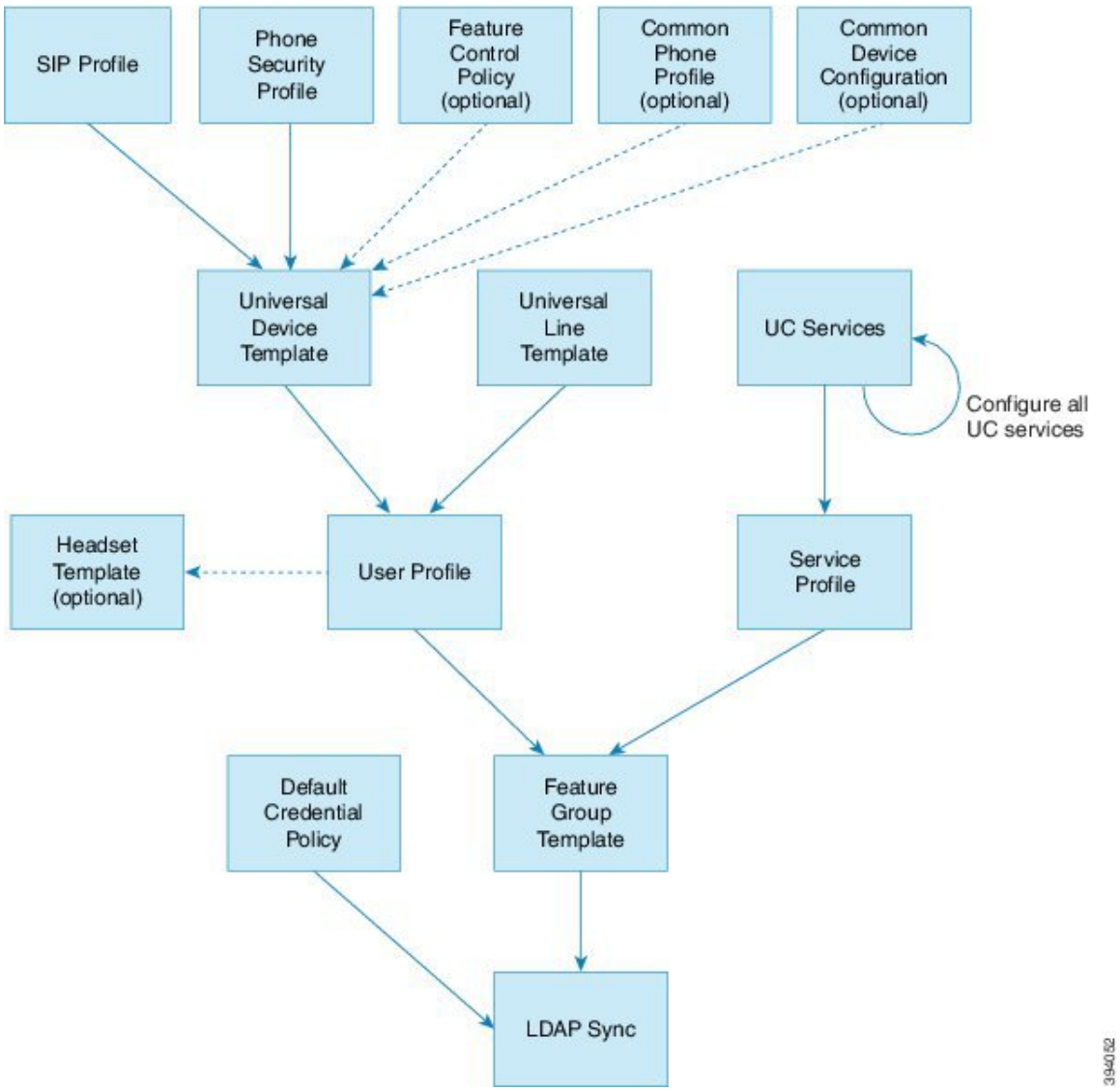
프로비저닝 프로파일 구성

프로비저닝 프로파일 개요

Unified Communications Manager에는 새 사용자에게 할당할 수 있는 일련의 프로파일 및 템플릿이 포함되어 있습니다. 이러한 프로파일 및 일반 설정을 미리 설정한 경우, 새 사용자를 프로비저닝하고 디바이스를 할당할 때는 적용되는 설정에 따라 사용자 및 디바이스가 자동으로 구성됩니다.

사용자를 프로비저닝할 경우, 필요한 설정을 포함하는 사용자 프로파일 및 서비스 프로파일에 사용자를 연결합니다. 또한 사용자에 대한 디바이스를 추가할 때에도, 사용자의 사용자 프로파일에 연결된 범용 회선 및 범용 디바이스 템플릿을 사용하여 디바이스 및 디렉터리 번호가 신속하게 구성됩니다.

다음과 같은 프로파일 및 템플릿을 사용하여 사용자의 필요에 따라 사용자 및 엔드포인트에 일반 설정을 적용할 수 있습니다.



프로비저닝 프로파일 작업 플로우

프로비저닝할 사용자와 디바이스의 수가 대량인 경우, 특정 그룹의 사용자에게 적용되는 템플릿 및 일반 설정을 사용하여 사용자 프로파일 및 서비스 프로파일을 설정하여 구성 프로세스를 단순화할 수 있습니다(예: 고객 지원).

사용자를 프로비저닝할 경우, 필요한 설정을 포함하는 사용자 프로파일 및 서비스 프로파일에 사용자를 연결합니다. 또한 사용자에 대한 디바이스를 추가할 때에도, 사용자의 사용자 프로파일에 연결된 범용 회선 및 범용 디바이스 템플릿을 사용하여 디바이스 및 디렉터리 번호가 신속하게 구성됩니다.

다음과 같은 프로파일 및 템플릿을 사용하여 사용자의 필요에 따라 사용자 및 엔드포인트에 일반 설정을 적용할 수 있습니다.

프로시저

	명령 또는 동작	목적
단계 **1**	SIP 프로파일 구성, 4 페이지	구축하는 SIP 엔드포인트와 연결되는 일반 SIP 설정을 구성합니다.
단계 **2**	전화기 보안 프로파일 구성, 5 페이지	프로비저닝된 엔드포인트에 할당될 보안 프로파일을 구성합니다. TLS 및 TFTP 암호화와 같은 설정을 할당합니다.
단계 **3**	기능 제어 정책 생성, 5 페이지	선택 사항. 이 정책을 사용하여 특정 기능을 활성화하고 전화기 소프트 키의 모양을 조정할 수 있습니다.
단계 **4**	일반 전화기 프로파일 생성, 6 페이지	선택 사항. 이 프로파일을 사용하여 엔드포인트 그룹에 할당할 수 있는 프로파일에 TFTP 데이터 및 제품별 구성 기본값을 할당합니다.
단계 **5**	일반 디바이스 설정 구성, 7 페이지	선택 사항. 이 구성을 사용하여 엔드포인트에 사용자별 설정 및 IPv6 기본 설정을 할당합니다.
단계 **6**	범용 디바이스 템플릿 구성, 8 페이지	이 템플릿에는 새롭게 프로비저닝된 전화기를 구성하는 데 사용되는 일반 설정이 포함되어 있습니다. 이 템플릿에 구성한 프로파일을 할당할 수도 있습니다.
단계 **7**	범용 회선 템플릿 구성, 8 페이지	이 템플릿에는 새롭게 프로비저닝된 내선 번호를 구성하는 데 사용되는 일반 설정이 포함되어 있습니다. 내선 번호에 대해 엔터프라이즈 및 E.164 번호를 구성할 수도 있습니다.
단계 **8**	사용자 프로파일 구성, 9 페이지	새롭게 프로비저닝된 사용자에 대한 디바이스 템플릿, 회선 템플릿 및 일반 설정을 사용하여 사용자 프로파일을 설정합니다.
단계 **9**	헤드셋 템플릿 구성, 10 페이지	선택 사항. Cisco 헤드셋을 사용하여 헤드셋 템플릿을 구성하고 설정된 사용자 프로파일에 할당하려는 경우.
단계 **10**	UC 서비스 구성, 11 페이지	IM and Presence 서비스 및 디렉터리 서비스와 같은 UC 서비스를 구성합니다.
단계 **11**	서비스 프로파일 구성, 12 페이지	프로비저닝된 사용자에게 할당하려는 UC 서비스를 포함하는 서비스 프로파일을 생성합니다.

	명령 또는 동작	목적
단계 **12**	기능 그룹 템플릿 구성, 13 페이지	LDAP 동기화를 위해, 사용자 프로파일 및 서비스 프로파일을 LDAP 동기화 사용자에게 할당할 수 있는 기능 그룹 템플릿에 추가합니다.
단계 **13**	기본 자격 증명 정책 구성, 14 페이지	새롭게 프로비저닝된 사용자에게 할당할 자격 증명 정책을 구성합니다.

다음에 수행할 작업

- LDAP 동기화를 설정하여 새 사용자를 프로비저닝합니다.
- LDAP를 구축하고 있지 않는 경우, 벌크 관리를 사용하여 대량으로 사용자를 프로비저닝할 수 있습니다.

SIP 프로파일 구성

이 절차를 사용하여 SIP 디바이스에 할당할 수 있는 공통 SIP 설정으로 SIP 프로파일을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > **SIP** 프로파일을 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 기존 프로파일을 편집하려면, 찾기를 클릭하고 SIP 프로파일을 선택합니다.
- 새 프로파일을 추가하려면 새로 추가를 클릭합니다.

단계 **3** 프로파일의 이름을 입력합니다.

단계 **4** URI 다이얼링을 구축 중인 경우, 다이얼 문자열 해석을 구성하여 시스템에서 통화를 디렉터리 URI 또는 전화 번호로 처리할지 여부에 대해 시스템에 지시합니다.

단계 **5** 전화기에 사용되는 매개변수에서 DSCP 설정을 완료하여 이 프로파일을 사용하는 통화 유형에 대한 QoS 처리를 정의합니다.

단계 **6** (선택 사항) 정규화 스크립트를 할당해야 하는 경우, 정규화 스크립트 드롭다운 목록에서 기본 스크립트 중 하나를 선택합니다.

참고 스크립트를 직접 만들 수도 있습니다. 자세한 내용은 *Cisco Unified Communications Manager* 기능 구성 설명서를 참조하십시오.

단계 **7** 이 프로 파일에서 IPv4 및 IPv6 스택을 모두 동시에 지원하게 하려는 경우, **AnaT** 활성화 확인란에 체크 표시합니다.

단계 **8** 사용자가 프레젠테이션을 공유할 수 있게 하려는 경우, **BFCP**를 사용하여 프레젠테이션 공유 허용 확인란에 체크 표시합니다.

단계 **9** SIP 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **10** 저장을 클릭합니다.

전화기 보안 프로파일 구성

엔드포인트에 대한 TLS 신호 처리, CAPF 및 다이제스트 인증 요구 사항과 같은 보안 기능을 활성화하려는 경우, 엔드포인트에 적용할 수 있는 새 보안 프로파일을 구성해야 합니다.

참고 프로비저닝된 디바이스에 SIP 전화기 보안 프로파일을 적용하지 않으면, 기본값으로 디바이스에서 비보안 프로파일을 사용합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 보안 > 전화기 보안 프로파일에 체크 표시합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 전화기 보안 프로파일 유형 드롭다운 목록에서 범용 디바이스 템플릿을 선택하여 디바이스 템플릿을 통해 프로비저닝할 때 사용할 수 있는 프로파일을 생성합니다.

참고 선택적으로 특정 디바이스 모델에 대한 보안 프로파일을 만들 수도 있습니다.

단계 **4** 프로토콜을 선택합니다.

단계 **5** 프로파일에 대한 적절한 이름을 이름 필드에 입력합니다.

단계 **6** TLS 신호 처리를 사용하여 디바이스에 연결하려면 디바이스 보안 모드를 인증 또는 암호화로, 전송 유형을 **TLS**로 설정합니다.

단계 **7** (선택 사항) 전화기에서 다이제스트 인증을 사용하려면 **OAuth** 인증 활성화 확인란에 체크 표시합니다.

단계 **8** (선택 사항) 암호화된 TFTP를 사용하려면 **TFTP** 암호화 구성 확인란에 체크 표시합니다.

단계 **9** 전화기 보안 프로파일 구성 창에서 남아 있는 필드를 완료해야 합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **10** 저장을 클릭합니다.

기능 제어 정책 생성

다음 단계에 따라 기능 제어 정책을 만듭니다. 이 정책을 사용하여 특정 기능을 활성화 또는 비활성화하여 전화기에 표시되는 소프트 키의 모양을 조정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 기능 제어 정책을 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- 기존 정책에 대한 설정을 수정하려면 검색 기준을 입력하고 찾기를 클릭하여 결과 목록에서 정책을 선택합니다.
- 새 정책을 추가하려면 새로 추가를 클릭합니다.

기능 제어 정책 구성 창이 표시됩니다.

단계 **3** 이름 필드에 기능 제어 정책의 이름을 입력합니다.

단계 **4** 설명 필드에 기능 제어 정책에 대한 간단한 설명을 입력합니다.

단계 **5** 나열된 각 기능에 대해 기능 제어 섹션에서 시스템 기본값을 재정의할지 여부와 해당 설정을 활성화 또는 비활성화할지 여부를 선택합니다.

- 기능이 기본값으로 활성화되어 있는 경우 이 설정을 비활성화하려면, 기본값 재정의에서 확인란에 체크 표시하고 설정 활성화에서 확인란에 체크 표시를 해제합니다.
- 기능이 기본값으로 비활성화되어 있는 경우 이 설정을 활성화하려면, 기본값 재정의에서 확인란에 체크 표시하고 설정 활성화에서 확인란에 체크 표시합니다.

단계 **6** 저장을 클릭합니다.

일반 전화기 프로파일 생성

일반 전화기 프로파일은 프로파일을 사용하는 전화기에 대한 TFTP 데이터 및 제품별 구성 기본값을 구성하기 위해 사용할 수 있는 선택적 프로파일입니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 전화기 프로파일 메뉴 경로를 선택하여 일반 전화기 프로파일을 구성합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 프로파일의 이름을 입력합니다.

단계 **4** 프로파일에 대한 설명을 입력합니다.

단계 **5** 이 프로파일을 사용하는 전화기에 기능 제어 정책을 설정하는 경우, 드롭다운 목록에서 정책을 선택합니다.

단계 **6** 일반 전화기 프로파일 구성 창에서 나머지 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.

단계 **7** 제품별 구성 레이아웃에서 필드를 구성합니다. 필드 설명의 경우, (?)를 클릭하여 필드별 도움말을 확인합니다.

단계 **8** (선택 사항) 모바일 및 원격 액세스 전화기에 대해 ICE(상호 연결 설정)를 활성화하려는 경우, 다음을 수행합니다.

a) ICE 드롭다운을 활성화 됨으로 설정합니다.

b) 기본 후보 유형을 다음 중 하나로 설정합니다.

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

c) 나머지 ICE 필드를 구성합니다.

단계 **9** 저장을 클릭합니다.

일반 디바이스 설정 구성

일반 디바이스 구성은 사용자별 기능 특성 세트로 이루어집니다. IPv6을 구축하는 경우, 이 구성을 사용하여 SIP 트렁크 또는 SCCP 전화기에 대한 IPv6 기본 설정을 할당할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 디바이스 설정 > 일반 디바이스 구성을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** SIP 트렁크, SIP 전화기 또는 SCCP 전화기의 경우, **IP** 주소 지정 모드 드롭다운 목록에 대한 값을 다음과 같이 선택합니다.

- **IPv4** 전용—디바이스에서 미디어 및 신호 처리에 IPv4 주소만 사용합니다.
- **IPv6** 전용—디바이스에서 미디어 및 신호 처리에 IPv6 주소만 사용합니다.
- **IPv4** 및 **IPv6(**기본값**)**—디바이스는 듀얼 스택 디바이스로 어떤 것이든 사용할 수 있는 IP 주소 유형을 사용합니다. 해당 디바이스에 두 IP 주소 유형이 모두 구성된 경우, 신호 처리를 위해 디바이스에서 신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 설정을 사용하고 미디어를 위해 디바이스에서 미디어를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수를 사용합니다.

단계 **4** 이전 단계에서 IPv6을 구성한 경우, 신호 처리를 위한 **IP** 주소 지정 모드 드롭다운 목록에 대해 IP 주소 지정 기본 설정을 다음과 같이 구성합니다.

- **IPv4** —이중 스택 디바이스는 신호 처리를 위해 IPv4 주소를 선호합니다.
- **IPv6** —이중 스택 디바이스는 신호 처리를 위해 IPv6 주소를 선호합니다.

- 시스템 기본값 사용—신호 처리를 위한 **IP** 주소 지정 모드 기본 설정 엔터프라이즈 매개변수에 대한 설정을 사용합니다.

단계 **5** 일반 디바이스 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 시스템 온라인 도움말을 참조하십시오.

단계 **6** 저장을 클릭합니다.

범용 디바이스 템플릿 구성

범용 디바이스 템플릿을 사용하면 구성 설정을 새로 프로비저닝된 디바이스에 쉽게 적용할 수 있습니다. 프로비저닝된 디바이스는 범용 디바이스 템플릿의 설정을 사용합니다. 서로 다른 사용자 그룹의 요구 사항을 충족하도록 서로 다른 디바이스 템플릿을 구성할 수 있습니다. 이 템플릿에 구성한 프로파일을 할당할 수도 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 디바이스 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 필수 필드인

a) 템플릿에 대한 디바이스 설명을 입력합니다.
b) 드롭다운 목록에서 디바이스 풀을 선택합니다.
c) 드롭다운 목록에서 디바이스 보안 프로파일을 선택합니다.
d) 드롭다운 목록에서 **SIP** 프로파일을 선택합니다.
e) 드롭다운 목록에서 전화기 버튼 템플릿을 선택합니다.

단계 **4** 범용 디바이스 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **5** 전화기 설정 아래에서 다음 옵션 필드를 완성합니다.

a) 일반 전화기 프로파일을 구성한 경우 프로파일을 할당합니다.
b) 일반 디바이스 구성을 구성한 경우 구성을 할당합니다.
c) 기능 제어 정책을 구성한 경우 정책을 할당합니다.

단계 **6** 저장을 클릭합니다.

범용 회선 템플릿 구성

범용 회선 템플릿을 사용하면 새로 할당된 디렉터리 번호에 일반 설정을 쉽게 적용할 수 있습니다. 서로 다른 사용자 그룹의 요구 사항을 충족하도록 서로 다른 템플릿을 구성합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리 > 사용자/전화기 추가 > 범용 회선 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 범용 회선 템플릿 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 대체 번호를 사용하여 전역 다이얼 플랜 복제를 배포하는 경우 엔터프라이즈 대체 번호와 **+E.164** 대체 번호 섹션을 확장하고 다음을 수행합니다.

a) 엔터프라이즈 대체 번호 추가 버튼 및/또는 **+E.164** 대체 번호 추가 버튼을 클릭합니다.

b) 대체 번호에 할당하는 데 사용할 번호 마스크를 추가합니다. 예를 들어, 4자리 내선 번호는 5XXXX를 엔터프라이즈 번호 마스크로 사용하고 1972555XXXX를 +E.164 대체 번호 마스크로 사용할 수 있습니다.

c) 대체 번호를 할당할 파티션을 할당합니다.

d) ILS를 통해 이 번호를 광고하려면 **ILS**를 통해 전역으로 광고 확인란에 체크 표시합니다. 광고된 패턴을 사용하여 대체 번호 범위를 요약하는 경우 개별 대체 번호를 광고할 필요가 없습니다.

e) **PSTN** 페일오버 섹션을 확장하고 일반 콜 라우팅이 실패하는 경우 사용할 PSTN 페일오버으로 엔터프라이즈 번호 또는 **+E.164** 대체 번호를 선택합니다.

단계 **5** 저장을 클릭합니다.

사용자 프로파일 구성

사용자 프로파일을 통해 범용 회선 및 범용 디바이스 템플릿을 사용자에게 할당합니다. 서로 다른 사용자 그룹에 대한 여러 사용자 프로파일을 구성합니다. 이 서비스 프로파일을 사용하는 사용자에 대한 셀프 프로비저닝을 활성화할 수도 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 다음 메뉴를 선택합니다.사용자 관리 > 사용자 설정 > 사용자 프로파일.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 사용자 프로파일의 이름 및 설명을 입력합니다.

단계 **4** 사용자의 데스크폰, 모바일 및 데스크탑 디바이스 및 원격 대상/디바이스 프로파일에 적용할 유니버셜 디바이스 템플릿을 할당합니다.

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

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

a) 최종 사용자에게 자신의 전화기 프로비저닝 허용 확인란을 선택합니다.

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

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

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

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

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

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

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

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

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

단계 **10** 저장을 클릭합니다.

헤드셋 템플릿 구성

이 절차를 사용하여 Cisco 헤드셋에 적용할 수 있는 사용자 지정된 설정으로 헤드셋 템플릿을 구성합니다. 사용자 지정 템플릿을 만들거나 시스템 정의 표준 기본 헤드셋 템플릿을 사용할 수 있습니다.

참고 표준 기본 헤드셋 구성 템플릿은 시스템 정의 템플릿입니다. 표준 기본 헤드셋 템플릿에 새 사용자 프로파일을 할당할 수 있지만 템플릿을 편집할 수는 없습니다. 기본적으로 모든 사용자 프로파일은 이 템플릿에 할당됩니다. 이 템플릿에서 사용자 프로파일의 연결을 해제하려면 프로파일을 새 템플릿에 할당해야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 디바이스 > 헤드셋 > 헤드셋 템플릿을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 기존 템플릿을 편집하려면 템플릿을 선택합니다.
- 새 템플릿을 만들려면 기존 템플릿을 선택하고 복사를 클릭합니다. 기존 설정이 새 템플릿에 적용됩니다.

단계 **3** 템플릿에 대한 이름 및 설명을 추가합니다.

단계 **4** 모델 및 펌웨어 설정] 아래에서 이 템플릿에 적용할 사용자 지정된 헤드셋 설정을 할당합니다. 새 설정을 추가하려면 추가 버튼을 클릭하고 설정을 구성합니다.

단계 **5** 위쪽 및 아래쪽 화살표를 사용하여 이 템플릿에 할당하려는 사용자 프로파일을 할당된 사용자 프로파일 목록 상자로 이동합니다. 해당 프로파일에 할당된 모든 사용자도 이 헤드셋 템플릿에 할당됩니다.

단계 **6** 저장을 클릭합니다.

단계 **7** 기본값으로 설정 버튼을 사용하여 기본 템플릿 설정으로 돌아갑니다.

단계 **8** 구성 적용을 클릭합니다.

표준 기본 헤드셋 구성 템플릿의 경우 구성 적용 버튼이 다음 항목에 적용됩니다.

- 할당된 사용자 프로파일 목록에 추가한 사용자가 소유한 디바이스
- 익명의 디바이스

사용자 지정된 헤드셋 구성 템플릿의 경우 구성 적용 버튼은 할당된 사용자 프로파일 목록에 추가한 사용자가 소유한 디바이스에만 적용됩니다.

UC 서비스 구성

이 절차를 사용하여 사용자가 사용할 UC 서비스 연결을 구성합니다. 다음 UC 서비스에 대한 연결을 구성할 수 있습니다.

- 음성 메일
- 메일 저장소

- 전화회의
- 디렉터리
- IM and Presence Service
- CTI
- 화상 회의 예약 포털
- Jabber 클라이언트 구성(jabber-config.xml)

참고 이 필드는 구성하는 UC 서비스에 따라 달라질 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 사용자 관리>사용자 설정>**UC** 서비스를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** [UC 서비스 유형] 드롭다운에서 구성하려는 UC 서비스를 선택하고 다음을 클릭합니다.

단계 **4** 제품 유형을 선택합니다.

단계 **5** 서비스의 이름을 입력합니다.

단계 **6** 서비스가 홈 인 서버의 호스트네임 또는 **IP** 주소를 입력합니다.

단계 **7** 포트 및 프로토콜 정보를 완료합니다.

단계 **8** 나머지 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오. 필드 옵션은 구축하는 UC 서비스에 따라 달라집니다.

단계 **9** 저장을 클릭합니다.

단계 **10** 필요한 모든 UC 서비스를 프로비저닝할 때까지 이 절차를 반복합니다.

참고 여러 서버에 서비스를 배치하려면 다른 서버를 가리키는 다른 UC 서비스 연결을 구성합니다. 예를 들어, IM and Presence Service 중앙 집중식 구축을 통해 서로 다른 IM 및 Presence 노드를 가리키는 여러 IM Presence UC 서비스를 구성하는 것이 좋습니다. 모든 UC 연결을 구성한 후에는 서비스 프로파일에 추가할 수 있습니다.

서비스 프로파일 구성

프로파일을 사용하는 엔드 유저에 게 할당하려는 UC 서비스를 포함한 서비스 프로파일을 구성합니다.

시작하기 전에

Unified Communications(UC) 서비스를 설정해야만 이들 서비스를 서비스 프로파일에 추가할 수 있습니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자 설정 > 서비스 프로파일을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 선택한 서비스 프로파일 구성에 대한 이름을 입력합니다.

단계 **4** 선택한 서비스 프로파일 구성에 대한 설명을 입력합니다.

단계 **5** 이 프로파일의 일부가 되려는 각 UC 서비스의 경우, 해당 서비스에 대한 기본, 보조 및 **3**차 연결을 할당합니다.

단계 **6** 서비스 프로파일 구성 창에서 나머지 필드를 완료합니다. 자세한 필드 설명은 온라인 도움말을 참조하십시오.

단계 **7** 저장을 클릭합니다.

기능 그룹 템플릿 구성

기능 그룹 템플릿은 프로비저닝된 사용자를 위해 전화기, 회선 및 기능을 신속하게 구성하도록 도와 시스템 구축을 지원합니다. 회사 LDAP 디렉터리에서 사용자를 동기화하는 경우 사용자가 디렉터리에서 동기화할 사용자 프로파일 및 서비스 프로파일을 사용하여 기능 그룹 템플릿을 구성합니다. 이 템플릿을 통해 동기화된 사용자에 대한 IM and Presence Service를 활성화할 수도 있습니다.

프로시저

단계 **1** [Cisco Unified CM 관리]에서 사용자 관리 > 사용자/전화기 추가 > 기능 그룹 템플릿을 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** 기능 그룹 템플릿에 대한 이름 및 설명을 입력합니다.

단계 **4** 이 템플릿을 사용하는 모든 사용자에 대해 로컬 클러스터를 홈 클러스터로 사용하려는 경우 홈 클러스터 확인란을 선택합니다.

단계 **5** 이 템플릿을 사용하는 사용자가 인스턴트 메시징 및 프레전스 정보를 교환하도록 하려면 **Unified CM IM and Presence**에 대해 사용자 활성화 확인란을 선택합니다.

단계 **6** 드롭다운 목록에서 서비스 프로파일 및 사용자 프로파일을 선택합니다.

단계 **7** 기능 그룹 템플릿 구성 창에서 나머지 필드를 완성합니다. 필드 설명은 온라인 도움말을 참조하십시오.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

기능 그룹 템플릿을 LDAP 디렉터리 동기화와 연결하여 템플릿의 설정을 동기화된 최종 사용자에게 적용합니다.

기본 자격 증명 정책 구성

이 절차를 사용하여 새롭게 프로비저닝된 사용자에게 적용되는 클러스터 수준 기본 자격 증명 정책을 구성합니다. 다음과 같은 각각의 자격 증명 유형에 대해 별도의 자격 증명 정책을 적용할 수 있습니다.

- 애플리케이션 사용자 암호
- 엔드 유저 암호
- 엔드 유저 PIN

프로시저

단계 **1** 자격 증명 정책에 대한 설정을 다음과 같이 구성합니다.

a) Cisco Unified CM 관리에서사용자 관리 > 사용자 설정 > 인증서 정책을 선택합니다.
b) 다음 중 하나를 수행합니다.
   - 찾기를 클릭하고 기존 인증서 정책을 선택합니다.
   - 새로 추가를 클릭하여 새 인증서 정책을 생성합니다.
c) 시스템에서 ABCD 또는 123456과 같이 쉽게 해킹되는 암호를 확인할 수 있게 하려는 경우, 단순한 암호 확인 확인란에 체크 표시합니다.
d) 인증서 정책 구성 창에서 필드를 완료합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
e) 저장을 클릭합니다.
f) 다른 자격 증명 유형 중 하나에 대해 다른 자격 증명 정책을 생성하려는 경우, 이러한 단계를 반복합니다.

단계 **2** 다음 자격 증명 유형 중 하나에 자격 증명 정책을 다음과 같이 적용합니다.

a) Cisco Unified CM 관리에서 사용자 관리 > 사용자 설정 > 자격 증명 정책 기본값을 선택합니다.
b) 자격 증명 정책을 적용하려는 자격 증명 유형을 선택합니다.
c) 자격 증명 정책 드롭다운에서 이 자격 증명 유형에 적용하려는 자격 증명 정책을 선택합니다. 예를 들어, 자신이 생성한 자격 증명 정책을 선택할 수 있습니다.
d) 자격 증명 변경 및 자격 증명 확인 필드 모두에 기본 암호를 입력합니다. 사용자는 다음 로그인 시 이러한 암호를 입력해야 합니다.
e) 자격 증명 정책 기본 구성 창에서 나머지 필드를 구성합니다. 필드 및 해당 설정에 대한 도움이 필요한 경우 온라인 도움말을 참조하십시오.
f) 저장을 클릭합니다.

g) 다른 자격 증명 유형 중 하나에 대한 자격 증명 정책을 할당하려는 경우, 이러한 단계를 반복합니다.

참고 개별 사용자의 경우, 해당 사용자에 대한 엔드 유저 구성 창 또는 애플리케이션 사용자 구성 창에서 특정 사용자 자격 증명으로 정책을 할당할 수도 있습니다. 자격 증명 유형(암호 또는 PIN)에 인접한 자격 증명 편집 버튼을 클릭하여 해당 사용자 자격 증명에 대한 자격 증명 구성 설정을 엽니다.