모바일 및 원격 액세스 구성

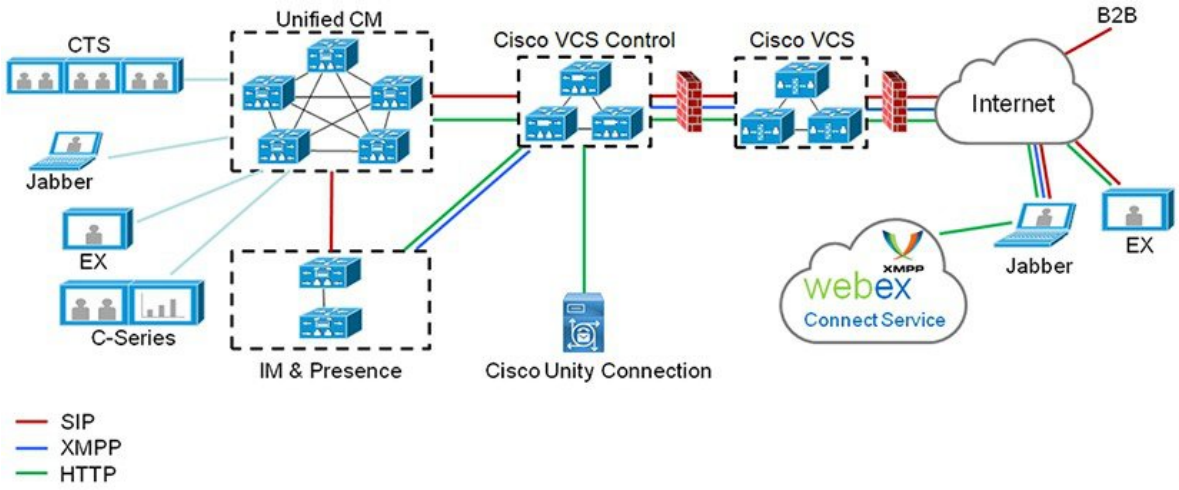
모바일 및 원격 액세스 개요

Unified Communications Manager 모바일 및 원격 액세스는 Cisco Collaboration Edge Architecture의 핵심 부분입니다. Cisco Jabber와 같은 엔드포인트가 엔터프라이즈 네트워크에 없는 경우, 해당 엔드포인트에서 Unified Communications Manager에서 제공하는 등록, 통화 제어, 제공, 메시징 및 프레즌스 서비스를 사용할 수 있습니다. Cisco Expressway는 모바일 엔드포인트를 온프레미스 네트워크에 연결하여 Unified CM 등록을 위한 안전한 방화벽 트래버설 및 회선 측 지원을 제공합니다.

전체 솔루션은 다음과 같은 기능을 제공합니다.

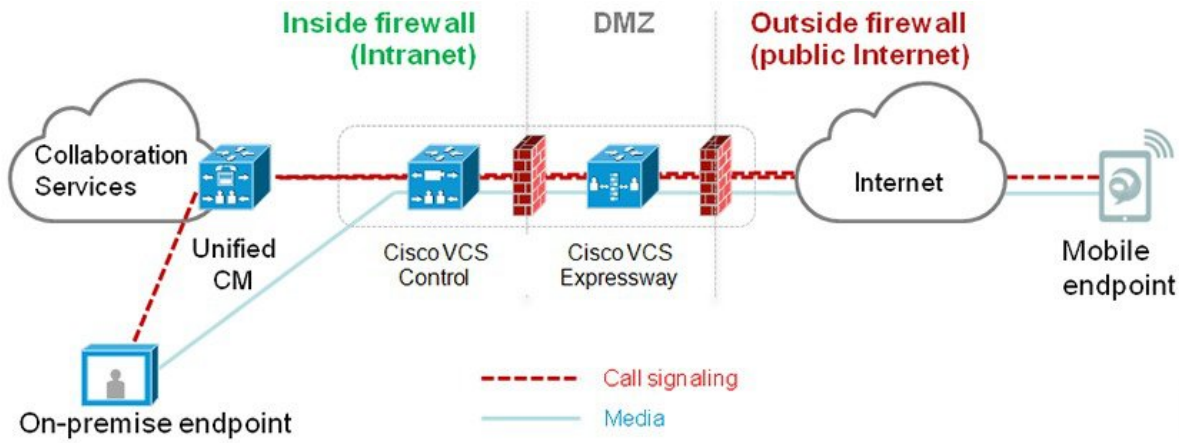
- 오프-프레미스 액세스: Jabber 및 EX/MX/SX 시리즈 클라이언트에 대해 네트워크 외부의 일관된 경험.
- 보안: 비즈니스 간 통신 보호.
- 클라우드 서비스: 풍부한 Webex 통합 및 서비스 공급자 오퍼링을 제공하는 엔터프라이즈급 유연성 및 확장 가능한 솔루션.
- 게이트웨이 및 상호운용성 서비스: 미디어 및 신호 정규화, 비표준 엔드포인트 지원.

그림 ***1: Unified Communications:*** 모바일 및 원격 액세스



타사 SIP 또는 H.323 디바이스는 Expressway-C에 등록할 수 있으며, 필요한 경우 SIP 트렁크를 통해 Unified CM 등록 디바이스와 상호 작용할 수 있습니다.

그림 ***2:*** 일반적인 통화 흐름*:* 신호 처리 및 미디어 경로



- Unified CM은 모바일 및 온-프레미스 엔드포인트 모두에 대해 통화 제어 기능을 제공합니다.
- 신호 처리는 모바일 엔드포인트와 Unified CM 간에 Expressway 솔루션을 트래버스합니다.
- 미디어는 Expressway 솔루션을 트래버스하고 엔드포인트 간에 직접 릴레이됩니다. Expressway-C와 모바일 엔드포인트 간에 모든 미디어가 암호화됩니다.

모바일 및 원격 액세스 구성

모바일 및 원격 액세스 기능을 사용하여 Cisco Jabber 사용자를 활성화하려면 Unified Communications Manager의 사용자 프로파일 구성 창에서 모바일 및 원격 액세스 사용자 정책을 설정합니다. 비 Jabber 엔드포인트에는 모바일 및 원격 액세스 사용자 정책이 필요하지 않습니다.

뿐만 아니라, 모바일 및 원격 액세스를 사용하여 Cisco Expressway를 구성해야 합니다. 자세한 내용은 Mobile and Remote Access via Cisco Expressway 구축 설명서를 참조하십시오.

모바일 및 원격 액세스 사전 요건

Cisco Unified Communications Manager 요구 사항

다음과 같은 요구 사항이 적용됩니다.

- 여러 Unified Communications Manager 클러스터를 구축하는 경우에는 ILS 네트워크를 설정합니다.
- 모바일 및 원격 액세스를 사용하려면 구축을 위해 NTP 서버를 설정해야 합니다. 네트워크에 NTP 서버가 구축되어 있고 SIP 엔드포인트에 대해 전화기 NTP 참조가 있는지 확인합니다.
- 미디어 경로 최적화를 위해 ICE를 배포하는 경우에는 TURN 및 STUN 서비스를 제공할 수 있는 서버를 구축해야 합니다.

DNS 요구 사항

Cisco Expressway에 대한 내부 연결의 경우 Unified Communications Manager를 가리키는 로컬에서 확인할 수 있는 DNS SRV를 구성합니다.

`_cisco-uds._tcp<도메인>`

모바일 및 원격 액세스에 사용되는 모든 통합 커뮤니케이션 노드에 대한 정방향 및 역방향 조회 모두에 대해 내부 DNS 레코드를 생성해야 합니다. 이렇게 하면 Expressway-C가 FQDN 대신 IP 주소 또는 호스트 이름을 사용하는 경우 노드를 찾을 수 있습니다. 로컬 네트워크 외부에서 SRV 레코드를 확인할 수 없는지 확인합니다.

Cisco Expressway 요구 사항

이 기능을 사용하려면 Unified Communications Manager를 Cisco Expressway와 통합해야 합니다. 모바일 및 원격 액세스에 대한 Cisco Expressway 구성 세부 정보는 Cisco Expressway 구축 설명서를 통한 모바일 및 원격 액세스를 참조하십시오.

Cisco Jabber에서 지원하는 모바일 및 원격 액세스 액세스 정책에 대한 최소 Expressway 릴리스는 X8.10입니다.

인증서 사전 요건

Unified Communications Manager, IM and Presence Service 및 Cisco Expressway-C 사이에 인증서를 교환해야 합니다. 각 시스템에 대해 동일한 CA를 사용하는 CA 서명 인증서를 사용하는 것이 좋습니다. 이러한 경우:

- 각 시스템에 CA 루트 인증서 체인을 설치합니다(Unified Communications Manager 및 IM and Presence 서비스서비스의 경우 tomcat 신뢰 저장소에 인증서 체인을 설치).

- Unified Communications Manager의 경우 CA 서명 tomcat(AXL 및 UDS 트래픽의 경우) 및 Cisco CallManager(SIP의 경우) 인증서를 요청하는 CSR을 발행합니다.
- IM and Presence 서비스 서비스의 경우 CA 서명 tomcat 인증서를 요청하는 CSR을 발행합니다.

참고 다른 CA를 사용하는 경우 Unified Communications Manager, IM and Presence 서비스 서비스 및 Expressway-C에 각 CA의 루트 인증서 체인을 설치해야 합니다.

참고 Unified Communications Manager 및 IM and Presence 서비스 서비스 모두에 대해 자체 서명 인증서를 사용할 수도 있습니다. 이 경우에는 Expressway-C에 Unified Communications Manager의 경우 tomcat 및 Cisco CallManager 인증서, IM and Presence 서비스 서비스의 경우 tomcat 인증서를 업로드해야 합니다.

모바일 및 원격 액세스 구성 작업 흐름

모바일 및 원격 액세스 엔드포인트를 배포하려는 경우 Unified Communications Manager에서 이러한 작업을 완료합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco AXL 웹 서비스 활성화, 5 페이지	Cisco AXL 웹 서비스가 퍼블리셔 노드에서 활성화되어 있는지 확인합니다.
단계 **2**	비디오에 대한 최대 세션 비트 레이트 구성, 5 페이지	선택 사항. 모바일 및 원격 액세스 엔드포인트에 대한 지역별 설정을 구성합니다. 예를 들어, 모바일 및 원격 액세스 엔드포인트에서 비디오를 사용할 것으로 예상되는 경우 기본 설정인 384 kbps는 일부 비디오 엔드포인트에 대해 너무 낮을 수 있으므로 영상 통화에 대한 최대 세션 비트 속도 설정을 증가시킬 수 있습니다.
단계 **3**	모바일 및 원격 액세스를 위한 디바이스풀 구성, 6 페이지	모바일 및 원격 액세스 엔드포인트에서 사용하는 디바이스풀에 날짜/시간 그룹 및 지역 구성을 할당합니다.
단계 **4**	ICE 구성, 6 페이지	선택 사항. ICE는 STUN 및 TURN 서비스를 사용하여 모바일 및 원격 액세스 통화에 사용할 수 있는 미디어 경로를 분석하고 최적의 경로를 선택하는 선택적 배포입니다. ICE는 통화 설정 시간에 잠재적으로 추가되지만 모바일 및 원격 액세스 통화의 신뢰성이 향상됩니다.

	명령 또는 동작	목적
단계 5	모바일 및 원격 액세스용 전화기 보안 프로파일 구성, 7 페이지	이 절차를 사용하여 모바일 및 원격 액세스 엔드포인트에서 사용할 전화기 보안 프로파일을 설정합니다.
단계 6	Cisco Jabber 사용자에 대한 모바일 및 원격 액세스 액세스 정책 구성, 8 페이지	Cisco Jabber만 해당. Cisco Jabber 사용자에 대한 모바일 및 원격 액세스 액세스 정책을 설정합니다. 모바일 및 원격 액세스 기능을 사용하려면 사용자 프로파일 내에서 Cisco Jabber 사용자의 모바일 및 원격 액세스를 활성화해야 합니다.
단계 7	모바일 및 원격 액세스를 위한 사용자 구성, 9 페이지	Cisco Jabber 사용자의 경우 설정하는 사용자 정책이 최종 사용자 구성에 적용되어야 합니다.
단계 8	모바일 및 원격 액세스를 위한 엔드포인트 구성, 9 페이지	모바일 및 원격 액세스 기능을 사용하는 엔드포인트를 구성하고 프로비전합니다.
단계 9	모바일 및 원격 액세스를 위한 Cisco Expressway 구성, 10 페이지	모바일 및 원격 액세스를 위해 Cisco Expressway를 구성합니다.

Cisco AXL 웹 서비스 활성화

Cisco AXL 웹 서비스가 퍼블리셔 노드에서 활성화되어 있는지 확인합니다.

단계 1 Cisco 통합 서비스 가용성에서 다음을 선택합니다 도구 > 서비스 활성화.
단계 2 서버 드롭다운 목록에서 퍼블리셔 노드를 선택하고 이동을 클릭합니다.
단계 3 데이터베이스 및 관리 서비스에서 **Cisco AXL** 웹 서비스가 활성화되었는지 확인합니다.
단계 4 서비스가 활성화되지 않은 경우 해당 확인란을 선택하고 저장을 클릭하여 서비스를 활성화합니다.

비디오에 대한 최대 세션 비트 레이트 구성

모바일 및 원격 액세스 엔드포인트에 대한 지역 설정을 구성합니다. 대부분의 경우 기본 설정으로 충분하지만, 모바일 및 원격 액세스 엔드포인트에서 비디오를 사용하는 것으로 예상되는 경우 지역 구성 내에서 영상 통화에 대한 최대 세션 비트 레이트를 증가시킬 수 있습니다. 기본 설정인 384kbps가 일부 비디오 엔드포인트(예: DX 시리즈)에 비해 너무 낮을 수 있습니다.

단계 1 Cisco Unified CM 관리에서 다음을 선택합니다 시스템 > 지역 정보 > 지역.
단계 2 다음 중 하나를 수행합니다.

- 찾기를 클릭하고 지역을 선택하여 기존 지역 내의 비트 레이트를 편집합니다.
- 새로 추가를 클릭하여 새 지역을 생성합니다.

단계 **3** 다른 지역에 대한 관계 수정 영역에서 영상 통화에 대한 최대 세션 비트 레이트에 대한 새 설정을 구성합니다. 예를 들어, 6000kbps가 있습니다.

단계 **4** 지역 구성 창에서 다른 필드를 구성합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오..

단계 **5** 저장을 클릭합니다.

모바일 및 원격 액세스를 위한 디바이스풀 구성

새 지역을 만들 때 모바일 및 원격 액세스 엔드포인트에서 사용하는 디바이스풀에 지역을 할당합니다.

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다 시스템 > 디바이스풀.

단계 **2** 다음 중 하나를 수행합니다.

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

단계 **3** 디바이스 풀 이름을 입력합니다.

단계 **4** 중복 **Cisco Unified Communications Manager** 그룹을 선택합니다.

단계 **5** 설정하는 날짜/시간 그룹을 할당합니다. 이 그룹에는 모바일 및 원격 액세스 엔드포인트에 대해 설정된 전화기 NTP 참조가 포함되어 있습니다.

단계 **6** 지역 드롭다운 목록에서 모바일 및 원격 액세스를 위해 구성한 지역을 선택합니다.

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

단계 **8** 저장을 클릭합니다.

ICE 구성

이 절차는 사용자가 모바일 및 원격 액세스 통화에 대한 통화 설정을 처리하도록 ICE를 구축하려는 경우에 사용합니다. ICE는 STUN 및 TURN 서비스를 사용하여 모바일 및 원격 액세스 통화에 사용할 수 있는 미디어 경로를 분석하고 최적의 경로를 선택하는 선택적 배포입니다. ICE는 통화 설정 시간에 잠재적으로 추가되지만 모바일 및 원격 액세스 통화의 신뢰성이 향상됩니다.

시작하기 전에

ICE를 구축하는 방법을 결정합니다. 일반 전화 프로파일 구성, 개별 Cisco Jabber 데스크톱 디바이스 또는 모든 전화기에 적용되는 시스템 수준 기본값을 통해 전화기 그룹에 대한 ICE를 구성할 수 있습니다.

ICE는 대체 메커니즘으로 TURN 서버를 사용하여 미디어를 릴레이할 수 있습니다. TURN 서버를 구축했는지 확인합니다.

단계 **1** Cisco Unified CM 관리에서:

- 시스템 > 엔터프라이즈 전화기를 선택하여 ICE에 대한 시스템 기본값을 구성합니다.
- 디바이스 > 디바이스 설정 > 일반 전화 프로파일 을 선택하여 엔드포인트 그룹에 대한 ICE를 구성하고 편집할 프로파일을 선택합니다.
- 디바이스 > 전화기를 선택하여 개별 Cisco Jabber 데스크톱 엔드포인트에 대한 ICE를 구성하고 편집할 엔드포인트를 선택합니다.

단계 **2** **ICE(**상호 연결 설정**)** 섹션까지 아래로 스크롤합니다.

단계 **3** **ICE** 드롭다운 목록을 활성화됨으로 설정합니다.

단계 **4** 기본 후보 유형을 설정합니다.

- 호스트—호스트 디바이스에서 IP 주소를 선택하여 가져온 후보입니다. 이것이 기본값입니다.
- 서버 재귀—STUN 요청을 전송하여 가져온 IP 주소 및 포트 후보입니다. 대부분의 경우 이것은 NAT의 공용 IP 주소를 나타낼 수 있습니다.
- **Relayed**—TURN 서버에서 가져온 IP 주소 및 포트 후보입니다. IP 주소 및 포트는 해당 미디어가 TURN 서버를 통해 릴레이될 수 있도록 TURN 서버에 상주합니다.

단계 **5** 서버 재귀 주소 드롭다운 목록에서 이 필드를 활성화됨 또는 비활성화됨으로 설정하여 STUN와 유사한 서비스를 활성화할 지 여부를 선택합니다. 서버 재귀를 기본 후보로 구성한 경우 이 필드를 활성화로 설정해야 합니다.

단계 **6** 기본 및 보조 TURN 서버에 대한 IP 주소 또는 호스트 이름을 입력합니다.

단계 **7** **TURN** 서버 전송 유형을 자동**(**기본 설정**)**, **UDP**, **TCP** 또는 **TLS**로 설정합니다.

단계 **8** TURN 서버의 사용자 이름 및 암호를 입력합니다.

단계 **9** 저장을 클릭합니다.

참고 일반 전화 프로파일에 대해 ICE를 구성한 경우 전화기가 프로파일을 사용할 수 있도록 일반 전화 프로파일에 연결해야 합니다. 전화기 구성 창을 사용하여 전화기에 프로파일을 적용할 수 있습니다.

모바일 및 원격 액세스용 전화기 보안 프로파일 구성

이 절차를 사용하여 모바일 및 원격 액세스 엔드포인트에서 사용할 전화기 보안 프로파일을 설정합니다.

단계 **1** Cisco Unified CM 관리에서 다음을 선택합니다 시스템 > 보안 > 전화기 보안 프로파일.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화기 보안 프로파일 유형 드롭다운 목록에서 디바이스 유형을 선택합니다. 예를 들어, Jabber 애플리케이션에 대한 **Cisco Unified Client Service Framework**를 선택할 수 있습니다.

단계 **4** 다음을 클릭합니다.

단계 **5** 프로파일의 이름을 입력합니다. 모바일 및 원격 액세스의 경우 이름은 FQDN 형식이어야 하며 엔터프라이즈 도메인을 포함해야 합니다.

단계 6 디바이스 보안 모드 드롭다운 목록에서 암호화를 선택합니다.

참고 이 필드는 암호화됨으로 설정해야 합니다. 그렇지 않으면 Expressway가 통신을 거부합니다.

단계 7 전송 유형을 **TLS**로 설정합니다.

단계 8 이 옵션을 활성화한 경우 전화기에 모바일 및 원격 액세스가 작동하지 않으므로 DX 시리즈, IP 전화기 7800 또는 IP 전화기 8811, 8841, 8845, 8861 및 8865 전화기에 대한 **TFTP** 암호화 구성 확인란을 선택하지 않은 상태로 둡니다.

단계 9 전화기 보안 프로파일 구성 창에서 남아 있는 필드를 완료해야 합니다. 필드 및 관련 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 10 저장을 클릭합니다.

참고 모바일 및 원격 액세스 엔드포인트 각각에 대한 전화기 구성에 이 프로파일을 적용해야 합니다.

Cisco Jabber 사용자에 대한 모바일 및 원격 액세스 액세스 정책 구성

이 절차를 사용하여 Cisco Jabber 사용자에 대한 모바일 및 원격 액세스 액세스 정책을 설정합니다. 모바일 및 원격 액세스 기능을 사용하려면 사용자 프로파일 내에서 Cisco Jabber 사용자의 모바일 및 원격 액세스를 활성화해야 합니다. Cisco Jabber에서 지원되는 모바일 및 원격 액세스 정책에 대한 최소 Expressway 릴리스는 X8.10입니다.

참고 비 Jabber 사용자에게는 모바일 및 원격 액세스 정책이 필요하지 않습니다.

사용자 프로파일에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "사용자 프로파일 개요" 섹션을 참조하십시오.

단계 1 Cisco Unified CM 관리에서 다음을 선택합니다 사용자 관리 > 사용자 설정 > 사용자 프로파일.

단계 2 새로 추가를 클릭합니다.

단계 3 사용자 프로파일의 이름 및 설명을 입력합니다.

단계 4 사용자의 사무실 전화기, 모바일 및 데스크톱 디바이스 및 원격 대상/디바이스 프로파일에 적용할 범용 디바이스 템플릿을 할당합니다.

단계 5 이 사용자 프로파일의 사용자에 대한 전화 회선에 적용할 범용 회선 템플릿을 할당합니다.

단계 6 이 사용자 프로파일의 사용자가 자신의 전화기를 프로비저닝하는 데 셀프 프로비저닝 기능을 사용할 있도록하려면 다음을 수행합니다.

a) 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.

b) 최종 사용자가 이렇게 많은 전화기를 가지고 있으면 프로비저닝 제한 필드에 사용자가 프로비저닝하도록 허용되는 전화기의 최대 수를 입력합니다. 최대값은 20입니다.

c) 다른 엔드 유저에게 이미 할당된 전화의 프로비저닝 허용 확인란에 체크 표시하여 이 프로파일에 연결된 사용자에게 이미 다른 사용자가 소유하는 디바이스를 마이그레이션 또는 재할당할 권한이 있는지 여부를 결정합니다. 기본값으로 이 확인란은 선택되어 있지 않습니다.

단계 **7** 이 사용자 프로파일과 연결된 Cisco Jabber 사용자가 모바일 및 원격 액세스 기능을 사용할 수 있도록 하려면 모바일 및 원격 액세스 활성화 확인란에 체크 표시합니다.

참고
- 기본적으로 이 확인란은 선택되어 있습니다. 이 확인란을 선택 취소하면 **Jabber** 정책 섹션이 비활성화되고 기본적으로 서비스 클라이언트 없음 정책 옵션이 선택됩니다.
- 이 설정은 OAuth 새로 고침 로그인을 사용하는 Cisco Jabber 사용자의 경우에만 필수입니다. 비 Jabber 사용자는 이 설정이 없어도 모바일 및 원격 액세스를 사용할 수 있습니다. 모바일 및 원격 액세스 기능은 Jabber 모바일 및 원격 액세스 사용자에 대해서만 적용 가능하며, 다른 엔드포인트 또는 클라이언트에게는 적용되지 않습니다.

단계 **8** 이 사용자 프로파일에 대해 Jabber 정책을 할당합니다. **Jabber** 데스크톱 클라이언트 정책 및 **Jabber** 모바일 클라이언트 정책 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 서비스 없음 - 이 정책은 모든 Cisco Jabber 서비스에 대한 액세스를 비활성화합니다.
- IM & 프레즌스만 해당—이 정책은 인스턴트 메시징 및 프레즌스 기능을 활성화합니다.
- IM & 프레즌스, 음성 및 영상 통화—이 정책은 음성 또는 영상 디바이스가 있는 모든 사용자에 대해 인스턴트 메시징, 프레즌스, 음성 메일 및 전화 회의 기능을 활성화합니다. 이것이 기본 옵션입니다.

참고 Jabber 데스크톱 클라이언트는 Windows용 Cisco Jabber와 Mac용 Cisco Jabber 사용자를 포함합니다. Jabber 모바일 클라이언트는 iPad 및 iPhone용 Cisco Jabber 사용자와 Android용 Cisco Jabber 사용자를 포함합니다.

단계 **9** 사용자가 Unified Communications 셀프 서비스 포털을 통해 내선 이동 또는 인터클러스터 내선 이동에 대한 최대 로그인 시간을 설정하도록 허용하려면 엔드 유저가 내선 이동을 최대 로그인 시간을 설정하도록 허용 확인란에 체크 표시합니다.

참고 기본적으로 최종 사용자가 **Extension Mobility**를 최대 로그인 시간을 설정하도록 허용 확인란은 선택 해제되어 있습니다.

단계 **10** 저장을 클릭합니다.

모바일 및 원격 액세스를 위한 사용자 구성

Cisco Jabber 사용자의 경우, 구성하는 모바일 및 원격 액세스 액세스 정책이 LDAP 동기화 중에 Cisco Jabber 사용자에 연결되어 있어야 합니다. 최종 사용자를 프로비저닝하는 방법에 대한 자세한 내용은 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "최종 사용자 구성" 섹션을 참조하십시오.

모바일 및 원격 액세스를 위한 엔드포인트 구성

모바일 및 원격 액세스용 엔드포인트 프로비저닝 및 구성:

- Cisco Jabber 클라이언트의 경우 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "*Cisco Jabber* 구성 작업 흐름" 섹션을 참조하십시오
- 다른 엔드포인트의 경우 Cisco 통합 커뮤니케이션 매니저 시스템 구성 설명서의 "엔드포인트 디바이스 구성" 섹션을 참조하십시오.

모바일 및 원격 액세스를 위한 **Cisco Expressway** 구성

모바일 및 원격 액세스를 위해 Cisco Expressway를 구성하는 방법에 대한 자세한 내용은 Cisco Expressway를 통한 모바일 및 원격 액세스 구축 설명서를 참조하십시오.