소프트폰 구성

소프트폰 워크플로 생성

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco Jabber 장치 생성 및 구성, 2 페이지	Cisco Jabber에 액세스하는 모든 사용자에 대해 하나 이상의 장치를 생성합니다. 사용자에게 제공할 인증 문자열을 생성합니다.
단계 **2**	장치에 디렉터리 번호를 추가합니다., 5 페이지	생성하는 각 장치에 디렉터리 번호를 추가합니다.
단계 **3**	사용자를 장치에 연결, 6 페이지	사용자를 디바이스와 연결합니다.
단계 **4**	모바일 SIP 프로파일 생성, 7 페이지.	Cisco Unified Communications Manager 9 릴리스가 있고 모바일 클라이언트에 대해 장치를 구성할 계획이 있다면, 이 작업을 완료하십시오.
단계 **5**	전화기 보안 프로파일 구성, 8 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

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.
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 입력

하는 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 디렉터리 번호를 추가합니다.

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.

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 디바이스와 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.

단계 **1** 사용자를 디바이스와 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) 디바이스 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.

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.

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.

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.