisco Unity Connection	HTTP(Tomcat)
Webex Meetings 서버	HTTP(Tomcat)
Cisco VCS Expressway Cisco Expressway-E	서버 인증서(HTTP, XMPP 및 SIP 통화 신호 처리에 사용됨)

중요 참고 사항

- SAML(Security Assertion Markup Language) SSO(Single Sign-On) 및 IdP(ID 공급자)에는 x.509 인증서가 필요합니다.
- 인증서 서명 프로세스를 시작하기 전에 Cisco Unified Communications Manager IM and Presence Service에 대해 최근 서비스 업데이트(SU)를 적용해야 합니다.
- 필요한 인증서는 모든 서버 버전에 적용됩니다.
- 각 클러스터 노드의 경우 가입자 및 게시자는 Tomcat 서비스를 실행하고 클라이언트에 HTTP 인증서를 제공할 수 있습니다.

  클러스터의 각 노드에 대해 인증서에 서명하도록 계획해야 합니다.

- 클라이언트 및 Cisco Unified Communications Manager 간 SIP 신호 처리를 보호하려면 CAPF(인증 기관 프록시 기능) 등록을 사용해야 합니다.

인증서 서명 요청 형식 및 요구 사항

일반적으로 CA(인증 기관)에는 특정 형식을 준수하기 위해 CSR(인증서 서명 요청)이 필요합니다. 예를 들어, 공개 CA는 다음과 같은 요구 사항이 있는 CSR만 받아들일 수 있습니다.

- Base64로 인코딩됩니다.
- 조직, **OU** 또는 기타 필드에 특정 문자(예: `@&!`)를 포함하지 마십시오.
- 서버의 공개 키에서 특정 비트 길이를 사용합니다.

여러 노드에서 CSR을 제출하는 경우, 공용 CA가 모든 CSR에서 일관되게 정보를 받도록 요구할 수 있습니다.

CSR에 대한 문제를 방지하려면 CSR을 제출하려는 공용 CA의 형식 요구 사항을 검토해야 합니다. 그런 다음 서버를 구성할 때 입력하는 정보가 공개 CA에 필요한 형식을 준수하는지 확인해야 합니다.

FQDN 당 인증서 하나 - 일부 공개 CA는 FQDN(Fully Qualified Domain Name) 당 하나의 인증서만 서명합니다.

예를 들어 단일 Cisco Unified Communications Manager IM and Presence Service 노드에 대한 HTTP 및 XMPP 인증서에 서명하려면 각 CSR을 서로 다른 공용 CA에 제출해야 할 수 있습니다.

해지 서버

해지 서버에 연결할 수 없는 경우 Cisco Jabber에서 Cisco Unified Communications Manager 서버에 연결할 수 없습니다. CA(인증 기관)에서 인증서를 해지하는 경우에는 Cisco Jabber에서 사용자가 해당 서버에 연결할 수 없습니다.

사용자에게 다음 결과에 대한 알림이 표시 되지 않습니다.

- 인증서에 해제 정보가 포함되어 있지 않습니다.
- 해지 서버에 연결할 수 없습니다.

인증서를 확인하려면 인증서에 해지 정보를 제공할 수 있는 연결 가능한 서버의 **CDP** 또는 **AIA** 필드에 HTTP URL이 포함되어 있어야 합니다.

CA에서 발급한 인증서를 가져올 때 인증서가 유효한지 확인하려면 다음 요구 사항 중 하나를 충족해야 합니다.

- **CRL** 구축 지점(CDP) 필드에 해지 서버의 CRL(인증서 해지 목록)에 대한 HTTP URL이 포함되어 있는지 확인합니다.
- 기관 정보 액세스(AIA) 필드에 OCSP(온라인 인증서 상태 프로토콜) 서버에 대한 HTTP URL이 포함되어 있는지 확인합니다.

인증서의 서버 ID

서명 프로세스의 일부로 CA는 인증서에 서버 ID를 지정합니다. 클라이언트가 인증서를 확인할 때 다음 사항을 확인합니다.

- 신뢰할 수 있는 기관에서 인증서를 발급했습니다.
- 인증서를 제공하는 서버의 ID가 인증서에 지정된 서버의 ID와 일치합니다.

참고 일반적으로 공개 CA에는 IP 주소가 아닌 서버 ID로서 FQDN(Fully Qualified Domain Name)이 필요합니다.

식별자 필드

클라이언트는 ID 일치를 위해 서버 인증서에서 다음 식별자 필드를 확인합니다.

- XMPP 인증서
  - `SubjectAltName\OtherName\xmppAddr`
  - `SubjectAltName\OtherName\srvName`
  - `SubjectAltName\dnsNames`
  - 제목 `CN`
- HTTP 인증서
  - `SubjectAltName\dnsNames`
  - 제목 `CN`

팁 제목 `CN` 필드에는 와일드카드(*)를 가장 왼쪽에 있는 문자로 사용할 수 있습니다(예: `*.cisco.com`).

ID 불일치 방지

사용자가 IP 주소 또는 호스트 이름을 사용하여 서버에 연결을 시도하고 서버 인증서가 FQDN을 사용하여 서버를 식별하는 경우 클라이언트는 서버를 신뢰할 수 있는 것으로 식별하고 사용자에게 메시지를 표시합니다.

서버 인증서가 FQDN을 사용하는 서버를 식별하는 경우 서버의 여러 위치에서 각 서버 이름을 FQDN으로 지정하도록 계획해야 합니다. 자세한 내용은 문제 해결 기술 노트의 *ID* 불일치 방지 섹션을 참조하십시오.

다중 서버 SAN용 인증서

다중 서버 SAN을 사용하는 경우에는 tomcat 인증서당 클러스터당, XMPP 인증서당 클러스터당 각각 한 번씩만 서비스에 인증서를 업로드하면 됩니다. 다중 서버 SAN을 사용하지 않는 경우에는 모든 Cisco Unified Communications Manager 노드의 서비스에 인증서를 업로드해야 합니다.

클라우드 구축을 위한 인증서 확인

Webex Messenger및 Webex Meetings Center는 기본적으로 다음 인증서를 클라이언트에 제공합니다.

- CAS
- WAPI

참고 Webex 공공 CA(Certificate Authority)가 인증서에 서명합니다. Cisco Jabber는 이러한 인증서의 유효성을 확인하여 클라우드 기반 서비스와의 보안 연결을 설정합니다.

Cisco Jabber은(는) Webex Messenger에서 수신한 다음 XMPP 인증서를 확인합니다. 이러한 인증서가 운영체제에 포함되어 있지 않다면, 해당 인증서를 제공해야 합니다.

- VeriSign Class 3 Public Primary Certification Authority - G5 - 이 인증서는 신뢰할 수 있는 루트 인증 기관에 저장됩니다.
- VeriSign Class 3 Secure Server CA - G3 - 이 인증서는 Webex Messenger 서버 ID를 확인하며 Intermediate Certificate Authority에 저장됩니다.
- AddTrust External CA Root
- GoDaddy Class 2 Certification Authority 루트 인증서

Windows용 Cisco Jabber의 루트 인증서에 관한 자세한 내용은 https://www.identrust.co.uk/certificates/trustid/install-nes36.html을(를) 참조하십시오.

Mac용 Cisco Jabber의 루트 인증서에 관한 자세한 내용은 https://support.apple.com을(를) 참조하십시오.

다중 테넌트 호스팅 협업 솔루션에 대한 서버 이름 표시 지원

Cisco Jabber는 다중 테 넌 트 호스팅 협업 솔루션을 사용 하 여 MRA (Remote Access) 구축에서 SNI (서버 이름 표시)를 지원 합니다.

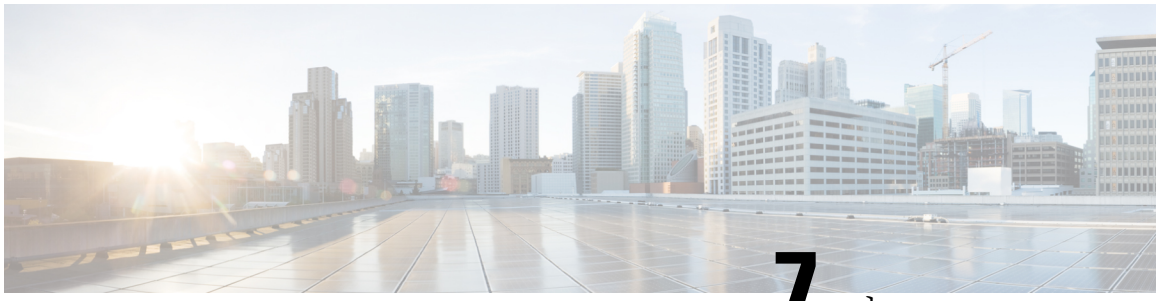
Cisco Jabber는 SNI를 사용하여 도메인 정보를 Expressway로 전송합니다. Expressway는 인증서 저장소를 조회하여 도메인 정보가 포함된 인증서를 찾고 인증서를 Cisco Jabber에 반환하여 유효성을 확인합니다.

다중 테넌트 구축에 대한 자세한 내용은 Cisco Hosted Collaboration Solution, 릴리스 11.5 다중 테넌트 Expressway 구성 설명서의 도메인 인증서를 사용한 엔드포인트 서비스 검색 및 도메인 인증서를 사용한 *Jabber Service* 검색 섹션을 참조하십시오.

바이러스 백신 제외

바이러스 백신 소프트웨어를 구축하는 경우 바이러스 백신 제외 목록에 다음 폴더 위치를 포함하십시오.

- `C:\Users\<User>\AppData\Local\Cisco\Unified Communications\Jabber`
- `C:\Users\<User>\AppData\Roaming\Cisco\Unified Communications\Jabber`
- `C:\ProgramData\Cisco Systems\Cisco Jabber`



7 장

컨피그레이션 관리

빠른 로그인

이 기능을 사용하면 전처럼 순차적인 로그인 프로세스 대신 모든 Cisco Jabber 서비스에 동시에 로그인할 수 있습니다. 각 서비스가 개별적으로 각각의 서버에 연결되어 캐시된 데이터를 기반으로 사용자를 인증합니다. 이렇게 하면 로그인 프로세스가 빠르고 동적으로 처리됩니다. 그러나 이 기능은 Jabber에 다시 로그인할 때만 유효합니다.

빠른 로그인은 모든 클라이언트에 대해 STARTUP_AUTHENTICATION_REQUIRED 매개변수를 사용하여 설정할 수 있습니다. 그러나, 모바일 클라이언트의 경우 STARTUP_AUTHENTICATION_REQUIRED 및 CachePasswordMobile 매개 변수를 모두 구성해야 합니다. 이러한 매개 변수를 구성하는 자세한 내용은 최신 *Cisco Jabber*용 매개 변수 참조 설명서를 참조하십시오.

구성 다시 가져오기 - 빠른 로그인은 모든 로그인 또는 로그아웃 시 서버측 설정을 동기적으로 검색하지 않습니다. 이는 이전 Jabber 릴리스의 첫 번째 로그인 중에만 발생합니다.

후속 로그인의 경우에는 로그인 후 1 ~ 5분 내에 여러 지점에 있는 서버로부터 새로운 구성을 가져오거나, 로그인 후 7시간 내에 또는 사용자가 구성 가져오기에 대한 수동 새로 고침을 수행할 때마다 요청이 전송됩니다.

서버에서 7 ~ 8시간 마다 구성을 가져오도록 ConfigRefetchInterval 매개 변수를 구성할 수 있습니다. 이 매개 변수에 대한 자세한 내용은 최신 *Cisco Jabber*용 매개 변수 참조 설명서를 참조하십시오.

동적 구성 변경에 대한 작업

Jabber 11.9에서는 구성 변경에 대한 구성 요소 및 서비스가 동적으로 반응합니다. 다음 시나리오에 따라 Jabber에서 로그아웃하거나 재설정하라는 알림 메시지가 표시됩니다.

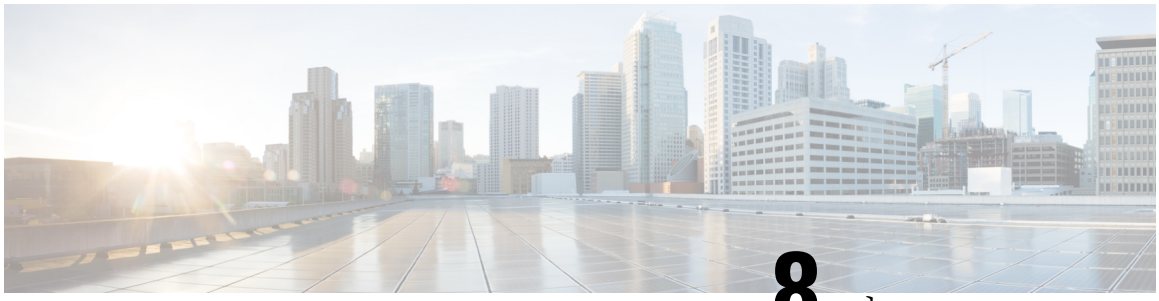
Jabber 재설정 - 기본 서비스가 변경된 경우 Jabber를 재설정하라는 알림 메시지가 표시됩니다. 예를 들어, IM&P 및 전화 통신 계정이 전화기 전용 계정으로 변경되는 경우 Jabber를 재설정해야 합니다.

Jabber에서 로그아웃 - 다음 표에 나열된 구성 키에 변경 사항이 있는 경우 Jabber가 사용자에게 로그아웃한 후 다시 로그인하여 새 구성을 사용하라는 메시지를 표시합니다.

- **Windows** - 구성이 변경되었다는 팝업 알림을 수신합니다. 알림을 무시하거나 로그아웃한 후 로그인하여 새 구성을 사용할 수 있습니다.
- 모바일 클라이언트 - Jabber가 자동으로 로그아웃됩니다. 그런 다음 구성이 변경되었음을 나타내는 팝업 알림을 수신합니다. 확인을 클릭하여 Jabber에 자동으로 로그인하는 구성 변경 사항을 승인합니다.

키 이름	플랫폼	사인아웃
RemoteAccess	모든 클라이언트	로그아웃
Meetings_Enabled	모든 클라이언트	로그아웃
DirectoryServerType	모든 클라이언트	로그아웃
DirectoryUri	모든 클라이언트	로그아웃
UseSipUriToResolveContacts	모든 클라이언트	로그아웃
SipUri	모든 클라이언트	로그아웃
UriPrefix	모든 클라이언트	로그아웃
DirectoryUriPrefix	모든 클라이언트	로그아웃
SwapDisplayNameOrder	모든 클라이언트	로그아웃
PresenceDomain	모든 클라이언트	로그아웃
Support_SSL_Encoding	모든 클라이언트	로그아웃
Support_No_Encoding	모든 클라이언트	로그아웃
IM_Logging_Enabled	모든 클라이언트	로그아웃
IGS_CUP_ENABLESECURE	모든 클라이언트	로그아웃
DISALLOW_FILE_TRANSFER_ON_MOBILE	모든 클라이언트	로그아웃
Persistent_Chat_Enabled	데스크톱 클라이언트	로그아웃
Persistent_Chat_Mobile_Enabled	□모바일클라이언트	로그아웃
Disable_MultiDevice_Message	모든 클라이언트	로그아웃
Location_Enabled/Location_Matching_Mode	모든 클라이언트	로그아웃
IP_MODE	모든 클라이언트	로그아웃
Telephony_Enabled	모든 클라이언트	로그아웃
Voicemail_Enabled	모든 클라이언트	로그아웃
EnableLoadAddressBook	□모바일클라이언트	로그아웃
ShowRecentsTab	Jabber Windows만 해당	로그아웃
IM_Enabled	모든 클라이언트	로그아웃

키 이름	플랫폼	사인아웃
Disallow-jaibreak-device	□모바일클라이언트	로그아웃
EnableChats	Jabber Windows만 해당	로그아웃



8 장

화면 공유

화면 공유

화면 공유 유형은 다음 네 가지입니다.

- Cisco Webex Share
- BFCP 공유
- IM 전용 공유
- 미팅으로 에스컬레이션 및 공유

Webex 화면 공유

클라우드 구축에서 데스크톱 클라이언트용 Cisco Jabber에 적용합니다.

클라우드 구축의 경우 BFCP 및 IM 전용 화면 공유 옵션을 사용할 수 없는 경우 연락처를 선택한 후에 Webex 화면 공유가 자동으로 선택됩니다.

다음 방법 중 하나를 사용하여 Webex 화면 공유를 시작할 수 있습니다.

- 허브 창에서 연락처를 마우스 오른쪽 단추로 클릭하고 메뉴 옵션에서 화면 공유..를 선택합니다.
- 허브 창에서 연락처를 선택하고 설정 메뉴를 클릭합니다. 통신을 선택하고 메뉴 옵션에서 화면 공유...를 선택합니다.
- BFCP 및 IM 전용 화면 공유 옵션을 사용할 수 없는 경우 대화 창의 메뉴 옵션에서 ... > 화면 공유를 선택합니다.

BFCP 화면 공유

Cisco Jabber 데스크톱 클라이언트에 적용되며, 모바일 클라이언트용 Cisco Jabber는 BFCP 화면 공유만 수신할 수 있습니다.

BFCP(Binary Floor Control Protocol) 화면 공유는 Cisco Unified Communications Manager에 의해 제어됩니다. Cisco Unified Communications Manager는 비디오 데스크톱 공유 기능을 사용할 때 사용자가 전송하는 BFCP 패킷을 처리합니다. 통화 중일 때 **...** > 화면 공유를 선택하여 BFCP 화면 공유를 시작합니다.

이 기능에서는 원격 화면 제어가 지원되지 않습니다.

소프트웨어 전화기 장치에서**Trusted Relay Point** 또는 **Media Termination Point**가 활성화된 경우 BFCP를 사용한 영상 데스크톱 공유가 지원되지 않습니다.

참고 Windows용 Jabber에서 화면 공유 버튼은 기본적으로 BFCP 화면 공유를 시작합니다. BFCP 기반 공유를 사용할 수 없는 경우 이 버튼은 가능한 경우에만 IM 전용 화면 공유를 시작합니다.

IM 전용 화면 공유

Windows용 Cisco Jabber에 적용됩니다.

IM 전용 화면 공유는 RDP(원격 데스크톱 프로토콜)를 통한 일대일 클라이언트-클라이언트 화면 공유입니다. EnableP2PDesktopShare 매개 변수는 IM 전용 화면 공유를 사용할 수 있는지 여부를 제어합니다. PreferP2PDesktopShare 매개 변수는 Jabber가 비디오 공유 또는 IM 전용 화면 공유를 선호하는지 여부를 제어합니다.

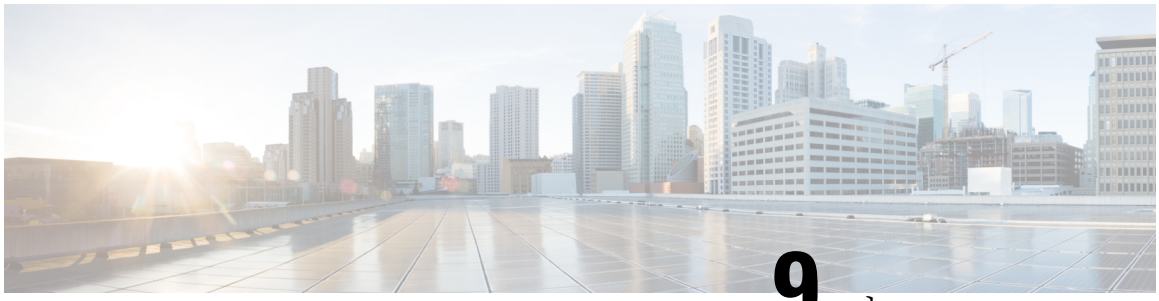
구축에서 IM 전용 화면 공유를 허용하는 경우 채팅 창에서 **...** > 화면 공유를 클릭하여 화면 공유를 시작합니다.

기본적으로 RDP에는 포트 3389가 필요합니다. IM 전용 화면 공유 기본 포트 범위는 49152 – 65535 TCP 및 UDP입니다. SharePortRangeStart 및 shareportrangesize 매개 변수를 사용하여 포트 범위를 제한할 수 있습니다.

미팅으로 에스컬레이션 및 공유

모든 Cisco Jabber 클라이언트에 적용됩니다.

Webex Meetings 컨트롤을 사용하여 인스턴트 Webex Meetings로 에스컬레이션하고 화면을 공유할 수 있습니다.



9 장

연합

도메인 간 페더레이션

도메인 간 페더레이션을 사용하면 엔터프라이즈 도메인의 Cisco Jabber 사용자가 사용 가능성을 공유하고 다른 도메인의 사용자와 인스턴트 메시지를 전송할 수 있습니다.

- Cisco Jabber 사용자는 다른 도메인에서 연락처를 수동으로 입력해야 합니다.
- Cisco Jabber는 다음과 같은 페더레이션을 지원합니다.
  - Microsoft Office Communications Server
  - Microsoft Lync
  - IBM Sametime
  - XMPP 표준 기반 환경(예: Google Talk)

참고 모바일 및 Remote Access용 Expressway는 XMPP 도메인 간 페더레이션 자체를 활성화 하지 않습니다. 모바일 및 Remote Access용 Expressway를 통해 연결하는 Cisco Jabber 클라이언트는 Cisco Unified Communications Manager IM and Presence에서 활성화된 경우 XMPP 도메인 간 페더레이션을 사용할 수 있습니다.

  - AOL Instant Messenger

Cisco Unified Communications Manager IM and Presence Service에서 Cisco Jabber에 대한 도메인 간 페더레이션을 구성합니다. 자세한 내용은 해당 서버 설명서를 참조하십시오.

도메인 내 페더레이션

도메인 내 페더레이션은 동일한 도메인 내 사용자가 가용성을 공유하고 Cisco Unified Communications Manager IM and Presence Service와 Microsoft Office Communications Server, Microsoft Live Communications Server 또는 다른 프레즌스 서버 간에 인스턴트 메시지를 보낼 수 있도록 합니다.

도메인 내 페더레이션을 사용하면 사용자를 다른 프레즌스 서버에서 Cisco Unified Communications Manager IM and Presence Service로 마이그레이션할 수 있습니다. 이러한 이유로, 프레즌스 서버에서 Cisco Jabber에 대한 도메인 내 페더레이션을 구성합니다. 자세한 내용은 다음 링크를 참고하십시오.

- Cisco Unified Communications Manager IM and Presence Service: Cisco Unified Communications Manager의 *Partitioned Intradomain Federation for IM and Presence* 서비스

A 부록

Jabber에서 지원되는 언어

지원되는 언어

다음 표에는 Cisco Jabber 클라이언트가 지원하는 언어에 대한 LCID(로캘 식별자) 또는 LangID(언어 식별자)가 나열되어 있습니다.

지원되는 언어	**Windows용 Cisco Jabber**	**Mac용 Cisco Jabber**	**Android용 Cisco Jabber, iPhone 및 iPad용 Cisco Jabber**	**LCID/LangID**
아랍어 - 사우디아라비아	X		X	1025
불가리아어 - 불가리아	X	X		1026
카탈로니아어 - 스페인	X	X		1027
중국어(간체) - 중국	X	X	X	2052
중국어(번체) - 대만	X	X	X	1028
크로아티아어 - 크로아티아	X	X	X	1050
체코어 - 체코	X	X		1029
덴마크어 - 덴마크	X	X	X	1030
네덜란드어 - 네덜란드	X	X	X	1043

Jabber에서 지원되는 언어

지원되는 언어	Windows용 Cisco Jabber	Mac용 Cisco Jabber	Android용 Cisco Jabber, iPhone 및 iPad용 Cisco Jabber	LCID/LangID
영어 - 미국	X	X	X	1033
핀란드어 - 핀란드	X	X		1035
프랑스어 - 프랑스	X	X	X	1036
독일어 - 독일	X	X	X	1031
그리스어 - 그리스	X	X		1032
히브리어 - 이스라엘	X			1037
헝가리어 - 헝가리	X	X	X	1038
이탈리아어 - 이탈리아	X	X	X	1040
일본어 - 일본	X	X	X	1041
한국어 - 한국	X	X	X	1042
노르웨이어 - 노르웨이	X	X		2068
폴란드어 - 폴란드	X	X		1045
포르투갈어 - 브라질	X	X	X	1046
포르투갈어 - 포르투갈	X	X		2070
루마니아어 - 루마니아	X	X	X	1048
러시아어 - 러시아	X	X	X	1049
세르비아어	X	X		1050
슬로바키아어 - 슬로바키아	X	X	X	1051
슬로베니아어 - 슬로베니아	X	X		1060

Jabber에서 지원되는 언어

지원되는 언어	**Windows용 Cisco Jabber**	**Mac용 Cisco Jabber**	**Android용 Cisco Jabber, iPhone 및 iPad용 Cisco Jabber**	**LCID/LangID**
스페인어-스페인 (현대 정렬)	X	X	X	3082
스웨덴어 - 스웨덴	X	X	X	5149
태국어 - 태국	X	X		1054
터키어	X	X	X	1055

Jabber에서 지원되는 언어