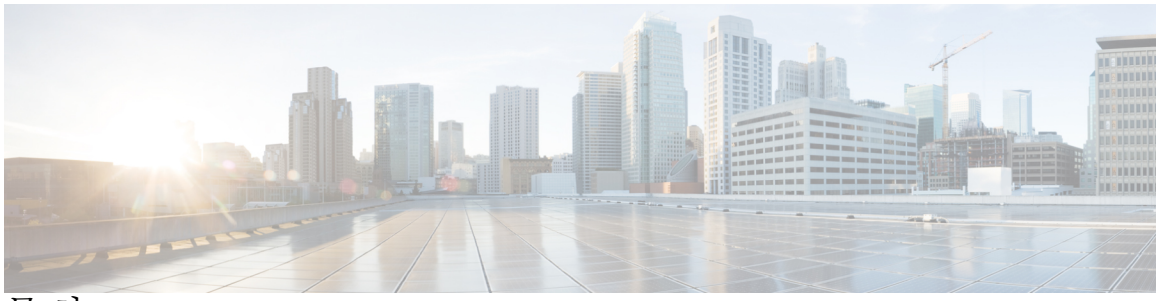
Cisco Jabber 14.0용 Webex Messenger 구축

초판: 2021년 3월 25일

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



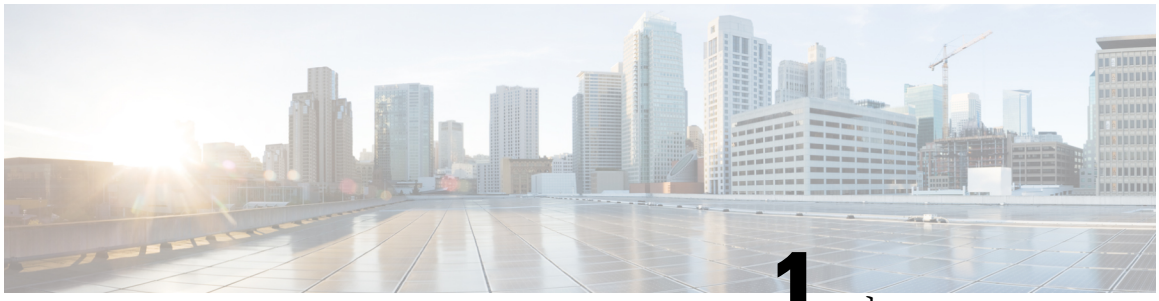
목 차

변경 이력

신규 및 변경된 정보

날짜	매개 변수	변경 사항 설명	섹션
2021년 3월		최초 게시	

변경 이력



1 장

Jabber 개요

본 설명서의 목적

이 설명서에는 Cisco Jabber를 배포하고 설치하는 데 필요한 다음과 같은 작업 기반 정보가 포함되어 있습니다.

- 클라우드 또는 하이브리드 구축을 구성하고 설치하는 프로세스를 개략적으로 설명하는 구성 및 설치 워크플로
- Cisco Jabber 클라이언트에서 IM and Presence 서비스, 음성 및 비디오 통신, 시각적 음성 메일 및 전화 회의와 같은 다양한 서비스를 구성하는 방법
- 디렉터리 통합, 인증서 확인 및 서비스 검색을 구성하는 방법
- 클라이언트를 설치하는 방법

Cisco Jabber를 구축하고 설치하기 전에 https://www.cisco.com/c/en/us/support/unified-communications/jabber-windows/products-installation-guides-list.html의 *Cisco Jabber* 계획 가이드를 참고하여 비즈니스 요구 사항에 가장 적합한 구축 옵션을 결정하십시오.

Cisco Jabber 정보

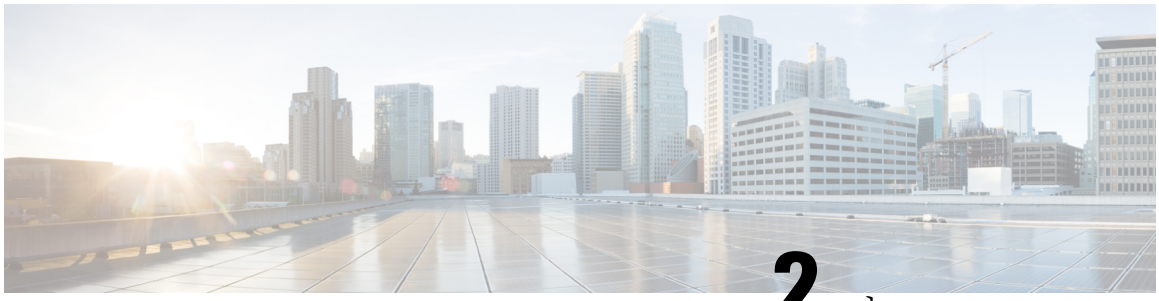
Cisco Jabber는 어디에서나 연락처와 원활하게 상호작용할 수 있게 해주는 유니파이드 커뮤니케이션 애플리케이션 모음입니다. Cisco Jabber는 IM, 프레즌스, 음성 및 영상 통화, 음성 메일 및 전화 회의를 제공합니다.

Cisco Jabber 제품군의 애플리케이션은 다음과 같습니다.

- Windows용 Cisco Jabber
- Mac용 Cisco Jabber
- iPhone 및 iPad용 Cisco Jabber

- Android용 Cisco Jabber
- VDI용 Cisco Jabber Softphone

Cisco Jabber 제품군에 대한 자세한 내용은 https://www.cisco.com/go/jabber 또는 https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html을(를) 참조하십시오.



2 장

클라우드 및 하이브리드 구축 워크플로

Cisco Webex Messenger를 사용한 클라우드 구축 워크플로

프로시저

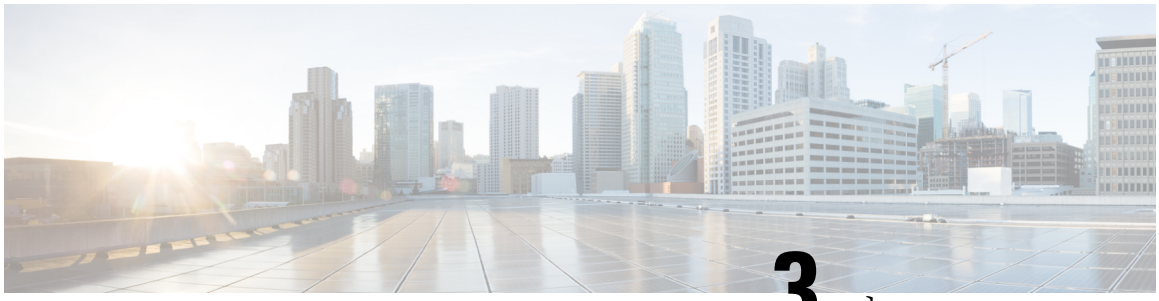
	명령 또는 동작	목적
단계 1	정책 구성, 5 페이지	
단계 2	클라우드 구축을 위한 사용자 생성, 17 페이지	
단계 3	인증서 확인 설정, 57 페이지	
단계 4	클라이언트 구성, 59 페이지	
단계 5	VDI용 Cisco Jabber 애플리케이션 및 Jabber 소프트폰 구축, 71 페이지	

Webex Messenger를 사용한 하이브리드 구축 워크플로

프로시저

	명령 또는 동작	목적
단계 1	정책 구성, 5 페이지	
단계 2	클러스터 구성, 13 페이지	
단계 3	통합 커뮤니케이션 관리자에서 사용자 생성, 25 페이지	

	명령 또는 동작	목적
단계 **4**	소프트폰 구성, 39 페이지	
단계 **5**	사무실 전화기 제어 구성, 31 페이지	
단계 **6**	확장 및 연결 구성, 49 페이지	
단계 **7**	Remote Access 서비스 검색 구성, 55 페이지	
단계 **8**	인증서 확인 설정, 57 페이지	
단계 **9**	클라이언트 구성, 59 페이지	
단계 **10**	VDI용 Cisco Jabber 애플리케이션 및 Jabber 소프트폰 구축, 71 페이지	
단계 **11**	Remote Access, 119 페이지	



3 장

정책 구성

정책 추가

프로시저

단계 **1** 정책 편집기 탭을 선택합니다.
정책 화면에서 정책 목록이 왼쪽에 표시되고 작업 목록이 오른쪽에 표시됩니다.

단계 **2** 정책 목록에서 추가를 선택합니다.
새 정책이 기존 정책 목록의 맨 위에 나타납니다.

단계 **3** 정책의 고유한 이름을 입력합니다.

다음에 수행할 작업

이 정책에 작업을 추가하는 방법은 다음을 참조하십시오. 정책에 작업 추가, 5 페이지

정책에 작업 추가

프로시저

단계 **1** 정책 편집기 탭을 선택합니다.
정책 편집기 화면에서 정책 목록이 왼쪽에 표시되고 작업 목록이 오른쪽에 표시됩니다.

단계 **2** 정책 이름에서 작업을 추가할 정책을 선택합니다.

단계 **3** 작업을 추가하려면 화면 오른쪽의 작업 목록에서 추가를 선택합니다.

작업 편집기 화면이 표시됩니다.

단계 **4** 작업 태그 이름 목록에서 정책 작업을 선택합니다.

단계 **5** 저장을 선택합니다.

단계 **6** 모든 정책에 작업이 할당될 때까지 3~5 단계를 반복합니다.

정책 작업 **Cisco Webex**

기본적으로 새로 프로비저닝된 Cisco Webex 조직에는 모든 사용자에게 부여된 기능 전체가 있습니다.

참고 종단간 암호화 정책은 기본적으로 비활성화 상태입니다. 조직 관리자가 이 정책을 활성화할 수 있습니다. 관리자는 모든 사용자 또는 특정 사용자 그룹에 대해 특정 기능을 비활성화해야 할 때 정책을 만들 수 있습니다.

타사 XMPP IM 애플리케이션을 사용하는 사용자에게는 정책 작업을 적용할 수 없습니다.

VoIP 전화회의 참가자는 10명까지만 동일한 VoIP 전화 회의에 동시 연결될 수 있습니다.

외부 사용자는 Cisco Webex 조직에 속하지 않는 사용자입니다. Cisco Webex을(를) 이용해 Cisco Webex 조직에 속하지 않는 사용자와 통신할 수 있습니다.

정책 작업	설명	영향	기본값
외부 파일 전송	조직 사용자와 조직 외부 사용자 간 IM 세션에서의 파일 전송을 제어합니다.	비활성화됨 - 조직 사용자와 외부 사용자 간의 모든 파일 전송을 중지합니다. 이 설정은 외부 사용자가 한 명 이상 있는 다중 상대 IM 세션에도 적용됩니다.	활성화됨
내부 파일 전송	조직 내 사용자 간 IM 세션에서의 파일 전송을 제어합니다.	비활성화됨 - 모든 내부 파일 전송을 중지합니다. 활성화됨 - 조직 내 모든 사용자가 내부 사용자와 파일을 교환할 수 있습니다.	활성화됨

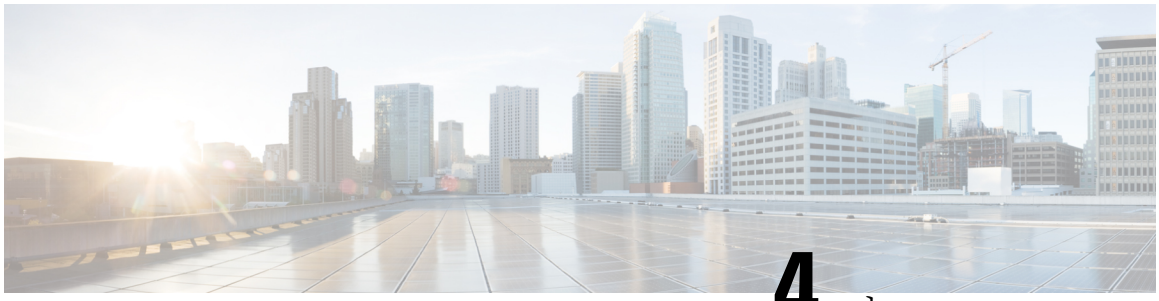
정책 작업	설명	영향	기본값
외부 IM	조직 내 사용자와 조직 외부 사용자 간의 IM 세션을 제어합니다.	비활성화됨 - 조직 내 사용자와 조직 외부 사용자 간의 모든 IM 세션을 중지합니다. 음성, 비디오 및 VoIP 같은 모든 종속 서비스도 중지됩니다.	활성화됨
외부 VoIP	조직 내 사용자와 조직 외부 사용자 간 IM 세션의 VoIP 통신 제어	비활성화됨 - 조직 내 사용자와 조직 외부 사용자 간 IM 세션의 모든 VoIP 통신을 중지합니다. 그러나 텍스트 기반 IM 세션 및 파일 전송 같은 다른 서비스는 사용할 수 있습니다.	활성화됨
내부 VoIP	조직 내 사용자 간 IM 세션에서의 VoIP 통신을 제어합니다.	비활성화됨 - 조직 내 사용자 간 IM 세션에서의 모든 VoIP 통신을 중지합니다. 그러나 텍스트 기반 IM 세션 및 파일 전송 같은 다른 서비스는 사용할 수 있습니다. 활성화됨 - 조직 내 모든 사용자가 IM 세션에서 VoIP 통신을 사용할 수 있습니다.	활성화됨
외부 비디오	조직 내 사용자와 조직 외부 사용자 간 IM 세션의 비디오 서비스 제어	비활성화됨 - 조직 내 사용자와 조직 외부 사용자 간 IM 세션에서의 모든 비디오 서비스를 중지합니다. 그러나 텍스트 기반 IM 세션 및 파일 전송 같은 다른 서비스는 사용할 수 있습니다.	활성화됨

정책 작업	설명	영향	기본값
내부 비디오	조직 내 사용자 간 IM 세션에서의 비디오 서비스를 제어합니다.	비활성화됨 - 조직 내 사용자 간 IM 세션에서의 모든 비디오 서비스를 중지합니다. 그러나 텍스트 기반 IM 세션 및 파일 전송 같은 다른 서비스는 사용할 수 있습니다. 활성화됨 - 조직 내 모든 사용자가 IM 세션에서 비디오 통신을 사용할 수 있습니다.	활성화됨
로컬 보관	IM 텍스트 메시지를 로컬로 보관하는 사용자 기능을 제어합니다.		활성화됨
외부 데스크톱 공유	조직 내의 사용자가 자신의 데스크톱을 조직 외부 사용자와 공유하는 기능을 제어합니다.	비활성화됨 - 조직 내 사용자가 자신의 (로컬) 데스크톱을 조직 외부 사용자와 공유하지 못합니다. 활성화됨 - 사용자가 자신의 (로컬) 데스크톱을 조직 외부 사용자와 공유할 수 있습니다.	활성화됨
내부 데스크톱 공유	조직 내의 사용자가 자신의 데스크톱을 다른 조직 내 사용자와 공유하는 기능을 제어합니다.	비활성화됨 - 조직 내 사용자가 자신의 데스크톱을 조직 내의 다른 사용자와 공유할 수 없습니다. 활성화됨 - 사용자가 자신의 데스크톱을 조직 내 다른 사용자와 공유할 수 있습니다.	활성화됨
IM에 대한 종단간 암호화 지원	IM 세션에 대한 종단간 암호화 지원 여부를 지정합니다.	활성화됨 - IM 세션에 대한 종단간 암호화를 지원합니다. 로그인한 사용자에는 종단간 암호화가 지원되지 않습니다.	비활성화됨

정책 작업	설명	영향	기본값
IM에 대한 인코딩 지원 안 함	종단간 암호화를 지원하는 애플리케이션이 종단간 암호화를 활성화하지 않은 애플리케이션이나 종단간 암호화를 지원하지 않는 타사 애플리케이션으로 IM 세션을 시작할 수 있는지를 제어합니다.	비활성화됨 - 종단간 암호화를 지원하는 애플리케이션이 종단간 암호화를 활성화하지 않은 애플리케이션 또는 타사 애플리케이션으로 IM 세션을 시작하지 못하게 합니다. 활성화됨 - 협상된 암호화 수준이 다른 상대방이 지원하는 최고 수준입니다.	활성화됨
내부 IM(화이트리스트에 있는 도메인 포함)	조직 내 사용자와 화이트리스트에 있는 특정 도메인 간의 IM 통신을 제어합니다.	비활성화됨 - 조직 내 사용자가 화이트리스트에 지정된 도메인 내에서 IM 사용자가 될 수 없게 합니다. 그러나 도메인 내 사용자는 함께 IM을 시작할 수 있습니다. VoIP, 비디오 및 파일 전송 같은 기타 종속 서비스도 비활성화됩니다.	활성화됨
위젯 업로드			활성화됨
사용자가 프로파일을 편집할 수 있습니다.	사용자가 자신의 프로파일 정보를 편집하지 못하게 하는 기능을 제어합니다.	비활성화됨 - 사용자가 프로파일 정보를 편집하지 못하게 합니다. 이 정책 작업은 구성 탭의 프로파일 설정 화면에 있는 설정에 영향을 줍니다.	활성화됨

정책 작업	설명	영향	기본값
사용자가 프로파일 보기 설정을 편집할 수 있습니다.	사용자 그룹이 자신의 사용자 프로파일 보기 설정을 변경하지 못하게 하는 기능을 제어합니다.	비활성화됨 - 사용자가 자신의 사용자 프로파일 보기 설정을 변경하지 못하게 합니다. 이 정책 작업은 구성 탭의 프로파일 설정 화면에 있는 사용자가 자신의 프로파일 보기 설정을 변경하도록 허용 확인란에 영향을 줍니다. 사용자가 자신의 프로파일 보기 설정을 변경하도록 허용 획인란 선택 여부는 아무런 영향도 주지 않습니다.	활성화됨
내부 화면 캡처	사용자가 조직 내 사용자에게 화면 캡처를 보내는 기능을 제어합니다.	비활성화됨 - 조직 내 사용자가 화면 캡처를 조직 내부로 보내지 못하게 합니다.	활성화됨
외부 화면 캡처	사용자가 조직 외부 사용자에게 화면 캡처를 보내는 기능을 제어합니다.	비활성화됨 - 조직 내 사용자가 화면 캡처를 조직 외부로 보내지 못하게 합니다.	활성화됨
내부 브로드캐스트 메시지 전송	사용자가 조직 내 사용자에게 브로드캐스트 메시지를 보내는 기능을 제어합니다.	비활성화됨 - 조직 내 사용자가 브로드캐스트 메시지를 조직 내부로 보내지 못하게 합니다.	활성화됨
외부 브로드캐스트 메시지 전송	사용자가 조직 외부 사용자에 게 브로드캐스트 메시지를 보내는 기능을 제어합니다.	비활성화됨 - 조직 내 사용자가 브로드캐스트 메시지를 조직 외부로 보내지 못하게 합니다.	활성화됨
사용자가 디렉터리 그룹에 브로드캐스트를 보낼 수 있습니다.	사용자가 조직 내 디렉터리 그룹에 브로드캐스트 메시지를 보내는 기능을 제어합니다.	비활성화됨 - 조직 내 사용자가 브로드캐스트 메시지를 조직 내 디렉터리 그룹으로 보내지 못하게 합니다.	활성화됨

정책 작업	설명	영향	기본값
HD 동영상	외부 비디오 또는 내부 비디오 정책이 활성화된 경우 컴퓨터 간 통화의 HD 비디오 기능을 제어합니다.	비활성화됨 - 모든 컴퓨터 간 통화의 HD 비디오 기능을 금지합니다.	활성화됨



4 장

클러스터 구성

Visual Voicemail 구성

프로시저

단계 **1** Visual Voicemail을 구성하려면 구성 탭 > 통합 커뮤니케이션을 선택합니다.
통합 커뮤니케이션 창이 열립니다.

단계 **2** 음성 메일을 선택해 **CUCI**용 **Visual Voicemail** 기본 설정 화면을 엽니다.

Unity Connection 고객은 Unity Connection 서버 IP 주소 또는 DNS 이름을 '음성 메일 서버' 및 '메일 저장소 서버' 필드에 입력해야 합니다. 다른 모든 설정은 기본값을 유지하는 것이 좋습니다.

단계 **3** Visual Voicemail을 활성화하려면 **Visual Voicemail** 활성화를 선택합니다.

단계 **4** Visual Voicemail 설정을 수동으로 입력하고 싶다면 사용자가 수동 설정을 입력하도록 허용을 선택합니다.

단계 **5** 다음 정보를 입력합니다.

- 음성 메일 서버: 음성 메일을 검색하기 위해 Cisco Webex 애플리케이션에서 통신해야 하는 Visual Voicemail 서버의 이름입니다.
- 음성 메일 프로토콜: Visual Voicemail 서버와 통신하는 데 사용하는 프로토콜입니다. HTTPS 또는 HTTP를 선택할 수 있습니다.
- 음성 메일 포트: Visual Voicemail 서버에 연결된 포트입니다.

다음 메일 저장소 매개변수 옵션은 지원되지 않습니다. Cisco Webex 관리 도구는 값을 입력해야 합니다. `10.0.0.0`을 메일 저장소 서버로 입력하고 나머지 필드에는 기본값을 사용합니다.

- 메일 저장소 서버: 메일 저장소 서버의 이름입니다.

- 메일 저장소 프로토콜: 메일 저장소 서버에서 사용하는 프로토콜입니다. TLS 또는 Plain을 선택할 수 있습니다.
- 메일 저장소 포트**:** 메일 저장소 서버와 연결된 포트입니다.
- **IMAP** 유휴 만료 시간: 만료 후 서버가 자동으로 음성 메일 확인을 중지할 때까지 걸리는 시간(분)입니다.
- 메일 저장소 받은 편지함 폴더 이름: 메일 저장소 서버에 구성된 받은 편지함 폴더의 이름입니다.
- 메일 저장소 휴지통 폴더 이름: 메일 저장소 서버에 구성된 휴지통 폴더(대부분의 경우 삭제된 항목 폴더)의 이름입니다.

단계 **6** 저장을 선택합니다.

Cisco Unified Communications Manager 통합 구성

프로시저

단계 **1** 구성 탭 > 추가 서비스 > 통합 커뮤니케이션을 선택합니다.

단계 **2** 클러스터 탭을 선택하고 추가를 선택합니다.

단계 **3** **Cisco UC Manager**와 메신저 서비스 클라이언트 통합 활성화를 선택합니다.

단계 **4** 사용자가 수동 설정을 입력하도록 허용을 선택하면 사용자는 기본 모드에서는 기본 서버 값을, 고급 모드에서는 TFTP/CTI/CCMCIP 서버 값을 변경할 수 있습니다.

참고 이 옵션을 활성화하면 사용자가 입력한 설정이 Cisco Webex 조직에 대해 지정된 기본 또는 전역 Cisco Unified Communications Manager 설정에 우선하게 됩니다.

단계 **5** **Cisco Unified Communications Manager** 서버 설정에서 다음을 선택합니다.

- 기본 서버 설정: Cisco Unified Communications Manager 서버에 대한 기본 설정을 입력합니다.
- 고급 서버 설정: Cisco Unified Communications Manager 서버에 대한 세부 설정을 입력합니다.

참고 서버 구성 옵션은 기본 또는 고급 설정 여부에 따라 달라집니다.

단계 **6** 기본 서버 설정에 다음 값을 입력합니다.

- 기본 서버: 기본 Cisco Unified Communications Manager 서버의 IP 주소를 입력합니다. 이 서버는 TFTP, CTI 및 CCMCIP 설정으로 구성합니다.
- 백업 서버: 백업 Cisco Unified Communications Manager 서버의 IP 주소를 입력합니다. 이 서버는 TFTP, CTI 및 CCMCIP 설정으로 구성하며, 기본 통합 커뮤니케이션 매니저 서버에 장애 발생 시 장애 조치 지원을 제공합니다.

단계 **7** 고급 서버 설정을 선택했다면, TFTP(Trivial File Transfer Protocol), CTI(Computer Telephony Integration) 및 CCMCIP(Cisco Unified Communications Manager IP Phone) 서버에 대한 설정을 각각 지정합니다.

단계 **8** 다음 서버 각각에 IP 주소를 입력합니다.

참고 TFTP 서버에 백업 서버를 2개까지, CTI 서버 및 CCMCIP 서버에 각각 백업 서버를 하나씩 지정할 수 있습니다. 각 백업 서버에 적절한 IP 주소를 입력합니다.

- **TFTP** 서버
- **CTI** 서버
- **CCMCIP Server** - Cisco Unified Communications Manager(UDS) 서버의 주소입니다.

나열된 서버는 사용자의 홈 클러스터에 있어야 합니다.

단계 **9** 음성 메일 파일럿 번호 입력란에 Cisco Unified Communications 서버에 있는 음성 메시지 서비스의 번호를 입력합니다.

일반적으로 조직 관리자는 전체 Cisco Webex 조직에 기본 음성 메시지 번호를 제공합니다. 그러나 사용자가 수동 설정을 입력하도록 허용 확인란을 선택하면 클러스터 사용자가 이 기본 음성 메시지 번호를 무시할 수 있습니다.

단계 **10** 음성 메일을 선택합니다.

단계 **11** **Visual Voicemail** 활성화를 선택합니다.

여기에 입력한 Visual Voicemail 설정은 이 클러스터에 속하는 사용자에게만 적용됩니다.

단계 **12** 클러스터 탭에서 이 클러스터에 대한 전용 음성 메일 서버를 선택하여 음성 메일 서버를 지정합니다. 이 서버는 전체 조직에 제공된 음성 메일 서버 설정과는 다릅니다.

단계 **13** 사용자가 이 클러스터에 대한 Visual Voicemail 설정을 수동으로 입력하게 하려면 사용자가 수동 설정을 입력하도록 허용을 선택합니다.

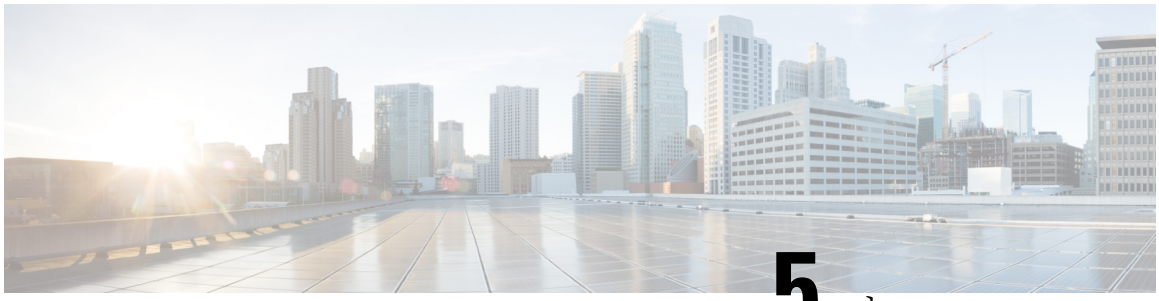
단계 **14** 다음 정보를 입력합니다.

음성 메일 서버	음성 메일 서버의 IP 주소 또는 FQDN을 입력합니다.
음성 메일 프로토콜	HTTP 또는 HTTPS를 선택합니다.
음성 메일 포트	포트 번호를 입력합니다.

메일 저장소 서버 정보는 지원되지 않습니다. Cisco Webex 관리 도구에서는 이 필드의 값을 예상합니다. `10.0.0.0`을 입력합니다. 메일 저장소 프로토콜, 포트 및 IMAP 유휴 만료 시간 필드는 지원되지 않습니다. 이러한 필드의 기본값은 삭제하지 마십시오.

메일 저장소 받은 편지함 폴더 이름	메일 저장소 서버에 구성된 받은 편지함 폴더 이름
메일 저장소 휴지통 폴더 이름	메일 저장소 서버에 구성된 휴지통 또는 삭제한 항목 폴더 이름

단계 **15** 저장을 선택합니다.



5 장

클라우드 구축을 위한 사용자 생성

사용자 워크플로 생성

Cisco Webex 관리 도구를 이용하면 조직은 다양한 방ㅂ버으로 사용자를 만들 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	다음 방법 중 하나를 사용하여 Cisco Webex 관리 도구에서 사용자를 만드십시오. • Cisco Webex 관리 도구를 사용하여 사용자를 개별적으로 추가할 수 있습니다. 새 사용자 생성, 18 페이지 • 사용자가 Cisco Webex 계정을 직접 등록하도록 이메일 초대장을 작성할 수 있습니다. 사용자 프로비저닝 정보, 19 페이지 • 사용자 정보를 사용하여 CSV 파일을 만들고 가져옵니다. CSV 파일 생성 및 가져오기, 20 페이지	
단계 **2**	정책 그룹에 사용자를 할당합니다. 정책에 사용자 할당, 23 페이지	

새 사용자 생성

프로시저

단계 **1** 새 사용자 또는 관리자를 만들려면 사용자 탭 > 추가를 선택합니다.

단계 **2** 각 필드에 정보를 입력합니다. 기본 역할은 (관리자가 아닌) 사용자입니다.

참고 비즈니스 이메일은 사용자 이름입니다. 사용자 이름은 편집할 수 없습니다.

단계 **3** (선택사항) 정책 그룹 할당 탭을 선택하여 정책 그룹을 사용자에게 할당합니다.

단계 **4** Cisco Webex 메신저 기관에서 IM 보관 기능이 활성화되었다면, **IM** 보관 확인란이 사용자 추가 확인란에 표시됩니다. 보관을 위해 이 사용자에 대한 IM을 로그하려면 **IM** 보관 확인란을 선택합니다.

단계 **5** 엔드포인트를 변경하려면 드롭다운 목록에서 다른 엔드포인트를 선택합니다.
기본값을 선택하면 **IM** 보관 화면에서 기본 엔드포인트로 미리 구성된 엔드포인트에 사용자가 할당됩니다.

단계 **6** 이 사용자를 업그레이드 사이트에 할당하려면, 업그레이드 사이트 드롭다운 목록에서 사이트를 선택합니다.

단계 **7** Cisco Webex 메신저 조직이 Cisco Unified Communications로 활성화되었다면, 통합 커뮤니케이션 탭이 사용자 추가 확인란에 표시됩니다. 통합 커뮤니케이션 탭을 선택하여 Cisco Unified Communications에 사용할 수 있는 설정을 확인합니다.

단계 **8** 클러스터에서 이 사용자를 추가할 적절한 Cisco Unified Communications 클러스터를 선택합니다.

단계 **9** Cisco Webex 메신저 조직이 Cisco Webex Meeting Center 통합으로 활성화되었다면, 사용자 추가 대화상자가 표시됩니다. 조직 관리자 역할을 사용자에게 할당 하려면 조직 관리자 확인란을 선택합니다.

참고
- 미팅 페이지에서 새 사용자를 만들 때 미팅 계정 자동 활성화를 활성화했다면, 기본적으로 미팅 계정 확인란이 선택됩니다. 이러한 경우에는 미팅 계정 확인란을 선택 해제해선 안 됩니다.
- 미팅 계정 확인란을 선택하면, 이 사용자에 대한 대응하는 Cisco Webex Meeting Center 계정이 생성됩니다.

단계 **10** 저장을 선택합니다.

새 사용자는 Cisco Webex메신저 관리 도구의 환영 이메일 템플릿을 기반으로 환영 이메일을 받습니다.

단계 **11** 이전 단계를 반복하여 새 사용자를 계속 추가합니다.

사용자 프로비저닝 정보

사용자 프로비저닝에는 등록 정보 같은 사용자 프로비저닝 정보와, 사용자의 프로파일을 만들 때 필요한 필드를 지정하는 작업이 포함됩니다. 여기서 하는 설정은 사용자가 Cisco Webex Messenger 조직에 프로비저닝될 때 영향을 발휘합니다. 예를 들어 여기서 특정 필드를 필수로 설정하면, 사용자는 사용자 프로파일을 만들 때 이러한 필드를 반드시 입력해야 합니다.

Cisco Webex Messenger 고객은 SAML 또는 디렉터리 통합이 활성화되지 않았다면 셀프 등록을 활성화할 수 있습니다. 이 경우 조직 관리자는 등록 URL을 지정하지 않아도 됩니다. 등록이 활성화되지 않았다면, 고객은 사용자 정의 웹 페이지를 지정할 수 있습니다. 고객의 도메인과 일치하는 이메일 주소를 등록하려는 사용자는 사용자 정의 웹 페이지로 리디렉션됩니다. 고객은 이 웹 페이지를 사용하여 새 Cisco Webex Messenger 계정을 만드는 데 필요한 내부 프로세스 관련 정보를 표시할 수 있습니다.

예:

Cisco Webex Messenger □□□□ □□□□ ithelpdesk@mycompany.com□□ □□□□ □□□□ +1 800 555 5555□ □□□ □□□□.

사용자 프로비저닝 정보 입력

프로시저

단계 **1** 사용자 프로비저닝 정보를 입력하려면 구성 탭에서 시스템 설정 > 사용자 프로비저닝을 선택합니다.

단계 **2** 사용자가 Cisco Jabber 애플리케이션을 사용하여 계정에 셀프 등록할 수 있게 하려면, 등록 페이지를 이용한 사용자 셀프 등록 활성화Cisco Webex를 선택합니다.

셀프 등록 페이지의 URL은 www.webex.com/go/wc입니다. 이 URL은 일반적으로 Cisco Webex Messenger 조직 관리자가 제공합니다.

참고 Cisco Webex 등록 페이지를 이용한 사용자 셀프 등록 활성화를 선택하지 않으면, 사용자 정의 등록 URL 필드와 상요자 정의 메시지 상자가 표시됩니다. 이 경우에는 사용자 정의 사용자 등록 페이지의 URL을 입력해야 합니다.

단계 **3** 사용자 정의 등록 **URL** 필드에 사용자 정의한 셀프 등록 페이지의 URL을 입력합니다.

사용자 정의 URL을 입력하지 않으면 www.webex.com/go/wc라는 셀프 등록 페이지(기본값) URL이 표시됩니다.

단계 **4** 사용자 정의 메시지 상자에 사용자 정의 셀프 등록 페이지에 대한 설명을 입력합니다.

단계 **5** 사용자가 셀프 등록 페이지를 이용해 등록할 때마다 조직 관리자에게 이메일로 통보하려면, 사용자가 **Cisco Webex** 등록 페이지를 이용하 셀프 등록할 때 관리자에게 알림 전송을 선택합니다.

단계 **6** 사용자 프로파일의 필수 필드로 설정에서, 사용자 프로파일을 생성하거나 확인할 때마다 표시되어야 하는 필수 필드를 선택합니다. 이러한 필드는 사용자가 다음을 수행할 때 항상 표시됩니다.

- 새 사용자 생성
- 기존 사용자 프로필 수정
- CSV 파일에서 사용자 가져오기

단계 **7** 저장을 선택합니다.

CSV 파일 생성 및 가져오기

CSV(쉼표로 구분된 값) 파일에서 다수 사용자를 Cisco Webex Messenger 조직으로 쉽게 가져올 수 있습니다. 마찬가지로 사용자를 CSV 파일로 내보낼 수도 있습니다. 가져오기를 이용하면 수많은 사용자를 조직에 간편하게 추가할 수 있어, 각 사용자를 수동으로 추가하는 수고를 하지 않아도 됩니다.

가져오기가 완료되면 가져오기를 시작한 조직 관리자는 가져오기 상태를 설명하는 이메일을 받습니다. 이메일에는 가져오기 성공, 실패 또는 중단 여부가 명시됩니다.

CSV 파일을 가져오면 사용자 탭에 사용자가 표시됩니다.

CSV 필드

참고: 조직 관리자 및 사용자 관리자는 CSV 가져오기 프로세스로는 만들 수 없습니다.

사용자를 Cisco Webex(으)로 가져오기 전에 다음 필드(순서는 상관없음)가 CSV 파일에 있어야 합니다. 일부 필드는 반드시 정보를 입력해야 하는 필수 필드이며, 다른 필드는 선택 사항입니다.

참고: 필드에 정보를 입력하지 않으려면 "-" 문자를 입력하면 됩니다. 데이터베이스에는 빈 필드로 가져옵니다. 이 작업은 선택 사항 필드에서만 할 수 있습니다. 필수 필드에 "-"를 입력하면, 가져오기 시 오류가 보고됩니다. 값 N/A는 사용하지 마십시오.

필드 이름	설명
employeeID	필수*(SSO*만 활성화) 사용자의 ID를 입력합니다.
displayName	선택 사항 사용자의 표시 이름을 입력합니다.
firstName	필수 사용자의 이름을 입력합니다.
lastName	필수 사용자의 성을 입력합니다.
email	필수 사용자의 이메일 주소를 입력합니다.
userName	필수 사용자의 사용자 이름을 user@email.com 형식으로 입력합니다.
jobTitle	선택 사항 사용자의 직함 또는 직책을 입력합니다.

필드 이름	설명
address1	선택 사항 사용자 주소의 첫 번째 줄을 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
address2	선택 사항 사용자 주소의 두 번째 줄을 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
시	선택 사항 사용자가 사는 도시를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
state	선택 사항 사용자가 사는 주를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
zipCode	선택 사항 사용자의 우편번호를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
ISOcountry	선택 사항 사용자가 사는 국가의 두 자리 국가 코드(예: IN, US, CN)를 입력합니다. 자세한 내용은 http://www.iso.org/iso/country_codes/iso_3166_code_lists/country_names_and_code_elements.htm을 참조하십시오. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
phoneBusinessISOCountry	선택 사항 사용자의 회사 전화 번호에 해당하는 국가 코드(예: IN, US, CN)를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
phoneBusinessNumber	선택 사항 사용자의 근무처 전화 번호를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
phoneMobileISOCountry	선택 사항 사용자의 휴대폰 번호에 해당하는 국가 코드(예: IN, US, CN)를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
phoneMobileNumber	선택 사항 사용자의 휴대폰 번호를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
팩스	선택 사항 사용자의 팩스 번호를 입력합니다.

필드 이름	설명
policyGroupName	선택 사항 사용자가 속한 기본 정책 그룹을 입력합니다.
userProfilePhotoURL	선택 사항 사용자의 프로파일 사진을 액세스할 수 있는 URL을 입력합니다.
activeConnect	선택 사항 Cisco Webex에서 사용자의 상태가 활성인지를 표시합니다. 활성 상태를 표시하려면 예를 입력하고 비활성 상태를 표시하려면 아니요를 입력합니다.
센터	선택 사항 Cisco Jabber 애플리케이션 사용자에 대한 센터 계정을 할당(예)하거나 제거(아니요)합니다. 센터는 하나만 지정할 수 있습니다.
storageAllocated	선택 사항 사용자에게 할당된 저장 용량(메가바이트)을 입력합니다. 숫자 값이어야 합니다.
CUCMClusterName	선택 사항 사용자가 속한 Cisco Unified Communications Manager 클러스터의 이름을 입력합니다.
businessUnit	선택 사항 사용자의 사업 부문 또는 부서를 입력합니다. 조직 관리자는 사용자에게 필수 필드가 되도록 이 필드를 구성할 수 있습니다.
IMLoggingEnable	선택 사항 이 사용자에 대해 IM 로깅이 활성화되었는지를 나타냅니다. 활성화됨 상태를 표시하려면 **True**를 입력하고 비활성화됨 상태를 표시하려면 **false**를 입력합니다.
endpointName	선택 사항 IM을 기록하도록 구성된 엔드포인트 이름을 입력합니다.
autoUpgradeSiteName	선택 사항 업그레이드 사이트 이름을 입력합니다.

참고 탭 또는 쉼표로 구분된 CSV 파일을 사용할 수 있습니다. CSV 파일이 UTF-8 또는 UTF16 형식으로 인코딩되었는지 확인합니다.

인코딩 형식으로 **UTF-8** 선택

프로시저

단계 **1** Microsoft Excel에서 파일 > 다른 이름으로 저장을 선택합니다.
단계 **2** 다른 이름으로 저장 대화 상자에서 도구 및 웹 옵션을 선택합니다.
단계 **3** 웹 옵션 대화 상자에서 인코딩 탭을 선택합니다.
단계 **4** 이 문서 를 다음 형식으로 저장 목록 에서 **u t f-8**을 선택 합니다.
단계 **5** 확인을 선택하여 다른 이름으로 저장 대화 상자로 돌아갑니다.
단계 **6** 다음 형식으로 저장 목록에서 **CSV(**쉼표로 구분**)(*.csv)**를 선택합니다.
단계 **7** 파일 이름 필드에 CSV 파일의 이름을 입력하고 저장을 선택합니다.

사용자 가져오기 및 내보내기

프로시저

단계 **1** CSV 파일에서 사용자를 가져오려면 Cisco Webex Messenger 관리 도구에서 사용자 탭 > 추가 작업 > 가져오기/내보내기를 선택합니다.
단계 **2** 찾아보기를 선택하고, 가져올 사용자 목록이 포함된 CSV 파일을 선택합니다.
단계 **3** 가져오기를 선택해 가져오기 프로세스를 시작합니다.
단계 **4** 사용자를 내보내려면 사용자 가져오기/내보내기 대화 상자에서 내보내기를 선택합니다.

진행 메시지를 통해 내보내기 프로세스의 진행률을 확인할 수 있습니다.

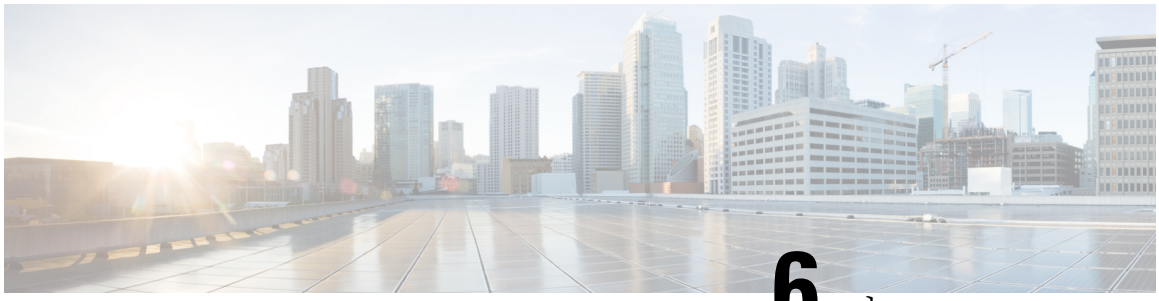
단계 **5** 내보낸 사용자가 포함된 CSV 파일을 보려면, 내보내기 메시지의 타임스탬프를 선택합니다.
확인 메시지가 나타납니다. 메시지는 마지막 내보내기: 2009-06-24 09:02:01 같은 형식을 취합니다.
단계 **6** 열기를 선택해 메신저 조직의 사용자가 포함된 CSV 파일을 확인합니다. 또는 저장을 선택하여 CSV 파일을 로컬 컴퓨터에 저장합니다.

정책에 사용자 할당

프로시저

단계 **1** 정책 그룹에 사용자를 할당하려면 사용자 탭을 선택합니다.

단계 **2** 정책 그룹을 새 사용자에게 할당하려면 먼저 추가를 선택하여 새 사용자를 생성합니다.
단계 **3** 정책 그룹을 기존 사용자에게 할당하려면 사용자를 검색합니다.
단계 **4** 검색 결과에서 해당 사용자의 이름을 두 번 클릭하여 사용자 편집 대화 상자를 엽니다.
단계 **5** 정책 그룹 할당 탭을 선택하여 정책 그룹 할당 대화 상자를 엽니다.
단계 **6** 검색 필드에 검색하여 이 사용자에게 할당할 정책 그룹의 문자를 하나 이상 입력합니다.
단계 **7** 검색을 선택합니다.
단계 **8** 검색 결과 창에서 적절한 정책 그룹을 선택하고, 할당을 선택하여 정책을 이 사용자에게 할당합니다.
단계 **9** 저장을 선택하여 정책 그룹 할당을 저장하고 사용자 탭으로 돌아합니다.



6 장

통합 커뮤니케이션 관리자에서 사용자 생성

동기화 활성화

디렉터리 서버의 연결 데이터가 Cisco Unified Communications Manager에 복제되게 하려면 디렉터리 서버와 동기화해야 합니다. 디렉터리 서버와 동기화하려면 먼저 동기화를 활성화해야 합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 시스템 > **LDAP** > **LDAP** 시스템을 선택합니다.

LDAP 시스템 구성 창이 열립니다.

단계 **3** **LDAP** 시스템 정보 섹션을 찾습니다.

단계 **4** **LDAP** 서버와의 동기화 활성화를 선택합니다.

단계 **5** **LDAP** 서버 유형 드롭다운 목록에서 데이터를 동기화할 디렉터리 서버의 유형을 선택합니다.

다음에 수행할 작업

사용자 ID의 LDAP 특성을 지정합니다.

사용자 ID에 대한 LDAP 특성 지정

디렉터리 소스에서 Cisco Unified Communications Manager로 동기화되면 디렉터리에 있는 속성으로 사용자 ID를 채울 수 있습니다. 사용자 ID를 보유하는 기본 속성은 `sAMAccountName`입니다.

프로시저

단계 **1** **LDAP** 시스템 구성 창에서 **User ID**의 **LDAP** 속성 드롭다운 목록을 찾습니다.

단계 **2** 사용자 ID의 속성을 적절하게 지정한 다음 저장을 선택합니다.

중요 사용자 ID의 속성이 `sAMAccountName`이 아니고 Cisco Unified Communications Manager IM and Presence Service에서 기본 IM 주소 체계를 사용 중이라면, 다음과 같이 클라이언트 구성 파일의 매개변수에 대한 값으로 속성을 지정해야 합니다.

CDI 매개변수는 `UserAccountName`입니다.

`<UserAccountName>attribute-name</UserAccountName>`

구성에 속성을 지정하지 않고 속성이 `sAMAccountName`이 아니라면, 클라이언트는 디렉터리에서 연락처를 확인할 수 없습니다. 결과적으로 사용자는 프레즌스를 얻지 못하며 인스턴트 메시지를 보내거나 받을 수 없습니다.

디렉터리 URI에 대한 LDAP 특성 지정

Cisco Unified Communications Manager 릴리스 9.0(1) 이상에서는 디렉터리의 속성에서 디렉터리 URI를 입력할 수 있습니다.

시작하기 전에

동기화 활성화.

프로시저

단계 **1** 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 적절한 LDAP 디렉터리를 선택하거나, 새로 추가를 선택하여 LDAP 디렉터리를 추가합니다.

단계 **3** 동기화할 표준 사용자 필드 섹션을 찾습니다.

단계 **4** 디렉터리 **URI** 드롭다운 목록에서 다음 LDAP 속성 중 하나를 선택합니다.

- **msRTCSIP-primaryuseraddress** - 이 속성은 Microsoft Lync 또는 Microsoft OCS가 사용되는 경우, AD에 채워집니다. 이것은 기본 속성입니다.
- **mail**

단계 **5** 저장을 선택합니다.

동기화 수행

디렉터리 서버를 추가하고 필수 매개변수를 지정하면, Cisco Unified Communications Manager를 디렉터리 서버와 동기화할 수 있습니다.

프로시저

단계 **1** 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 새로 추가를 선택합니다.

LDAP 디렉터리 창이 열립니다.

단계 **3** **LDAP** 디렉터리 창에서 필요한 상세정보를 지정합니다.

지정 가능한 값과 형식에 관한 자세한 내용은 Cisco Unified Communications Manager 관리 설명서를 참조하십시오.

단계 **4** 정보를 정기적으로 동기화할 수 있도록 LDAP 디렉터리 동기화 일정을 만듭니다.

단계 **5** 저장을 선택합니다.

단계 **6** 지금 전체 동기화 수행을 선택합니다.

참고 동기화 프로세스가 완료되는 데 걸리는 시간은 디렉터리에 있는 사용자의 수에 따라 달라집니다. 대규모 디렉터리를 수천 명의 사용자와 동기화하는 경우에는 이 프로세스를 완료하는 데 시간이 얼마나 걸릴지 예상해야 합니다.

디렉터리 서버의 사용자 데이터는 Cisco Unified Communications Manager 데이터베이스에 동기화됩니다. 그러면 Cisco Unified Communications Manager가 사용자 데이터를 프레즌스 서버 데이터베이스에 동기화합니다.

역할 및 그룹 할당

모든 구축 유형에 대해 사용자를 표준 **CCM** 최종 사용자 그룹에 할당합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 사용자 관리 > 최종 사용자를 선택합니다.
사용자 찾기 및 나열 창이 열립니다.

단계 **3** 목록에서 사용자를 찾아 선택합니다.
최종 사용자 구성 창이 열립니다.

단계 **4** 권한 정보 섹션을 찾습니다.

단계 **5** 액세스 제어 그룹에 추가를 선택합니다.
액세스 제어 그룹 찾기 및 나열 확인란이 열립니다.

단계 **6** 사용자에 대한 액세스 제어 그룹을 선택합니다.

최소한 다음 액세스 제어 그룹에 사용자를 할당해야 합니다.

- 표준 **CCM** 최종 사용자
- 표준 **CTI** 활성화 - 이 옵션은 사무실 전화기 제어에 사용합니다.

보안 전화 기능으로 사용자를 프로비저닝한다면 사용자를 표준 **CTI** 보안 연결 그룹에 할당하지 마십시오.

특정 전화기 모델에는 다음과 같이 추가 제어 그룹이 필요합니다.

- Cisco Unified IP Phone 9900, 8900 또는 8800 시리즈 또는 DX 시리즈의 경우에는, 연결된 **Xfer** 및 **conf**를 지원하는 전화의 표준 **CTI** 컨트롤 허용을 선택합니다.
- Cisco Unified IP Phone 6900 시리즈의 경우, 롤오버 모드를 지원하는 전화의 표준 **CTI** 컨트롤 허용을 선택합니다.

단계 **7** 선택한 항목 추가를 선택합니다.
액세스 제어 그룹 찾기 및 나열 창이 닫힙니다.

단계 **8** 최종 사용자 구성 창에서 저장을 선택합니다.

인증 옵션

클라이언트에서 **SAML SSO** 활성화

시작하기 전에

- Cisco Unity Connection 버전 10.5에서 SSO 활성화 - 이 서비스에서 SAML SSO를 활성화하는 자세한 방법은 *Cisco Unity Connection*에서 *SAML SSO* 관리를 참조하십시오.
- Cisco Unified 커뮤니케이션 애플리케이션 및 Cisco Unity Connection를 지원하려면 Cisco Webex Messenger 서비스에서 SSO를 활성화해야 합니다.

  이 서비스에서 SAML SSO를 활성화하는 자세한 방법은 *Cisco Webex Messenger* 관리자 설명서의 단일 로그인을 참조하십시오.

프로시저

단계 **1** 웹 브라우저에서 인증서를 확인할 수 있도록 모든 서버에 인증서를 구축합니다. 이렇게 하지 않으면 사용자가 잘못된 인증서 관련 경고 메시지를 받게 됩니다. 인증서 확인에 관한 자세한 내용은 인증서 확인을 참조하십시오.

단계 **2** 클라이언트에서 SAML SSO의 서비스 검색을 지원해야 합니다. 클라이언트는 표준 서비스 검색을 사용하여 클라이언트에서 SAML SSO를 활성화합니다. ServicesDomain, VoiceServicesDomain, ServiceDiscoveryExcludedServices 구성 매개변수를 사용하여 서비스 검색을 활성화합니다. 서비스 검색을 활성화하는 자세한 방법은 *Remote Access*를 위한 서비스 검색 구성을 참조하십시오.

단계 **3** 세션이 지속되는 기간을 정의합니다.

세션은 쿠키 및 토큰 값으로 구성됩니다. 일반적으로 쿠키는 토큰보다 오래 지속됩니다. 쿠키의 수명은 ID 제공자에서 정의하며, 토큰의 지속 시간은 서비스에서 정의합니다.

단계 **4** SSO가 활성화되면 모든 Cisco Jabber 사용자가 기본적으로 SSO를 사용하여 로그인합니다. 관리자는 이를 사용자별로 변경할 수 있으며, 따라서 특정 사용자는 SSO를 사용하지 않고 대신 자신의 Cisco Jabber 사용자 이름과 비밀번호를 이용해 로그인합니다. Cisco Jabber 사용자에 대해 SSO를 비활성화하려면, SSO_Enabled 매개변수 값을 FALSE로 설정합니다.

사용자에게 이메일 주소를 요청하지 않도록 Cisco Jabber를 구성했다면, Cisco Jabber에 대한 첫 번째 로그인은 SSO를 사용하지 않을 수도 있습니다. 일부 구축에서는 ServicesDomainSsoEmailPrompt 매개변수를 켜기로 설정해야 합니다. 이렇게 하면 첫 번째 SSO 로그인을 수행하는 데 필요한 정보를 Cisco Jabber가 확보할 수 있습니다. 사용자가 Cisco Jabber에 로그인한 적 있다면, 필요한 정보를 사용할 수 있기 때문에 이 메시지는 필요 없습니다.

SSO를 Unified CM과 통합하여 Webex Teams 사용자가 단일 자격 증명 집합을 사용하여 로그인하게 하는 방법은 *Cisco Unified* 커뮤니케이션 애플리케이션용 *SAML SSO* 구축 설명서를 참조하십시오.

LDAP 서버로 인증합니다.

회사 LDAP 디렉터리에 할당된 암호에 대해 최종 사용자 암호가 인증되도록 LDAP 인증을 활성화하려면 이 절차를 수행하십시오. LDAP 인증은 시스템 관리자가 모든 회사 애플리케이션에 대해 최종 사용자에게 단일 암호를 할당하는 기능을 제공합니다. 이 구성은 최종 사용자 암호에만 적용되며 최종 사용자 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다. 사용자가 클라이언트에 로그인하면 현재 서버에서 해당 인증을 Cisco Unified Communications Manager로 라우팅합니다. 그러면 Cisco Unified Communications Manager는 디렉터리 서버에 대한 인증을 전송합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

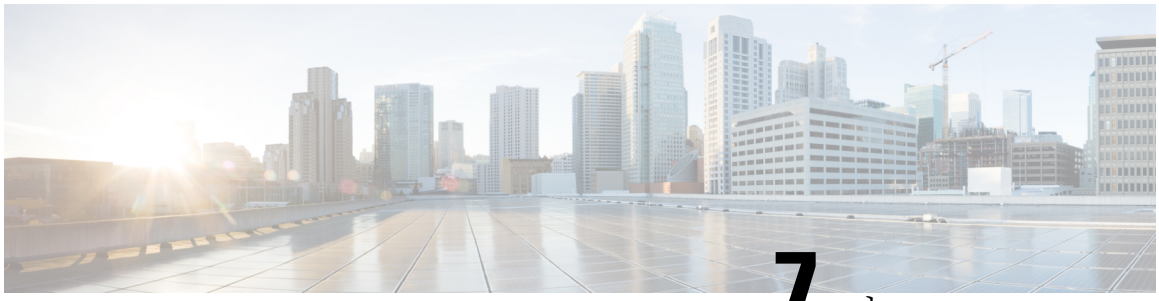
단계 **2** 시스템 > **LDAP** > **LDAP** 인증을 선택합니다.

단계 **3** 최종 사용자에 대한 **LDAP** 인증 사용을 선택합니다.

단계 **4** LDAP 자격 증명과 사용자 검색 기준을 적절하게 지정합니다.

LDAP 인증 창의 필드에 관한 자세한 내용은 *Cisco Unified Communications Manager* 관리 설명서 를 참조하십시오.

단계 **5** 저장을 선택합니다.



7 장

사무실 전화기 제어 구성

사전 요구 사항

Cisco CTIManager 서비스가 Cisco Unified Communications Manager 서버에서 실행 중이어야 합니다.

사무실 전화기 제어 작업 흐름 구성

프로시저

	명령 또는 동작	목적
단계 **1**	CTI에 장치 활성화, 32 페이지	Cisco Jabber 데스크톱 클라이언트가 사용자의 사무실 전화기를 제어할 수 있게 해줍니다.
단계 **2**	사무실 전화기 비디오 구성, 32 페이지.	사용자가 클라이언트를 통해 컴퓨터의 사무실 전화기로 전송된 비디오를 수신할 수 있게 합니다.
단계 **3**	비디오 속도 적응 활성화, 34 페이지	클라이언트는 비디오 속도 적응을 사용하여 최적의 비디오 품질을 결정합니다.
단계 **4**	사용자 연결 설정, 35 페이지	사용자를 장치와 연결하고 사용자를 액세스 제어 그룹에 할당합니다.

	명령 또는 동작	목적
단계 5	장치 재설정, 37 페이지	사용자 연결을 구성한 후에는 장치를 재설정해야 합니다.

CTI에 장치 활성화

Cisco Jabber 데스크톱 클라이언트가 사용자의 사무실 전화기를 사용하게 하려면, 사용자의 장치를 만들 때 **CTI**에서 장치 제어 허용 옵션을 선택해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 장치 > 전화기를 선택하고 전화기를 검색합니다.

단계 **2** 장치 정보 섹션에서 **CTI**에서 장치 제어 허용을 선택합니다.

단계 **3** 저장을 클릭합니다.

사무실 전화기 비디오 구성

사무실 전화기 비디오 기능을 사용하면 노트북에서 비디오 신호를, 사무실 전화기에서 오디오 신호를 수신할 수 있습니다. 컴퓨터를 클라이언트의 컴퓨터 포트를 통해 사무실 전화기에 물리적으로 연결하여, Jabber 클라이언트에 대한 연결을 설정합니다. 이 기능은 사무실 전화기에 대한 무선 연결에는 사용할 수 없습니다.

참고 무선 및 유선 연결을 모두 사용할 수 있다면, 무선 연결이 유선 연결에 우선하지 않도록 Microsoft Windows를 구성합니다. 자세한 내용은 Microsoft의 인터넷 프로토콜 라우트의 자동 메트릭 기능에 대한 설명을 참조하십시오.

먼저 Cisco.com에서 Jabber 사무실 전화기 비디오 서비스 인터페이스를 다운로드하고 설치합니다. Jabber 사무실 전화기 비디오 서비스 인터페이스는 CDP(Cisco Discover Protocol) 드라이버를 제공합니다. CDP를 사용하면 클라이언트는 다음을 수행할 수 있습니다.

- 사무실 전화기를 검색합니다.
- CAST(Cisco 오디오 세션 터널) 프로토콜을 사용하여 사무실 전화기에 대한 연결을 설정 하고 유지합니다.

사무실 전화기 비디오 고려사항

사무실 전화기 비디오 기능을 설정하기 전에 다음 고려사항 및 제한사항을 검토하십시오.

- CAST에는 비디오 장치를 두 개 이상 연결할 수 없습니다. 내장 카메라가 있는 사무실 전화기에서는 이 기능을 사용할 수 없습니다. 사무실 전화기에 로컬 USB 카메라가 있다면, 이 기능을 사용하기 전에 제거하십시오.
- CTI를 지원하지 않는 장치에서는 이 기능을 사용할 수 없습니다.
- BFCP 프로토콜을 이용한 비디오 화면 공유와 사무실 전화기 비디오를 동시에 사용할 수는 없습니다.
- SCCP를 사용하는 엔드포인트는 비디오만 수신할 수는 없습니다. SCCP 엔드포인트는 비디오를 송수신해야 합니다. SCCP 엔드포인트가 비디오 신호를 전송하지 못하는 인스턴스에서는 오디오 전용 통화를 하게 됩니다.
- 7900 시리즈 전화기는 사무실 전화기 비디오 기능에 SCCP를 사용해야 합니다. 7900 시리즈 전화기는 사무실 전화기 비디오 기능에 SIP를 사용할 수 없습니다.
- 사무실 전화기의 키패드를 이용해 통화를 시작했다면, 통화는 사무실 전화기에서 오디오 전용 통화로 시작됩니다. 이후 Jabber에서 통화를 비디오로 에스컬레이트합니다. 따라서 H.323 엔드포인트처럼 에스컬레이션을 지원하지 않는 장치에는 영상 통화를 걸 수 없습니다. 에스컬레이션을 지원하지 않는 장치에서 이 기능을 사용하려면 Jabber 클라이언트에서 통화를 시작해야 합니다.
- 펌웨어 버전 SCCP45.9-2-1S를 사용하는 Cisco Unified IP Phone에서는 호환성 문제가 발생합니다. 이 기능을 사용하려면 펌웨어를 버전 SCCP45.9-3-1로 업그레이드해야 합니다.
- Symantec EndPoint Protection 같은 일부 안티바이러스 또는 방화벽 애플리케이션은 인바운드 CDP 패킷을 차단합니다. 이러한 차단은 사무실 전화기 비디오를 비활성화합니다. 인바운드 CDP 패킷을 허용하도록 안티바이러스 또는 방화벽 애플리케이션을 구성하십시오.

  이 문제에 관한 자세한 내용은 Symantec 기술 문서인 네트워크 위협 보호 때문에 *Cisco IP* 전화기 버전 *7970* 및 *Cisco Unified Video Advantage*가 차단됨을 참조하십시오.
- Cisco Unified Communications Manager(Unified CM)의 SIP 트렁크 구성에 있는 미디어 터미네이션 포인트 필요 확인란은 선택하지 마십시오. 이 설정은 사무실 전화기 비디오를 비활성화합니다.

프로시저

단계 **1** 컴퓨터를 사무실 전화기의 컴퓨터 포트에 물리적으로 연결합니다.

단계 **2** Unified CM에서 사무실 전화기의 비디오를 활성화합니다.

단계 **3** Jabber 사무실 전화기 비디오 서비스 인터페이스를 컴퓨터에 설치합니다.

사무실 전화기 비디오 문제 해결

사무실 전화기 비디오 기능을 사용할 수 없거나 사무실 전화기를 확인할 수 없다는 오류가 발생한다면, 다음을 수행하십시오.

1. Cisco Unified Communications Manager에서 사무실 전화기의 비디오를 활성화했는지 확인합니다.
2. 실제 사무실 전화기를 재설정합니다.
3. 클라이언트를 종료합니다.
4. 클라이언트를 설치한 컴퓨터에서 services.msc를 실행합니다.
5. Windows 작업 관리자의 서비스 탭에서 Jabber 사무실 전화기 비디오 서비스 인터페이스를 다시 시작합니다.
6. 클라이언트를 다시 시작합니다.

비디오 속도 적응 활성화

클라이언트는 비디오 속도 적응을 사용하여 최적의 비디오 품질을 결정합니다. 비디오 레이트 적응은 네트워크 상태를 기반으로 비디오 품질을 동적으로 높이거나 줄입니다.

비디오 레이트 적응을 사용하려면 Cisco Unified Communications Manager에서 RTCP(실시간 전송 제어 프로토콜)를 활성화해야 합니다.

참고 RTCP는 소프트웨어 전화기 장치에서 기본적으로 활성화됩니다. 하지만 사무실 전화기 장치에서 RTCP를 활성화해야 합니다.

일반 전화기 프로파일에서 **RTCP** 활성화

일반 전화기 프로파일에서 RTCP를 활성화하면 프로파일을 사용하는 모든 장치에서 비디오 레이트 적용을 활성화할 수 있습니다.

참고 RTCP는 Jabber 전화 통신 서비스의 필수 구성 요소입니다. Jabber는 비활성화해도 계속 RTCP 패킷을 전송합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 장치 > 장치 설정 > 일반 전화기 프로파일을 선택합니다.

일반 전화기 프로파일 찾기 및 나열 창이 열립니다.

단계 **3** 일반 전화기 프로파일을 찾을 장소 필드에 적절한 필터를 지정한 다음 찾기를 선택하여 프로파일 목록을 검색합니다.

단계 **4** 목록에서 적절한 프로 파일을 선택합니다.

일반 전화기 프로파일 구성 창이 열립니다.

단계 **5** 제품별 구성 레이아웃 섹션을 찾습니다.

단계 **6** **RTCP** 드롭다운 목록에서 활성화됨을 선택합니다.

단계 **7** 저장을 선택합니다.

장치 구성에서 **RTCP** 활성화

일반 전화기 프로파일 대신 특정 장치 구성에 대한 RTCP를 활성화할 수도 있습니다. 특정 장치 구성은 일반 전화기 프로파일에 지정한 설정을 무시합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 장치 > 전화기를 선택합니다.

전화기 찾기 및 나열 창이 열립니다.

단계 **3** 전화기 위치 찾기 필드에 적절한 필터를 지정한 다음 찾기를 선택하여 전화기 목록을 검색합니다.

단계 **4** 목록에서 적절한 전화기를 선택합니다.

전화기 구성 창이 열립니다.

단계 **5** 제품별 구성 레이아웃 섹션을 찾습니다.

단계 **6** **RTCP** 드롭다운 목록에서 활성화됨을 선택합니다.

단계 **7** 저장을 선택합니다.

사용자 연결 설정

사용자를 장치에 연결하면 해당 장치를 사용자에게 프로비저닝하게 됩니다.

시작하기 전에

Cisco Jabber 장치를 만들고 구성합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 사용자 관리 > 최종 사용자를 선택합니다.

사용자 찾기 및 나열 창이 열립니다.

단계 **3** 사용자 위치 찾기 필드에 적절한 필터를 지정한 다음, 찾기를 선택하여 사용자 목록을 검색합니다.

단계 **4** 목록에서 적절한 사용자를 선택합니다.

최종 사용자 구성 창이 열립니다.

단계 **5** 서비스 설정 섹션을 찾습니다.

단계 **6** **UC** 서비스 프로파일 드롭다운 목록에서 사용자의 적절한 서비스 프로파일을 선택합니다.

단계 **7** 장치 정보 섹션을 찾습니다.

단계 **8** 장치 연결을 선택합니다.

사용자 장치 연결 창이 열립니다.

단계 **9** 사용자를 연결할 장치를 선택합니다. Jabber는 장치 유형별로 하나의 소프트폰 연결만 지원합니다. 예를 들어 개별 사용자에는 TCT, BOT, CSF 및 TAB 장치를 하나만 연결할 수 있습니다.

단계 **10** 선택 항목/변경 사항 저장을 선택합니다.

단계 **11** 사용자 관리 > 최종 사용자를 선택하고 사용자 찾기 및 나열 창으로 돌아갑니다.

단계 **12** 목록에서 사용자를 찾아 선택합니다.

최종 사용자 구성 창이 열립니다.

단계 **13** 권한 정보 섹션을 찾습니다.

단계 **14** 액세스 제어 그룹에 추가를 선택합니다.

액세스 제어 그룹 찾기 및 나열 확인란이 열립니다.

단계 **15** 사용자에게 할당할 액세스 제어 그룹을 선택합니다.

최소한 다음 액세스 제어 그룹에 사용자를 할당해야 합니다.

- 표준 **CCM** 최종 사용자
- 표준 **CTI** 활성화

기억 보안 전화 기능으로 사용자를 프로비저닝한다면 사용자를 표준 **CTI** 보안 연결 그룹에 할당하지 마십시오.

특정 전화기 모델에는 다음과 같이 추가 제어 그룹이 필요합니다.

- Cisco Unified IP Phone 9900, 8900 또는 8800 시리즈 또는 DX 시리즈의 경우에는, 연결된 **Xfer** 및 **conf**를 지원하는 전화의 표준 **CTI** 컨트롤 허용을 선택합니다.
- Cisco Unified IP Phone 6900 시리즈의 경우, 롤오버 모드를 지원하는 전화의 표준 **CTI** 컨트롤 허용을 선택합니다.

단계 **16** 선택한 항목 추가를 선택합니다.

액세스 제어 그룹 찾기 및 나열 창이 닫힙니다.

단계 **17** 최종 사용자 구성 창에서 저장을 선택합니다.

장치 재설정

사용자를 만들고 장치와 연결한 후에는 해당 장치를 재설정해야 합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 장치 > 전화기를 선택합니다.

전화기 찾기 및 나열 창이 열립니다.

단계 **3** 전화기 위치 찾기 필드에 적절한 필터를 지정한 다음 찾기를 선택하여 장치 목록을 검색합니다.

단계 **4** 목록에서 적절한 장치를 선택합니다.

전화기 구성 창이 열립니다.

단계 **5** 연결 정보 섹션을 찾습니다.

단계 **6** 적절한 디렉터리 번호 구성을 선택합니다.

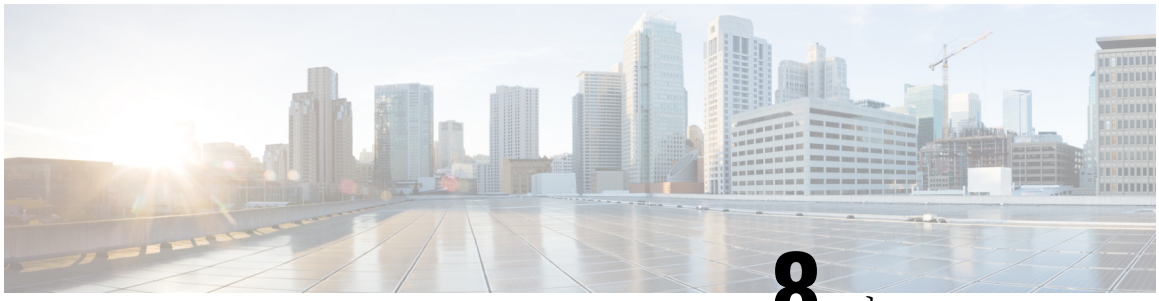
디렉터리 번호 구성 창이 열립니다.

단계 **7** 재설정을 선택합니다.

장치 재설정 대화 상자가 열립니다.

단계 **8** 재설정을 선택합니다.

단계 **9** 닫기를 선택하여 장치 재설정 대화 상자를 닫습니다.



8 장

소프트폰 구성

소프트폰 워크플로 생성

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco Jabber 장치 생성 및 구성, 40 페이지	Cisco Jabber에 액세스하는 모든 사용자에 대해 하나 이상의 장치를 생성합니다. 사용자에게 제공할 인증 문자열을 생성합니다.
단계 **2**	장치에 전화 번호 추가, 43 페이지	생성하는 각 장치에 디렉터리 번호를 추가합니다.
단계 **3**	사용자를 장치에 연결, 44 페이지	사용자를 장치와 연결합니다.
단계 **4**	모바일 SIP 프로파일 생성, 45 페이지.	Cisco Unified Communications Manager 9 릴리스가 있고 모바일 클라이언트에 대해 장치를 구성할 계획이 있다면, 이 작업을 완료하십시오.
단계 **5**	전화기 보안 프로파일 구성, 47 페이지	이 작업을 완료하여 모든 장치에 보안 전화 기능을 설정합니다.

Cisco Jabber 장치 생성 및 구성

Cisco Jabber에 액세스하는 모든 사용자에 대해 하나 이상의 장치를 생성합니다. 사용자는 여러 장치를 보유할 수 있습니다.

참고 사용자는 소프트폰(CSF) 장치를 사용하여 전화를 걸 때 다자간 통화의 참가자만 제거할 수 있습니다.

시작하기 전에

- COP 파일을 설치합니다.
- Cisco Unified Communications Manager 9 이하 릴리스가 있고 모바일 클라이언트에 대해 장치를 구성할 계획이 있는 경우, SIP 프로파일을 완료하십시오.
- 모든 장치에 대해 보안 전화기 기능을 설정할 계획이라면 전화기 보안 프로 파일을 생성합니다.
- Capf 등록을 사용하는 경우, Cisco Unified Communications Manager 릴리스 10 이상 버전에서는 엔드포인트에 대한 인증서 발급자의 Cisco CAPF(인증 센터 프록시 기능) 서비스 매개변수 값이 **Cisco** 인증 센터 프록시 기능인지 확인하십시오. 이 옵션은 Cisco Jabber에서 지원하는 유일한 옵션입니다. CAPF 서비스 매개변수 구성에 대한 자세한 내용은 Cisco Unified Communications Manager 보안 설명서의 *CAPF* 서비스 매개변수 업데이트 항목을 참조하십시오.
- 모바일 사용자용 Cisco Jabber에 대해 TCT 장치, BOT 장치 또는 TAB 장치를 생성하기 전에 Cisco Jabber와 Cisco Unified Communications Manager 간 등록을 지원하는 조직 최상위 도메인 이름을 지정하십시오. Unified CM 관리 인터페이스에서 시스템 > 엔터프라이즈 매개변수를 선택합니다. 클러스터 수준 도메인 구성 섹션에서 조직 최상위 도메인 이름을 입력합니다. 예: cisco.com 이 최상위 도메인 이름은 Jabber에서 전화기 등록을 위해 Cisco Unified Communications Manager 서버의 DNS 도메인으로 사용됩니다. 예: CUCMServer1@cisco.com

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스에 로그인합니다.

단계 **2** 장치 > 전화기를 선택합니다.
전화기 찾기 및 나열 창이 열립니다.

단계 **3** 새로 추가를 선택합니다.

단계 **4** 전화기 유형 드롭다운 목록에서 구성하려는 장치 유형에 해당하는 옵션을 선택하고 다음을 선택합니다.

Jabber 사용자의 경우에는 각 사용자에 대해 여러 장치를 생성할 수 있지만, 사용자당 하나의 장치 유형만 생성할 수 있습니다. 예를 들어 태블릿 장치 하나와 CSF 장치 하나를 생성할 수 있지만, 두 개의 CSF 장치는 생성할 수 없습니다.

- **Cisco Unified** 클라이언트 서비스 프레임워크 - 이 옵션을 선택하여 Mac용 Cisco Jabber 또는 Windows용 Cisco Jabber에 대해 CSF 장치를 생성합니다.
- **IPhone**용 **Cisco** 듀얼 모드 - iPhone용 TCT 장치를 생성하려면 이 옵션을 선택하십시오.
- 태블릿용 **Cisco Jabber** - IPad 또는 Android 태블릿 또는 Chromebooks에 대한 TAB 장치를 만들려면 이 옵션을 선택하십시오.
- **Android**용 **Cisco** 듀얼 모드 - Android 장치에 대한 BOT 장치를 생성하려면 이 옵션을 선택하십시오.

단계 **5** 소유자 사용자 **ID** 드롭다운 목록에서 장치를 생성할 사용자를 선택합니다.

전화기 모드 구축의 **Cisco Unified** 클라이언트 서비스 프레임워크 옵션의 경우, 사용자가 선택되어 있는지 확인합니다.

단계 **6** 장치 이름 필드에서 해당 형식을 사용하여 장치에 이름을 지정합니다.

선택하는 경우	필수 형식
Cisco Unified Client Services Framework	• 유효한 문자: a–z, A–Z, 0–9. • 15자 제한.
iPhone용 **Cisco** 이중 모드	• 장치 이름은 *TCT*로 시작해야 합니다. 예를 들어 사용자 이름이 tadams인 Tanya Adams 사용자에 대한 TCT 장치를 생성한다면, **TCTTADAMS**를 입력합니다. • 반드시 대문자여야 합니다. • 유효한 문자: A~Z, 0~9, 마침표(.), 밑줄(_), 하이픈(-). • 15자 제한.
태블릿용 **Cisco Jabber**	• 장치 이름은 *TAB*으로 시작해야 합니다. 예를 들어 사용자 이름이 tadams인 Tanya Adams라는 사용자에 대해 TAB 장치를 생성하는 경우, **TABTADAMS**를 입력합니다. • 반드시 대문자여야 합니다. • 유효한 문자: A~Z, 0~9, 마침표(.), 밑줄(_), 하이픈(-). • 15자 제한.

선택하는 경우	필수 형식
Android용 **Cisco** 이중 모드	• 장치 이름은 *BOT*로 시작해야 합니다. 예를 들어 사용자 이름이 tadams인 Tanya Adams라는 사용자에 대해 BOT 장치를 생성하는 경우, **BOTTADAMS**를 입력합니다. • 반드시 대문자여야 합니다. • 유효한 문자: A~Z, 0~9, 마침표(.), 밑줄(_), 하이픈(-). • 15자 제한.

단계 **7** CAPF 등록을 사용하는 경우, 다음 단계를 완료하여 인증 문자열을 생성하십시오.

1. 사용자는 장치에 액세스하고 Cisco Unified Communications Manager에 안전하게 등록하기 위해 제공할 수 있는 인증 문자열을 사용하여 **CAPF(**인증 기관 프록시 기능**)** 정보 섹션으로 이동할 수 있습니다.
2. 인증서 작업 드롭다운 목록에서 설치/업그레이드를 선택합니다.
3. 인증 모드 드롭다운 목록에서 인증 문자열 기준 또는 **Null** 문자열 기준을 선택합니다. JVDI 및 Windows용 Jabber CSF 장치에서 CAPF 인증 모드 **Null** 문자열 기준을 사용하는 것은 지원되지 않습니다. Cisco Unified Communications Manager에서 Jabber 등록이 실패하는 원인이 되기 때문입니다.
4. 문자열 생성을 클릭합니다. 인증 문자열은 문자열 값으로 자동 입력됩니다. 이 문자열은 최종 사용자에게 제공되는 문자열입니다.
5. 키 크기**(**비트**)** 드롭다운 목록에서 전화기 보안 프로파일에 설정한 것과 동일한 키 크기를 선택합니다.
6. 작업 완료 기한 필드에서 인증 문자열의 만료 값을 지정하거나 기본값을 유지합니다.
7. 그룹 구성 파일을 사용한다면, 데스크톱 클라이언트 설정의 **Cisco** 지원 필드에 지정합니다. Cisco Jabber는 데스크톱 클라이언트 설정에서 사용할 수 있는 다른 설정을 사용하지 않습니다.

단계 **8** 저장을 선택합니다.

단계 **9** 구성 적용을 클릭합니다.

다음에 수행할 작업

장치에 디렉터리 번호를 추가합니다.

사용자에게 인증 문자열 제공

CAPF 등록을 사용하여 보안 전화기를 구성한다면, 사용자에게 인증 문자열을 제공해야 합니다. 사용자는 클라이언트 인터페이스에 인증 문자열을 지정해야 장치에 액세스하고 Cisco Unified Communications Manager를 안전하게 등록할 수 있습니다.

사용자가 클라이언트 인터페이스에 인증 문자열을 입력하면 CAPF 등록 프로세스가 시작됩니다.

참고 등록 프로세스가 완료되는 데 걸리는 시간은 사용자의 컴퓨터나 모바일 장치 및 Cisco Unified Communications Manager의 현재 로드 상태에 따라 다릅니다. 클라이언트가 CAPF 등록 프로세스를 완료하는 데는 최대 1분 정도 걸립니다.

다음과 같은 경우 클라이언트에 오류가 표시됩니다.

- 사용자가 잘못된 인증 문자열을 입력합니다.

  사용자는 인증 문자열을 다시 입력해 CAPF 등록을 완료할 수 있습니다. 하지만 사용자가 잘못된 인증 문자열을 계속 입력한다면, 클라이언트는 문자열이 올바르다 하더라도 사용자가 입력하는 문자열을 거부할 수 있습니다. 이 경우에는 사용자의 장치에서 새 인증 문자열을 생성한 다음 사용자에게 제공해야 합니다.

- 사용자가 운영 완료 기한 필드에 설정한 만료 시간이 다 될 때까지 인증 문자열을 입력하지 않습니다.

  이 경우에는 사용자의 장치에 새 인증 문자열을 생성해야 합니다. 그런 다음 사용자가 만료 시간 전에 해당 인증 문자열을 입력해야 합니다.

중요 Cisco Unified Communications Manager에서 최종 사용자를 구성한다면, 이들을 다음 사용자 그룹에 추가해야 합니다.

- 표준 **CCM** 최종 사용자
- 표준 **CTI** 활성화

사용자는 표준 CTI 보안 연결 사용자 그룹에 속해선 안 됩니다.

장치에 전화 번호 추가

각 장치를 생성하고 구성한 후에는 장치에 디렉터리 번호를 추가해야 합니다. 이 주제에서는 장치 > 전화기 메뉴 옵션을 사용하여 디렉터리 번호를 추가하는 방법에 관한 지침을 제공합니다.

시작하기 전에

장치를 만듭니다.

프로시저

단계 **1** 전화기 구성 창에서 연결 정보 섹션을 찾습니다.
단계 **2** 새 **DN** 추가를 클릭합니다.
단계 **3** 디렉터리 번호 필드에서 디렉터리 번호를 지정합니다.
단계 **4** 회선에 연결된 사용자 섹션에서 최종 사용자 연결을 클릭합니다.
단계 **5** 사용자 위치 찾기 필드에서 적절한 필터를 지정한 다음, 찾기를 클릭합니다.
단계 **6** 표시되는 목록에서 해당되는 사용자를 선택하고 선택한 항목 추가를 클릭합니다.
단계 **7** 다른 모든 필요한 구성 설정을 적절히 지정합니다.
단계 **8** 구성 적용을 선택합니다.
단계 **9** 저장을 선택합니다.

사용자를 장치에 연결

Cisco Unified Communications Manager 버전 9.x 한정으로, 클라이언트는 사용자에 대한 서비스 프로파일을 검색할 때 먼저 Cisco Unified Communications Manager에서 장치 구성 파일을 얻습니다. 그러면 클라이언트는 사용자에게 적용한 서비스 프로파일을 장치 구성을 사용하여 가져올 수 있습니다.

예를 들어 `CSFAKenzi`라는 CSF 장치를 이용하여 Adam McKenzie를 프로비저닝하는 식입니다. 클라이언트는 Adam이 로그인하면 Cisco Unified Communications Manager에서 `CSFAKenzi.cnf.xml`을 검색합니다. 그러면 클라이언트는 `CSFAKenzi.cnf.xml`에서 다음을 찾습니다.

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

따라서 Cisco Unified Communications Manager 버전 9.x를 사용한다면, 사용자에게 적용할 서비스 프로파일을 클라이언트가 검색할 수 있도록 다음을 수행해야 합니다.

- 사용자를 장치와 연결합니다.
- 장치 구성의 사용자 소유자 **ID** 필드를 적절한 사용자로 설정합니다. 이 값을 설정하지 않으면 클라이언트는 기본 서비스 프로파일을 검색합니다.

시작하기 전에

참고 여러 사용자에 서로 다른 서비스 프로파일을 사용할 계획이라면, CSF를 여러 사용자에 연결하지 마십시오.

프로시저

단계 **1** 사용자를 장치와 연결합니다.

a) **Unified CM** 관리 인터페이스를 엽니다.
b) 사용자 관리 > 최종 사용자를 선택합니다.
c) 적절한 사용자를 찾아 선택합니다.
최종 사용자 구성 창이 열립니다.
d) 장치 정보 섹션에서 장치 연결을 선택합니다.
e) 사용자와 장치를 적절하게 연결합니다.
f) 최종 사용자 구성 창으로 돌아와 저장을 선택합니다.

단계 **2** 장치 구성의 사용자 소유자 **ID** 필드를 설정합니다.

a) 장치 > 전화기를 선택합니다.
b) 적절한 장치를 찾아 선택합니다.
전화기 구성 창이 열립니다.
c) 장치 정보 섹션을 찾습니다.
d) 소유자 필드의 값으로 사용자를 선택합니다.
e) 소유자 사용자 **ID** 필드에서 적절한 사용자 ID를 선택합니다.
f) 저장을 선택합니다.

모바일 **SIP** 프로파일 생성

이 절차는 Cisco Unified Communications Manager 릴리스 9를 사용하고 모바일 클라이언트에 대한 장치를 구성하는 경우에만 필요합니다. 데스크톱 클라이언트에 제공된 기본 SIP 프로파일을 사용합니다. 모바일 클라이언트용 장치를 만들고 구성하기 전에, Cisco Jabber가 Cisco Unified Communication Manager에 계속 연결되며 Cisco Jabber는 백그라운드에서 실행되게 하는 SIP 프로파일을 생성해야 합니다.

Cisco Unified Communication Manager 릴리스 10을 사용한다면, 모바일 클라이언트용 장치를 만들고 구성할 때 모바일 장치용 표준 **SIP** 프로파일 기본 프로파일을 선택합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 장치 > 장치 설정 > **SIP** 프로파일을 선택합니다.

SIP 프로파일 찾기 및 나열 창이 열립니다.

단계 **3** 다음 중 하나를 수행하여 새 SIP 프로파일을 생성합니다.

- 기본 SIP 프로파일을 찾은 다음 편집할 수 있는 복사본을 만듭니다.
- 새로 추가 를 선택하여 새 SIP 프로파일을 만듭니다.

단계 **4** 새 SIP 프로파일에서 다음 값을 설정합니다.

- 등록 델타 타이머 = 120
- 등록 만료 타이머 = 720
- 연결 유지 만료 타이머 = 720
- 가입 만료 타이머 = 21600
- 가입 델타 타이머 = 15

단계 **5** 저장을 선택합니다.

시스템 SIP 매개변수 설정

저대역폭 네트워크에 연결된 상태에서 모바일 장치에서 걸려오는 전화를 받기가 어렵다면, SIP 매개변수를 설정하여 조건을 개선할 수 있습니다. SIP 듀얼 모드 알림 타이머 값을 늘려, Cisco Jabber 내선 번호로 걸려오는 통화가 모바일-네트워크 전화번호로 너무 빨리 라우팅되지 않게 합니다.

시작하기 전에

이 구성은 모바일 클라이언트에만 해당됩니다.

워크콜을 수신하려면 Cisco Jabber가 실행 중이어야 합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 시스템 > 서비스 매개 변수를 선택합니다.

단계 **3** 노드를 선택합니다.

단계 **4** **Cisco CallManager(**활성**)** 서비스를 선택합니다.

단계 **5** 클러스터 파라미터**(**시스템 - 이동성**)** 섹션으로 스크롤합니다.

단계 **6** **SIP** 듀얼 모드 알림 타이머 값을 1만 밀리초로 늘립니다.

단계 **7** 저장을 선택합니다.

참고 SIP 듀얼 모드 알림 타이머 값을 늘린 후에도 Cisco Jabber로 도달한 걸려오는 전화가 중단되며 Mobile Connect를 이용해 착신 전환된다면, SIP 듀얼 모드 알림 타이머 값을 500 밀리초 단위로 늘리십시오.

전화기 보안 프로파일 구성

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.

시작하기 전에

- Cisco CTL 클라이언트를 사용하여 Cisco Unified Communications Manager 보안 모드를 구성합니다. 혼합 모드 보안을 이상을 선택해야 합니다.

  Cisco CTL Client와의 혼합 모드를 구성하는 자세한 방법은 Cisco Unified Communications Manager 보안 설명서를 참조하십시오.

- 전화 회의 통화의 경우 전화 회의 브리지가 보안 전화기 기능을 지원하는지 확인하십시오. 전화 회의 브리지가 보안 전화기 기능을 지원하지 않는다면, 해당 브리지에 대한 통화는 안전하지 않습니다. 마찬가지로, 모든 당사자는 클라이언트에서 전화 회의 통화의 미디어를 암호화하는 공통 암호화 알고리즘을 지원해야 합니다.

- 구축에서 Unified Communications Manager 릴리스 12.5 이상을 사용한다면, SIP OAuth를 Cisco Jabber와 함께 사용하는 것이 좋습니다. 자세한 내용은 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html에 있는 *Cisco Unified Communications Manager* 기능 구성 설명서의 SIP OAuth 장을 참조하십시오.

프로시저

단계 **1** **Cisco Unified Communications Manager**에서 시스템 > 보안 > 전화기 보안 프로파일을 선택합니다.

단계 **2** 새로 추가를 선택합니다.

단계 **3** 전화기 유형 드롭다운 목록에서 구성하려는 장치 유형에 해당하는 옵션을 선택하고 다음을 선택합니다.

- **Cisco Unified** 클라이언트 서비스 프레임워크 - 이 옵션을 선택하여 Mac용 Cisco Jabber 또는 Windows용 Cisco Jabber에 대해 CSF 장치를 생성합니다.
- **IPhone**용 **Cisco** 듀얼 모드 - iPhone용 TFT 장치를 생성하려면 이 옵션을 선택하십시오.
- 태블릿용 **Cisco Jabber** - IPad 또는 Android 태블릿 또는 Chromebooks에 대한 TAB 장치를 만들려면 이 옵션을 선택하십시오.
- **Android**용 **Cisco** 듀얼 모드 - Android 장치에 대한 BOT 장치를 생성하려면 이 옵션을 선택하십시오.
- **CTI** 원격 장치 - CTI 원격 장치를 생성하려면 이 옵션을 선택합니다.

  CTI 원격 장치는 사용자의 원격 대상을 모니터링하고 통화 제어권을 갖는 가상 장치입니다.

단계 **4** 전화기 보안 프로파일 구성 창의 이름 필드에 전화기 보안 프로파일의 이름을 지정합니다.

단계 **5** 장치 보안 모드에서 다음 옵션 중 하나를 선택합니다.

- 인증됨 - SIP 연결은 NULL-SHA 암호화를 사용하는 TLS를 이용합니다.
- 암호화됨 - SIP 연결은 AES 128/SHA 암호화를 사용하는 TLS를 이용합니다. 클라이언트는 SRTP(안전한 실시간 전송 프로토콜)를 사용하여, 암호화된 미디어 스트림을 제공합니다.

단계 **6** 전송 유형에는 기본값인 **TLS**를 그대로 선택합니다.

단계 **7** TFTP 서버에 있는 장치 구성 파일을 암호화하려면 **TFTP** 암호화 구성 확인란을 선택합니다.

참고 TCT/BOT/태블릿 장치의 경우에는 TFTP 암호화 구성 확인란을 선택하면 안 됩니다. 인증 모드에서는 인증 문자열 기준 또는 Null 문자열 기준을 선택합니다.

단계 **8** 인증 모드에서는 인증 문자열 기준 또는 **Null** 문자열 기준을 선택합니다.

참고 JVDI 및 Windows용 Jabber CSF 장치에서 CAPF 인증 모드 **Null** 문자열 기준을 사용하는 것은 지원되지 않습니다. Cisco Unified Communications Manager에서 Jabber 등록이 실패하는 원인이 되기 때문입니다.

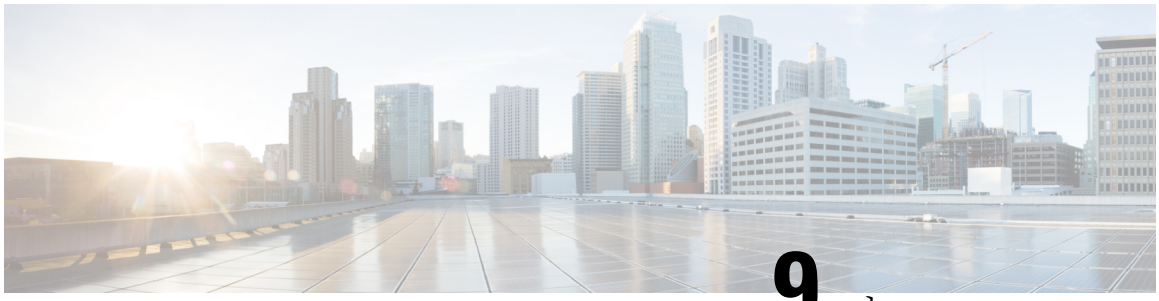
단계 **9** 키 크기**(**비트**)**에서는 인증서에 적합한 키 크기를 선택합니다. 키 크기는 CAPF 등록 프로세스에서 클라이언트가 생성하는 공개 및 개인 키의 비트 길이를 말합니다.

Cisco Jabber 클라이언트는 1024 비트 길이 키가 있는 인증 문자열을 사용하여 테스트되었습니다. Cisco Jabber 클라이언트에서는 1024 비트 길이 키보다 2048 비트 길이 키를 생성하는 데 시간이 더 오래 걸립니다. 따라서 2048을 선택하면 CAPF 등록 프로세스를 완료하는 시간이 길어질 수 있습니다.

단계 **10** **SIP** 전화기 포트에서는 기본값을 그대로 둡니다.

이 필드에 지정하는 포트는 장치 보안 모드의 값으로 보안되지 않음을 선택하는 경우에만 적용됩니다.

단계 **11** 저장을 클릭합니다.



9 장

확장 및 연결 구성

확장 및 연결 워크플로 구성

프로시저

	명령 또는 동작	목적
단계 **1**	사용자 이동성 활성화, 49 페이지	사용자 이동성을 활성화하면 사용자를 CTI 원격 장치의 소유자로 할당할 수 있습니다.
단계 **2**	CTI 원격 장치 생성, 50 페이지	CTI 원격 장치를 생성하면 이 가상 장치가 사용자의 원격 대상에 대해 모니터링을 실행하고 통화 제어권을 갖게 됩니다.
단계 **3**	원격 대상 추가, 51 페이지	(선택 사항) 전용 CTI 원격 장치로 사용자를 프로비저닝할 계획이라면, Cisco Unified Communications Manager에 원격 대상을 추가하십시오.

사용자 이동성 활성화

이 작업은 데스크톱 클라이언트에만 적용됩니다.

사용자 이동성을 활성화하여 CTI 원격 장치를 프로비저닝해야 합니다. 사용자의 이동성을 활성화하지 않는 경우 이러한 사용자를 CTI 원격 장치의 소유자로 할당할 수 있습니다.

시작하기 전에

이 작업은 다음 경우에만 적용됩니다.

- Mac용 Cisco Jabber 또는 Windows용 Cisco Jabber 사용자를 CTI 원격 장치에 할당할 계획입니다.
- Cisco Unified Communication Manager 릴리스 9.x 이상입니다.

프로시저

단계 **1** 사용자 관리 > 최종 사용자를 선택합니다.

사용자 찾기 및 나열 창이 열립니다.

단계 **2** 사용자 위치 찾기 필드에 적절한 필터를 지정한 다음, 찾기를 선택하여 사용자 목록을 검색합니다.

단계 **3** 목록에서 사용자를 선택합니다.

최종 사용자 구성 창이 열립니다.

단계 **4** 이동성 정보 섹션을 찾습니다.

단계 **5** 이동성 활성화를 선택합니다.

단계 **6** 저장을 선택합니다.

CTI 원격 장치 생성

CTI 원격 장치는 사용자의 원격 대상을 모니터링하고 통화 제어권을 갖는 가상 장치입니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 장치 > 전화기를 선택합니다.

전화기 찾기 및 나열 창이 열립니다.

단계 **3** 새로 추가를 선택합니다.

단계 **4** 전화기 유형 드롭다운 목록에서 **CTI** 원격 장치를 선택하고 다음을 선택합니다.

전화기 구성 창이 열립니다.

단계 **5** 소유자 사용자 **ID** 드롭다운 목록에서 적절한 사용자 ID를 선택합니다.

참고 이동성을 활성화한 사용자만 소유자 사용자 **ID** 드롭다운 목록에서 사용할 수 있습니다. 자세한 내용은 클라이언트에서 *SAML SSO* 활성화를 참조하십시오.

Cisco Unified Communications Manager이(가) 장치 이름 필드에 사용자 ID와 **CTIRD** 접두사를 입력합니다(예: **CTIRDusername**).

단계 **6** 필요하다면 장치 이름 필드의 기본값을 편집합니다.

단계 **7** 프로토콜별 정보 섹션의 재라우팅 발신 검색 공간 드롭다운 목록에서 적절한 옵션을 선택해야 합니다.

재라우팅 발신 검색 공간 드롭다운 목록은 재전송할 발신 검색 공간을 정의하고 사용자가 CTI 원격 장치에서 통화를 송수신할 수 있게 합니다.

단계 **8** 전화기 구성 창에서 다른 모든 구성 설정을 적절히 지정합니다.

자세한 내용은 Cisco Unified Communications Manager 시스템 구성 설명서의 *CTI* 원격 장치 설정 항목을 참조하십시오.

단계 **9** 저장을 선택합니다.

디렉터리 번호를 연결하고 원격 대상을 추가하는 필드가 전화기 구성 창에 표시됩니다.

원격 대상 추가

원격 대상은 사용자가 사용할 수 있는 CTI 제어 가능 장치를 나타냅니다.

전용 CTI 원격 장치로 사용자를 프로비저닝할 계획이라면 **Cisco Unified CM** 관리 인터페이스를 이용해 원격 대상을 추가해야 합니다. 이 작업을 수행하면 사용자가 전화기를 자동으로 제어하고 클라이언트를 시작할 때 전화를 걸 수 있습니다.

사용자에게 CTI 원격 장치를 소프트웨어 전화기 및 사무실 전화기와 함께 프로비저닝할 계획이라면, **Cisco Unified CM** 관리 인터페이스를 통해 원격 대상을 추가해선 안 됩니다. 사용자는 클라이언트 인터페이스를 통해 원격 대상을 입력할 수 있습니다.

참고

- 사용자별로 하나의 원격 대상만 생성해야 합니다. 사용자에 두 개 이상의 원격 대상을 추가하지 마십시오.
- Cisco Unified Communications Manager는 **Cisco Unified CM** 관리 인터페이스를 통해 추가한 원격 대상 라우팅 여부는 확인하지 않습니다. 따라서 사용자가 추가하는 원격 대상을 Cisco Unified Communications Manager에서 라우팅할 수 있는지 확인해야 합니다.
- Cisco Unified Communications Manager는 CTI 원격 장치에 대한 애플리케이션 다이얼 규칙을 모든 원격 대상 번호에 자동으로 적용합니다.

프로시저

단계 **1** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **2** 장치 > 전화기를 선택합니다.

전화기 찾기 및 나열 창이 열립니다.

단계 **3** 전화기 위치 찾기 필드에 적절한 필터를 지정한 다음 찾기를 선택하여 전화기 목록을 검색합니다.

단계 **4** 목록에서 CTI 원격 장치를 선택합니다.

전화기 구성 창이 열립니다.

단계 **5** 연결된 원격 대상 섹션을 찾습니다.

단계 **6** 새 원격 대상 추가를 선택합니다.

원격 대상 정보 창이 열립니다.

단계 **7** 이름 필드에 JabberRD를 지정합니다.

제한 이름 필드에 JabberRD를 지정해야 합니다. 클라이언트는 JabberRD 원격 대상만 사용합니다. JabberRD가 아닌 다른 이름을 지정하면 사용자가 해당 원격 대상에 액세스할 수 없습니다.

사용자가 클라이언트 인터페이스를 통해 원격 대상을 추가하면, 클라이언트는 JabberRD 이름을 자동으로 설정합니다.

단계 **8** 대상 번호 필드에 대상 번호를 입력합니다.

단계 **9** 다른 모든 값을 적절하게 지정합니다.

단계 **10** 저장을 선택합니다.

다음에 수행할 작업

다음 단계를 수행하여 원격 대상을 확인하고 구성을 CTI 원격 장치에 적용합니다.

1. CTI 원격 장치의 전화기 구성 창을 여는 단계를 반복합니다.
2. 연결된 원격 대상 섹션을 찾습니다.
3. 원격 대상을 사용할 수 있는지 확인합니다.
4. 구성 적용을 선택합니다.

참고 전화기 구성 창의 장치 정보 섹션에는 활성 원격 대상 필드가 있습니다.

사용자가 클라이언트에서 원격 대상을 선택하면, 활성 원격 대상의 값으로 표시됩니다.

다음과 같은 경우에는 없음이 활성 원격 대상의 값으로 표시됩니다.

- 사용자가 클라이언트에서 원격 대상을 선택하지 않습니다.
- 사용자가 클라이언트에서 나가거나 클라이언트에 로그인하지 않습니다.

10 장

Remote Access 서비스 검색 구성

서비스 검색 요구 사항

서비스 검색을 통해 클라이언트는 엔터프라이즈 네트워크에서 서비스를 자동으로 감지하고 찾을 수 있습니다. 모바일 및 Remote Access를 위한 Expressway를 사용하면 엔터프라이즈 네트워크에서 서비스에 액세스할 수 있습니다. 클라이언트가 모바일 및 Remote Access 및 검색 서비스를 위한 Expressway를 통해 연결할 수 있게 하려면 다음 요구 사항을 충족해야 합니다.

- DNS 요구 사항
- 인증서 요구 사항
- 외부 SRV `_collab-edge`를 테스트합니다.

DNS 요구 사항

Remote Access를 통한 서비스 검색에 대한 DNS 요구 사항은 다음과 같습니다.

- 외부 DNS 서버에서 `_collab-edge` DNS SRV 레코드를 구성해야 합니다.
- 내부 이름 서버에 `_cisco-uds` DNS SRV 레코드를 구성해야 합니다.
- IM and Presence 서버 및 음성 서버에 대해 다른 도메인을 사용하는 하이브리드 클라우드 기반 구축의 경우에는 선택 사항으로 `_collab-edge` 레코드를 사용하여 DNS 서버를 찾도록 음성 서비스 도메인을 구성할 수 있습니다.

인증서 요구 사항

Remote Access를 구성하기 전에 Cisco VCS Expressway 및 Cisco Expressway-E 서버 인증서를 다운로드하십시오. 이 서버 인증서는 HTTP와 XMPP 모두에 사용합니다.

Cisco VCS Expressway 인증서 구성에 대한 자세한 내용은 Cisco VCS Expressway에서 인증서 구성을 참조하십시오.

_collab-edge SRV 레코드 테스트

프로시저

단계 **1** 명령 프롬프트를 엽니다.

단계 **2** **nslookup**을 입력합니다.
기본 DNS 서버 및 주소가 표시됩니다. 예상했던 DNS 서버인지 확인합니다.

단계 **3** **set type=SRV**를 입력합니다.

단계 **4** 각 SRV 레코드에 이름을 입력합니다.

예: `_collab-edge.exampledomain`

- 서버 및 주소를 표시합니다 - SRV 레코드에 액세스할 수 있습니다.
- `_collab-edge.exampledomain: 존재하지 않는 도메인`이 표시됩니다 - SRV 레코드에 문제가 있습니다.

11 장

인증서 확인 설정

클라우드 구축을 위한 인증서 확인

Cisco Webex Messenger및 Cisco Webex Meetings Center는 기본적으로 다음 인증서를 클라이언트에 제공합니다.

- CAS
- WAPI

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

Cisco Jabber은(는) Cisco 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.

프로필 사진 URL 업데이트

클라우드 기반 구축에서 Cisco Webex은(는) 사용자를 추가하거나 가져올 때 프로파일 사진에 고유한 URL을 할당합니다. Cisco Jabber에서 연락처 정보를 확인하면, 사진이 호스팅되는 URL의 Cisco Webex에서 프로파일 사진을 검색합니다.

프로파일 사진 URL은 HTTP 보안(`https://server_name/`)을 사용하며 클라이언트에 인증서를 제공 합니다. URL의 서버 이름이 다음과 같다면:

- Cisco Webex 도메인을 포함 하는 FQDN(정규화된 도메인 이름) - 클라이언트는 Cisco Webex 인증서에 프로파일 사진을 호스팅하는 웹 서버를 확인할 수 있습니다.
- IP 주소 - 클라이언트는 Cisco Webex 인증서에 프로파일 사진을 호스팅하는 웹 서버를 확인할 수 없습니다. 이 경우 클라이언트는 사용자에게 프로파일 사진 URL의 IP 주소를 사용하여 연락처를 조회할 때마다 인증서를 수락하도록 요청합니다.

중요

- IP 주소이 서버 이름으로 포함된 모든 프로파일 사진 URL을 업데이트하는 것이 좋습니다. IP 주소를 Cisco Webex 도메인이 포함된 FQDN으로 대체하여 클라이언트가 사용자에게 인증서를 수락하라는 메시지를 표시하지 않게 합니다.
- 사진을 업데이트하면, 클라이언트에서 사진을 갱신하는 데 최대 24시간이 걸립니다.

다음 단계에서는 프로파일 사진 URL을 업데이트하는 방법을 설명합니다. 자세한 내용은 Cisco Webex 설명서를 참조하십시오.

프로시저

단계 **1** Cisco Webex 관리 도구를 사용하여 CSV 파일 형식으로 사용자 연락처 데이터를 내보냅니다.

단계 **2** **UserProfilePhotoURL** 필드에서 IP 주소를 Cisco Webex 도메인으로 대체합니다.

단계 **3** CSV 파일을 저장합니다.

단계 **4** Cisco Webex 관리 도구를 사용하여 CSV 파일을 가져옵니다.

12 장

클라이언트 구성

클라이언트 구성 워크플로

프로시저

	명령 또는 동작	목적
단계 **1**	클라이언트 구성 소개	
단계 **2**	*Unified CM*에서 클라이언트 구성 매개 변수 설정(최고 우선순위) 또는 클라이언트 구성 파일 생성 및 호스팅	
단계 **3**	데스크톱 클라이언트용 전화기 구성에서 매개변수 설정	
단계 **4**	모바일 클라이언트용 전화기 구성에서 매개변수 설정	
단계 **5**	프록시 설정 구성-선택 사항	

클라이언트 구성 소개

Cisco Jabber를 이용하면 다음 소스에서 구성 설정을 검색할 수 있습니다.

- 클라이언트 구성 - 사용자가 로그인할 때 적용되는 클라이언트 구성 매개변수를 다음 중 하나로 설정할 수 있습니다.
  - Unified CM에서 클라이언트 구성 매개변수를 설정합니다.
  - 구성 매개변수를 포함하는 XML 편집기를 사용하여 XML 파일을 만듭니다. 그런 다음 TFTP 서버에서 XML 파일을 호스팅합니다.
- Cisco Webex 관리 도구 - Cisco Webex 관리 도구를 이용해 일부 클라이언트 설정을 구성할 수 있습니다.

  `jabber-config.xml` 클라이언트 구성 파일을 Cisco Webex 관리 도구에 업로드할 수 있습니다. Cisco Webex Messenger 관리 도구에서 그룹에 대해 별도의 구성 파일을 적용할 수 있습니다. 클라이언트가 Cisco Webex Messenger에 연결되면 XML 파일을 다운로드하고 구성을 적용합니다.

  클라이언트는 구성 설정을 다음 순서를 사용합니다.

  1. Cisco Webex Messenger 관리 도구의 설정
  2. Cisco Webex Messenger 관리 도구에 있는 `jabber-config.xml` 파일의 설정

     참고 그룹 구성 파일 설정은 Cisco Webex Messenger 관리 도구의 구성 파일보다 우선합니다.

  3. TFTP 서버에서 `jabber-config.xml` 파일의 설정.

  구성 설정에 상충되는 부분이 있다면, Cisco Webex 관리 도구의 설정이 이 구성 파일보다 우선합니다.

Unified CM에서 클라이언트 구성 매개변수 설정

클라우드 기반 구축의 경우에는 Cisco Webex 관리 도구를 사용하여 클라이언트를 구성합니다. 그러나 Cisco Webex 관리 도구에서 사용할 수 없는 설정으로 클라이언트를 구성하도록 클라이언트 구성 매개변수를 설정할 수도 있습니다.

iPhone 및 iPad용 Cisco Jabber와 Android용 Cisco Jabber의 경우에는 다음에 대한 매개변수를 설정해야 합니다.

- 온프레미스 구축을 위한 디렉터리 통합.
- 하이브리드 클라우드 구축에 대한 음성 메일 서비스 자격 증명.

참고 대부분의 환경에서 Windows용 Cisco Jabber 및 Mac용 Cisco Jabber는 서비스 연결을 위한 구성을 요구하지 않습니다. 자동 업데이트, 문제 보고 또는 사용자 정책 및 옵션 같은 사용자 지정 콘텐츠가 필요한 경우에만 클라이언트 구성 매개변수를 설정합니다.

프로시저

단계 1 Jabber 구성 매개변수 정의, 61 페이지

단계 2 서비스 프로파일에 Jabber 클라이언트 구성 할당, 61 페이지

Jabber 구성 매개변수 정의

Unified CM을 사용하면 Jabber 클라이언트 구성을 포함하여 UC 서비스에 대한 정보를 추가, 검색, 표시 및 유지 관리할 수 있습니다.

프로시저

단계 1 **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 2 사용자 관리 > 사용자 설정 > **UC** 서비스를 선택합니다.

단계 3 새로 추가를 선택합니다.

단계 4 **Jabber** 클라이언트 구성**(jabber-config.xml)**을 **UC** 서비스 유형으로 선택합니다.

단계 5 다음을 선택합니다.

단계 6 **UC** 서비스 정보 섹션에 이름을 입력하고 추가 요구 사항은 Unified CM 도움말을 참조합니다.

단계 7 **Jabber** 구성 매개변수 섹션에 매개변수를 입력합니다. 매개변수에 대한 정보는 *Cisco Jabber* 매개변수 참조 설명서 최신 버전을 참조하십시오.

단계 8 저장을 선택합니다.

서비스 프로파일에 Jabber 클라이언트 구성 할당

Unified CM을 사용하면 서비스 프로파일을 통해 사용자에게 Jabber 클라이언트 구성을 할당할 수 있습니다.

프로시저

단계 1 **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 2 사용자 관리 > 사용자 설정 > 서비스 프로파일을 선택합니다.

단계 3 새로 추가를 선택하거나 Jabber 클라이언트 구성을 할당할 기존 서비스 프로파일을 선택합니다.

단계 4 **Jabber** 클라이언트 구성**(jabber-config.xml)** 프로파일 섹션에서 프로파일에 적용할 구성의 이름을 선택합니다.

단계 5 저장을 선택합니다.

클라이언트 구성 파일 생성 및 호스팅

Cisco Webex 관리 도구를 사용하여 클라이언트를 구성합니다. 그러나 Cisco Webex 관리 도구에서 사용할 수 없는 설정으로 클라이언트를 구성하도록 TFTP 서버를 설정할 수도 있습니다.

iPhone 및 iPad용 Cisco Jabber와 Android용 Cisco Jabber의 경우에는, 설정할 전역 구성 파일을 생성해야 합니다.

- 온프레미스 구축을 위한 디렉터리 통합.
- 하이브리드 클라우드 구축에 대한 음성 메일 서비스 자격 증명.

참고 대부분의 환경에서 Windows용 Cisco Jabber 및 Mac용 Cisco Jabber는 서비스 연결을 위한 구성을 요구하지 않습니다. 자동 업데이트, 문제 보고 또는 사용자 정책 및 옵션 같은 사용자 지정 콘텐츠가 필요한 경우에만 구성 파일을 생성합니다.

시작하기 전에

다음 구성 파일 요구 사항을 확인하십시오.

- 구성 파일명은 대소문자를 구분합니다. 파일명에 소문자를 사용해야 오류를 방지하고 클라이언트가 TFTP 서버에서 파일을 검색할 수 있습니다.
- 구성 파일에는 UTF-8 인코딩을 사용합니다.
- 클라이언트는 유효한 XML 구조가 없는 구성 파일은 읽지 못합니다. 요소 닫기 및 올바른 요소 중첩에 대한 구성 파일의 구조를 확인하십시오.
- 구성 파일에서 유효한 XML 문자 엔터티 참조만 사용해야 합니다. 예를 들어 & 대신 &를 사용합니다. XML에 잘못된 문자가 포함되어 있다면 클라이언트는 구성 파일을 구문 분석하지 못합니다.

  구성 파일을 확인하려면 Microsoft Internet Explorer에서 파일을 엽니다.

  - Internet Explorer에 전체 XML 구조가 표시된다면, 구성 파일이 유효하다는 뜻입니다.
  - Internet Explorer에 XML 구조의 일부만 표시된다면, 구성 파일에 잘못된 문자나 엔티티가 있을 가능성이 큽니다.

프로시저

	명령 또는 동작	목적
단계 **1**	TFTP 서버 주소 지정, 63 페이지	클라이언트에서 구성 파일에 대한 액세스를 활성화하는 TFTP 서버 주소를 지정합니다.

	명령 또는 동작	목적
단계 2	전역 구성 만들기, 64 페이지	구축에 존재하는 사용자에 대한 클라이언트를 구성합니다.
단계 3	그룹 구성 만들기, 64 페이지	서로 다른 사용자 집합에 서로 다른 구성을 적용합니다.
단계 4	구성 파일 호스팅, 65 페이지	아무 TFTP 서버에서 구성 파일을 호스팅합니다.
단계 5	TFTP 서버 다시 시작하기, 66 페이지	TFTP 서버를 재시작해야 클라이언트가 구성 파일에 액세스할 수 있습니다.

TFTP 서버 주소 지정

클라이언트는 TFTP 서버에서 구성 파일을 가져옵니다.

프로시저

	명령 또는 동작	목적
단계 1	클라이언트가 구성 파일에 액세스할 수 있도록 TFTP 서버 주소를 지정합니다.	주의 ICisco Jabber가 DNS 쿼리에서 `_cisco-uds` SRV 레코드를 가져온다면, 사용자의 홈 클러스터를 자동으로 찾을 수 있습니다. 따라서 클라이언트는 Cisco Unified Communications Manager TFTP 서비스도 찾을 수 있습니다. `_cisco-uds` SRV 레코드를 구축한다면 TFTP 서버 주소를 지정하지 않아도 됩니다.

전화 모드에서 TFTP 서버 지정

프로시저

	명령 또는 동작	목적
단계 1	클라이언트를 전화기 모드로 구축한다면, TFTP 서버의 주소를 다음과 같이 입력할 수 있습니다. • 사용자는 클라이언트를 시작할 때 TFTP 서버 주소를 수동으로 입력합니다.	

	명령 또는 동작	목적
	• Tftp 인수를 사용하여 설치하는 동안 TFTP 서버 주소를 지정합니다.	

전역 구성 만들기

클라이언트는 로그인 순서대로 TFTP 서버에서 전역 구성 파일을 다운로드합니다. 구축에 존재하는 모든 사용자에 대한 클라이언트를 구성합니다.

시작하기 전에

구성 파일의 구조가 유효하지 않으면 클라이언트는 사용자가 설정한 값을 읽을 수 없습니다. 자세한 내용은 이 장의 XML 샘플을 참조하십시오.

프로시저

단계 **1** 아무 텍스트 편집기를 이용해 `jabber-config.xml`이라는 파일을 생성합니다.

- 파일 이름에는 소문자를 사용합니다.
- UTF-8 인코딩을 사용합니다.

단계 **2** `jabber-config.xml`의 필수 구성 매개변수를 정의합니다.

단계 **3** TFTP 서버에서 그룹 구성 파일을 호스팅합니다.

환경에 여러 TFTP 서버가 있다면, 모든 TFTP 서버에서 구성 파일이 동일한지 확인하십시오.

그룹 구성 만들기

그룹 구성 파일은 사용자의 하위 집합에 적용되며 데스크톱용 Cisco Jabber(CSF 장치) 및 모바일 장치용 Cisco Jabber에서 지원됩니다. 그룹 구성 파일은 전역 구성 파일에 우선합니다.

CSF 장치를 사용하여 사용자를 프로비저닝한다면, 장치 구성의 **Cisco** 지원 필드 필드에 그룹 구성 파일명을 지정합니다. 사용자에게 CSF 장치가 없다면, TFTP_FILE_NAME 인수를 사용하여 설치하는 동안 각 그룹에 고유한 구성 파일명을 설정합니다.

시작하기 전에

구성 파일의 구조가 유효하지 않으면 클라이언트는 사용자가 설정한 값을 읽을 수 없습니다. 자세한 내용은 이 장의 XML 샘플을 참조하십시오.

프로시저

단계 **1** 텍스트 편집기를 사용하여 XML 그룹 구성 파일을 작성합니다.

그룹 구성 파일에는 `jabber-groupa-config.xml` 같은 적절한 이름을 지정합니다.

단계 **2** 그룹 구성 파일의 필수 구성 매개변수를 정의합니다.

단계 **3** 적용 가능한 CSF 장치에 그룹 구성 파일을 추가합니다.

a) **Cisco Unified CM** 관리 인터페이스를 엽니다.

b) 장치 > 전화기를 선택합니다.

c) 그룹 구성이 적용되는 적절한 CSF 장치를 찾아 선택합니다.

d) 전화기 구성 창에서 제품별 구성 레이아웃 > 데스크톱 클라이언트 설정으로 이동합니다.

e) **Cisco** 지원 필드 필드에 `configurationfile=group_configuration_file_name.xml`을 입력합니다. 예: `configurationfile=groupa-config.xml`을 입력합니다.

참고 기본 디렉터리가 아닌 곳에 있는 TFTP 서버에서 그룹 구성 파일을 호스트한다면, 경로와 파일명을 지정해야 합니다(예: `configurationfile =/Customfolder/groupa-config`).

그룹 구성 파일을 2개 이상 추가하지 마십시오. 클라이언트는 **Cisco** 지원 필드 필드의 첫 번째 그룹 구성만 사용합니다.

f) 저장을 선택합니다.

단계 **4** TFTP 서버에서 그룹 구성 파일을 호스팅합니다.

구성 파일 호스팅

아무 TFTP 서버에서 구성 파일을 호스팅할 수 있습니다. 하지만 장치 구성 파일이 존재하는 Cisco Unified Communications Manager TFTP 서버에서 구성 파일을 호스팅하는 것이 좋습니다.

프로시저

단계 **1** Cisco Unified Communications Manager에서 **Cisco Unified OS** 관리 인터페이스를 엽니다.

단계 **2** 소프트웨어 업그레이드 > **TFTP** 파일 관리를 선택합니다.

단계 **3** 파일 업로드를 선택합니다.

단계 **4** 파일 업로드 섹션에서 찾아보기를 선택합니다.

단계 **5** 파일 시스템에서 구성 파일을 선택합니다.

단계 **6** 파일 업로드 섹션의 디렉터리 텍스트 상자에는 값을 지정하지 마십시오.

구성 파일이 TFTP 서버의 기본 디렉터리에 상주할 수 있도록 디렉터리 텍스트 상자는 값을 입력하지 않아야 합니다.

단계 **7** 파일 업로드를 선택합니다.

TFTP 서버 다시 시작하기

TFTP 서버를 재시작해야 클라이언트가 구성 파일에 액세스할 수 있습니다.

프로시저

단계 **1** Cisco Unified Communications Manager에서 **Cisco Unified** 서비스 가용성 인터페이스를 엽니다.

단계 **2** 도구 > 제어 센터 - 기능 서비스를 선택합니다.

단계 **3** **CM** 서비스 섹션에서 **Cisco Tftp**를 선택합니다.

단계 **4** 재시작을 선택합니다.

재시작 여부를 확인하는 메시지가 표시됩니다.

단계 **5** 확인을 선택합니다.

Cisco Tftp 서비스 재시작 작업 성공 상태가 표시됩니다.

단계 **6** 새로고침을 선택해 **Cisco Tftp** 서비스가 제대로 시작되게 합니다.

다음에 수행할 작업

TFTP 서버에서 구성 파일을 사용할 수 있는지 확인하려면 아무 브라우저에서 구성 파일을 엽니다. 일반적으로 다음 URL ○에서 전역 구성 파일에 액세스할 수 있습니다.
`http://tftp_server_address:6970/jabber-config.xml`

컨피그레이션 파일

jabber-config.xml 구성 파일 구조, 그룹 요소, 매개변수에 대한 자세한 내용 및 예시는 Cisco Jabber용 매개변수 참조 설명서를 참고하십시오.

데스크톱 클라이언트용 전화기 구성에서 매개변수 설정

클라이언트는 Cisco Unified Communications Manager의 다음 위치에서 전화기 구성의 구성 설정을 검색할 수 있습니다.

엔터프라이즈 전화기 구성

전체 클러스터에 적용됩니다.

참고 IM 및 프레즌스 서비스 기능이 있는 사용자의 경우(IM 전용), 엔터프라이즈 전화기 구성 창에서 전화기 구성 매개변수를 설정해야 합니다.

일반 전화 프로파일 구성

장치 그룹에 적용되며 클러스터 구성보다 우선합니다.

Cisco Unified 클라이언트 서비스 프레임워크**(CSF)** 전화기 구성

개별 CSF 데스크톱 장치에 적용되며 그룹 구성보다 우선합니다.

전화기 구성의 매개변수

다음 표에는 전화기 구성의 제품별 구성 레이아웃 섹션에서 설정할 수 있는 구성 매개변수와 클라이언트 구성 파일의 매개변수에 대응하는 지도가 나와 있습니다.

데스크톱 클라이언트 설정 구성	설명
화상 통화	비디오 기능을 활성화하거나 비활성화합니다. 활성화됨**(**기본값**)** 사용자가 영상 통화를 걸고 받을 수 있습니다. 비활성화됨 사용자가 영상 통화를 걸거나 받을 수 없습니다. 제한 이 매개변수는 CSF 장치 구성에서만 사용할 수 있습니다.
파일 전송에서 차단할 파일 형식	사용자가 특정 파일 형식을 전송하지 못하도록 제한합니다. 파일 확장명을 값으로 설정합니다(예: `.exe`). 세미콜론을 사용하여 여러 값을 구분합니다. 예를 들면 다음과 같습니다. `.exe;.msi;.rar;.zip`
전화기 제어에서 자동으로 시작	클라이언트가 처음으로 시작될 때 사용자의 전화기 유형을 설정합니다. 사용자는 최초 시작 후에 전화기 유형을 변경할 수 있습니다. 그러면 클라이언트는 사용자 환경 설정을 저장하고, 이후 시작에서 이 설정을 사용합니다. 활성화됨 통화에 사무실 전화기를 사용합니다. 비활성화됨**(**기본값**)** 통화 소프트웨어 전화기(CSF) 장치를 사용합니다.

데스크톱 클라이언트 설정 구성	설명
Windows용 **Jabber** 소프트웨어 업데이트 서버 **URL**	클라이언트 업데이트 정보를 보유하는 XML 파일에 대한 URL을 지정합니다. 클라이언트는 이 URL을 사용하여 웹 서버에서 XML 파일을 검색합니다. 하이브리드 클라우드 기반 구축에서는 Cisco Webex관리 도구를 사용하여 자동 업데이트를 구성해야 합니다.
문제 보고서 서버 **URL**	사용자가 문제 보고서를 제출할 수 있는 사용자 정의 스크립트에 대한 URL을 지정합니다.

모바일 클라이언트용 전화기 구성에서 매개변수 설정

클라이언트는 Cisco Unified Communications Manager의 다음 위치에서 전화기 구성의 구성 설정을 검색할 수 있습니다.

- iPhone용 Cisco 듀얼 모드(TCT) 구성 - 개별 TCT 장치에 적용되면 그룹 구성보다 우선합니다.
- 태블릿용 Cisco Jabber(TAB) 구성 - 개별 TAB 장치에 적용되면 그룹 구성보다 우선합니다.

전화기 구성의 매개변수

다음 표에는 전화기 구성의 제품별 구성 레이아웃 섹션에서 설정할 수 있는 구성 매개변수와 클라이언트 구성 파일의 매개변수에 대응하는 지도가 나와 있습니다.

매개 변수	설명
온디맨드 VPN URL	온디맨드 VPN을 시작하는 URL입니다. 참고 IOS에만 해당됩니다.
미리 설정된 Wi-fi 네트워크	조직에서 승인한 Wi-Fi 네트워크의 SSID(SSID)를 입력합니다. SSID를 슬래시(/)로 구분합니다. 입력한 Wi-Fi 네트워크 중 하나에 연결된 장치는 보안 연결에 연결되지 않습니다.
기본 벨소리	기본 벨소리를 정상 또는 크게로 설정합니다.
비디오 기능	비디오 기능을 활성화하거나 비활성화합니다. • 활성화됨(기본값) - 사용자가 영상 통화를 걸고 받을 수 있습니다. • 비활성화됨 - 사용자가 영상 통화를 보내거나 받을 수 없습니다.

매개 변수	설명
DVO(Dial via Office) 참고 TCT 및 BOT 장치에만 해당됩니다.	DVO(Dial via Office)를 통해 다이얼을 활성화하거나 비활성화합니다. • 활성화됨 - 사용자가 DVO(Dial via Office)를 사용할 수 있습니다. • 비활성화됨(기본값) - 사용자가 DVO(Dial via Office)를 사용할 수 없습니다.

프록시 설정 구성 옵션

클라이언트에서 프록시 설정을 사용하여 서비스에 연결할 수 있습니다.

이러한 HTTP 요청에 대해 프록시를 사용하면, 다음과 같은 제한 사항이 적용됩니다.

- 프록시 인증은 지원되지 않습니다.
- 우회 목록의 와일드 카드가 지원됩니다.
- Cisco Jabber는 HTTP 연결을 사용하는 HTTP 요청에 대해서는 프록시를 지원하지만, HTTPS 연결을 사용하는 경우에는 프록시를 지원하지 않습니다.
- WAPD(Web Proxy Auto Discovery)는 지원되지 않으므로 비활성화해야 합니다.

필요한 경우, 클라이언트 유형에 대한 단계를 수행하여 프록시 설정을 구성하십시오.

Windows용 Cisco Jabber의 프록시 설정 구성

인터넷 속성에 대한 LAN(Local Area Network) 설정에서 Windows 프록시 설정을 구성합니다.

프로시저

단계 **1** 연결 탭에서 **LAN** 설정을 선택합니다.

단계 **2** 다음 옵션 중 하나를 사용하여 프록시를 구성합니다.

- 자동 구성의 경우에는 `.pac` 파일 URL을 지정합니다.
- 프록시 서버의 경우에는 명시적인 프록시 주소를 지정합니다.

Mac용 Cisco Jabber의 프록시 설정 구성

시스템 기본 설정에서 Mac에 대한 프록시 설정을 구성합니다.

프로시저

단계 **1** 시스템 기본 설정 > 네트워크를 선택합니다.

단계 **2** 목록에서 네트워크 서비스를 선택하고 고급 > 프록시를 선택합니다.

단계 **3** 다음 옵션 중 하나를 사용하여 프록시를 구성합니다.

- 자동 구성의 경우에는 .pac 파일 URL을 지정합니다.
- 프록시 서버의 경우에는 명시적인 프록시 주소를 지정합니다.

iPhone 및 iPad용 Cisco Jabber의 프록시 설정 구성

다음 방법 중 하나를 사용하여 iOS 장치의 Wi-Fi 설정에서 프록시 설정을 구성합니다.

프로시저

단계 **1** **Wi-Fi** > **HTTP** 프록시 > 자동을 선택하고 .pac 파일 URL을 자동 구성 스크립트로 지정합니다.

단계 **2** **Wi-Fi** > **HTTP** 프록시 > 설명서를 선택하고 명시적인 프록시 주소를 지정합니다.

Android용 Cisco Jabber의 프록시 설정 구성

프로시저

다음 방법 중 하나를 사용하여 Android 장치의 Wi-Fi 설정에서 프록시 설정을 구성합니다.

- **Wi-Fi** > 네트워크 수정 > 고급 옵션 표시 > 프록시 설정 > 자동 탭에서 .pac 파일 URL을 자동 구성 스크립트로 지정합니다.

  참고 이 방법은 Android OS 5.0 이상인 장치와 Cisco DX 시리즈 장치에서만 지원 됩니다.

- **Wi-Fi** 네트워크 > 네트워크 수정 > 고급 옵션 표시 > 프록시 설정 > 자동 탭에 명시적인 프록시 주소를 지정합니다.

13 장

VDI용 Cisco Jabber 애플리케이션 및 Jabber 소프트폰 구축

액세서리 관리자

액세서리 관리자

Jabber 데스크톱 클라이언트는 액세서리 관리자를 사용하여 헤드셋과 같은 액세서리와의 상호 작용을 활성화합니다. 액세서리 관리자는 액세서리 장치 공급업체에 유니파이드 커뮤니케이션 제어 API를 제공하는 구성 요소입니다.

일부 Cisco 헤드셋 및 타사 장치에서는 이 API를 사용하여 오디오 음소거, 통화 응답, 장치에서 통화 종료를 수행합니다. 타사 공급업체는 애플리케이션에서 로드하는 플러그인을 작성합니다. 표준 헤드셋은 API를 사용하여 스피커 및 마이크 지원과 연결합니다.

특정 장치만 통화 제어를 위해 액세서리 관리자와 상호 작용합니다. 자세한 내용은 장치 공급업체에 문의하십시오. 액세서리 관리자는 데스크톱 전화기는 지원하지 않습니다.

액세서리 관리자 기능은 기본적으로 활성화되어 있고 EnableAccessoriesManager 매개변수를 사용하여 구성됩니다. BlockAccessoriesManager 매개변수를 사용하여 타사 공급업체의 특정 액세서리 관리자 플러그인을 비활성화할 수 있습니다.

참고 `jabber-config.xml`에서 EnableAccessoriesManager를 false로 설정하면 일부 헤드셋의 통화 제어 버튼이 작동하지 않습니다.

클라이언트 설치 프로그램에는 공급업체의 타사 플러그인이 포함되어 있습니다. 이 플러그인은 `/Library/Cisco/Jabber/Accessories/` 폴더에 설치됩니다.

지원되는 타사 공급업체:

- Logitech
- Sennheiser
- Jabra
- Plantronics

Cisco Jabber 클라이언트 다운로드

필요하다면 클라이언트의 운영체제에서 서명 도구를 사용하여 자체 고객 서명을 Jabber 설치 프로그램이나 Cisco 동적 라이브러리에 추가할 수 있습니다.

참고 Mac용 Cisco Jabber의 경우 설치 프로그램에 제품 설치 프로그램 파일이 포함됩니다. 터미널 도구를 사용하여 설치 프로그램에서 `pkg` 파일을 추출하고 `pkg` 파일에 서명한 다음 설치 프로그램에 추가해야 합니다.

프로시저

적용 가능한 소스에서 클라이언트를 다운로드합니다.

- Cisco 소프트웨어 센터에서 Mac용 Cisco Jabber 및 Windows용 Cisco Jabber 클라이언트를 다운로드합니다.
- Android용 Cisco Jabber의 경우에는 Google Play에서 앱을 다운로드하십시오.
- iPhone 및 iPad용 Cisco Jabber의 경우에는 앱 스토어에서 앱을 다운로드하십시오.

Windows용 Cisco Jabber 설치

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

설치 옵션	설명
명령줄 사용, 73 페이지	명령줄 창에서 인수를 지정하여 설치 속성을 설정할 수 있습니다. 여러 인스턴스를 설치할 계획이라면 이 옵션을 선택합니다.

설치 옵션	설명
MSI를 수동으로 실행, 92 페이지	클라이언트 워크스테이션의 파일 시스템에서 수동으로 MSI를 실행한 다음 클라이언트를 시작할 때 연결 속성을 지정합니다. 테스트 또는 평가 목적으로 단일 인스턴스를 설치할 계획이라면 이 옵션을 선택합니다.
사용자 정의 설치 프로그램 생성, 93 페이지	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 정책을 사용하여 구축, 97 페이지	동일한 도메인에 있는 여러 컴퓨터에 클라이언트를 설치합니다.

시작하기 전에

로컬 관리자 권한을 사용하여 로그인해야 합니다.

명령줄 사용

명령줄 창에서 설치 인수를 지정합니다.

프로시저

단계 **1** 명령줄 창을 엽니다.

단계 **2** 다음의 명령을 입력합니다.

```
msiexec.exe /i CiscoJabberSetup.msi
```

단계 **3** 명령줄 인수를 매개변수=값 쌍으로 지정합니다.

```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

단계 **4** 명령을 실행하여 Windows용 Cisco Jabber를 설치합니다.

설치 명령의 예

Windows용 Cisco Jabber 설치에 대한 명령 예를 검토합니다.

Cisco Unified Communications Manager, 릴리스 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

여기서:

CLEAR=1 - 기존 부트스트랩 파일을 삭제합니다.
`/quiet` - 자동 설치를 지정합니다.

관련 항목

명령줄 인수, 74 페이지
언어에 대한 LCID, 90 페이지

명령줄 인수

Windows용 Cisco Jabber를 설치할 때 지정할 수 있는 명령줄 인수를 검토합니다.

관련 항목

설치 명령의 예, 73 페이지
언어에 대한 LCID, 90 페이지

재정의 인수

다음 표에서는 이전 설치에서 기존 부트스트랩 파일을 재정의하기 위해 지정해야 하는 매개변수를 설명합니다.

인수	값	설명
지우기	1	클라이언트가 이전 설치의 기존 부트스트랩 파일을 재정의할지 여부를 지정합니다. 클라이언트는 설치 중에 설정하는 인수와 값을 부트스트랩 파일에 저장합니다. 이후 클라이언트는 시작 시에 부트스트랩 파일에서 설정을 로드합니다.

CLEAR를 지정하면, 설치 중에 다음 작업이 진행됩니다.

1. 클라이언트가 기존 부트스트랩 파일을 삭제합니다.
2. 클라이언트가 새 부트스트랩 파일을 생성합니다.

CLEAR를 지정하지 않으면, 클라이언트는 설치 중에 기존 부트스트랩 파일을 확인합니다.

- 부트스트랩 파일이 없는 경우, 클라이언트는 설치 중에 부트스트랩 파일을 생성합니다.
- 부트스트랩 파일이 있는 경우, 클라이언트는 해당 부트스트랩 파일을 재정의하지 않고 기존 설정을 유지합니다.

참고 Windows용 Cisco Jabber를 다시 설치한다면 다음 사항을 고려해야 합니다.

- 클라이언트는 기존 부트스트랩 파일의 설정을 유지하지 않습니다. CLEAR를 지정한다면, 다른 설치 인수도 적절하게 지정해야 합니다.
- 클라이언트는 설치 인수를 기존 부트스트랩 파일에 저장하지 않습니다. 설치 인수의 값을 변경하거나 추가 설치 인수를 지정하려면, CLEAR를 지정하여 기존 설정을 무시해야 합니다.

기존 부트스트랩 파일을 무시하려면 다음과 같이 명령줄에 CLEAR를 지정합니다.

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

모드 유형 인수

다음 표에서는 제품 모드를 지정하는 명령줄 인수를 설명합니다.

인수	값	설명
PRODUCT_MODE	Phone_Mode	클라이언트에 대한 제품 모드를 지정합니다. 다음 값을 설정할 수 있습니다. • Phone_Mode - Cisco Unified Communications Manager가 인증자입니다. 오디오 장치를 기본 기능으로 사용하여 사용자를 프로비저닝하려면 이 값을 선택합니다.

제품 모드를 설정해야 할 시점

전화기 모드 구축에서는 Cisco Unified Communications Manager가 인증자입니다. 인증자를 받으면, 클라이언트는 제품 모드가 전화기 모드인지 확인합니다. 그러나 클라이언트는 최초 시작 시에는 항상 기본 제품 모드에서 시작하기 때문에, 사용자는 로그인한 후 전화 모드에 들어가려면 클라이언트를 다시 시작해야 합니다.

참고 Cisco Unified Communications Manager, 릴리스 9.x 이상 - 설치 중에 PRODUCT_MODE를 설정하면 안 됩니다. 클라이언트는 서비스 프로파일에서 인증자를 가져옵니다. 사용자가 로그인하면, 클라이언트를 다시 시작 해야 전화기 모드에 들어갈 수 있습니다.

제품 모드 변경

제품 모드를 변경하려면 클라이언트에 대한 인증자를 변경해야 합니다. 그러면 클라이언트가 인증자에서 제품 모드를 결정할 수 있습니다.

설치 후에 제품 모드를 다른 제품 모드로 변경하는 방법은 구축에 따라 다릅니다.

참고 모든 구축에서, 사용자는 고급 설정 창에서 인증자를 수동으로 설정할 수 있습니다.

이 경우에는 사용자에게 제품 모드를 변경하려면 고급 설정 창에서 인증자를 변경해야 한다고 지시해야 합니다. 클라이언트를 제거한 다음 다시 설치해도 수동 설정은 무시할 수 없습니다.

Cisco Unified Communications Manager 버전 9.x에서 제품 모드 변경

Cisco Unified Communications Manager 버전 9.x 이상에서 제품 모드를 변경하려면, 서비스 프로파일에서 인증자를 변경해야 합니다.

프로시저

단계 **1** 관련 사용자의 서비스 프로파일에서 인증자를 변경합니다.

기본 모드 > 전화기 모드 변경

IM 및 프레즌스 서비스를 사용하여 사용자를 프로비저닝하면 안 됩니다.

서비스 프로파일에 IM 및 프레즌스 서비스 구성이 없다면, 인증자는 Cisco Unified Communications Manager가 됩니다.

전화기 모드 > 기본 모드 변경

IM 및 프레즌스 서비스를 사용하여 사용자를 프로비저닝합니다.

IM 및 프레즌스 프로파일에서 제품 유형 필드 값을 다음으로 설정하는 경우:

- **Unified CM(IM** 및 프레즌스**)** Cisco Unified Communications Manager IM and Presence Service 인증자가 됩니다.
- Webex**(IM** 및 프레즌스**)** Cisco Webex Messenger 서비스가 인증자입니다.

단계 **2** 사용자에게 로그아웃한 다음 다시 로그인하라고 지시합니다.

사용자가 클라이언트에 로그인하면 서비스 프로파일의 변경 사항을 검색하고 사용자를 인증자에 로그인합니다. 그러면 클라이언트는 제품 모드를 결정하고 사용자에 게 클라이언트를 다시 시작하라는 메시지를 표시합니다.

사용자가 클라이언트를 다시 시작하면 제품 모드 변경이 완료됩니다.

인증 인수

다음 표에서는 인증 소스를 지정 하기 위해 설정할 수 있는 명령줄 인수에 대해 설명 합니다.

인수	값	설명
인증자	Webex	클라이언트에 대한 인증 소스를 지정합니다. 이 값은 서비스 검색에 실패할 때 사용합니다. 다음 값으로 설정합니다. • Webex—Cisco Webex Messenger 서비스 클라우드 기반 또는 하이브리드 클라우드 기반 구축
CUP_ADDRESS	IP 주소 호스트 이름 FQDN	Cisco Unified Communications Manager IM and Presence Service의 주소를 지정합니다. 다음 중 하나를 값으로 설정합니다. • 호스트 이름(호스트 이름) • IP 주소(*123.45.254.1*) • FQDN(*hostname.domain.com*)
TFTP	IP 주소 호스트 이름 FQDN	TFTP 서버의 주소를 지정합니다. 다음 중 하나를 값으로 설정합니다. • 호스트 이름(호스트 이름) • IP 주소(*123.45.254.1*) • FQDN(*hostname.domain.com*) Cisco Unified Communications Manager를 인증자로 설정한 경우, 이 인수를 지정해야 합니다. 구축 하는 경우: • 전화 모드 - 클라이언트 구성을 호스팅하는 TFTP 서버의 주소를 지정해야 합니다. • 기본 모드 - 장치 구성을 호스팅하는 Cisco Unified Communications Manager TFTP 서비스의 주소를 지정할 수 있습니다.
CTI	IP 주소 호스트 이름 FQDN	CTI 서버의 주소를 설정합니다. 다음과 같은 경우 이 인수를 지정합니다. • Cisco Unified Communications Manager를 인증자로 설정합니다. • 사용자에게 사무실 전화기 장치가 있으며 CTI 서버가 필요합니다.

인수	값	설명
CCMCIP	IP 주소 호스트 이름 FQDN	CCMCIP 서버의 주소를 설정합니다. 다음과 같은 경우 이 인수를 지정합니다. • Cisco Unified Communications Manager를 인증자로 설정합니다. • CCMCIP 서버의 주소는 TFTP 서버 주소와 동일하지 않습니다. 두 주소가 동일한 경우 클라이언트는 TFTP 서버 주소로 CCMCIP 서버를 찾을 수 있습니다.
SERVICES_DOMAIN	도메인	서비스 검색에 대한 DNS SRV 레코드가 상주하는 도메인의 값을 설정합니다. 클라이언트가 이 정보에 대한 설치 프로그램 설정 또는 수동 구성을 사용하도록 하려면 이 인수를 DNS SRV 레코드가 상주하지 않는 도메인으로 설정할 수 있습니다. 이 인수가 지정되어 있지 않고 서비스 검색이 실패하는 경우, 사용자에게 서비스 도메인 정보를 요청하는 메시지가 표시됩니다.
VOICE_SERVICES_DOMAIN	도메인	하이브리드 구축에서는 CAS 조회를 통해 Webex을(를) 검색하는 데 필요한 도메인이 DNS 기록이 구축되는 도메인과 다를 수 있습니다. 이 경우에는 SERVICES_DOMAIN을 Webex 검색에 사용하는 도메인으로 설정하고(또는 사용자가 이메일 주소를 입력하게 하고) VOICE_SERVICES_DOMAIN을 DNS 기록이 구축되는 도메인으로 설정합니다. 이 설정을 지정하면 클라이언트는 VOICE_SERVICES_DOMAIN의 값을 사용하여 서비스 검색 및 에지 감지를 위해 다음 DNS 레코드를 조회합니다. • `_cisco-uds` • `_cuplogin` • `_collab-edge` 이 설정은 선택 사항이며 지정하지 않으면 SERVICES_DOMAIN에서 얻은 서비스 도메인, 사용자가 입력한 이메일 주소 또는 캐시된 사용자 구성에서 DNS 레코드가 쿼리됩니다.

인수	값	설명
EXCLUDED_SERVICES	다음 중 하나 이상: • Webex • CUCM	Jabber가 서비스 검색에서 제외하도록 할 서비스를 나열합니다. 예를 들어 Webex의 평가판을 사용해 보았고 회사 도메인이 Webex에 등록된 경우를 가정해 봅시다. 하지만 Jabber가 Webex이(가) 아닌 CUCM 서버를 인증하게 하고 싶다면 다음과 같이 설정하십시오. • EXCLUDED_SERVICES=WEBEX 가능한 값은 CUCM입니다. Webex 모든 서비스를 제외하는 경우, 수동 구성 또는 부트스트랩 구성을 사용하여 Jabber 클라이언트를 구성해야 합니다.
UPN_DISCOVERY_ENABLED	true false	클라이언트가 서비스를 검색할 때 Windows 세션의 UPN(User Principal Name)을 사용하여 사용자 ID와 사용자의 도메인을 가져올지 여부를 정의할 수 있습니다. • true(기본값) - UPN은 서비스 검색 중에 사용되는 사용자 ID와 사용자의 도메인을 찾는 데 사용합니다. UPN에서 검색한 사용자만 클라이언트에 로그인할 수 있습니다. • false - 사용자 ID와 사용자의 도메인을 찾는 데 UPN을 사용하지 않습니다. 서비스 검색을 위해 도메인을 찾는 데 필요한 자격 증명을 입력하라는 메시지가 사용자에게 표시됩니다. 설치 명령 예: `msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP 서버 주소

Windows용 Cisco Jabber는 TFTP 서버에서 다음과 같은 두 가지 구성 파일을 검색합니다.

- 사용자가 생성한 클라이언트 구성 파일.
- 장치를 사용하여 사용자를 프로비저닝할 때 Cisco Unified Communications Manager TFTP 서비스에 있던 장치 구성 파일.

작업을 최소화하려면 Cisco Unified Communications Manager TFTP 서비스에서 클라이언트 구성 파일을 호스팅해야 합니다. 그러면 모든 구성 파일에 대해 하나의 TFTP 서버 주소만 존재하게 되며, 필요에 따라 이 주소를 지정하면 됩니다.

하지만 장치 구성을 포함하는 TFTP 서버와 다른 서버에서 클라이언트 구성을 호스팅할 수도 있습니다. 이 경우 두 가지 TFTP 서버 주소가 존재하게 됩니다. 하나는 장치 구성을 호스팅하는 TFTP 서버용 주소이며, 다른 하나는 클라이언트 구성 파일을 호스팅하는 TFTP 서버용 주소입니다.

기본 구축

이 섹션에서는 프레즌스 서버가 있는 구축에서 두 가지 TFTP 서버 주소를 처리하는 방법을 설명합니다.

다음 작업을 수행해야 합니다.

1. 프레즌스 서버에서 클라이언트 구성을 호스팅하는 TFTP 서버의 주소를 지정합니다.
2. 설치하는 동안 TFTP 인수를 사용하여 Cisco Unified Communications Manager TFTP 서비스의 주소를 지정합니다.

클라이언트를 처음으로 시작하면 다음 작업이 수행됩니다.

1. 부트스트랩 파일에서 Cisco Unified Communications Manager TFTP 서비스의 주소를 검색합니다.
2. Cisco Unified Communications Manager TFTP 서비스에서 장치 구성을 가져옵니다.
3. 프레즌스 서버에 연결합니다.
4. 프레즌스 서버에서 클라이언트 구성을 호스팅하는 TFTP 서비스의 주소를 검색합니다.
5. TFTP 서버에서 클라이언트 구성을 가져옵니다.

전화기 모드 구축

이 섹션에서는 전화기 모드 구축에서 두 가지 TFTP 서버 주소를 처리하는 방법을 설명합니다.

다음 작업을 수행해야 합니다.

1. 설치하는 동안 TFTP 인수를 사용하여 클라이언트 구성을 호스팅하는 TFTP 서버의 주소를 지정합니다.
2. TftpServer1 매개변수를 사용하여 클라이언트 구성 파일에서 장치 구성을 호스팅하는 TFTP 서버의 주소를 지정합니다.
3. TFTP 서버에서 클라이언트 구성 파일을 호스팅합니다.

클라이언트를 처음으로 시작하면 다음 작업이 수행됩니다.

1. 부트스트랩 파일에서 TFTP 서버의 주소를 검색합니다.
2. TFTP 서버에서 클라이언트 구성을 가져옵니다.
3. 클라이언트 구성에서 Cisco Unified Communications Manager TFTP 서비스의 주소를 검색합니다.
4. Cisco Unified Communications Manager TFTP 서비스에서 장치 구성을 가져옵니다.

일반 설치 인수

다음 표에서는 몇 가지 일반적인 명령줄 인수에 대해 설명합니다.

인수	값	설명
AUTOMATIC_SIGN_IN	true false	사용자가 클라이언트를 설치할 때 **Cisco Jabber** 시작 시 로그인 확인란을 선택할지 여부를 지정합니다. • true - 사용자가 클라이언트를 설치할 때 **Cisco Jabber** 시작 시 로그인 확인란을 선택합니다. • false(기본값) - 사용자가 클라이언트를 설치할 때 **Cisco Jabber** 시작 시 로그인 확인란을 선택하지 않습니다.
CC_MODE	true false	Jabber를 Common Criteria 모드에서 실행할지 여부를 지정합니다. 기본값은 false입니다.
CLICK2X	DISABLE Click2Call	Cisco Jabber에서 Click-to-X 기능을 비활성화합니다. 설치 중에 이 인수를 지정하는 경우, 클라이언트는 운영 체제에서 Click-to-X 기능에 대한 처리기로 등록되지 않습니다. 이 인수로 인해 설치하는 동안 클라이언트가 Microsoft Windows 레지스트리에 쓰는 것이 방지됩니다. 설치 후 클라이언트에서 Click-to-X 기능을 활성화하려면 클라이언트를 다시 설치하고 이 인수를 생략해야 합니다. 브라우저의 **Click2Call** 함수 - 이제 새로 추가된 Click2Call 매개변수를 사용하여 Click2X 매개변수를 구성할 수 있습니다. 이렇게 하면 브라우저에서 클릭 투 콜(Click-to-call) 기능만 활성화되고 Click2X 기능은 비활성화됩니다.

인수	값	설명
DIAGNOSTICSTOOLENABLED	true false	Cisco Jabber 진단 도구를 Windows용 Cisco Jabber 사용자에게 제공할지 여부를 지정합니다. • true(기본값) - 사용자는 Ctrl + Shift + D를 입력하여 Cisco Jabber 진단 도구를 표시할 수 있습니다. • false - Cisco Jabber 진단 도구가 사용자에게 제공되지 않습니다.
ENABLE_DPI_AWARE	true false	DPI 인식을 활성화합니다. DPI 인식을 사용하면 Cisco Jabber가 다른 화면 크기에 맞게 텍스트와 이미지의 표시를 자동으로 조정할 수 있습니다. • true(기본값) - • Windows 8.1 및 Windows 10에서는 Cisco Jabber가 각 모니터에서 다양한 DPI 설정에 맞게 조정됩니다. • Windows 7 및 Windows 8에서 Cisco Jabber는 시스템 DPI 설정에 따라 표시됩니다. • false - DPI 인식이 활성화되지 않습니다. DPI 인식은 기본적으로 활성화되어 있습니다. DPI 인식 기능을 비활성화하려면 `msiexec.exe/i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false`라는 명령을 사용하십시오. 참고 명령줄을 사용하여 Cisco Jabber를 설치한다면, CLEAR=1 인수를 포함해야 합니다. 명령줄에서 Cisco Jabber를 설치하지 않는다면, jabber-bootstrap.properties 파일을 수동으로 삭제해야 합니다.

인수	값	설명
ENABLE_PRT	true false	• true(기본값) - 클라이언트의 도움말 메뉴에서 문제 보고 메뉴 항목이 활성화됩니다. • false - Jabber 메뉴 항목 옵션인 문제 보고가 클라이언트의 도움말 메뉴에서 제거됩니다. 인수를 false로 설정해도 사용자는 수동으로 시작 메뉴 > **Cisco jabber** 디렉터리 또는 Program Files 디렉터리를 사용하여 문제 보고서 도구를 수동으로 시작할 수 있습니다. 사용자가 수동으로 PRT를 생성하고 이 매개변수 값이 false로 설정된다면, PRT에서 생성된 zip 파일에는 컨텐츠가 없습니다.
ENABLE_PRT_ENCRYPTION	true false	문제 보고서 암호화를 활성화합니다. PRT_CERTIFICATE_NAME 인수를 사용하여 이 인수를 구성해야 합니다. • true - Jabber 클라이언트에서 전송하는 PRT 파일이 암호화됩니다. • false(기본값) - Jabber 클라이언트에서 전송하는 PRT 파일은 암호화되지 않습니다. PRT를 암호화하려면 Cisco Jabber 문제 보고서를 암호화하고 해독하는 데 공개/개인 키 쌍이 필요합니다.
FIPS_MODE	true false	Cisco Jabber를 FIPS 모드로 할지 여부를 지정합니다. Cisco Jabber는 FIPS가 활성화되어 있지 않은 운영 체제에서는 FIPS 모드가 될 수 있습니다. 비 Windows API를 사용한 연결만 FIPS 모드입니다. 이 설정을 포함하지 않으면 Cisco Jabber가 운영 체제에서 FIPS 모드를 확인합니다.

인수	값	설명
FORGOT_PASSWORD_URL	URL	사용자가 분실하거나 잊어버린 암호를 재설정할 수 있는 URL을 지정합니다. 선택 사항이긴 하지만 이 인수를 사용하는 것이 좋습니다. 참고 클라우드 기반 구축에서는 Cisco Webex 관리 도구를 사용하여 암호 잊음 URL을 지정할 수 있습니다. 그러나 클라이언트가 암호 잊음 URL을 검색하려면 사용자가 로그인해야 합니다.
FORWARD_VOICEMAIL	true false	음성 메시지 탭에서 음성 메일 착신 전환을 활성화합니다. • true(기본값) - 사용자가 음성 메일을 연락처로 착신 전환할 수 있습니다. • false - 음성 메일 착신 전환이 활성화되지 않습니다.
INVALID_CERTIFICATE_BEHAVIOR	RejectAndNotify PromptPerSession	잘못된 인증서에 대한 클라이언트 동작을 지정합니다. • RejectAndNotify - 경고 대화 상자가 표시되고 클라이언트가 로드되지 않습니다. • PromptPerSession - 경고 대화 상자가 표시되고 사용자가 잘못된 인증서를 승인하거나 거부할 수 있습니다. FIPS 모드의 잘못된 인증서의 경우, 이 인수가 무시되고 클라이언트는 경고 메시지를 표시하고 로드되지 않습니다.

인수	값	설명
IP_Mode	IPv4-Only IPv6 전용 두 개의 스택	Jabber 클라이언트에 대한 네트워크 IP 프로토콜을 지정합니다. • IPv4 전용 - Jabber는 IPv4 연결만 시도합니다. • IPv6 전용 - Jabber는 IPv6 연결만 시도합니다. • 두 개의 스택(기본값) - Jabber에서 IPv4 또는 IPv6로 연결할 수 있습니다. 참고 IPv6 전용 지원 기능은 데스크톱 장치 온-프레미스 구축에만 사용할 수 있습니다. 모든 Jabber 모바일 장치는 Two Stacks로 구성해야 합니다. IPv6 구축에 대한 자세한 내용은 IPv6 Deployment Guide for Cisco Collaboration Systems 릴리스를 참조하십시오. Jabber에서 사용하는 네트워크 IP 프로토콜을 다양한 요소를 사용해 결정합니다. 자세한 내용은 계획 설명서의 IPv6 요구 사항 섹션을 참조하십시오.

인수	값	설명
언어	LCID(십진수)	Windows용 Cisco Jabber가 사용하는 언어의 로캘 ID(LCID)를 십진수로 정의합니다. 값은 지원되는 언어에 해당하는 십진수의 LCID여야 합니다. 예를 들어, 다음 중 하나를 지정할 수 있습니다. • 1033은 영어를 지정 • 1036은 프랑스어를 지정 지정할 수 있는 언어의 전체 목록은 언어에 대한 *LCID* 항목을 참조하십시오. 이 인수는 선택 사항입니다. 값을 지정하지 않으면 Windows용 Cisco Jabber가 UseSystemLanguage 매개변수에 대한 값을 확인합니다. UseSystemLanguage 매개변수를 true로 설정하면, 운영체제와 같은 언어를 사용합니다. UseSystemLanguage 매개변수를 false로 설정하거나 정의하지 않으면, 클라이언트는 현재 사용자의 지역 언어를 기본값으로 사용합니다. 국가별 언어는 제어판 > 지역 및 언어 > 날짜, 시간 또는 숫자 형식 변경 > 형식 탭 > 형식 드롭다운에서 설정합니다.
LOCATION_MODE	활성화됨 비활성화됨 ENABLEDNOPROMPT	위치 기능 활성화 여부와 새 위치 감지 시 사용자에게 알릴지 여부를 지정합니다. • ENABLED(기본값) - 위치 기능을 켭니다. 새 위치를 감지하면 사용자에게 알림이 표시됩니다. • DISABLED - 위치 기능을 끕니다. 새 위치를 감지해도 사용자에게 알림이 표시되지 않습니다. • ENABLEDNOPROMPT - 위치 기능을 켭니다. 새 위치를 감지해도 사용자에게 알림이 표시되지 않습니다.

인수	값	설명
LOG_DIRECTORY	로컬 파일 시스템의 절대 경로	클라이언트가 로그 파일을 쓰는 디렉터리를 정의합니다. 다음 예에서처럼 따옴표를 사용하여 경로의 공백 문자를 이스케이프합니다. `"C:\my_directory\Log Directory"` 지정한 경로에 Windows에서 허용하지 않는 문자가 있으면 안 됩니다. 기본값은 `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`입니다.
LOGIN_RESOURCE	WBX MUT	여러 클라이언트 인스턴스에 대한 사용자 로그인을 제어합니다. 기본적으로 사용자는 Cisco Jabber의 여러 인스턴스에 동시에 로그인할 수 있습니다. 다음 값 중 하나를 설정하여 기본 동작을 변경합니다. • WBX - 사용자는 한 번에 하나의 Windows용 Cisco Jabber 인스턴스에만 로그인할 수 있습니다. Windows용 Cisco Jabber는 `wbxconnect` 접미사를 사용자의 JID에 추가합니다. 사용자는 `wbxconnect` 접미사를 사용하는 다른 Cisco Jabber 클라이언트에 로그인할 수 없습니다. • MUT - 사용자는 한 번에 하나의 Windows용 Cisco Jabber 인스턴스에만 로그인할 수 있지만 동시에 다른 Cisco Jabber 클라이언트에 로그인할 수 있습니다. Windows용 Cisco Jabber의 각 인스턴스는 사용자의 JID에 고유한 접미사를 추가합니다.

인수	값	설명
PRT_CERTIFICATE_NAME	인증서 이름	엔터프라이즈 신뢰 또는 신뢰할 수 있는 루트 인증 기관 인증서 저장소에서 공개 키가 있는 인증서 이름을 지정합니다. 인증서 공개 키는 Jabber 문제 보고서를 암호화하는 데 사용합니다. ENABLE_PRT_ENCRYPTION 인수를 사용하여 이 인수를 구성해야 합니다.
RESET_JABBER	1	사용자의 로컬 및 로밍 프로파일 데이터를 재설정합니다. 다음 폴더가 삭제됩니다. • `%appdata%\Cisco\Unified Communications\Jabber` • `%localappdata%\Cisco\Unified Communications\Jabber`
SSO_EMAIL_PROMPT	ON OFF	홈 클러스터를 결정하는 이메일 프롬프트를 사용자에게 표시할지 여부를 지정합니다. 이메일 프롬프트가 ServicesDomainSsoEmailPrompt에서 정의한 대로 작동하려면, 다음 설치 프로그램 요구 사항을 충족해야 합니다. • SSO_EMAIL_PROMPT=ON • UPN_DISCOVERY_ENABLED=False • VOICE_SERVICES_DOMAIN=<domain_name> • SERVICES_DOMAIN=<domain_name> Example: msiexec.exe /i CiscoJabberSetup.msi SSO_EMAIL_PROMPT=ON UPN_DISCOVERY_ENABLED=False VOICE_SERVICES_DOMAIN=example.cisco.com SERVICES_DOMAIN=example.cisco.com CLEAR=1

인수	값	설명
Telemetry_Enabled	true false	분석 데이터 수집 여부를 지정합니다. 기본값은 true입니다. 경험 및 제품 성능을 개선하기 위해 Cisco Jabber는 비 개인 식별 가능 사용량 및 성능 데이터를 수집하여 Cisco로 전송할 수 있습니다. 집계된 데이터는 Cisco가 Jabber 클라이언트의 사용 방법 추세와 성능을 확인하는 데 사용합니다. Cisco Jabber가 수집하고 수집하지 않는 분석 데이터에 대한 자세한 내용은 https://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html에 있는 Cisco의 온라인 개인정보 보호정책의 Cisco Jabber 부분에서 확인할 수 있습니다.
TFTP_FILE_NAME	파일 이름	그룹 구성 파일의 고유한 이름을 지정합니다. 정규화되지 않거나 정규화된 파일 이름을 값으로 지정할 수 있습니다. 이 인수의 값으로 지정하는 파일 이름은 TFTP 서버에 있는 다른 모든 구성 파일에 우선합니다. 이 인수는 선택 사항입니다. 기억 Cisco Unified Communications Manager의 CSF 장치 설정에 있는 **Cisco** 지원 필드에서 그룹 구성 파일을 지정할 수 있습니다.

인수	값	설명
UXModel	모던 클래식	데스크톱 클라이언트용 Cisco Jabber에 적용 모든 구축에서 Jabber의 기본값은 모던 디자인입니다. 하지만 Webex Messenger 구축는 클래식 디자인도 지원합니다. Jabber 팀 메시지 모드는 모던 디자인만 지원합니다. Webex Messenger 구축이 클래식 디자인으로 시작되게 하려면 UXModel 매개변수를 사용하십시오. 허용되는 값은 다음과 같습니다. • 모던(기본값) - Jabber는 모던 디자인으로 시작됩니다. • 클래식 - Jabber가 클래식 디자인으로 시작됩니다. 각 사용자는 Jabber에서 이 매개변수에 우선하는 개인 환경설정을 설정할 수 있습니다.

언어에 대한 LCID

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

지원되는 언어	Windows용 Cisco Jabber	Mac용 Cisco Jabber	Android용 Cisco Jabber, iPhone 및 iPad용 Cisco Jabber	LCID/LangID
체코어 - 체코	X	X		1029
덴마크어 - 덴마크	X	X	X	1030
네덜란드어 - 네덜란드	X	X	X	1043
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

지원되는 언어	Windows용 Cisco Jabber	Mac용 Cisco Jabber	Android용 Cisco Jabber, iPhone 및 iPad용 Cisco Jabber	LCID/LangID
슬로바키아어 - 슬로바키아	X	X	X	1051
슬로베니아어 - 슬로베니아	X	X		1060
스페인어-스페인(현대 정렬)	X	X	X	3082
스웨덴어 - 스웨덴	X	X	X	5149
태국어 - 태국	X	X		1054
터키어	X	X	X	1055

관련 항목

설치 명령의 예, 73 페이지
명령줄 인수, 74 페이지

MSI를 수동으로 실행

설치 프로그램을 수동으로 실행하여 클라이언트의 단일 인스턴스를 설치하고 고급 설정에서 연결 설정을 지정할 수 있습니다.

프로시저

단계 **1** `CiscoJabberSetup.msi`를 실행합니다.

설치 프로그램에서 설치 과정을 안내하는 창이 열립니다.

단계 **2** 단계에 따라 설치 프로세스를 완료합니다.

단계 **3** Windows용 Cisco Jabber를 시작합니다.

단계 **4** 수동 설치 및 로그인을 선택합니다.

고급 설정 창이 열립니다.

단계 **5** 연결 설정 속성의 값을 지정합니다.

단계 **6** 저장을 선택합니다.

사용자 정의 설치 프로그램 생성

기본 설치 패키지를 변환하여 사용자 정의 설치 프로그램을 만들 수 있습니다.

참고 Microsoft Orca를 사용하여 사용자 정의 설치 프로그램을 만들 수 있습니다. Microsoft Orca는 Windows 7용 Microsoft Windows SDK와 .NET Framework 4의 일부로 제공됩니다.

Microsoft 웹사이트에서 Windows 7용 Microsoft Windows SDK와 .NET Framework 4를 다운로드하고 설치하십시오.

프로시저

	명령 또는 동작	목적
단계 1	기본 변환 파일 가져오기, 93 페이지	Microsoft Orca를 사용하여 설치 패키지를 수정하려면 기본 변환 파일이 있어야 합니다.
단계 2	사용자 정의 변환 파일 생성, 93 페이지	변환 파일에는 설치 프로그램에 적용하는 설치 속성이 포함됩니다.
단계 3	설치 프로그램 변환, 94 페이지	변환 파일을 적용하여 설치 프로그램을 사용자 정의합니다.

기본 변환 파일 가져오기

Microsoft Orca를 사용하여 설치 패키지를 수정하려면 기본 변환 파일이 있어야 합니다.

프로시저

단계 1 소프트웨어 다운로드 페이지에서 Cisco Jabber 관리 패키지를 다운로드합니다.

단계 2 Cisco Jabber 관리 패키지에서 `CiscoJabberProperties.msi`를 파일 시스템으로 복사합니다.

다음에 수행할 작업

사용자 정의 변환 파일 생성, 93 페이지

사용자 정의 변환 파일 생성

사용자 정의 설치 프로그램을 만들려면 변환 파일을 사용해야 합니다. 변환 파일에는 설치 프로그램에 적용하는 설치 속성이 포함됩니다.

기본 변환 파일을 사용하면 설치 프로그램을 변환할 때 속성의 값을 지정할 수 있습니다. 사용자 지정 설치 프로그램을 하나만 만든다면 기본 변환 파일을 사용해야 합니다.

원한다면 사용자 정의 변환 파일을 생성해도 됩니다. 사용자 정의 변환 파일에서 속성 값을 지정한 다음 이를 설치 프로그램에 적용합니다.

속성 값이 다른 두 개 이상의 사용자 지정 설치 프로그램이 필요하다면, 사용자 정의 변환 파일을 생성해야 합니다. 예를 들어 기본 언어를 프랑스어로 설정하는 변환 파일과 기본 언어를 스페인어로 설정하는 다른 변환 파일을 생성하는 식입니다. 이렇게 하면 각 변환 파일을 개별적으로 설치 패키지에 적용할 수 있습니다. 결과적으로 언어별로 하나씩 두 개의 설치 프로그램이 생성됩니다.

시작하기 전에

기본 변환 파일 가져오기, 93 페이지

프로시저

단계 **1** Microsoft Orca를 시작합니다.

단계 **2** `CiscoJabberSetup.msi`를 열고 `CiscoJabberProperties.msi`를 적용합니다.

단계 **3** 적절한 설치 프로그램 속성의 값을 지정합니다.

단계 **4** 변환 파일을 생성하고 저장합니다.

a) 변환 > 변환 생성을 선택합니다.
b) 파일 시스템에서 변환 파일을 저장할 위치를 선택합니다.
c) 변환 파일의 이름을 지정하고 저장을 선택합니다.

생성한 변환 파일은 *`file_name`*`.mst`로 저장됩니다. 이 변환 파일을 적용하여 `CiscoJabberSetup.msi` 속성을 수정할 수 있습니다.

다음에 수행할 작업

설치 프로그램 변환, 94 페이지

설치 프로그램 변환

변환 파일을 적용하여 설치 프로그램을 사용자 정의합니다.

참고 변환 파일을 적용하면 `CiscoJabberSetup`의 디지털 서명이 변경됩니다. `CiscoJabberSetup.msi`를 수정하거나 이름을 변경하려고 하면 서명이 완전히 제거됩니다.

시작하기 전에

사용자 정의 변환 파일 생성, 93 페이지

프로시저

단계 **1** Microsoft Orca를 시작합니다.

단계 **2** Microsoft Orca에서 `CiscoJabberSetup.msi`를 엽니다.

a) 파일 > 열기를 선택합니다.
b) 파일 시스템에서 `CiscoJabberSetup.msi`의 위치를 찾습니다.
c) `CiscoJabberSetup.msi`를 선택하고 열기를 선택합니다.

설치 패키지가 Microsoft Orca에서 열립니다. 설치 프로그램의 테이블 목록이 테이블 창에서 열립니다.

단계 **3** 필수: 1033(영어)을 제외한 모든 언어 코드를 제거합니다.

제한 사용자 정의 설치 프로그램에서 1033(영어)을 제외한 모든 언어 코드를 제거해야 합니다.

Microsoft Orca 사용자 정의 설치 프로그램에는 기본값인 1033을 제외한 어떤 언어 파일도 유지되지 않습니다. 사용자 정의 설치 프로그램에서 모든 언어 코드를 제거하지 않으면, 언어가 영어가 아닌 운영 체제에서는 설치 프로그램을 실행할 수 없습니다.

a) 보기 > 요약 정보를 선택합니다.

요약 정보 편집 창이 표시됩니다.

b) 언어 필드를 찾습니다.
c) 1033을 제외한 모든 언어 코드를 삭제합니다.
d) 확인을 선택합니다.

사용자 정의 설치 프로그램의 언어로 영어가 설정됩니다.

단계 **4** 변환 파일을 적용합니다.

a) 변환 > 변환 적용을 선택합니다.
b) 파일 시스템에서 변환 파일의 위치를 검색합니다.
c) 변환 파일을 선택한 다음 열기를 선택합니다.

단계 **5** 테이블 창의 테이블 목록에서 속성을 선택합니다.

애플리케이션 창의 오른쪽 패널에서 `CiscoJabberSetup.msi`의 속성 목록이 열립니다.

단계 **6** 필요한 속성의 값을 지정합니다.

팁 값은 대/소문자를 구분합니다. 입력 한 값이이 문서의 값과 일치 하는지 확인 합니다.

팁 CLEAR 속성 값을 1로 설정하여 이전 설치의 기존 부트스트랩 파일을 무시합니다. 기존 부트스트랩 파일을 무시하지 않으면 사용자 정의 설치 프로그램에서 설정한 값이 적용되지 않습니다.

단계 **7** 필요 없는 속성을 제거합니다.

설정되지 않은 속성은 반드시 제거해야 합니다. 제거하지 않으면 설정되는 속성이 적용되지 않습니다. 필요 없는 속성을 한 번에 하나씩 제거합니다.

a) 제거할 속성을 마우스 오른쪽 단추로 클릭합니다.
b) 행 삭제를 선택합니다.
c) Microsoft Orca에서 계속할 것인지 묻는 메시지가 표시되면 확인을 선택합니다.

단계 **8** 필수: 사용자 정의 설치 프로그램을 활성화하여 포함된 스트림을 저장합니다.

a) 도구 > 옵션을 선택합니다.
b) 데이터베이스 탭을 선택합니다.
c) '다른 이름으로 저장' 중에 포함된 스트림 복사를 선택합니다.
d) 적용을 선택한 다음 확인을 선택합니다.

단계 **9** 사용자 정의 설치 프로그램을 저장합니다.

a) 파일 > 변환을 다른 이름으로 저장을 선택합니다.
b) 파일 시스템에서 설치 프로그램을 저장할 위치를 선택합니다.
c) 설치 프로그램의 이름을 지정한 다음 저장을 선택합니다.

설치 프로그램 속성

다음은 사용자 정의 설치 프로그램에서 수정할 수 있는 속성입니다.

- 지우기
- PRODUCT_MODE
- 인증자
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- 언어
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

이러한 속성은 설치 인수에 상응하며 값이 동일합니다.

그룹 정책을 사용하여 구축

Microsoft Windows 서버에서 Microsoft GPMC(그룹 정책 관리 콘솔)을 이용해, 그룹 정책을 바탕으로 Windows용 Cisco Jabber를 설치합니다.

참고 그룹 정책을 바탕으로 Windows용 Cisco Jabber를 설치하려면, Windows용 Cisco Jabber를 구축할 컴퓨터나 사용자가 모두 같은 도메인에 있어야 합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	언어 코드 설정, 97 페이지	어떤 식으로든 Orca를 이용해 MSI를 수정해야 할 때만 이 절차를 사용하고 언어 필드를 1033으로 설정해야 합니다.
단계 **2**	그룹 정책을 사용하여 클라이언트 구축, 98 페이지	그룹 정책을 사용하여 Windows용 Cisco Jabber를 구축합니다.

언어 코드 설정

Cisco가 제공한 MSI 파일을 사용할 예정이라면 그룹 정책 구축에서 설치 언어를 변경하지 않아도 됩니다. 설치 언어는 이러한 상황에서의 Windows 사용자 로캘(형식)을 바탕으로 결정됩니다. 어떤 식으로든 Orca를 이용해 MSI를 수정해야 할 때만 이 절차를 사용하고 언어 필드를 1033으로 설정해야 합니다.

Jabber 클라이언트가 지원하는 언어에 대한 LCID(로캘 식별자) 또는 LangID(언어 식별자) 목록은 언어에 대한 LCID, 90 페이지에서 확인할 수 있습니다.

프로시저

단계 **1** Microsoft Orca를 시작합니다.

Microsoft Orca는 Microsoft 웹사이트에서 다운로드할 수 있는 Windows 7용 Microsoft Windows SDK와 .NET Framework 4의 일부로 제공됩니다.

단계 **2** `CiscoJabberSetup.msi`를 엽니다.

a) 파일 > 열기를 선택합니다.
b) 파일 시스템에서 `CiscoJabberSetup.msi`의 위치를 찾습니다.
c) `CiscoJabberSetup.msi`를 선택하고 열기를 선택합니다.

단계 **3** 보기 > 요약 정보를 선택합니다.

단계 **4** 언어 필드를 찾습니다.

단계 **5** 언어 필드를 1033으로 설정합니다.

단계 **6** 확인을 선택합니다.

단계 **7** 필수: 사용자 정의 설치 프로그램을 활성화하여 포함된 스트림을 저장합니다.

a) 도구 > 옵션을 선택합니다.
b) 데이터베이스 탭을 선택합니다.
c) '다른 이름으로 저장' 중에 포함된 스트림 복사를 선택합니다.
d) 적용을 선택한 다음 확인을 선택합니다.

단계 **8** 사용자 정의 설치 프로그램을 저장합니다.

a) 파일 > 변환을 다른 이름으로 저장을 선택합니다.
b) 파일 시스템에서 설치 프로그램을 저장할 위치를 선택합니다.
c) 설치 프로그램의 이름을 지정한 다음 저장을 선택합니다.

다음에 수행할 작업

그룹 정책을 사용하여 클라이언트 구축, 98 페이지

그룹 정책을 사용하여 클라이언트 구축

이 작업의 단계를 완료하여 그룹 정책을 사용해 Windows용 Cisco Jabber를 구축합니다.

시작하기 전에

언어 코드 설정, 97 페이지

프로시저

단계 **1** 설치 패키지를 구축용 소프트웨어 구축 지점에 복사합니다.

Windows용 Cisco Jabber를 구축할 계획인 모든 컴퓨터나 사용자가 구축 지점의 설치 패키지에 액세스할 수 있어야 합니다.

단계 **2** 시작 > 실행을 선택하고 다음 명령을 입력합니다.

```
GPMC.msc
```

그룹 정책 관리 콘솔이 열립니다.

단계 **3** 새 그룹 정책 개체를 만듭니다.

a) 왼쪽 창에서 적절한 도메인을 마우스 오른쪽 단추로 클릭합니다.
b) 이 도메인에서 **GPO**를 만들고 여기에 링크를 선택합니다.

새 **GPO** 창이 열립니다.

c) **Name(**이름**)** 필드에 그룹 정책 개체의 이름을 입력합니다.
d) 기본값을 그대로 두거나 소스 스타터 **GPO** 드롭다운 목록에서 적절한 옵션을 선택한 다음 확인을 선택합니다.

새 그룹 정책이 도메인의 그룹 정책 목록에 표시됩니다.

단계 **4** 구축의 범위를 설정합니다.

a) 왼쪽 창에서 도메인 아래에 있는 그룹 정책 개체를 선택합니다.

그룹 정책 개체가 오른쪽 창에 표시됩니다.

b) 범위 탭의 보안 필터링 섹션에서 추가를 선택합니다.

사용자**,** 컴퓨터 또는 그룹 선택 창이 열립니다.

c) Windows용 Cisco Jabber을(를) 구축할 컴퓨터 및 사용자를 지정합니다.

단계 **5** 설치 패키지를 지정합니다.

a) 왼쪽 창에서 그룹 정책 개체를 마우스 오른쪽 단추로 클릭한 다음 편집을 선택합니다.

그룹 정책 관리 편집기가 열립니다.

b) 컴퓨터 구성을 선택한 다음 정책 > 소프트웨어 설정을 선택합니다.

c) 소프트웨어 설치를 마우스 오른쪽 단추로 클릭한 다음 신규 > 패키지를 선택합니다.

d) 파일 이름 옆에 설치 패키지의 위치를 입력합니다(예: `\\server\software_distribution`).

중요 UNC(유니폼 명명 규칙) 경로를 설치 패키지의 위치로 입력해야 합니다. UNC 경로를 입력하지 않으면 그룹 정책에서 Windows용 Cisco Jabber를 구축할 수 없습니다.

e) 설치 패키지를 선택하고 열기를 선택합니다.

f) 소프트웨어 구축 대화 상자에서 할당됨을 선택하고 확인을 선택합니다.

그룹 정책은 각 컴퓨터의 다음 시작 시에 Windows용 Cisco Jabber를 설치합니다.

Windows용 자동 업데이트 구성

자동 업데이트를 활성화하려면 HTTP 서버에 설치 패키지의 URL을 포함해 최신 버전에 대한 정보가 담긴 XML 파일을 생성하십시오. 클라이언트는 사용자가 로그인할 때 XML 파일을 검색하고, 절전 모드에서 컴퓨터를 다시 시작하거나 도움말 메뉴에서 수동 업데이트 요청을 수행합니다.

참고 인스턴트 메시징 및 프레즌스 기능에 Cisco Webex Messenger 서비스를 사용한다면, Cisco Webex 관리 도구를 이사용하여 자동 업데이트를 구성해야 합니다.

XML 파일 구조

자동 업데이트를 위한 XML 파일의 구조는 다음과 같습니다.

```
<JabberUpdate>
          <App name="JabberWin">
               <LatestBuildNum>12345</LatestBuildNum>
               <LatestVersion>11.8.x</LatestVersion>
               <Mandatory>true</Mandatory>
               <Message>
```

```
                    <![CDATA[<b>This new version of Cisco Jabber lets you do the
                    following:</b><ul><li>Feature 1</li><li>Feature 2</li></ul>For
                    more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
                </Message>
                <DownloadURL>http://http_server_name/CiscoJabberSetup.msi</DownloadURL>

            </App>
        </JabberUpdate>
```

시작하기 전에

- XML 파일 및 설치 패키지를 호스팅할 HTTP 서버를 설치하고 구성합니다.
- 사용자에게 워크스테이션에 소프트웨어 업데이트를 설치할 권한이 있는지 확인합니다.

  사용자에게 워크스테이션 관리 권한이 없다면 Microsoft Windows는 업데이트 설치를 중지합니다. 설치를 완료하려면 관리자 권한으로 로그인해야 합니다.

프로시저

단계 **1** HTTP 서버에서 업데이트 설치 프로그램을 호스팅합니다.

단계 **2** 텍스트 편집기를 사용하여 업데이트 XML 파일을 작성합니다.

단계 **3** 다음과 같이 XML에서 값을 지정합니다.

- 이름 - 다음 ID를 앱 요소에 대한 이름 속성의 값으로 지정합니다.
  - Jabwin Win - 이 업데이트는 Windows용 Cisco Jabber에 적용됩니다.
- `LatestBuildNum` - 업데이트의 빌드 번호입니다.
- `LatestVersion` - 업데이트의 버전 번호입니다.
- `Mandatory` - (Windows 클라이언트에만 해당) True 또는 False입니다. 메시지가 표시될 때 사용자가 클라이언트 버전을 업그레이드해야 하는지 여부를 결정합니다.
- `Message` - 다음과 같은 형식의 HTML입니다.

  ```
  <![CDATA[your_html]]>
  ```

- `DownloadURL` - HTTP 서버에 있는 설치 패키지의 URL입니다.
- `AllowUpdatesViaExpressway` - (Windows 클라이언트에만 해당). False(기본값) 또는 True입니다. 모바일 및 Remote Access를 위해 Expressway를 통해 회사 네트워크에 연결된 상태에서 Jabber가 자동 업데이트를 수행할 수 있는지 여부를 결정합니다.

  업데이트 XML 파일이 공용 웹 서버에서 호스트된다면, 이 매개변수를 false로 설정합니다. 그렇지 않다면 업데이트 파일은 모바일 및 Remote Access를 위해 Expressway를 통해 액세스해야 하는 내부 서버에서 호스트되는 Jabber를 알려줍니다.

단계 **4** 업데이트 XML 파일을 저장하고 닫습니다.

단계 **5** HTTP 서버에서 업데이트 XML 파일을 호스팅합니다.

단계 **6** 업데이트 XML 파일의 URL을 구성 파일에 있는 UpdateUrl 매개변수의 값으로 지정합니다.

Windows용 Cisco Jabber 제거

명령줄 또는 Microsoft Windows 제어판을 사용하여 Windows용 Cisco Jabber를 제거할 수 있습니다. 이 문서에서는 명령줄을 사용 하 여 Windows용 Cisco Jabber를 제거 하는 방법에 대해 설명 합니다.

설치 프로그램 사용

파일 시스템에서 설치 프로그램을 사용할 수 있다면, 설치 프로그램을 사용하여 Windows용 Cisco Jabber를 제거합니다.

프로시저

단계 **1** 명령줄 창을 엽니다.

단계 **2** 다음의 명령을 입력합니다.

```
msiexec.exe /x path_to_CiscoJabberSetup.msi
```

예를 들어,

```
msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet
```

여기서 `/quiet`는 자동 제거를 지정합니다.

이 명령은 컴퓨터에서 Windows용 Cisco Jabber를 제거합니다.

제품 코드 사용

파일 시스템에서 설치 프로그램을 사용할 수 없다면, 제품 코드를 사용하여 Windows용 Cisco Jabber를 제거합니다.

프로시저

단계 **1** 제품 코드를 찾습니다.

a) Microsoft Windows 레지스트리 편집기를 엽니다.

b) `HKEY_CLASSES_ROOT\Installer\Products` 레지스트리 키를 찾습니다.

c) 편집 > 찾기를 선택합니다.

d) 찾기 창의 찾을 대상 텍스트 상자에 Cisco Jabber를 입력하고 다음 찾기를 선택합니다.

e) **ProductIcon** 키의 값을 찾습니다.

제품 코드는 **ProductIcon** 키의 값입니다(예: `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`).

참고 제품 코드는 Windows용 Cisco Jabber의 각 버전에 따라 다릅니다.

단계 **2** 명령줄 창을 엽니다.

단계 **3** 다음의 명령을 입력합니다.

```
msiexec.exe /x product_code
```

예를 들어,

```
msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet
```

여기서 `/quiet`는 자동 제거를 지정합니다.

이 명령은 컴퓨터에서 Windows용 Cisco Jabber를 제거합니다.

Mac용 Cisco Jabber 설치

Mac용 Cisco Jabber 설치 프로그램

클라이언트 설치

클라이언트 설치와 관련해 다음 방법 중 하나를 선택할 수 있습니다.

- 사용자가 애플리케이션을 수동으로 설치할 수 있도록 설치 프로그램을 제공합니다. 클라이언트는 `Applications` 폴더에 설치됩니다. 이전 버전의 클라이언트를 제거해야 합니다.
- 사용자를 위한 자동 업데이트를 구성하면 설치 프로그램에서 애플리케이션을 자동으로 업데이트합니다.

  자동 업데이트의 경우 클라이언트는 항상 `Applications` 폴더에 추가됩니다.

  - 클라이언트가 다른 폴더 또는 `Applications` 폴더의 하위 폴더에 있다면, Applications 폴더에서 클라이언트를 실행 링크가 해당 폴더에 생성됩니다.
  - 사용자가 이전에 클라이언트 이름을 변경했다면, 설치 프로그램에서는 새 클라이언트의 이름이 이와 일치하도록 변경합니다.

다른 OS X 설치 프로그램 설치와 유사한 시스템 자격 증명을 요구하는 메시지가 사용자에게 표시됩니다.

자동 설치 - 클라이언트를 자동으로 설치하려면 터미널 도구에서 다음과 같은 Mac OS X 명령을 사용하십시오.

```
sudo installer -pkg /path_to/Install_Cisco-Jabber-Mac.pkg -target /
```

설치 프로그램 명령에 대한 자세한 내용은 Mac의 설치 프로그램 매뉴얼 페이지를 참조하십시오.

구성

사용자가 클라이언트에 로그인하는 데 필요한 구성 정보를 제공합니다. 다음 중 하나를 선택합니다.

- 사용자에게 선택적 서버 정보가 포함된 구성 URL을 제공합니다. 자세한 내용은 *Mac*용 *Cisco Jabber*를 위한 *URL* 구성 섹션을 참조하십시오.
- 사용자에게 서버 정보를 제공하여 수동으로 연결합니다. 자세한 내용은 수동 연결 설정 섹션을 참조하십시오.
- 서비스 검색을 사용합니다. 자세한 내용은 서비스 검색 섹션을 참조하십시오.

수동으로 설치 프로그램 실행

설치 프로그램을 수동으로 실행하여 클라이언트의 단일 인스턴스를 설치하고 기본 설정에서 연결 설정을 지정할 수 있습니다.

시작하기 전에

이전 버전의 클라이언트를 제거합니다.

프로시저

단계 **1** `jabber-mac.pkg`를 시작합니다.
설치 프로그램에서 설치 과정을 안내하는 창이 열립니다.

단계 **2** 단계에 따라 설치 프로세스를 완료합니다.
설치 프로그램에서 사용자에게 시스템 자격 증명을 입력하라는 메시지가 표시됩니다.

단계 **3** 구성 URL을 사용하거나 클라이언트를 직접 실행하여 클라이언트를 시작합니다.
사용자 자격 증명을 입력합니다.

Mac용 Cisco Jabber에 대한 URL 구성

사용자가 서비스 검색 정보를 입력하지 않고 Cisco Jabber를 시작하게 하려면, 구성 URL을 만들고 사용자에게 배포해야 합니다.

사용자에게 구성 URL 링크를 이메일로 바로 전송하거나, 링크를 웹사이트에 게시하면 됩니다.

URL에 다음 매개변수를 포함하고 지정할 수 있습니다.

- ServicesDomain - 필수입니다. 모든 구성 URL에는 Cisco Jabber가 서비스를 검색하는 데 필요한 IM 및 프레즌스 서버의 도메인이 포함되어야 합니다.
- ServiceDiscoveryExcludedServices - 선택 사항입니다. 서비스 검색 프로세스에서 다음 서비스를 제외할 수 있습니다.
  - Webex- 이 값을 설정할 때 클라이언트는 다음 상태가 됩니다.
    - CAS 조회를 수행하지 않습니다.

- 다음을 찾습니다.
  - _cisco-uds
  - _cuplogin
  - _collab-edge
- CUCM - 이 값을 설정할 때 클라이언트는 다음 상태가 됩니다.
  - _cisco-uds를 찾지 않습니다.
  - 다음을 찾습니다.
    - _cuplogin
    - _collab-edge
- CUP - 이 값을 설정할 때 클라이언트는 다음 상태가 됩니다.
  - _cuplogin을 찾지 않습니다.
  - 다음을 찾습니다.
    - _cisco-uds
    - _collab-edge

쉼표로 구분된 값을 어려 개 지정하면 여러 서비스를 제외할 수 있습니다.

3가지 서비스를 모두 제외하면, 클라이언트는 서비스 검색을 수행하지 않으며 사용자에게 연결 설정을 수동으로 입력 하라는 메시지를 표시합니다.

- ServicesDomainSsoEmailPrompt - 선택 사항입니다. 홈 클러스터를 결정하는 용도의 이메일 프롬프트를 사용자에게 표시할지 여부를 지정합니다.
  - ON
  - OFF
- EnablePRTEncryption - 선택 사항입니다. PRT 파일이 암호화되도록 지정합니다. Mac용 Cisco Jabber에 적용됩니다.
  - true
  - false
- PRTCertificateName - 선택 사항입니다. 인증서의 이름을 지정합니다. Mac용 Cisco Jabber에 적용됩니다.
- InvalidCertificateBehavior - 선택 사항입니다. 잘못된 인증서에 대한 클라이언트 동작을 지정합니다.

- RejectAndNotify - 경고 대화 상자가 표시되고 클라이언트가 로드되지 않습니다.
- PromptPerSession - 경고 대화 상자가 표시되고 사용자가 잘못된 인증서를 승인하거나 거부할 수 있습니다.

- Telephony_Enabled - 사용자에게 전화 기능이 있는지 여부를 지정합니다. 기본값은 true입니다.
  - True
  - False
- DiagnosticsToolEnabled - 클라이언트에서 진단 도구를 사용할 수 있는지를 지정합니다. 기본값은 true입니다.
  - True
  - False

다음 형식으로 구성 URL을 생성합니다.

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

참고 매개변수는 대소문자를 구분합니다.

예

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Mac용 자동 업데이트 구성

자동 업데이트를 활성화하려면 HTTP 서버에 설치 패키지의 URL을 포함해 최신 버전에 대한 정보가 담긴 XML 파일을 생성하십시오. 클라이언트는 사용자가 로그인할 때 XML 파일을 검색하고, 절전 모드에서 컴퓨터를 다시 시작하거나 도움말 메뉴에서 수동 업데이트 요청을 수행합니다.

참고 인스턴트 메시징 및 프레즌스 기능에 Cisco Webex Messenger 서비스를 사용한다면, Cisco Webex 관리 도구를 이사용하여 자동 업데이트를 구성해야 합니다.

XML 파일 구조

다음은 자동 업데이트를 위한 XML 파일의 예입니다.

```
<JabberUpdate>
<App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>
</App>
</JabberUpdate>
```

XML 파일 예 2

다음은 Windows용 Cisco Jabber 및 Mac용 Cisco Jabber를 자동으로 업데이트하는 XML 파일의 예입니다.

```
<JabberUpdate>
 <App name="JabberMac">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.6.1</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2</li>
  </ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>

<DownloadURL>http://http_server_name/Install_Cisco-Jabber-Mac-1.1.1-12345-MrbCdd.zip</DownloadURL>

 </App>
 <App name="JabberWin">
  <LatestBuildNum>12345</LatestBuildNum>
  <LatestVersion>9.0</LatestVersion>
  <Message><![CDATA[<b>This new version of Cisco Jabber lets you do the
following:</b><ul><li>Feature 1</li><li>Feature 2
  </li></ul>For more information click <a target="_blank"
href="http://cisco.com/go/jabber">here</a>.]]>
  </Message>
  <DownloadURL>http://http_server_name/CiscoJabberSetup.msi
  </DownloadURL>
</App>
</JabberUpdate>
```

시작하기 전에

XML 파일 및 설치 패키지를 호스팅할 HTTP 서버를 설치하고 구성합니다.

참고 DSA 서명이 성공하게 하려면 특수 문자를 이스케이프하도록 웹 서버를 구성하십시오. 예를 들어, Microsoft IIS에서 옵션은 이중 공백 허용입니다.

프로시저

단계 **1** HTTP 서버에서 업데이트 설치 프로그램을 호스팅합니다.

단계 **2** 텍스트 편집기를 사용하여 업데이트 XML 파일을 작성합니다.

단계 **3** 다음과 같이 XML에서 값을 지정합니다.

- 이름 - 다음 ID를 앱 요소에 대한 이름 속성의 값으로 지정합니다.
  - Jabwin Win - 이 업데이트는 Windows용 Cisco Jabber에 적용됩니다.
  - Jabsl Mac - 이 업데이트는 Mac용 Cisco Jabber에 적용됩니다.
- `LatestBuildNum` - 업데이트의 빌드 번호입니다.
- `LatestVersion` - 업데이트의 버전 번호입니다.
- `Mandatory` - True 또는 False입니다. 메시지가 표시될 때 사용자가 클라이언트 버전을 업그레이드해야 하는지 여부를 결정합니다.
- `Message` - 다음과 같은 형식의 HTML입니다.

  ```
  <![CDATA[your_html]]>
  ```

- `DownloadURL` - HTTP 서버에 있는 설치 패키지의 URL입니다.

  Mac용 Cisco Jabber의 경우, URL 파일은 다음과 같은 형식이어야 합니다.

  ```
  Install_Cisco-Jabber-Mac-version-size-dsaSignature.zip
  ```

단계 **4** 업데이트 XML 파일을 저장하고 닫습니다.

단계 **5** HTTP 서버에서 업데이트 XML 파일을 호스팅합니다.

단계 **6** 업데이트 XML 파일의 URL을 구성 파일에 있는 UpdateUrl 매개변수의 값으로 지정합니다.

Cisco Jabber 모바일 클라이언트 설치

프로시저

단계 **1** Android용 Cisco Jabber를 설치하려면 모바일 장치의 Google Play에서 앱을 다운로드하십시오.

단계 2 iPhone 및 iPad용 Cisco Jabber를 설치하려면 모바일 장치의 앱 스토어에서 앱을 다운로드하십시오.

Android, iPhone 및 iPad용 Cisco Jabber에 대한 URL 구성

사용자가 서비스 검색 정보를 입력하지 않고 Cisco Jabber를 시작하게 하려면, 구성 URL을 만들고 사용자에게 배포해야 합니다.

사용자에게 구성 URL 링크를 이메일로 바로 전송하거나, 링크를 웹사이트에 게시하면 됩니다.

URL에 다음 매개변수를 포함하고 지정할 수 있습니다.

- ServicesDomain - 필수입니다. 모든 구성 URL에는 Cisco Jabber가 서비스를 검색하는 데 필요한 IM 및 프레즌스 서버의 도메인이 포함되어야 합니다.
- ServiceDiscoveryExcludedServices - 선택 사항입니다. 서비스 검색 프로세스에서 다음 서비스를 제외할 수 있습니다.
  - Webex- 이 값을 설정할 때 클라이언트는 다음 상태가 됩니다.
    - CAS 조회를 수행하지 않습니다.
    - 다음을 찾습니다.
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM - 이 값을 설정할 때 클라이언트는 다음 상태가 됩니다.
    - `_cisco-uds`를 찾지 않습니다.
    - 다음을 찾습니다.
      - `_cuplogin`
      - `_collab-edge`
  - CUP - 이 값을 설정할 때 클라이언트는 다음 상태가 됩니다.
    - `_cuplogin`을 찾지 않습니다.
    - 다음을 찾습니다.
      - `_cisco-uds`
      - `_collab-edge`

쉼표로 구분된 값을 어려 개 지정하면 여러 서비스를 제외할 수 있습니다.

3가지 서비스를 모두 제외하면, 클라이언트는 서비스 검색을 수행하지 않으며 사용자에게 연결 설정을 수동으로 입력 하라는 메시지를 표시합니다.

- ServicesDomainSsoEmailPrompt - 선택 사항입니다. 홈 클러스터를 결정하는 용도의 이메일 프롬프트를 사용자에게 표시할지 여부를 지정합니다.
  - ON
  - OFF
- InvalidCertificateBehavior - 선택 사항입니다. 잘못된 인증서에 대한 클라이언트 동작을 지정합니다.
  - RejectAndNotify - 경고 대화 상자가 표시되고 클라이언트가 로드되지 않습니다.
  - PromptPerSession - 경고 대화 상자가 표시되고 사용자가 잘못된 인증서를 승인하거나 거부할 수 있습니다.
- PRTCertificateUrl - 신뢰할 수 있는 루트 인증서 저장소에서 공개 키가 있는 인증서 이름을 지정합니다. Cisco Jabber 모바일 클라이언트에 적용됩니다.
- Telephony_Enabled - 사용자에게 전화 기능이 있는지 여부를 지정합니다. 기본값은 true입니다.
  - True
  - False
- ForceLaunchBrowser - 사용자가 외부 브라우저를 사용하도록 강제하는 데 사용합니다. Cisco Jabber 모바일 클라이언트에 적용됩니다.
  - True
  - False

참고 ForceLaunchBrowser는 클라이언트 인증서 구축 및 Android OS 5.0 미만의 장치에 사용합니다.

다음 형식으로 구성 URL을 생성합니다.

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

참고 매개변수는 대소문자를 구분합니다.

예

- `ciscojabber://provision?ServicesDomain=cisco.com`

- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

EMM(Enterprise Mobility Management)를 사용한 모바일 구성

AppConfig 표준이 포함된 **EMM(**엔터프라이즈 이동성 관리**)**

EMM(Enterprise Mobility Management)을 사용하기 전에 다음 사항을 확인하십시오.

- EMM 공급업체가 Android for Work 또는 Apple 관리형 앱 구성을 지원합니다.
- Android 장치 OS 5.0 이상입니다.

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.

Microsoft Exchange Server에서 가져온 로컬 연락처의 기본 다이얼 장치로 iPhone 및 iPad용 Cisco Jabber를 구성할 수 있습니다. **Exchange ActiveSync**를 사용하여 프로파일을 구성하고 MDM 구성 파일의 기본 오디오 통화 앱 필드에 `com.cisco.jabberIM` 값을 입력하십시오.

EMM을 사용한다면, EMM 애플리케이션에서 AllowUrlProvisioning 매개변수를 False로 설정하여 URL 구성을 비활성화하십시오. 매개변수 구성에 대한 자세한 내용은 *AllowUrlProvisioning* 매개변수 항목을 참조하십시오.

앱 래핑에 의한 **EMM**

EMM에 대한 또 다른 접근 방식은 앱 래핑입니다. 공급업체 앱 래핑 도구를 사용하여 Jabber를 캡슐화하고 정책을 적용하여 사용자가 Jabber에서 수행할 수 있는 작업을 제한합니다. 그런 다음 캡슐화된 Jabber를 사용자에게 배포합니다. 새 버전의 Jabber로 업그레이드할 때마다 캡슐화를 반복해야 합니다.

Cisco Jabber를 사용하여 앱 래핑 기능을 사용하려면 양방향 규약에 서명해야 합니다. `jabber-mobile-mam@cisco.com`에 자세한 내용을 문의해 주십시오.

SDK 통합별 EMM

릴리스 12.8에서는 EMM에 대한 또 다른 접근 방법으로 Microsoft Intune 및 BlackBerry Dynamics에 대한 지원을 추가했습니다. Microsoft 및 BlackBerry SDK를 사용하여 App Store 및 Google Play Store를 통해 사용할 수 있는 새 클라이언트를 만들었습니다.

- Intune용 Jabber
- BlackBerry용 Jabber

이러한 솔루션을 사용하면 포털에서 관리 정책을 만들 수 있습니다. 사용자가 새 클라이언트로 로그인하면 클라이언트가 포털과 동기화되고 정책을 적용합니다.

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.

주의 Intune용 Jabber는 iOS 플랫폼에서 APN(Apple Push Notification)을 지원하지 않습니다. 사용자가 Jabber를 백그라운드에 배치하면 iOS 장치에서 채팅 메시지와 통화를 수신하지 못할 수 있습니다.

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

제한 사항	Android	iPhone 및 iPad
조직의 데이터 사본 저장	예	예
잘라내기, 복사 및 다른 앱으로 붙여넣기	예	예
화면 캡처	예	해당 사항 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 사항 없음
액세스를 위한 직장 (또는 학교) 계정 자격 증명	예	예
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.

주의 BlackBerry용 Jabber는 iOS 플랫폼에서 APN(Apple Push Notification)을 지원하지 않습니다. 사용자가 Jabber를 백그라운드에 배치하면 iOS 장치에서 채팅 메시지와 통화를 수신하지 못할 수 있습니다.

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

필드	iOS에서 지원됨	Android에서 지원됨
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
BlackBerry Dynamics	비밀번호	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 사항 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
엔터프라이즈관리에이전트프로파일	개인 앱 모음 허용	예	예

그룹	기능	Android	iPhone 및 iPad
준수 프로파일	루트 OS 또는 실패한 증명	예	예
	제한된 OS 버전이 설치됨	예	예
	필수 보안 패치 수준이 설치되어 있지 않음	예	해당 사항 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.

MDM 구축에 유용한 매개 변수

EMM 공급업체는 애플리케이션 구성 설정에 다양한 값 유형이 설정되게 허용할 수 있지만, Cisco Jabber는 문자열 값 유형을 읽기만 합니다. EMM의 경우 다음 매개 변수를 유용하게 사용할 수 있습니다. 이러한 매개 변수에 대한 자세한 내용은 *Android, iPhone* 및 *iPad*용 *Cisco Jabber*에 대한 *URL* 구성 섹션을 참조하십시오.

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser
- FIPS_MODE
- CC_MODE
- LastLoadedUserProfile
- AllowUrlProvisioning

  EMM을 사용한다면, EMM 애플리케이션에서 AllowUrlProvisioning 매개변수를 **`False`**로 설정하여 URL 구성을 비활성화하십시오. 매개변수 구성에 대한 자세한 내용은 *AllowUrlProvisioning* 매개변수 항목을 참조하십시오.

- IP_Mode
- AllowTeamsUseEmbeddedSafari - iPhone 및 iPad용 Cisco Jabber 전용
- AutoLoginUserName
- AutoLoginUserPassword

다음 섹션에서는 MDM 구축에서 이러한 매개 변수 중 일부를 사용하는 방법에 대해 설명합니다.

AllowUrlProvisioning 매개변수

이 매개변수는 사용자를 URL 구성에서 EMM으로 마이그레이션할 때 사용합니다.

다음 값이 이 매개변수에 적용됩니다.

- true(기본값) - URL 구성을 사용하여 부트스트랩 구성을 수행합니다.
- false - URL 구성을 사용하여 부트스트랩 구성을 수행하지 않습니다.

예:`<AllowURLProvisioning>false</AllowURLProvisioning>`

AutoLoginUserName

iPhone 및 iPad용 Cisco Jabber에 적용됩니다.

EMM에서는 모바일 장치에서 사용자 이름을 정의합니다. 이 매개 변수는 AutoLoginUserPassword 매개 변수 및 ServicesDomain 매개 변수와 함께 사용해야 합니다. 이러한 매개 변수를 함께 사용하면 사용자의 로그인 세부 정보가 이미 입력된 상태로 Jabber 앱을 설치할 수 있습니다.

AutoLoginUserPassword

iPhone 및 iPad용 Cisco Jabber에 적용됩니다.

EMM에서는 모바일 장치에서 암호를 정의합니다. 이 매개 변수는 AutoLoginUserName 매개 변수 및 ServicesDomain 매개 변수와 함께 사용해야 합니다. 이러한 매개 변수를 함께 사용하면 사용자의 로그인 세부 정보가 이미 입력된 상태로 Jabber 앱을 설치할 수 있습니다.

CC_MODE 매개변수

EMM을 사용하여 Cisco Jabber 모바일 클라이언트에서 Common Criteria 모드를 활성화하거나 비활성화하려면 이 매개변수를 사용하십시오.

- *true* - Common Criteria 모드에서 Cisco Jabber를 실행합니다.
- *false*(기본값) - Common Criteria 모드에서 Cisco Jabber를 실행하지 않습니다.

예:`< CC_MODE >true</CC_MODE >`

참고 CC_MODE를 활성화하려면 RSA 키 크기가 2048비트 이상이어야 합니다. 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.

FIPS_MODE 매개변수

EMM을 사용하여 Cisco Jabber 모바일 클라이언트에서 FIPS 모드를 활성화하거나 비활성화하려면 이 매개변수를 사용하십시오.

- *true* - FIPS 모드에서 Cisco Jabber를 실행합니다.
- *false* - FIPS 모드에서 Cisco Jabber를 실행하지 않습니다.

예:`< FIPS_MODE >false</FIPS_MODE >`

VDI용 Jabber Softphone 설치

프로시저

단계 **1** Jabber 구축을 위한 워크플로를 완료합니다.

단계 **2** VDI용 Jabber 소프트폰를 설치하려면 설치 중인 클라이언트에 대한 VDI용 Cisco Jabber Softphone 구축 및 설치 설명서의 지침을 따르십시오.

14 장

Remote Access

서비스 검색 요구 사항 워크플로

프로시저

	명령 또는 동작	목적
단계 **1**	서비스 검색 요구 사항, 55 페이지	
단계 **2**	DNS 요구 사항, 55 페이지	
단계 **3**	인증서 요구 사항, 55 페이지	
단계 **4**	_collab-edge SRV 레코드 테스트, 120 페이지	

서비스 검색 요구 사항

서비스 검색을 통해 클라이언트는 엔터프라이즈 네트워크에서 서비스를 자동으로 감지하고 찾을 수 있습니다. 모바일 및 Remote Access를 위한 Expressway를 사용하면 엔터프라이즈 네트워크에서 서비스에 액세스할 수 있습니다. 클라이언트가 모바일 및 Remote Access 및 검색 서비스를 위한 Expressway를 통해 연결할 수 있게 하려면 다음 요구 사항을 충족해야 합니다.

- DNS 요구 사항
- 인증서 요구 사항
- 외부 SRV `_collab-edge`를 테스트합니다.

DNS 요구 사항

Remote Access를 통한 서비스 검색에 대한 DNS 요구 사항은 다음과 같습니다.

- 외부 DNS 서버에서 `_collab-edge` DNS SRV 레코드를 구성해야 합니다.
- 내부 이름 서버에 `_cisco-uds` DNS SRV 레코드를 구성해야 합니다.
- IM and Presence 서버 및 음성 서버에 대해 다른 도메인을 사용하는 하이브리드 클라우드 기반 구축의 경우에는 선택 사항으로 `_collab-edge` 레코드를 사용하여 DNS 서버를 찾도록 음성 서비스 도메인을 구성할 수 있습니다.

인증서 요구 사항

Remote Access를 구성하기 전에 Cisco VCS Expressway 및 Cisco Expressway-E 서버 인증서를 다운로드하십시오. 이 서버 인증서는 HTTP와 XMPP 모두에 사용합니다.

Cisco VCS Expressway 인증서 구성에 대한 자세한 내용은 Cisco VCS Expressway에서 인증서 구성을 참조하십시오.

_collab-edge SRV 레코드 테스트

SRV 레코드 테스트

SRV 레코드 테스트를 생성한 후 액세스할 수 있는지 확인합니다.

팁 웹 기반 옵션을 선호한다면 협업 솔루션 분석기 사이트에서 SRV 확인 도구를 사용해도 됩니다.

프로시저

단계 **1** 명령 프롬프트를 엽니다.

단계 **2** **nslookup**을 입력합니다.

기본 DNS 서버 및 주소가 표시됩니다. 예상했던 DNS 서버인지 확인합니다.

단계 **3** **set type=SRV**를 입력합니다.

단계 **4** 각 SRV 레코드에 이름을 입력합니다.

예: `_cisco-uds._tcp.exampledomain`

- 서버 및 주소를 표시합니다 - SRV 레코드에 액세스할 수 있습니다.

- `_cisco-uds_tcp.exampledomain`: 존재하지 않는 도메인이 표시됩니다 - SRV 레코드에 문제가 있습니다.

Cisco Anyconnect 구축 워크플로

프로시저

	명령 또는 동작	목적
단계 1	애플리케이션 프로파일, 121 페이지	
단계 2	VPN 연결 자동화, 122 페이지	
단계 3	AnyConnect 문서 참조, 126 페이지	
단계 4	세션 매개변수, 126 페이지	

Cisco AnyConnect 구축

애플리케이션 프로파일

After you download the Cisco AnyConnect Secure Mobility Client to their device, the ASA must provision a configuration profile to the application.

Cisco AnyConnect Secure Mobility Client용 구성 프로파일에는 회사 ASA VPN 게이트웨이, 연결 프로토콜(IPSec 또는 SSL), 온디맨드 정책 같은 VPN 정책 정보가 포함됩니다.

다음 방법 중 하나로 iPhone 및 iPad용 Cisco Jabber의 애플리케이션 프로파일을 프로비저닝할 수 있습니다.

ASDM

ASDM(ASA 장치 관리자)에서 프로파일 편집기를 이용해 Cisco AnyConnect Secure Mobility Client의 VPN 프로파일을 정의하는 방법을 권장합니다.

이 방법을 사용하면 클라이언트가 VPN 연결을 처음 설정한 후 VPN 프로파일이 Cisco AnyConnect Secure Mobility Client로 자동 다운로드됩니다. 이 방법은 모든 장치 및 OS 유형에서 사용할 수 있으며, ASA에서 VPN 프로파일을 중앙집중식으로 관리할 수 있습니다.

자세한 내용은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 프로파일 생성 및 편집 항목을 참조하십시오.

iPCU

IPCU(iPhone 구성 유틸리티)로 생성하는 Apple 구성 프로파일을 사용하여 iOS 장치를 프로비저닝할 수 있습니다. Apple 구성 프로파일은 장치 보안 정책, VPN 구성 정보, Wi-Fi, 메일 및 캘린더 설정 등의 정보가 포함된 XML 파일입니다.

고수준 절차는 다음과 같습니다.

1. IPCU를 사용하여 Apple 구성 프로파일을 생성합니다.

   자세한 내용은 iPCU 설명서를 참조하십시오.

2. XML 프로파일을 .mobileconfig 파일로 내보냅니다.
3. 사용자에게 .mobileconfig 파일을 이메일로 전송합니다.

   사용자가 파일을 열면 AnyConnect VPN 프로파일 및 기타 프로파일 설정이 클라이언트 애플리케이션에 설치됩니다.

MDM

타사 MDM(모바일 장치 관리) 소프트웨어로 만든 Apple 구성 프로파일을 사용하여 iOS 장치를 프로비저닝할 수 있습니다. Apple 구성 프로파일은 장치 보안 정책, VPN 구성 정보, Wi-Fi, 메일 및 캘린더 설정 등의 정보가 포함된 XML 파일입니다.

고수준 절차는 다음과 같습니다.

1. MDM을 사용하여 Apple 구성 프로파일을 만듭니다.

   MDM 사용에 관한 자세한 내용은 Apple 설명서를 참조하십시오.

2. Apple 구성 프로파일을 등록된 장치로 푸시합니다.

Android용 Cisco Jabber의 애플리케이션 프로파일을 프로비저닝하려면, ASDM(ASA 장치 관리자)에서 프로파일 편집기를 이용해 Cisco AnyConnect Secure Mobility Client의 VPN 프로파일을 정의하십시오. 클라이언트가 VPN 연결을 처음 설정한 후 VPN 프로파일이 Cisco AnyConnect Secure Mobility Client로 자동 다운로드됩니다. 이 방법은 모든 장치 및 OS 유형에서 사용할 수 있으며, ASA에서 VPN 프로파일을 중앙집중식으로 관리할 수 있습니다. 자세한 내용은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 프로파일 생성 및 편집 항목을 참조하십시오.

VPN 연결 자동화

사용자가 회사 Wi-Fi 네트워크 외부에서 Cisco Jabber를 열면, Cisco Jabber는 Cisco UC 애플리케이션 서버에 액세스하기 위해 VPN 연결을 요구합니다. Cisco AnyConnect Secure Mobility Client가 백그라운드에 자동으로 VPN 연결을 설정하도록 시스템을 설정할 수도 있습니다. 이렇게 하면 원활한 사용자 경험을 보장하는 데 도움이 됩니다.

참고 VPN을 자동 연결로 설정하더라도, 연결 우선순위가 높은 Expressway Mobile 및 Remote Access를 수행해야 VPN을 시작할 수 있습니다.

신뢰할 수 있는 네트워크 연결 설정

Trusted Network Detection 기능을 이용하면 사용자의 위치를 기반으로 VPN 연결을 자동화하여 사용자 환경을 개선할 수 있습니다. 사용자가 회사 Wi-Fi 네트워크 내부에 있다면 Cisco Jabber는 Cisco UC 인프라에 직접 연결할 수 있습니다. 사용자가 회사 Wi-Fi 네트워크에서 나가면, Cisco Jabber는 사용자가 신뢰할 수 있는 네트워크 외부에 있음을 자동으로 감지합니다. 이 현상이 발생하면, Cisco AnyConnect Secure Mobility Client는 VPN을 시작하여 UC 인프라에 대한 연결을 보장합니다.

참고 Trusted Network Detection 기능인 인증서 및 암호 기반 인증 모두에서 작동합니다. 그러나 인증서 기반 인증이 가장 원활한 사용자 환경을 제공합니다.

프로시저

단계 **1** ASDM을 사용하여 Cisco AnyConnect 클라이언트 프로파일을 엽니다.

단계 **2** 클라이언트가 회사 Wi-Fi 네트워크 내에 있을 때 인터페이스가 수신할 수 있는, 신뢰할 수 있는 DNS 서버 및 신뢰할 수 있는 DNS 도메인 접미사 목록을 입력합니다. Cisco AnyConnect 클라이언트는 현재 인터페이스 DNS 서버와 도메인 접미사를 이 프로파일의 설정과 비교합니다.

참고 Trusted Network Detection 기능이 올바르게 작동하려면 모든 DNS 서버를 지정해야 합니다. TrustedDNSDomains와 TrustedDNSServers를 모두 설정했다면, 세션은 두 설정을 일치시켜 신뢰할 수 있는 네트워크로 정의되게 해야 합니다.

Trusted Network Detection을 설정하는 자세한 방법은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 기능 구성 장(릴리스 2.5) 또는 *VPN* 액세스 구성(릴리스 3.0 또는 3.1)에 있는 *Trusted Network Detection* 섹션을 참조하십시오.

온디맨드 **VPN** 연결 설정

Apple iOS Connect On Demand 기능을 이용하면 사용자의 도메인을 기반으로 VPN 연결을 자동화하여 사용자 환경을 개선할 수 있습니다.

사용자가 회사 Wi-Fi 네트워크 내부에 있다면 Cisco Jabber는 Cisco UC 인프라에 직접 연결할 수 있습니다. AnyConnect 클라이언트 프로파일에 지정한 도메인에 연결된 Cisco AnyConnect는 사용자가 회사 Wi-Fi 네트워크에서 나갈 때 이를 자동으로 감지합니다. 이 경우 애플리케이션은 VPN을 시작하여 UC 인프라와의 연결을 보장합니다. Cisco Jabber를 포함한 장치의 모든 애플리케이션이 이 기능을 활용할 수 있습니다.

참고 Connect On Demand는 인증서 인증 연결만 지원합니다.

이 기능은 다음 옵션을 지원합니다.

- 항상 연결 — Apple iOS는 항상 이 목록에 있는 도메인과의 VPN 연결을 시작합니다.
- 필요한 경우 연결 — Apple iOS는 DNS를 이용해 주소를 확인할 수 없을 때만 목록에 있는 도메인과의 VPN 연결을 시작합니다.
- 연결 안함 — Apple iOS는 이 목록에 있는 도메인과의 VPN 연결을 시작하지 않습니다.

주의 Apple은 조만간 항상 연결 옵션을 제거할 예정입니다. [항상 연결] 옵션이 제거되면 사용자는 [필요한 경우 연결] 옵션을 선택하면 됩니다. [필요한 경우 연결] 옵션을 사용할 때 Cisco Jabber 사용자에게 문제가 발생하기도 합니다. 예를 들어 Cisco Unified Communications Manager의 호스트 이름을 회사 네트워크 회부에서 확인할 수 있다면, iOS는 VPN 연결을 트리거하지 않습니다. 사용자는 전화를 걸기 전에 Cisco AnyConnect Secure Mobility Client를 수동으로 시작하여 이러한 문제를 해결할 수 있습니다.

프로시저

단계 **1** ASDM 프로파일 편집기, iPCU 또는 MDM 소프트웨어를 사용하여 AnyConnect 클라이언트 프로파일을 엽니다.

단계 **2** AnyConnect 클라이언트 프로파일의 [필요한 경우 연결] 섹션에서 온디맨드 도메인 목록을 입력합니다.

도메인 목록에는 와일드 카드 옵션(예: cucm.cisco.com, cisco.com 및 *. webex.com)이 포함될 수 있습니다.

Cisco Unified Communications Manager에서 자동 VPN 액세스 설정

시작하기 전에

- 모바일 장치는 인증서 기반 인증을 이용한 VPN 온디맨드 액세스를 설정해야 합니다. VPN 액세스를 설정 관련 도움이 필요하다면, VPN 클라이언트 및 헤드 엔드 공급업체에 문의하십시오.
- Cisco AnyConnect Secure Mobility Client 및 Cisco Adaptive Security Appliance의 요구 사항은 소프트웨어 요구 사항 항목을 참조하십시오.
- Cisco AnyConnect 설정에 관한 자세한 내용은 *Cisco AnyConnect VPN Client* 유지 관리 및 작동 설명서를 참조하십시오.

프로시저

단계 **1** 클라이언트가 VPN을 요청 시 시작하게 하는 URL을 식별합니다.

a) 다음 방법 중 하나를 사용하여 클라이언트가 VPN을 요청 시 시작하게 하는 URL을 식별합니다.

- 필요한 경우 연결
  - (IP 주소가 아닌) 도메인 이름을 통해 액세스하도록 Cisco Unified Communications Manager를 구성하고, 이 도메인 이름이 방화벽 외부에서 확인할 수 없는지 확인합니다.
  - 이 도메인을 Cisco AnyConnect 클라이언트 연결의 요청 시 연결 도메인 목록의 "필요한 경우 연결" 목록에 포함합니다.
- 항상 연결
  - 4단계에서 매개변수를 존재하지 않는 도메인으로 설정합니다. 존재하지 않는 도메인을 이용하면 사용자가 방화벽 내부 또는 외부에 있을 때 DNS 쿼리가 실패하게 됩니다.
  - 이 도메인을 Cisco AnyConnect 클라이언트 연결의 요청 시 연결 도메인 목록의 "항상 연결" 목록에 포함합니다.

    URL은 도메인 이름만 포함해야 합니다. 프로토콜이나 경로는 포함하지 마십시오(예: "https://cm8ondemand.company.com/vpn" 대신 "cm8ondemand.company.com" 사용).

b) Cisco AnyConnect에 URL을 입력하고 이 도메인에서 DNS 쿼리가 실패하는지 확인합니다.

단계 **2** **Cisco Unified CM** 관리 인터페이스를 엽니다.

단계 **3** 사용자의 장치 페이지로 이동합니다.

단계 **4** 온디맨드 **VPN URL** 필드의 제품별 구성 레이아웃 섹션에, 1단계에서 Cisco AnyConnect에서 식별하고 사용한 URL을 입력합니다.

URL에는 프로토콜이나 경로가 없는 도메인 이름만 사용해야 합니다.

단계 **5** 저장을 선택합니다.

Cisco Jabber가 열리면 URL에 대한 DNS 쿼리를 시작합니다. 이 URL이 이번 절차에서 정의한 온디맨드 도메인 목록 항목(예: cisco.com)과 일치한다면, Cisco Jabber는 AnyConnect VPN 연결을 간접적으로 시작합니다.

다음에 수행할 작업

- 이 기능을 테스트합니다.
  - IOS 장치의 인터넷 브라우저에 URL을 입력하고 VPN이 자동으로 시작되는지 확인합니다. 상태 표시줄에 VPN 아이콘이 표시되어야 합니다.
  - IOS 장치에서 VPN을 사용하여 회사 네트워크에 연결할 수 있는지 확인합니다. 예를 들어 회사 인트라넷에서 웹 페이지에 액세스합니다. IOS 장치를 연결할 수 없다면, VPN 기술 공급업체에 문의하십시오.
  - IT 부서와 함께 VPN이 특정 트래픽 유형에 대한 액세스를 차단하지 않는지 확인합니다(예: 관리자가 이메일과 캘린더 트래픽만 허용하도록 시스템을 설정).
- 회사 네트워크에 직접 연결되도록 클라이언트를 설정했는지 확인합니다.

AnyConnect 문서 참조

AnyConnect 요구 사항 및 구축에 대한 자세한 내용은 아래의 릴리스 설명서를 참조하십시오.
https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-user-guide-list.html

세션 매개변수

ASA 세션 매개변수를 구성하여 보안 연결 성능을 향상할 수 있습니다. 최상의 사용자 경험을 위해서는 다음과 같은 ASA 세션 매개변수를 구성해야 합니다.

- 데이터그램 전송 계층 보안(DTLS) - DTLS는 지연 및 데이터 손실을 방지하는 데이터 경로를 제공하는 SSL 프로토콜입니다.
- 자동 재연결 - 자동 재연결 또는 세션 지속성을 사용하여 CiscoAnyConnect Secure Mobility Client에서 세션 중단을 복구하고 세션을 다시 설정할 수 있습니다.
- 세션 지속성 - 이 매개변수를 사용하면 VPN 세션에서 서비스 중단을 복구하고 연결을 다시 설정할 수 있습니다.
- 유휴 시간 제한 - 유휴 시간 제한은 통신 활동이 전혀 없는 경우, ASA가 보안 연결을 종료한 이후의 시간을 정의합니다.
- 데드 피어 감지(DTD) - DTD는 ASA 및 Cisco AnyConnect Secure Mobility Client가 실패한 연결을 신속하게 감지할 수 있도록 보장합니다.

ASA 세션 매개변수 설정

Cisco AnyConnect Secure Mobility Client에 대한 최종 사용자 경험을 최적화하려면 ASA 세션 매개변수를 다음과 같이 설정하는 것이 좋습니다.

프로시저

단계 **1** DTLS를 사용하도록 Cisco AnyConnect를 설정합니다.

자세한 내용은 *Cisco AnyConnect VPN Client* 관리자 설명서 버전 *2.0*, *ASDM*을 이용한 *AnyConnect* 기능 구성 장의 *AnyConnect(SSL)* 연결을 이용한 *DTLS(Datagram Transport Layer Security)* 활성화를 참조하십시오.

단계 **2** 세션 지속성(자동 재연결)을 설정합니다.

a) ASDM을 사용하여 VPN 클라이언트 프로파일을 엽니다.
b) 자동 재연결 동작 매개변수를 재개 후 재연결로 설정합니다.

자세한 내용은 사용자 릴리스의 *Cisco AnyConnect Secure Mobility Client* 관리자 설명서의 *AnyConnect* 기능 구성 장(릴리스 2.5) 또는 *VPN* 액세스 구성 장(릴리스 3.0 또는 3.1)에 있는 자동 재연결 구성 항목을 참조하십시오.

단계 **3** 유휴 시간 초과 값을 설정합니다.

a) Cisco Jabber 클라이언트와 관련된 그룹 정책을 만듭니다.
b) 유휴 시간 초과 값을 30분으로 설정합니다.

자세한 내용은 사용자 릴리스의 *Cisco ASA 5580* 적응형 보안 어플라이언스 명령 참조의 *vpn-idle-timeout* 섹션을 참조하십시오.

단계 **4** DPD(비활성 피어 감지)를 설정합니다.

a) 서버측 DPD를 비활성화합니다.
b) 클라이언트측 DPD를 활성화합니다.

자세한 내용은 *CLI, 8.4, 8.6*를 이용한 *Cisco ASA 5500* 시리즈 구성 설명서 *VPN* 구성 장의 비활성 피어 감지 활성화 및 조정 항목을 참조하십시오.

15 장

문제 해결하기

Cisco Jabber 도메인에 대한 SSO 인증서 업데이트

이 절차는 클라우드 또는 하이브리드 구축에 적용됩니다. 이 절차를 사용하여 Cisco Jabber 도메인에 대한 업데이트된 SSO(단일 로그인) 인증서를 업로드합니다.

참고 1024, 2048 또는 4096 암호화 비트 및 RC4-MD5 알고리즘이 있는 인증서만 지원됩니다.

시작하기 전에

인증서는 .CER 또는 .CRT 파일 형식이어야 합니다.

프로시저

단계 **1** https://www.webex.com/go/connectadmin에서 Webex 조직 관리 도구에 로그인합니다.

단계 **2** 관리 도구 로드가 끝나면 구성 탭을 클릭합니다.

단계 **3** 왼쪽 탐색 모음에서 보안 설정을 클릭합니다.

단계 **4** 조직 인증서 관리 링크를 클릭합니다.
이전에 가져온 X.509 인증서가 표시됩니다.

단계 **5** 별칭 필드에 회사의 Cisco Webex 조직을 입력합니다.

단계 **6** 찾아보기를 클릭하고 X.509 인증서로 이동합니다.
인증서는 .CER 또는 .CRT 파일 형식이어야 합니다.

단계 **7** 가져오기를 클릭하여 인증서를 가져옵니다.
인증서가 X.509 인증서에 지정된 형식을 따르지 않는다면 오류가 표시됩니다.

단계 **8** 닫기를 두 번 클릭하여 **SSO** 관련 옵션 화면으로 돌아갑니다.

단계 **9** 저장을 클릭하여 페더레이션된 웹 단일 로그인 구성 상세정보를 저장합니다.

Cisco Jabber 진단 도구

Windows 및 Mac

Cisco Jabber 진단 도구는 다음 기능에 대한 구성 및 진단 정보를 제공합니다.

- 서비스 검색
- Cisco Webex
- Cisco Unified Communications Manager 요약
- Cisco Unified Communications Manager 구성
- 음성 메일
- 인증서 확인
- Active Directory
- DNS 레코드

Cisco Jabber 진단 도구 창에 액세스하려면 허브 창에 포커스를 맞추고 **Ctrl + Shift + D**를 입력해야 합니다. 다시 로드 단추를 클릭하여 데이터를 업데이트할 수 있습니다. 저장 단추를 클릭하여 정보를 html 파일에 저장할 수도 있습니다.

Cisco Jabber 진단 도구는 기본적으로 사용할 수 있습니다. 이 도구를 비활성화하려면 DIAGNOSTICS_TOOL_ENABLED 설치 매개변수를 FALSE로 설정해야 합니다. 이 설치 매개변수에 대한 자세한 내용은 설정에 따라 *Cisco Jabber*의 온 프레미스 구축 또는 *Cisco Jabber*의 클라우드 및 하이브리드 구축을 참조하십시오.

Android, iPhone 및 iPad

사용자가 Cisco Jabber에 로그인할 수 없거나 Cisco Jabber IM 및 전화 서비스가 연결되지 않은 경우, 진단 오류 옵션을 사용하여 문제의 원인을 확인할 수 있습니다.

사용자는 Cisco Jabber 서비스에 연결할 때 로그인 페이지 또는 경고 알림에서 오류 진단 옵션을 누를 수 있습니다. 그러면 Cisco Jabber에서 다음을 확인합니다.

- 네트워크에 문제가 있는지 여부
- Cisco Jabber 서버에 연결할 수 있는지 여부
- Cisco Jabber에 다시 연결할 수 있는지 여부

이 중 하나라도 확인하지 못하면 Cisco Jabber에는 오류 보고서가 가능한 해결책과 함께 표시됩니다. 문제가 지속된다면 문제 보고서를 전송할 수 있습니다.