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.

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 ID에 대한 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.

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.

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.

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.

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 방법에 대한 자세한 내용은 *Cisco Unity Connection*에서 *SAML SSO* 관리를 참조하십시오.
- Cisco Unified 커뮤니케이션 애플리케이션 및 Cisco Unity Connection를 지원하려면 Webex Messenger 서비스에서 SSO를 활성화해야 합니다.

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

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.

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 설명서를 참조하십시오.

단계 **5** 저장을 선택합니다.

LDAP 서버로 인증합니다.