LDAP 디렉터리 구성

- LDAP 동기화 개요, 1 페이지
- LDAP 동기화 필수 조건, 3 페이지
- LDAP 동기화 구성 작업 흐름, 3 페이지

LDAP 동기화 개요

LDAP(Lightweight Directory Access Protocol) 동기화를 사용하면 시스템의 최종 사용자를 프로비저닝하고 구성할 수 있습니다. LDAP 동기화 중 시스템은 외부 LDAP 디렉터리의 사용자 목록 및 관련 사용자 데이터를 Unified Communications Manager 데이터베이스로 가져옵니다. 가져오는 동안 최종 사용자를 구성할 수도 있습니다.

참고 Unified Communications Manager는 LDAPS(SSL이 있는 LDAP)를 지원하지만 StartTLS가 있는 LDAP는 지원하지 않습니다. LDAP 서버 인증서를 Unified Communications Manager에 Tomcat-Trust로 업로드하십시오.

지원되는 LDAP 디렉터리에 대한 정보는 *Cisco Unified Communications Manager* 및 *IM and Presence* 서비스의 호환성 매트릭스를 참조하십시오.

LDAP 동기화는 다음과 같은 기능을 광고합니다.

- 최종 사용자 가져오기—초기 시스템 설정 중에 LDAP 동기화를 사용하여 사용자 목록을 회사 LDAP 디렉토리에서 Unified Communications Manager 데이터베이스로 가져올 수 있습니다. 기능 그룹 템플릿, 사용자 프로파일, 서비스 프로파일, 범용 디바이스 및 회선 템플릿 등의 항목을 미리 구성한 경우에는 사용자에게 구성을 적용하고 동기화 프로세스 중에 구성된 디렉터리 번호와 디렉터리 URI를 할당할 수 있습니다. LDAP 동기화 프로세스는 사용자 및 사용자 특정 데이터 목록을 가져오고 사용자가 설정한 구성 템플릿을 적용합니다.

참고 초기 동기화가 이미 발생한 후에는 LDAP 동기화를 편집할 수 없습니다.

- 예약된 업데이트—예약된 간격으로 여러 LDAP 디렉터리와 동기화하도록 Unified Communications Manager를 구성하여 데이터베이스가 정기적으로 업데이트되고 사용자 데이터가 최신 상태로 유지되도록 할 수 있습니다.
- 최종 사용자 인증—Cisco Unified Communications Manager 데이터베이스가 아닌 LDAP 디렉터리에 대해 최종 사용자 암호를 인증하도록 시스템을 구성할 수 있습니다. LDAP 인증은 회사가 모든 회사 애플리케이션에 대해 최종 사용자에게 단일 암호를 할당하는 기능을 제공합니다. 이 기능은 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.
- **Cisco** 모바일 및 원격 액세스 클라이언트와 엔드포인트에 대한 디렉터리 서버 사용자 검색— 엔터프라이즈 방화벽 외부에서 작동하는 경우에도 회사 디렉터리 서버를 검색할 수 있습니다. 이 기능을 활성화하면 사용자 데이터 서비스(UDS)가 프록시로 작동하고 사용자 검색 요청을 Unified Communications Manager 데이터베이스로 보내는 대신 회사 디렉터리로 보냅니다.

최종 사용자에 대한 **LDAP** 인증

LDAP 동기화를 사용하면 Cisco Unified Communications Manager 데이터베이스가 아닌 LDAP 디렉터리에 대해 최종 사용자 암호를 인증하도록 시스템을 구성할 수 있습니다. LDAP 인증은 회사가 모든 회사 애플리케이션에 대해 최종 사용자에게 단일 암호를 할당하는 기능을 제공합니다. 이 기능은 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.

Cisco 모바일 및 원격 액세스 클라이언트와 엔드포인트에 대한 디렉터리 서버 사용자 검색

이전 릴리스에서는 Cisco 모바일 및 원격 액세스 클라이언트(예: Cisco Jabber) 또는 엔드 포인트(예: Cisco DX 80 전화기)를 사용하는 사용자가 엔터프라이즈 방화벽 외부에서 사용자 검색을 수행했을 때 결과는 Cisco Unified Communications Manager 데이터베이스에 저장되는 해당 사용자 계정을 기반으로했습니다. 데이터베이스에는 로컬로 구성되거나 회사 디렉터리에서 동기화되는 사용자 계정이 포함됩니다.

이번 릴리스에서 Cisco 모바일 및 원격 액세스 클라이언트와 엔드포인트는 엔터프라이즈 방화벽 외부에서 작동하는 경우에도 회사 디렉터리 서버를 검색할 수 있습니다. 이 기능을 활성화하면 사용자 데이터 서비스(UDS)가 프록시로 작동하고 사용자 검색 요청을 Cisco Unified Communications Manager 데이터베이스로 보내는 대신 회사 디렉터리로 보냅니다.

다음 결과를 얻으려면 이 기능을 사용합니다.

- 지리적 위치와 상관없이 동일한 사용자 검색 결과 제공 - 모바일 및 원격 액세스 클라이언트와 엔드포인트는 엔터프라이즈 방화벽 외부에 연결되어 있는 경우에도 회사 디렉터리를 사용하여 사용자 검색을 수행할 수 있습니다.
- Cisco Unified Communications Manager 데이터베이스에 구성된 사용자 계정 수 감소 - 이제 모바일 클라이언트는 회사 디렉터리의 사용자를 검색할 수 있습니다. 이전 릴리스에서는 사용자 검색 결과가 데이터베이스에 구성된 사용자를 기반으로 했습니다. 이제 관리자는 더 이상 사용자 검색을 위해 데이터베이스에 사용자 계정을 구성하거나 동기화할 필요가 없습니다. 관리자는

클러스터가 제공하는 사용자 계정만 구성해야 합니다. 데이터베이스의 총 사용자 계정 수를 줄이면 전체 데이터베이스 성능이 향상되면서 소프트웨어 업그레이드 시간도 단축됩니다.

이 기능을 설정하려면 **LDAP** 검색 설정 창에서 엔터프라이즈 디렉터리 서버에 대한 사용자 검색 활성화 옵션을 활성화하고 LDAP 디렉터리 서버 세부 정보를 설정해야 합니다. 자세한 내용은 엔터프라이즈 디렉터리 사용자 검색 구성, 8 페이지 절차를 참조하십시오.

LDAP 동기화 필수 조건

필수 작업

LDAP 디렉터리에서 최종 사용자를 가져오기 전에 다음 작업을 완료하십시오.

- 사용자 액세스 구성
- 인증서 정책 구성
- 기능 그룹 템플릿 구성

데이터를 시스템에 동기화하려는 사용자의 경우, 활성 디렉터리 서버의 전자 메일 ID 필드가 고유한 항목인지 또는 공백으로 남겨져 있는지 확인하십시오.

LDAP 동기화 구성 작업 흐름

다음 작업을 사용하여 외부 LDAP 디렉터리에서 사용자 목록을 가져와서 Unified Communications Manager 데이터베이스로 가져올 수 있습니다.

참고 이미 LDAP 디렉터리를 한 번 동기화한 경우 외부 LDAP 디렉터리의 새 항목을 계속 동기화할 수 있지만 Unified Communications Manager의 새 구성을 LDAP 디렉터리 동기화에 추가할 수는 없습니다. 이 경우 사용자 업데이트 또는 사용자 삽입과 같은 벌크 관리 도구 및 메뉴를 사용할 수 있습니다. *Cisco Unified Communications Manager* 벌크 관리 설명서를 참조하십시오.

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco DirSync 서비스 활성화, 4 페이지	Cisco Unified 서비스 가용성에 로그인하고 Cisco DirSync 서비스를 활성화합니다.
단계 **2**	LDAP 디렉터리 동기화 활성화, 4 페이지	Unified Communications Manager에서 LDAP 디렉터리 동기화를 활성화합니다.

	명령 또는 동작	목적
단계 3	LDAP 필터 만들기, 5 페이지	선택 사항. Unified Communications Manager가 회사 LDAP 디렉터리의 사용자 하위 집합만 동기화하도록 하려면 LDAP 필터를 만듭니다.
단계 4	LDAP 디렉터리 동기화 구성, 6 페이지	필드 설정, LDAP 서버 위치, 동기화 일정 및 액세스 제어 그룹, 기능 그룹 템플릿 및 기본 내선 번호에 대한 할당과 같은 LDAP 디렉터리 동기화 설정을 구성합니다.
단계 5	엔터프라이즈 디렉터리 사용자 검색 구성, 8 페이지	선택 사항. 엔터프라이즈 디렉터리 서버 사용자 검색을 위해 시스템을 구성합니다. 이 절차에 따라 데이터베이스 대신 엔터프라이즈 디렉터리 서버에 대한 사용자 검색을 수행하도록 시스템의 전화기 및 클라이언트를 구성하십시오.
단계 6	LDAP 인증 구성, 10 페이지	선택 사항. 최종 사용자 암호 인증에 LDAP 디렉터리를 사용하려면 LDAP 인증 설정을 구성합니다.
단계 7	LDAP 계약 서비스 파라미터 사용자 지정, 10 페이지	선택 사항. 선택 사항 LDAP 동기화 서비스 파라미터를 구성합니다. 대부분의 구축의 경우 기본값으로 충분합니다.

Cisco DirSync 서비스 활성화

이 절차를 수행하여 Cisco Unified 서비스 가용성에서 Cisco DirSync 서비스를 활성화하십시오. 회사 LDAP 디렉터리에서 최종 사용자 설정을 동기화하려면 이 서비스를 활성화하십시오.

프로시저

단계 1 Cisco Unified 서비스 가용성에서 도구 > 서비스 활성화를 선택합니다.
단계 2 서버 드롭다운 목록에서 게시자 노드를 선택합니다.
단계 3 디렉터리 서비스 아래에서 **Cisco DirSync** 라디오 버튼을 클릭합니다.
단계 4 저장을 클릭합니다.

LDAP 디렉터리 동기화 활성화

회사 LDAP 디렉터리의 최종 사용자 설정을 동기화하기 위해 Unified Communications Manager를 구성하려는 경우, 이 절차를 수행합니다.

참고 이미 LDAP 디렉터리를 한 번 동기화한 경우 외부 LDAP 디렉터리의 새 사용자를 계속 동기화할 수 있지만 Unified Communications Manager의 새 구성을 LDAP 디렉터리 동기화에 추가할 수는 없습니다. 또한 기능 그룹 템플릿 또는 사용자 프로파일과 같은 기본 구성 항목에 편집을 추가할 수도 없습니다. 한 번의 LDAP 동기화를 이미 완료하고 다른 설정을 사용하여 사용자를 추가하려는 경우, 사용자 업데이트 또는 사용자 삽입과 같은 벌크 관리 메뉴를 사용할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 시스템을 선택합니다.

단계 **2** Cisco Unified Communications Manager가 LDAP 디렉터리에서 사용자를 가져오게 하려는 경우, **LDAP** 서버와 동기화 활성화 확인란을 선택합니다.

단계 **3** **LDAP** 서버 유형 드롭다운 목록에서 회사에서 사용하는 LDAP 디렉터리 서버 유형을 선택합니다.

단계 **4** 사용자 **ID**의 **LDAP** 특성 드롭다운 목록에서 Unified Communications Manager가 최종 사용자 설정 창의 사용자 **ID** 필드에 대해 동기화할 회사 LDAP 디렉터리에서 속성을 선택합니다.

단계 **5** 저장을 클릭합니다.

LDAP 필터 만들기

LDAP 디렉터리에서 사용자의 하위 집합으로 LDAP 동기화를 제한하기 위해 LDAP 필터를 만들 수 있습니다. LDAP 디렉터리에 LDAP 필터를 적용하면 Unified Communications Manager는 LDAP 디렉터리에서 필터와 일치하는 사용자만 가져옵니다.

참고 구성하는 모든 LDAP 필터는 RFC4515에 지정된 LDAP 검색 필터 표준을 준수하십시오.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 필터를 선택합니다.

단계 **2** 새로 추가를 클릭하여 새 LDAP 필터를 만듭니다.

단계 **3** 필터 이름 텍스트 상자에 LDAP 필터의 이름을 입력합니다.

단계 **4** 필터 텍스트 상자에 필터를 입력합니다. 필터에는 최대 1024자의 UTF-8 문자를 사용할 수 있으며 괄호 ()로 묶어 주어야 합니다.

단계 **5** 저장을 클릭합니다.

LDAP 디렉터리 동기화 구성

이 절차를 사용하여 LDAP 디렉터리와 동기화하도록 Unified Communications Manager를 구성합니다. LDAP 디렉터리 동기화를 사용하면 최종 사용자 데이터를 외부 LDAP 디렉터리에서 Unified Communications Manager 데이터베이스로 가져와 최종 사용자 구성 창에 표시할 수 있습니다. 범용 회선 및 장치 템플릿을 사용 하는 설정 기능 그룹 템플릿이 있는 경우 새로 프로비저닝된 사용자 및 해당 내선 번호에 대한 설정을 자동으로 할당할 수 있습니다.

팁 액세스 제어 그룹 또는 기능 그룹 템플릿을 할당하는 경우 LDAP 필터를 사용하여 동일한 구성 요구 사항을 가진 사용자 그룹으로 가져오기를 제한할 수 있습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 다음 단계 중 하나를 수행합니다.

- 찾기를 클릭하고 기존 LDAP 디렉터리를 선택합니다.
- 새로 추가를 클릭하여 새 LDAP 디렉터리를 만듭니다.

단계 **3** **LDAP** 디렉터리 구성에서 다음을 입력합니다.

a) **LDAP** 구성 이름 필드에서 LDAP 디렉터리에 고유한 이름을 할당합니다.
b) **LDAP** 관리자 고유 이름 필드에 LDAP 디렉터리 서버에 액세스할 수 있는 사용자 ID를 입력합니다.
c) 암호 세부 정보를 입력하고 확인합니다.
d) [**LDAP** 사용자 검색 공간] 필드에 검색 공간 세부 정보를 입력합니다.
e) [사용자 사용자에 대한 **LDAP** 사용자 정의 필터] 필드에서 사용자만 또는 사용자 및 그룹 중 하나를 선택합니다.
f) (선택 사항) 가져 오기를 특정 프로파일을 충족하는 사용자의 하위 집합으로만 제한하려는 경우 그룹에 대한 **LDAP** 사용자 정의 필터 드롭다운 목록에서 LDAP 필터를 선택합니다.

단계 **4** **LDAP** 디렉터리 동기화 일정 필드에서 Unified Communications Manager가 데이터를 외부 LDAP 디렉터리와 동기화하는 데 사용하는 일정을 만듭니다.

단계 **5** 동기화할 표준 사용자 필드 섹션을 완성합니다. 각 최종 사용자 필드에 대한 LDAP 특성을 선택합니다. 동기화 프로세스는 Unified Communications Manager의 최종 사용자 필드에 LDAP 특성의 값을 할당합니다.

단계 **6** URI 다이얼을 배포 하는 경우 사용자의 기본 디렉터리 URI 주소에 사용 될 LDAP 특성을 할당 하십시오.

단계 **7** 동기화 할 사용자 정의 사용자 필드 섹션에서 필수 LDAP 특성을 사용하여 사용자 정의 사용자 필드 이름을 입력합니다.

단계 **8** 가져온 최종 사용자를 모든 가져온 최종 사용자에 공통된 액세스 제어 그룹에 할당하려면 다음을 수행하십시오.

a) 액세스 제어 그룹에 추가를 클릭합니다.

b) 팝업 창에서 가져온 최종 사용자에게 할당할 각 액세스 제어 그룹에 해당하는 확인란을 클릭합니다.

c) 선택한 항목 추가를 클릭합니다.

단계 **9** 기능 그룹 템플릿을 할당하려면 기능 그룹 템플릿 드롭다운 목록에서 해당 템플릿을 선택합니다.

참고 최종 사용자는 사용자가 없을 때만 처음으로 할당된 기능 그룹 템플릿과 동기화됩니다. 기존 기능 그룹 템플릿이 수정되고 연결된 LDAP에 대해 전체 동기화가 수행되는 경우 수정 사항이 업데이트되지 않습니다.

단계 **10** 가져온 전화 번호에 마스크를 적용하여 기본 내선 번호를 할당하려면 다음을 수행하십시오.

a) 동기화된 전화 번호에 마스크를 적용하여 삽입된 사용자에 대한 새 회선 만들기 확인란을 선택합니다.

b) 마스크를 입력합니다. 예를 들어, 가져온 전화 번호가 8889945인 경우 11XX의 마스크는 기본 내선 번호 1145를 만듭니다.

단계 **11** 디렉터리 번호 풀에서 기본 내선 번호를 할당하려면 다음을 수행하십시오.

a) 동기화된 **LDAP** 전화 번호를 기준으로 새 회선이 만들어지지 않은 경우 풀 목록에서 새 회선 할당 확인란을 선택합니다.

b) **DN** 풀 시작 및 **DN** 풀 끝 텍스트 상자에 기본 내선 번호를 선택할 수 있는 디렉터리 번호의 범위를 입력합니다.

단계 **12** (선택사항) Jabber 엔드포인트 프로비저닝 섹션에서 Jabber 장치를 생성하려는 경우 다음 드롭다운에서 자동 프로비저닝에 필요한 Jabber 장치 중 하나를 선택합니다:

- Android용 Cisco 이중 모드(BOT)
- iPhone용 Cisco 이중 모드(TCT)
- 태블릿용 Cisco Jabber(TAB)
- Cisco Unified 클라이언트 서비스 프레임워크(CSF)

참고 **LDAP**에 다시 쓰기 옵션을 사용하면 Unified CM에서 선택한 기본 DN을 LDAP 서버에 다시 쓸 수 있습니다. 다시 쓰기에 사용할 수 있는 LDAP 특성은 **telephoneNumber**, **ipPhone** 및 **mobile**입니다.

단계 **13** **LDAP** 서버 정보 섹션에 LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **14** TKS를 사용하여 LDAP 서버에 대한 보안 연결을 생성하려면 **TLS** 사용 확인란을 선택합니다.

참고 Tomcat을 다시 시작한 후 보안 포트를 통해 사용자를 동기화하려고 하면 사용자가 동기화되지 않는 경우가 있습니다. 사용자 동기화가 성공적으로 이루어지려면 Cisco DirSync 서비스를 다시 시작해야 합니다.

단계 **15** 저장을 클릭합니다.

단계 **16** LDAP 동기화를 완료 하려면 지금 전체 동기화 수행을 클릭합니다. 그렇지 않으면 예약된 동기화를 기다릴 수 있습니다.

참고 LDAP에서 사용자를 삭제 하면 24 시간 후에 자동으로 Unified Communications Manager에서 해당 사용자가 제거 됩니다. 뿐만 아니라, 삭제 된 사용자가 다음 장치 중 하나에 대한 이동성 사용자로 구성된 경우 이러한 비활성 장치도 자동으로 삭제 됩니다.

- 원격 대상 프로파일
- 원격 대상 프로파일 템플릿
- 모바일 스마트 클라이언트
- CTI 원격 디바이스
- Spark 원격 디바이스
- Nokia S60
- iPhone용 Cisco 이중 모드
- IMS 통합 모바일(기본)
- 통신사업자 통합 모바일
- Android용 Cisco 이중 모드

엔터프라이즈 디렉터리 사용자 검색 구성

이 절차를 사용하여 데이터베이스 대신 엔터프라이즈 디렉터리 서버에 대한 사용자 검색을 수행하도록 시스템의 전화기 및 클라이언트를 구성하십시오.

시작하기 전에

- LDAP 사용자 검색을 위해 선택하는 1차, 2차 및 3차 서버가 Unified Communications Manager 가입자 노드에 연결할 수 있는 네트워크인지 확인하십시오.
- 시스템 > **LDAP** > **LDAP** 시스템에서 **LDAP** 시스템 설정 창의 **LDAP** 서버 유형 드롭다운 목록에서 LDAP 서버 유형을 설정합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 검색을 선택합니다.

단계 **2** 엔터프라이즈 LDAP 디렉터리 서버를 사용하여 사용자 검색을 수행할 수있도록 하려면 엔터프라이즈 디렉터리 서버에 대한 사용자 검색 활성화 확인란을 선택합니다.

단계 **3** **LDAP** 검색 구성 창에서 필드를 구성합니다. 필드 및 해당 구성 옵션에 대한 자세한 내용은 온라인 도움말을 참조하십시오.

단계 **4** 저장을 클릭합니다.

참고 OpenLDAP 서버에서 회의실 객체로 표시된 회의실을 검색하려면 사용자 지정 필터를 (objectClass=intOrgPerson)(objectClass=rooms))로 구성합니다. 따라서 Cisco Jabber 클라이언트가 이름으로 회의실을 검색하고 회의실과 연결된 번호로 전화를 걸 수 있습니다.

회의실 객체에 대해 OpenLDAP 서버에 **givenName** or **sn** or **mail** or **displayName** 또는 **telephonenumber** 특성이 구성된 경우 회의실을 검색할 수 있습니다.

디렉터리 서버의 UDS 검색을 위한 LDAP 특성

다음 표에는 엔터프라이즈 디렉터리 서버에 대한 사용자 검색 활성화 옵션을 사용할 때 UDS 사용자 검색 요청에서 사용하는 LDAP 특성이 나열되어 있습니다. 이러한 유형의 디렉터리 요청의 경우 UDS는 프록시 역할을 수행하고 검색 요청을 회사 디렉터리 서버로 릴레이합니다.

참고 UDS 사용자 응답 태그는 LDAP 특성 중 하나에 매핑될 수 있습니다. 특성 매핑은 **LDAP** 서버 유형 드롭다운 목록에서 선택한 옵션에 따라 결정됩니다. 시스템 > **LDAP** > **LDAP** 시스템 구성 창에서 이 드롭다운 목록에 액세스합니다.

UDS 사용자 응답 태그	**LDAP** 특성
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail

UDS 사용자 응답 태그	LDAP 특성
directoryUri	• msRTCSIP-primaryuseraddress • mail
department	• department • departmentNumber
관리자	관리자
title	title
pager	pager

LDAP 인증 구성

회사 LDAP 디렉터리에 할당된 암호에 대해 최종 사용자 암호가 인증되도록 LDAP 인증을 활성화하려면 이 절차를 수행하십시오. 이 구성은 최종 사용자 암호에만 적용되며 최종 사용자 PIN 또는 애플리케이션 사용자 암호에는 적용되지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 인증을 선택합니다.

단계 **2** 사용자 인증에 LDAP 디렉터리를 사용하려면 최종 사용자에 대한 **LDAP** 인증 확인란을 선택합니다.

단계 **3** **LDAP** 관리자 고유 이름 필드에 LDAP 디렉터리에 대한 액세스 권한이 있는 LDAP 관리자의 사용자 ID를 입력합니다.

단계 **4** 암호 확인 필드에 LDAP 관리자의 암호를 입력합니다.

단계 **5** [**LDAP** 사용자 검색 기준] 필드에 검색 조건을 입력합니다.

단계 **6** **LDAP** 서버 정보 섹션에 LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.

단계 **7** TKS를 사용하여 LDAP 서버에 대한 보안 연결을 생성하려면 **TLS** 사용 확인란을 선택합니다.

단계 **8** 저장을 클릭합니다.

다음에 수행할 작업

LDAP 계약 서비스 파라미터 사용자 지정, 10 페이지

LDAP 계약 서비스 파라미터 사용자 지정

LDAP 계약에 대한 시스템 수준 설정을 사용자 지정하는 서비스 파라미터를 구성하려면 이 절차를 수행하십시오. 이러한 서비스 파라미터를 구성하지 않을 경우 Unified Communications Manager는

LDAP 디렉터리 통합에 대한 기본 설정을 적용합니다. 파라미터에 대한 설명을 보려면 사용자 인터페이스에서 파라미터 이름을 클릭합니다.

서비스 파라미터를 사용하여 아래 설정을 사용자 지정할 수 있습니다.

- 계약의 최대 수—기본값은 20입니다.
- 최대 호스트 수—기본값은 3입니다.
- 호스트 장애 발생 시 재시도 지연**(**초**)**—호스트 장애의 기본값은 5입니다.
- **HotList** 장애 발생 시 재시도 지연**(**분**)**—hostlist 실패의 기본값은 10입니다.
- **LDAP** 연결 시간 초과**(**초**)**—기본값은 5입니다.
- 지연된 동기화 시작 시간**(**분**)**—기본값은 5입니다.
- 사용자 고객 맵 감사 시간

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > 서비스 파라미터를 선택합니다.
단계 **2** 서버 드롭다운 목록 상자에서 게시자 노드를 선택합니다.
단계 **3** 서비스 드롭다운 목록 상자에서 **Cisco DirSync**를 선택합니다.
단계 **4** Cisco DirSync 서비스 파라미터 값을 구성합니다.
단계 **5** 저장을 클릭합니다.

LDAP 디렉터리 서비스 파라미터

서비스 파라미터	설명
계약의 최대 수	구성할 수 있는 LDAP 디렉터리의 최대 수입니다. 기본 설정은 20입니다.
호스트의 최대 수	장애 조치를 위해 구성할 수 있는 LDAP 호스트 이름의 최대 수입니다. 기본값은 3입니다.
호스트 오류시 재시도 지연(초)	호스트 오류가 발생한 후 Cisco Unified Communications Manager가 첫 번째 LDAP 서버 (호스트 이름)에 대한 연결을 재시도하기까지 지연되는 시간(초)입니다. 기본값은 5입니다.
호스트 목록 오류 시 재시도 지연(분)	호스트 목록 오류가 발생한 후 Cisco Unified Communications Manager가 구성된 모든 LDAP 서버(호스트 이름)를 재시도하기까지 지연되는 시간(분)입니다. 기본값은 10입니다.

서비스 파라미터	설명
LDAP 연결 시간 초과(초)	Cisco Unified Communications Manager가 LDAP 연결을 설정할 때 허용하는 시간(초)입니다. LDAP 서비스 공급자는 지정된 시간 내에 연결을 설정할 수 없는 경우 연결 시도를 중단합니다. 기본값은 5입니다.
지연된 동기화 시작 시간(분)	Cisco DirSync 서비스가 시작된 후 디렉터리 동기화 프로세스를 시작할 때 Cisco Unified Communications Manager가 지연되는 시간(분)입니다. 기본값은 5입니다.

LDAP 동기화된 사용자를 로컬 사용자로 변환

LDAP 동기화된 최종 사용자의 경우 LDAP 디렉터리를 Cisco Unified Communications Manager와 동기화할 때 LDAP 동기화된 사용자를 로컬 사용자로 변환하지 않으면 최종 사용자 구성 창의 필드를 편집할 수 없습니다.

최종 사용자 구성 창에서 LDAP 동기화된 필드를 편집하려면 사용자를 로컬 사용자로 변환합니다. 그러나 이 변환을 수행하면 Cisco Unified Communications Manager가 LDAP 디렉터리와 동기화될 때 최종 사용자가 업데이트되지 않습니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 최종 사용자 > 최종 사용자 관리를 선택합니다.

단계 **2** 찾기를 클릭하고 최종 사용자를 선택합니다.

단계 **3** 로컬 사용자로 변환 버튼을 클릭합니다.

단계 **4** 최종 사용자 구성 창을 업데이트합니다.

단계 **5** 저장을 클릭합니다.

액세스 제어 그룹에 LDAP 동기화된 사용자 할당

이 절차를 수행하여 액세스 제어 그룹에 LDAP 동기화된 사용자를 할당합니다.

시작하기 전에

Cisco Unified Communications Manager는 최종 사용자가 외부 LDAP 디렉터리와 동기화하도록 구성되어야 합니다.

프로시저

단계 **1** Cisco Unified CM 관리에서 시스템 > **LDAP** > **LDAP** 디렉터리를 선택합니다.

단계 **2** 찾기를 클릭하고 구성된 LDAP 디렉터리를 선택합니다.

단계 **3** 액세스 제어 그룹에 추가 버튼을 클릭합니다.

단계 **4** 이 LDAP 디렉터리에서 최종 사용자에 적용하려는 액세스 제어 그룹을 선택합니다.

단계 **5** 선택한 항목 추가를 클릭합니다.

단계 **6** 저장을 클릭합니다.

단계 **7** 전체 동기화 수행을 클릭합니다.

Cisco Unified Communications Manager가 외부 LDAP 디렉터리와 동기화하고 동기화된 사용자를 올바른 액세스 제어 그룹에 삽입합니다.

참고 처음으로 액세스 제어 그룹을 추가할 때만 동기화된 사용자가 선택된 액세스 그룹에 삽입됩니다. 이후에 LDAP에 추가하는 그룹은 전체 동기화를 수행한 후 동기화된 사용자에게 적용되지 않습니다.

XMPP 클라이언트에서 연락처를 검색하기 위한 LDAP 디렉터리 통합

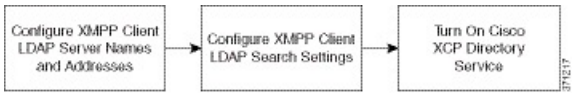
이 항목에서는 타사 XMPP 클라이언트 사용자가 LDAP 디렉터리에서 연락처를 검색 및 추가할 수 있도록 IM and Presence 서비스에서 LDAP 설정을 구성하는 방법에 대해 설명합니다.

IM and Presence 서비스의 JDS 구성 요소는 타사 XMPP 클라이언트와 LDAP 디렉터리의 통신을 처리합니다. 타사 XMPP 클라이언트는 IM and Presence 서비스의 JDS 구성 요소에 쿼리를 전송합니다. JDS 구성 요소는 프로비저닝된 LDAP 서버로 LDAP 쿼리를 전송한 다음 XMPP 클라이언트로 결과를 다시 전송합니다.

여기에 설명된 구성을 수행하기 전에 XMPP 클라이언트를 Cisco Unified Communications Manager 및 IM and Presence 서비스와 통합하기 위한 구성을 수행하십시오. 타사 XMPP 클라이언트 애플리케이션 통합과 관련된 항목을 참조하십시오.

그림 ***1: XMPP*** 클라이언트에서 연락처를 검색하기 위한 ***LDAP*** 디렉터리 통합 워크플로

다음 워크플로 다이어그램은 XMPP 클라이언트에서 연락처를 검색할 수 있도록 LDAP 디렉터리를 통합하는 간단한 단계를 보여줍니다.



다음 표에는 XMPP 클라이언트에서 연락처를 검색할 수 있도록 LDAP 디렉터리를 통합하기 위해 수행해야 할 작업이 나열되어 있습니다. 자세한 지침은 관련 작업을 참조하십시오.

표 *1: XMPP* 클라이언트에서 연락처를 검색하기 위한 *LDAP* 디렉터리 통합의 작업 목록

작업	설명
XMPP 클라이언트 LDAP 서버 이름 및 주소 구성	SSL을 활성화하고 LDAP 서버와 IM and Presence 서비스 간 보안 연결을 설정한 경우 루트 CA 인증서를 xmpp-trust-certificate로서 IM and Presence 서비스에 업로드하십시오. 팁 인증서의 제목 CN은 LDAP 서버의 FQDN과 일치해야 합니다.
XMPP 클라이언트 LDAP 검색 설정 구성	IM and Presence 서비스에서 타사 XMPP 클라이언트에 대해 연락처를 성공적으로 검색하도록 하려면 LDAP 검색 설정을 지정해야 합니다. 기본 LDAP 서버 하나와 백업 LDAP 서버 최대 2개를 지정할 수 있습니다. 팁 선택적으로 LDAP 서버에서 vCards를 검색하는 기능을 설정하거나 IM and Presence 서비스의 로컬 데이터베이스에 vCards를 저장하도록 허용할 수 있습니다.
Cisco XCP 디렉터리 서비스 설정	타사 XMPP 클라이언트의 사용자가 LDAP 디렉터리에서 연락처를 검색 및 추가하도록 허용하려면 XCP 디렉터리 서비스를 설정해야 합니다. 팁 타사 XMPP 클라이언트의 LDAP 서버 및 LDAP 검색 설정을 구성하기 전에는 Cisco XCP 디렉터리 서비스를 설정하지 마십시오. 그렇지 않으면 서비스 실행이 중단될 수 있습니다.

LDAP 계정 잠금 문제

타사 XMPP 클라이언트에 대해 구성한 LDAP 서버에 잘못된 암호를 입력하고 IM and Presence 서비스에 대해 XCP 서비스를 다시 시작하면, JDS 구성 요소는 잘못된 암호로 LDAP 서버에 여러 번 로그인을 시도하게 됩니다. 허용된 실패 횟수 이후 계정을 잠그도록 LDAP 서버가 구성된 경우 LDAP 서버는 특정 시점에 JDS 구성 요소를 잠글 수 있습니다. JDS 구성 요소가 LDAP에 연결된 다른 애플리케이션과 동일한 자격 증명을 사용하는 경우(애플리케이션이 반드시 IM and Presence 서비스에 있어야 하는 것은 아님), 이러한 애플리케이션도 LDAP에서 잠기게 됩니다.

이 문제를 해결하려면 기존 LDAP 사용자와 동일한 역할과 권한을 보유한 별도의 사용자를 구성하고, 이 두 번째 사용자로는 JDS에만 로그인하도록 구성하십시오. LDAP 서버에 잘못된 암호를 입력하면 LDAP 서버에서 JDS 구성 요소만 잠깁니다.

XMPP 클라이언트의 LDAP 서버 이름 및 주소 구성

SSL(Secured Sockets Layer)을 활성화하기로 선택한 경우, LDAP 서버와 IM and Presence 서비스 간 보안 연결을 구성하고 루트 CA(인증 기관) 인증서를 cup-xmpp-trust 인증서로서 IM and Presence 서비스에 업로드하십시오. 인증서의 제목 CN(공통 이름)은 LDAP 서버의 FQDN(정규화된 도메인 이름)과 일치해야 합니다.

인증서 체인(루트 노드에서 신뢰할 수 있는 노드로 하나 이상의 인증서)을 가져오는 경우 리프 노드를 제외한 체인의 모든 인증서를 가져오십시오. 예를 들어 CA가 LDAP 서버에 대한 인증서에 서명하는 경우, CA 인증서만 가져오고 LDAP 서버에 대한 인증서는 가져오지 마십시오.

IM and Presence 서비스와 Cisco Unified Communications Manager 간의 연결이 IPv4이더라도 IPv6을 사용하여 LDAP 서버에 연결할 수 있습니다. IM and Presence 서비스 노드에서 엔터프라이즈 파라미터 또는 ETH0에 대해 IPv6이 비활성화되면, 타사 XMPP 클라이언트에 대해 구성된 외부 LDAP 서버의 호스트 이름이 확인 가능한 IPv6 주소인 경우 해당 노드에서는 여전히 내부 DNS 쿼리를 수행하고 외부 LDAP 서버에 연결할 수 있습니다.

팁 타사 XMPP 클라이언트에 대한 외부 LDAP 서버의 호스트 이름은 **LDAP** 서버 - 타사 **XMPP** 클라이언트 창에서 구성합니다.

시작하기 전에

LDAP 디렉터리의 호스트 이름 또는 IP 주소를 확인합니다.

IPv6을 사용하여 LDAP 서버에 연결하는 경우 LDAP 서버를 구성하기 전에 구축의 각 IM and Presence 서비스 노드에서 엔터프라이즈 파라미터와 Eth0에 대해 IPv6을 활성화합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리애플리케이션 > 타사 클라이언트 > 타사 **LDAP** 서버를 선택합니다.

단계 **2** 새로 추가를 클릭합니다.

단계 **3** LDAP 서버의 ID를 입력합니다.

단계 **4** LDAP 서버의 호스트 이름을 입력합니다.

IPv6 연결의 경우 LDAP 서버의 IPv6 주소를 입력할 수 있습니다.

단계 **5** TCP 또는 SSL 연결을 수신 대기하는 LDAP 서버에서 포트 번호를 지정합니다.

기본 포트는 389입니다. SSL를 활성화할 경우 포트 636을 지정합니다.

단계 **6** LDAP 서버의 사용자 이름과 암호를 지정합니다. 이러한 값은 LDAP 서버에서 구성하는 자격 증명과 일치해야 합니다.

자세한 내용은 LDAP 디렉터리 설명서 또는 LDAP 디렉터리 구성 안내서를 참조하십시오.

단계 **7** LDAP 서버와 통신하는 데 SSL을 사용하려면 **SSL** 활성화를 선택합니다.

참고 SSL이 활성화된 경우 사용자가 입력하는 호스트 이름 값은 LDAP 서버의 호스트 이름이거나 FQDN일 수 있습니다. 사용되는 값은 보안 인증서 **CN** 또는 **SAN** 필드의 값과 일치해야 합니다.

IP 주소를 사용해야 하는 경우 이 값을 **CN** 또는 **SAN** 필드에 대한 인증서에도 사용해야 합니다.

단계 **8** 저장을 클릭합니다.

단계 **9** 클러스터의 모든 노드에서 Cisco XCP 라우터 서비스를 시작합니다(아직 실행되고 있지 않은 경우).

팁

- SSL을 활성화하면 IM and Presence 서비스에서 SSL 연결을 설정한 후 SSL 연결 설정 시 협상 절차 및 데이터 암호화/암호 해독 때문에 XMPP 연락처 검색이 느려질 수 있습니다. 그 결과 사용자가 구축에서 XMPP 연락처 검색을 폭넓게 수행하면 전반적인 시스템 성능에 영향이 미칠 수 있습니다.
- LDAP 서버에 대한 인증서를 업로드한 후 LDAP 서버 호스트 이름 및 포트 값 전달 상태를 확인하려면 인증서 가져오기 도구를 사용할 수 있습니다. **Cisco Unified CM IM and Presence** 관리 시스템 > 보안 > 인증서 가져오기 도구를 선택합니다.
- 타사 XMPP 클라이언트용 LDAP 서버 구성을 업데이트한 경우 Cisco XCP 디렉터리 서비스를 다시 시작하십시오. 이 서비스를 다시 시작하려면 **Cisco Unified IM and Presence** 서비스 가능성 > 도구 > 제어 센터 - 기능 서비스를 선택합니다.

다음에 수행할 작업

계속 진행하여 XMPP 클라이언트용 LDAP 검색 설정을 구성합니다.

XMPP 클라이언트용 LDAP 검색 설정 구성

IM and Presence 서비스에서 타사 XMPP 클라이언트에 대해 연락처를 성공적으로 검색하도록 하려면 LDAP 검색 설정을 지정해야 합니다.

타사 XMPP 클라이언트는 검색 단위로 LDAP 서버에 연결됩니다. 기본 서버에 대한 연결이 실패하면 XMPP 클라이언트는 첫 번째 백업 LDAP 서버를 시도하고, 해당 서버를 사용할 수 없는 경우 두 번째 백업 서버를 시도하는 방식으로 진행합니다. 시스템 장애 조치 중에 LDAP 쿼리가 진행 중이면, 사용 가능한 다음 서버가 이 LDAP 쿼리를 완료합니다.

선택적으로 LDAP 서버에서 vCard 검색 기능을 사용하도록 설정할 수 있습니다. vCard 검색을 설정하면:

- 회사 LDAP 디렉터리는 vCard를 저장합니다.
- XMPP 클라이언트가 자체 vCard 또는 연락처용 vCard를 검색하면, vCard는 JDS 서비스를 통해 LDAP에서 검색됩니다.
- 클라이언트는 회사 LDAP 디렉터리를 편집할 권한이 없으므로 자체 vCard를 설정하거나 수정할 수 없습니다.

LDAP 서버에서 vCard의 검색을 해제하면:

- IM and Presence 서비스는 로컬 데이터베이스에 vCard를 저장합니다.
- XMPP 클라이언트가 자체 vCard 또는 연락처용 vCard를 검색하면, vCard는 로컬 IM and Presence 서비스 데이터베이스에서 검색됩니다.
- 클라이언트는 자체 vCard를 설정하거나 수정할 수 있습니다.

다음 표에는 XMPP 클라이언트용 LDAP 검색 설정이 나열되어 있습니다.

표 *2: XMPP* 클라이언트용 *LDAP* 검색 설정

필드	설정
LDAP 서버 유형	이 목록에서 LDAP 서버 유형을 선택합니다. • Microsoft Active Directory • 일반 디렉터리 서버 - 지원되는 다른 LDAP 서버 유형(iPlanet, Sun ONE 또는 OpenLDAP)을 사용 중인 경우 이 메뉴를 선택합니다.
사용자 객체 클래스	LDAP 서버 유형에 맞는 사용자 객체 클래스 값을 입력합니다. 이 값은 LDAP 서버에 구성된 사용자 객체 클래스 값과 일치해야 합니다. Microsoft Active Directory를 사용하는 경우 기본값은 'user'입니다.
기본 컨텍스트	LDAP 서버에 맞는 기본 컨텍스트를 입력합니다. 이 값은 LDAP 서버에서 전에 구성한 도메인 및/또는 조직 구조와 일치해야 합니다.
사용자 속성	LDAP 서버 유형에 맞는 사용자 속성 값을 입력합니다. 이 값은 LDAP 서버에 구성된 사용자 속성 값과 일치해야 합니다. Microsoft Active Directory를 사용하는 경우 기본값은 sAMAccountName입니다. 디렉터리 URI IM 주소 체계가 사용되며 디렉터리 URI가 mail 또는 msRTCSIPPrimaryUserAddress로 매핑되는 경우, 사용자 속성으로 mail 또는 msRTCSIPPrimaryUserAddress를 지정해야 합니다.
LDAP 서버 1	기본 LDAP 서버를 선택합니다.
LDAP 서버 2	(선택 사항) 백업 LDAP 서버를 선택합니다.
LDAP 서버 3	(선택 사항) 백업 LDAP 서버를 선택합니다.

시작하기 전에

XMPP 클라이언트용 LDAP 서버의 이름과 주소를 지정합니다.

프로시저

단계 **1** **Cisco Unified CM IM and Presence** 관리애플리케이션 > 타사 클라이언트 > 타사 **LDAP** 설정을 선택합니다.

단계 **2** 필드에 정보를 입력합니다.

단계 **3** 사용자가 연락처에 대한 vCard를 요청하고 LDAP 서버에서 vCard 정보를 검색하도록 하려면 **LDAP** 에서 **vCards** 빌드를 선택합니다. 사용자가 연락처 목록에 추가될 때 클라이언트에서 사용자에 대한 vCard를 자동으로 요청하도록 하려면 이 확인란을 선택하지 않습니다. 이 경우 클라이언트는 로컬 IM and Presence 서비스 데이터베이스에서 vCard 정보를 검색합니다.

단계 **4** vCard FN 필드를 구성하는 데 필요한 LDAP 필드를 입력합니다. 사용자가 연락처의 vCard를 요청하면 클라이언트는 vCard FN 필드의 값을 사용하여 연락처 목록에 있는 연락처의 이름을 표시합니다.

단계 **5** 검색 가능한 LDAP 속성 테이블에서 클라이언트 사용자 필드를 LDAP 사용자 필드에 매핑합니다.

Microsoft Active Directory를 사용하는 경우 IM and Presence 서비스는 테이블의 기본 속성 값을 채웁니다.

단계 **6** 저장을 클릭합니다.

단계 **7** Cisco XCP 라우터 서비스를 시작합니다(아직 실행되고 있지 않은 경우).

팁 타사 XMPP 클라이언트용 LDAP 검색 구성으로 업데이트한 경우 Cisco XCP 디렉터리 서비스를 다시 시작하십시오. 이 서비스를 다시 시작하려면 **Cisco Unified IM and Presence** 서비스 가능성 > 도구 > 제어 센터 - 기능 서비스를 선택합니다.

다음에 수행할 작업

계속 진행하여 Cisco XCP 디렉터리 서비스를 설정합니다.

Cisco XCP 디렉터리 서비스 설정

타사 XMPP 클라이언트의 사용자가 LDAP 디렉터리에서 연락처를 검색 및 추가하도록 허용하려면 Cisco XCP 디렉터리 서비스를 설정해야 합니다. 클러스터의 모든 노드에서 Cisco XCP 디렉터리 서비스를 설정합니다.

참고 타사 XMPP 클라이언트에 대한 LDAP 검색 설정 및 LDAP 서버를 구성하기 전에는 Cisco XCP 디렉터리 서비스를 설정하지 마십시오. Cisco XCP 디렉터리 서비스를 설정한 상태에서 타사 XMPP 클라이언트에 대한 LDAP 검색 설정 및 LDAP 서버를 구성하지 않으면 서비스가 시작된 후 다시 중지됩니다.

시작하기 전에

타사 XMPP 클라이언트에 대한 LDAP 검색 설정 및 LDAP 서버를 구성합니다.

프로시저

단계 **1** **Cisco Unified IM and Presence** 서비스 가용성도구 > 서비스 활성화를 선택합니다.

단계 **2** [서버] 메뉴에서 IM and Presence 서비스 노드를 선택합니다.

단계 **3** **Cisco XCP** 디렉터리 서비스를 선택합니다.

단계 **4** 저장을 클릭합니다.