在 Unified Communications Manager 上创建用户

启用同步

要确保目录服务器中的联系人数据复制到 Cisco Unified Communications Manager，必须与目录服务器同步。您必须启用同步，然后才能与目录服务器同步。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**系统** > **LDAP** > **LDAP 系统**。

LDAP 系统配置窗口将会打开。

步骤 3 找到 **LDAP 系统信息**部分。

步骤 4 选择从 **LDAP 服务器启用同步**。

步骤 5 从 **LDAP 服务器类型**下拉列表中，选择您从中同步数据的目录服务器类型。

下一步做什么

为用户 ID 指定 LDAP 属性。

为用户 ID 指定 LDAP 属性

您从目录源同步到 Cisco Unified Communications Manager 时，您可以从目录属性填充用户 ID。保存用户 ID 的默认属性为 sAMAccountName。

过程

步骤 1 在 **LDAP 系统配置**窗口中找到**用户 ID 的 LDAP 属性**下拉列表。

步骤 2 根据需要为用户 ID 指定属性，然后选择**保存**。

重要事项 如果用户 ID 的属性不是 sAMAccountName，并且您在 Cisco Unified Communications Manager IM and Presence Service 中使用默认的 IM 地址方案，则必须将该属性指定为客户端配置文件中的参数值，如下所示：

CDI 参数为 UserAccountName。

<UserAccountName>*attribute-name*</UserAccountName>

如果未在配置中指定该属性，且该属性不是 sAMAccountName，则客户端将无法解析目录中的联系人。结果，用户不会获取在网状态，并且不能发送或接收即时消息。

指定目录 URI 的 LDAP 属性

在 Cisco Unified Communications Manager 版本 9.0 (1) 和更高版本中，您可以从目录中的属性填充目录 URI。

开始之前

启用同步。

过程

步骤 1 选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 选择相应的 LDAP 目录，或选择**新增**以添加 LDAP 目录。

步骤 3 找到**要同步的标准用户字段**部分。

步骤 4 从**目录 URI** 下拉列表中选择以下 LDAP 属性之一：

- **msRTCSIP-primaryuseraddress** — 使用 Microsoft Lync 或 Microsoft OCS 时，此属性将填充到 AD 中。这是默认属性。
- **mail**

步骤 5 选择**保存**。

执行同步

在添加目录服务器和指定所需的参数之后，您可以同步 Cisco Unified Communications Manager 和目录服务器。

过程

步骤 1 选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 选择**新增**。

LDAP 目录窗口将会打开。

步骤 3 在 **LDAP 目录**窗口中指定所需的详细信息。

有关您可以指定的值和格式的详细信息，请参阅《Cisco Unified Communications Manager 管理指南》。

步骤 4 创建 LDAP 目录同步计划，以确保您的信息定期同步。

步骤 5 选择**保存**。

步骤 6 选择**立即执行完全同步**。

注释 完成同步过程所需的时间取决于在您目录中存在的用户数。如果您同步有成千上万个用户的大目录，则此过程需要一些时间。

目录服务器中的用户数据会与 Cisco Unified Communications Manager 数据库同步。Cisco Unified Communications Manager 然后会同步用户数据与在线状态服务器数据库。

分配角色和组

对于所有部署类型，将用户分配到**标准 CCM 最终用户**组。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择**用户管理** > **最终用户**。
查找并列出用户窗口将会打开。

步骤 3 从列表中查找并选择用户。

最终用户配置窗口将会打开。

步骤 4 找到**权限信息**部分。

步骤 5 选择**添加至访问控制组**。
查找并列出访问控制组对话框将会打开。

步骤 6 为用户选择访问控制组。

您至少应该将用户分配到以下访问控制组：

- **标准 CCM 最终用户**
- **启用标准 CTI** — 此选项用于桌面电话控制。

如果您为用户配置安全电话功能，则不要将用户分配到**标准 CTI 安全连接**组。

某些电话型号需要其他控制组，如下所示：

- 对于 Cisco Unified IP Phone 9900、8900、8800 或 DX 系列，选择**标准 CTI 允许控制支持已连接转接和会议的电话**。
- 对于 Cisco Unified IP Phone 6900 系列，选择**标准 CTI 允许控制支持跳转模式的电话**。

步骤 7 选择**添加选定项**。
查找并列出访问控制组窗口将会关闭。

步骤 8 在**最终用户配置**窗口中选择**保存**。

认证选项

在客户端中启用 SAML SSO

开始之前

- 在 Cisco Unity Connection 版本 10.5 上启用 SSO — 有关对此服务启用 SAML SSO 的详细信息，请参阅 在 *Cisco Unity Connection* 中管理 *SAML SSO*。
- 对 Cisco Webex Messenger 服务启用 SSO 以支持 Cisco Unified Communications 应用程序和 Cisco Unity Connection。

  有关对此服务启用 SAML SSO 的详细信息，请参阅*Cisco Webex Messenger*管理员指南中的“单点登录”。

过程

步骤 1 在所有服务器上部署证书，以便 Web 浏览器能够验证证书，否则用户将收到关于无效证书的警告消息。有关证书验证的详细信息，请参阅证书验证。

步骤 2 确保客户端中已启用 SAML SSO 服务发现。客户端使用标准服务发现在客户端中启用 SAML SSO。通过使用以下配置参数启用服务发现：ServicesDomain、VoiceServicesDomain 和 ServiceDiscoveryExcludedServices。有关如何启用服务发现的详细信息，请参阅为*Remote Access*配置服务发现。

步骤 3 定义会话的持续时间。

会话由Cookie和令牌值组成。Cookie的持续时间通常比标记长。Cookie的生存期在标识提供商中定义，并且令牌的持续时间在服务中定义。

步骤 4 启用 SSO 后，所有 Cisco Jabber 用户默认使用 SSO 登录。管理员可为每个用户更改此设置，以便某些用户不使用 SSO，而是使用其 Cisco Jabber 用户名和密码登录。要为 Cisco Jabber 用户禁用 SSO，请将 SSO_Enabled 参数的值设置为 FALSE。

如果您已将 Cisco Jabber 配置为不要求用户提供电子邮件地址，则其第一次登录到 Cisco Jabber 时可能是非 SSO 登录。在某些部署中，参数 ServicesDomainSsoEmailPrompt 需要设置为 ON。这可确保 Cisco Jabber 具有执行第一次 SSO 登录所需的信息。如果用户之前登录到 Cisco Jabber，则不需要此提示，因为需要提供必要的信息。

有关将 SSO 与 Unified CM 集成（以便 Webex Teams 用户能够使用一组凭证进行登录）的详细信息，请参阅 *Cisco Unified Communications* 应用程序的 *SAML SSO* 部署指南。

通过 LDAP 服务器验证身份

如果要启用 LDAP 验证，请执行此程序，以便根据公司 LDAP 目录中分配的密码对最终用户密码进行验证。LDAP 验证使得系统管理员能够为最终用户分配一个适用于所有公司应用程序的密码。此配置仅适用于最终用户密码，不适用于最终用户 PIN 或应用程序用户密码。当用户登录到客户端时，在线状态服务会将身份验证路由到 Cisco Unified Communications Manager。Cisco Unified Communications Manager 随后会将该验证发送到目录服务器。

过程

步骤 1 打开 **Cisco Unified CM 管理**界面。

步骤 2 选择 **系统** > **LDAP** > **LDAP 身份验证**。

步骤 3 选择**为最终用户使用 LDAP 身份验证**。

步骤 4 根据需要指定 LDAP 凭证和用户搜索库。

有关 **LDAP 身份验证**的详细信息，请参阅 *Cisco Unified Communications Manager* 管理指南。

步骤 5 选择**保存**。