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.

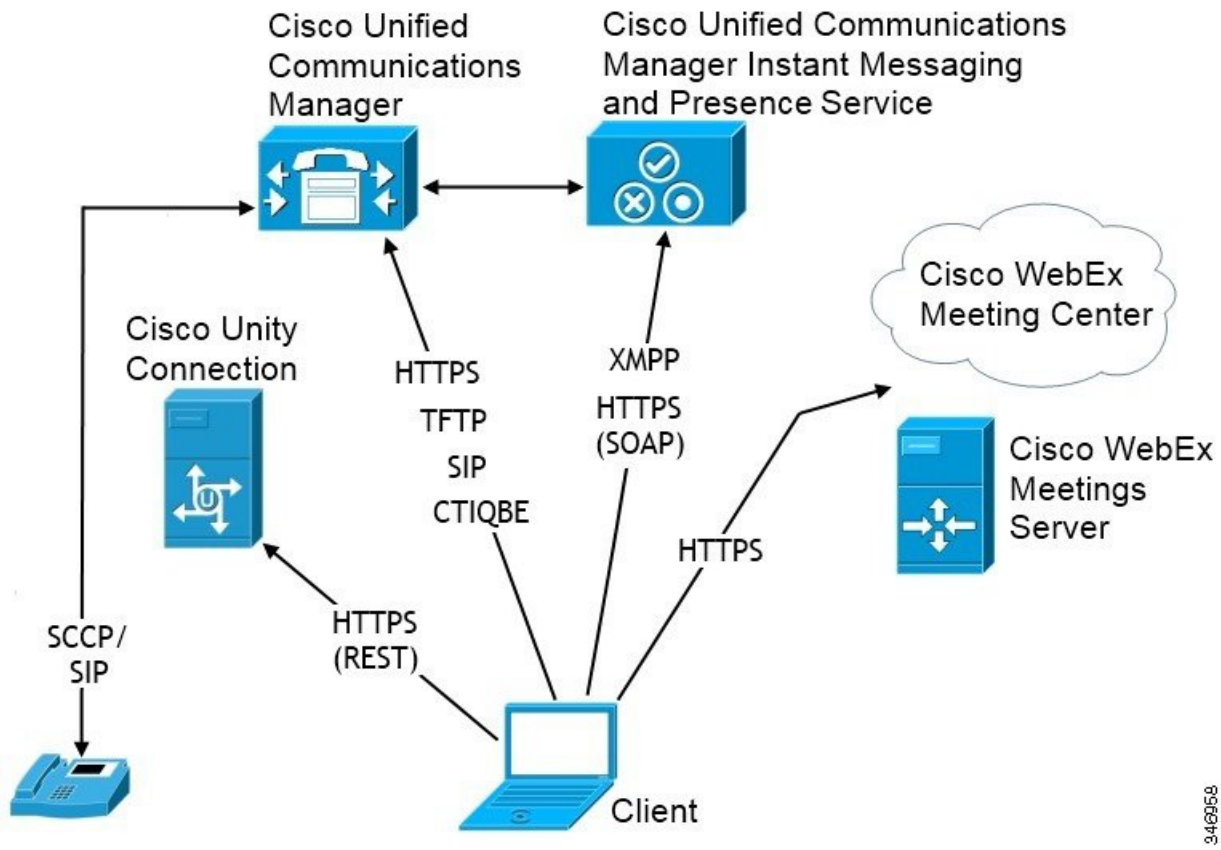
Cisco Unified Communications Manager IM and Presence Service를 사용한 온프레미스 구축

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

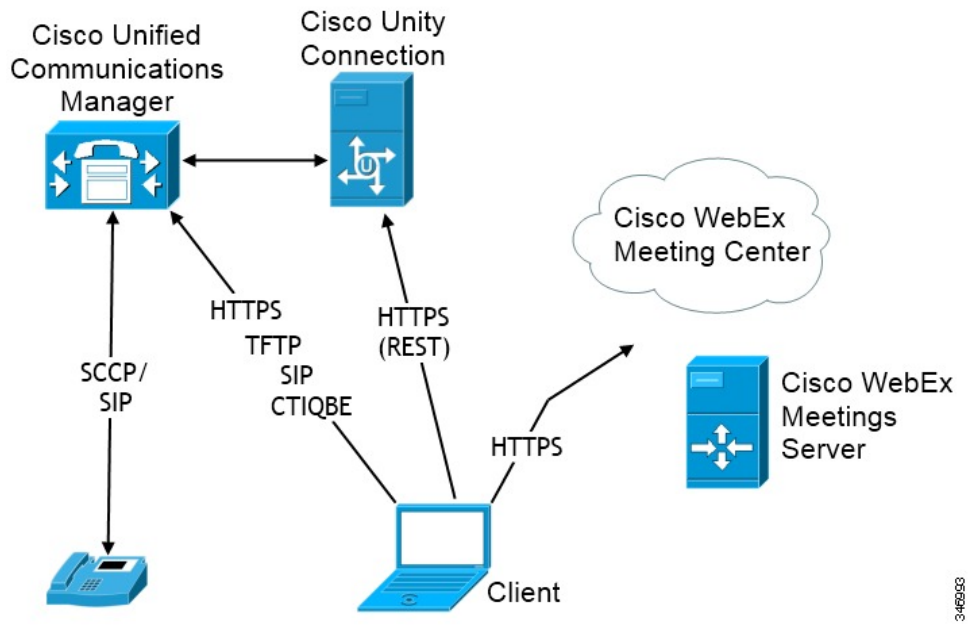
다음 서비스는 전화기 모드 구축에서 사용할 수 있습니다.

- 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.

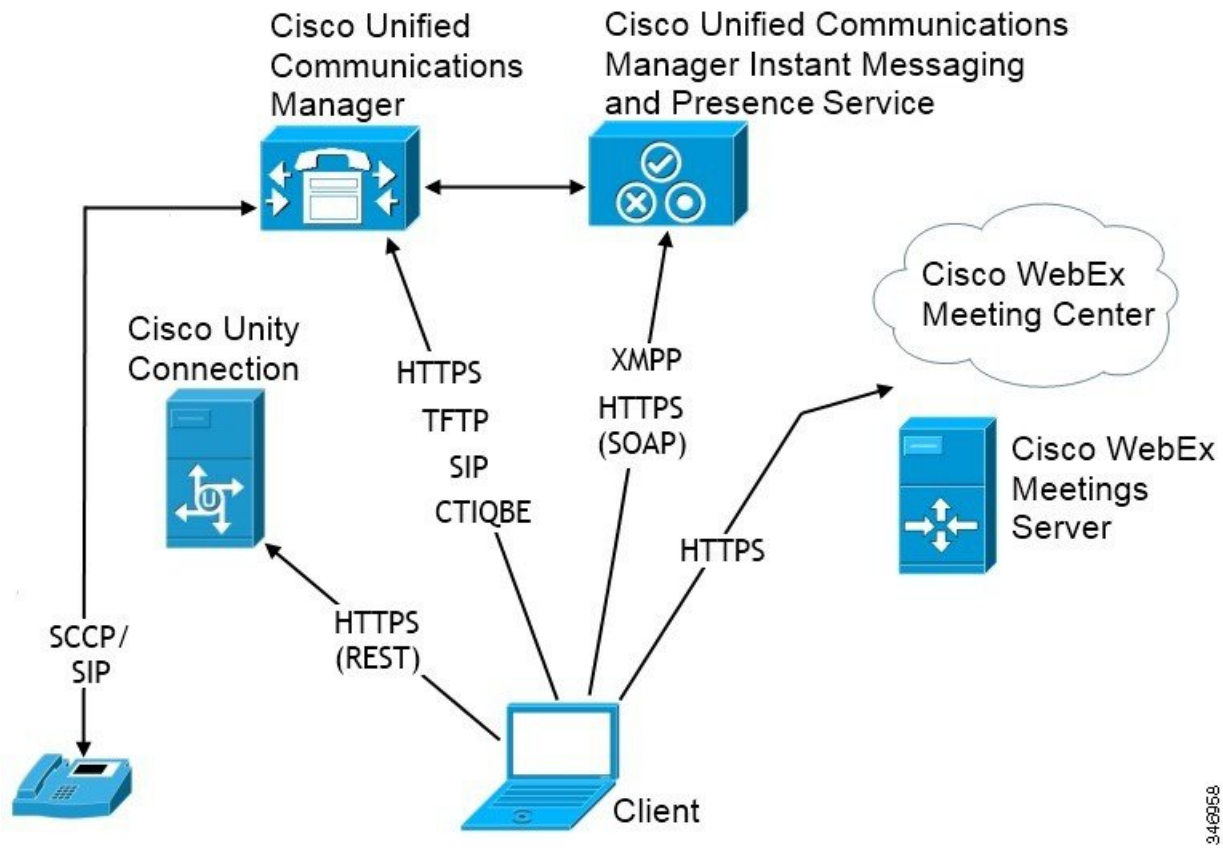
연락처 포함 전화기 모드 구축

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.

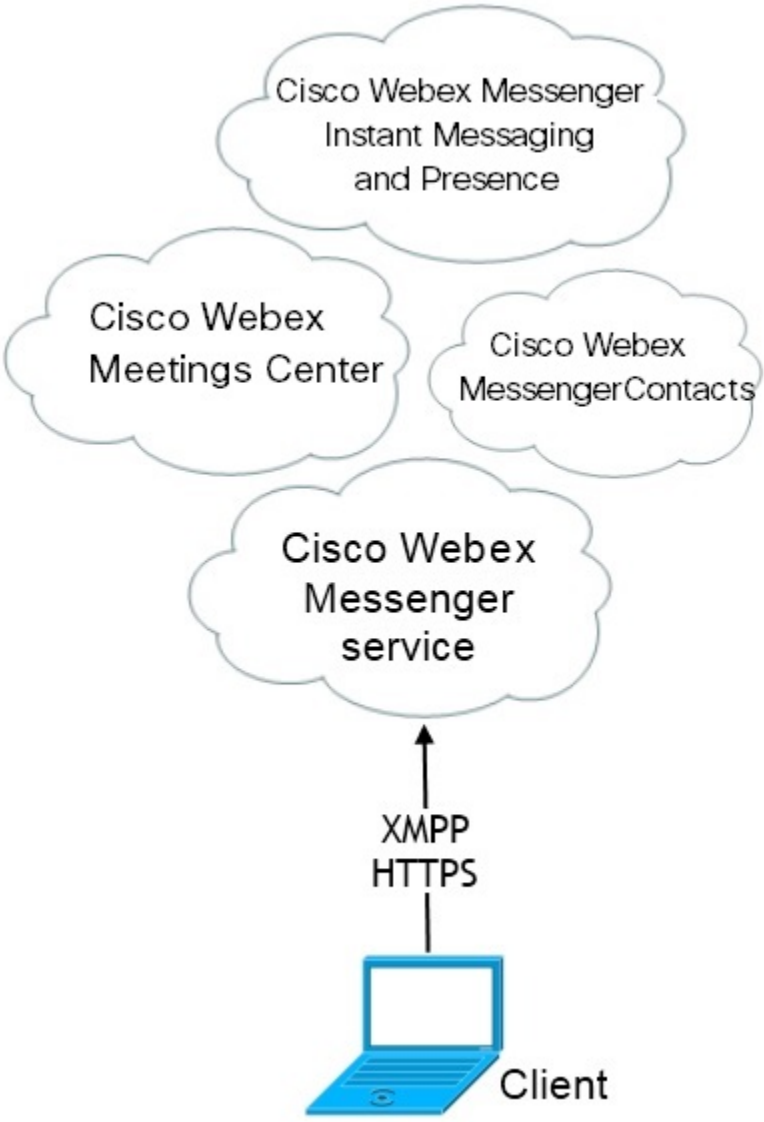
Cisco Webex Messenger를 통한 클라우드 기반 구축

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.



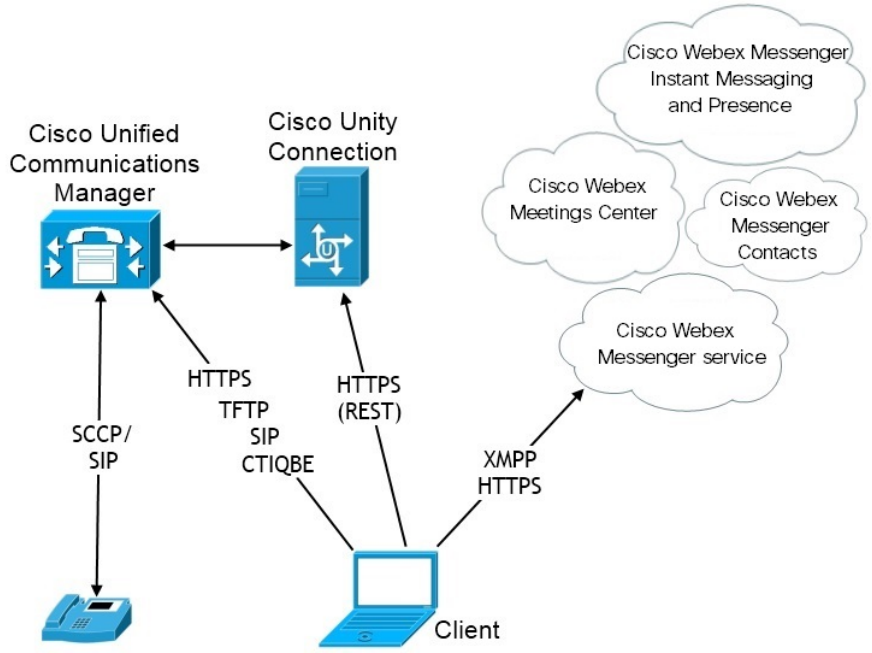
Cisco Webex Messenger 서비스를 통한 하이브리드 클라우드 기반 구축

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.



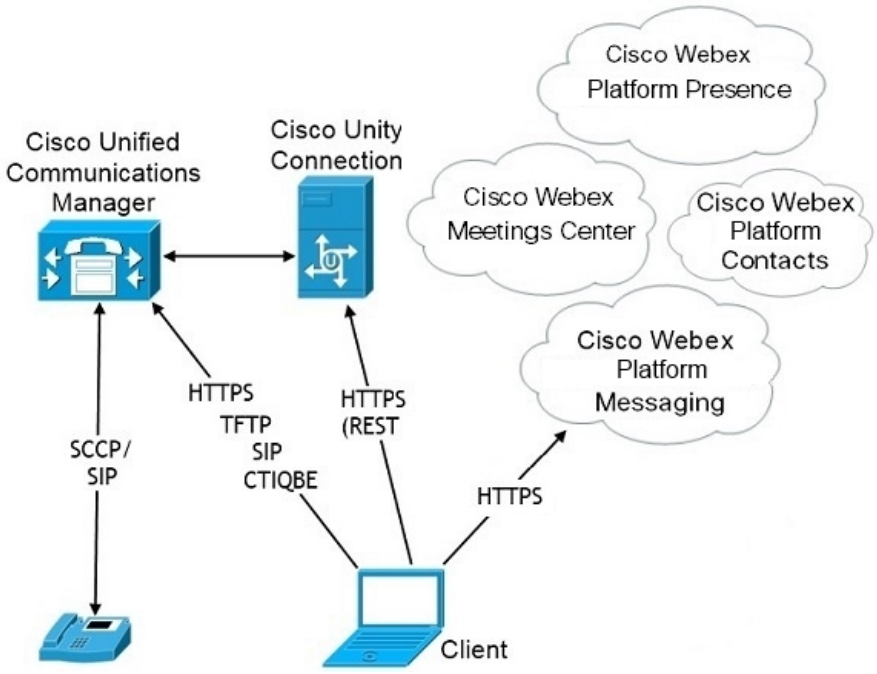
하이브리드 클라우드 기반 구축 **Cisco Webex** 플랫폼 서비스

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 [1]	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

[1] 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.

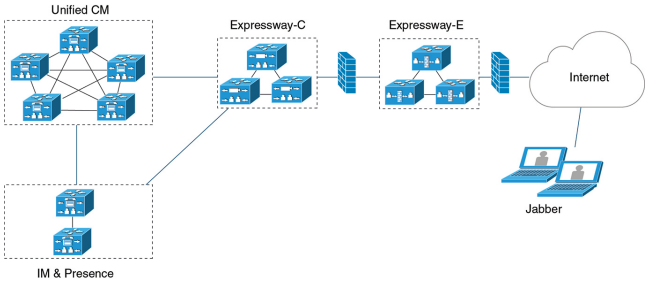
Jabber는 타사 VPN 클라이언트에서 테스트되거나 확인되지 않았습니다.

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 ***1:*** 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 페일오버됨을 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