



用户

- [LDAP 同步概述](#)，第 1 页
- [“配置用户”工作流程](#)，第 3 页
- [激活服务](#)，第 3 页
- [启用 LDAP 目录同步](#)，第 4 页
- [配置 LDAP 目录同步](#)，第 4 页
- [验证选项](#)，第 6 页
- [执行同步](#)，第 8 页
- [将服务配置文件关联到用户](#)，第 9 页
- [批量预填充联系人列表](#)，第 10 页
- [为 UDS 联系人搜索配置身份验证](#)，第 12 页
- [启用扩展 UDS 联系人搜索](#)，第 12 页

LDAP 同步概述

轻型目录访问协议 (LDAP) 同步可帮助为您的系统设置和配置最终用户。LDAP 同步期间，系统会将用户和关联的用户数据列表从外部 LDAP 目录导入 Cisco Unified Communications Manager 数据库。此外，您可以配置定期同步计划，以记录员工数据中的任何更改。

用户 ID 和目录 URI

将 LDAP 目录服务器与 Cisco Unified Communications Manager 同步时，您可以在 Cisco Unified Communications Manager 和 Cisco Unified Communications Manager IM and Presence Service 数据库中的最终用户配置表中填充包含下列值的属性：

- **用户 ID** — 必须在 Cisco Unified Communications Manager 上指定用户 ID 的值。对于默认 IM 地址方案和要登录的用户时，此值为必填。默认值为 `sAMAccountName`。



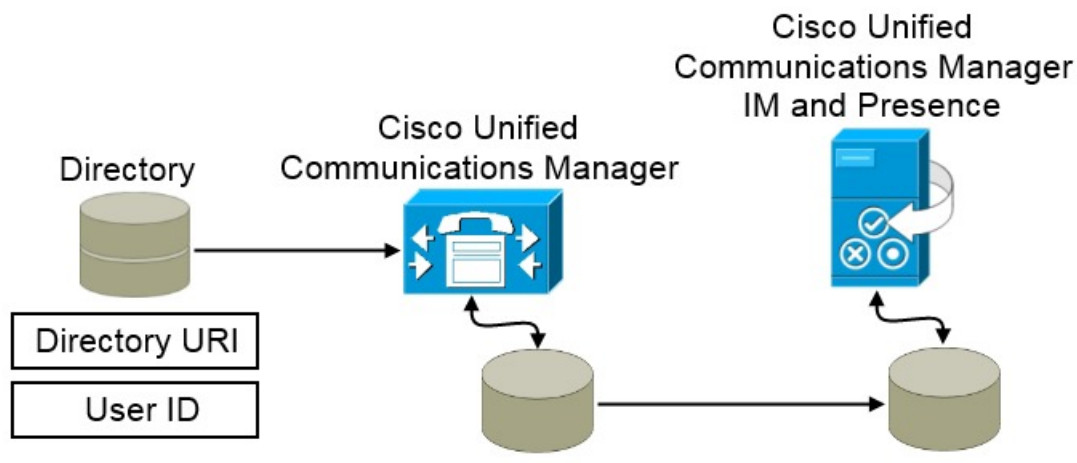
重要事项 如果用户 ID 的属性不是 `sAMAccountName`，并且您在 Cisco Unified Communications Manager IM and Presence Service 中使用默认的 IM 地址方案，则必须将该属性指定为客户端配置文件中的参数值，如下所示：

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。

- **目录 URI** — 如果您打算执行以下操作，则应为目录 URI 指定一个值：
 - 在 Cisco Jabber 中启用 URI 拨号。
 - 在 Cisco Unified Communications Manager IM and Presence Service 版本 10 和更高版本中使用目录 URI 地址方案。



当 Cisco Unified Communications Manager 与目录源同步时，将检索目录 URI 和用户 ID 的值并将这些值填充到 Cisco Unified Communications Manager 数据库的最终用户配置表中。

Cisco Unified Communications Manager 数据库随后将与 Cisco Unified Communications Manager IM and Presence Service 数据库同步。因此，目录 URI 和用户 ID 的值将填充到 Cisco Unified Communications Manager IM and Presence Service 数据库的最终用户配置表中。

“配置用户” 工作流程

过程

	命令或操作	目的
步骤 1	激活服务，第 3 页	打开所需的服務，以通过 Cisco Unified Communications Manager 和 IM and Presence Service 同步 LDAP 目录中的用户设置服务。
步骤 2	启用 LDAP 目录同步，第 4 页	允许 Cisco Unified Communications Manager 从 LDAP 目录同步用户设置。从您希望 Cisco Unified Communications Manager 为用户 ID 同步的 LDAP 目录中选择属性。
步骤 3	配置 LDAP 目录同步，第 4 页	配置 Cisco Unified Communications Manager 与 LDAP 目录同步。设置自动同步计划，映射标准用户字段，并将导入的用户分配到访问控制组。
步骤 4	验证选项，第 6 页	选择身份验证选项： <ul style="list-style-type: none"> • 在客户端中启用 SAML SSO。 • 通过 LDAP 服务器验证身份。
步骤 5	执行同步，第 8 页	将 Cisco Unified Communications Manager 与目录服务器同步。
步骤 6	将服务配置文件关联到用户，第 9 页	将服务配置文件与用户关联。
步骤 7	批量预填充联系人列表，第 10 页	为用户填充联系人列表。

激活服务

您必须先激活以下服务，然后才能与公司 LDAP 服务器集成：

- Cisco DirSync — 如果要同步公司 LDAP 目录中的最终用户设置，必须激活此服务。
- (Cisco Unified Communications Manager IM and Presence Service) 思科同步代理服务 — 此服务可保持 IM and Presence Service 服务节点和 Cisco Unified Communications Manager 之间的数据同步。当您执行与目录服务器的同步时，Cisco Unified Communications Manager 随后将与 IM and Presence Service 同步数据。

步骤 1 从 Cisco Unified 功能配置中，选择工具 > 服务激活。

步骤 2 从服务器下拉列表框中，选择发布方节点。

- 步骤 3** 在目录服务下，单击 **Cisco DirSync** 单选按键。
- 步骤 4** 单击保存。
- 步骤 5** 选择工具 > 控制中心 - 网络服务。
- 步骤 6** 从服务器下拉列表框中选择 IM and Presence Service 节点。
- 步骤 7** 在 **IM and Presence Service** 下，单击思科同步代理单选按钮。
- 步骤 8** 单击保存。

启用 LDAP 目录同步

如果要将 Cisco Unified Communications Manager 配置为从公司 LDAP 目录同步最终用户设置，请执行此程序。

- 步骤 1** 在 Cisco Unified CM 管理中，选择系统 > LDAP > LDAP 系统。
- LDAP 系统配置**窗口将会打开。
- 步骤 2** 如果您希望 Cisco Unified Communications Manager 从 LDAP 目录导入用户，则选中启用从 **LDAP 服务器同步**复选框。
- 步骤 3** 从 **LDAP 服务器类型**下拉列表框中，选择您公司使用的 LDAP 目录服务器类型。
- 步骤 4** 在用户 ID 的 **LDAP 属性**下拉列表框中，选择您希望 Cisco Unified Communications Manager 为最终用户配置窗口中的用户 ID 字段同步的公司 LDAP 目录属性。
- 对于默认 IM 地址方案和要登录的用户时，此值为必填。默认值为 `sAMAccountName`。
- 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。
- 步骤 5** 单击保存。

配置 LDAP 目录同步

此程序用于将 Cisco Unified Communications Manager 配置为与 LDAP 目录同步。通过 LDAP 目录同步，您可以将最终用户数据从外部 LDAP 目录导入 Cisco Unified Communications Manager 数据库，以便其显示在最终用户配置窗口中。您可以设置同步计划，以便对 LDAP 目录所做的更新定期传播到 Cisco Unified Communications Manager。

有关这些字段及其说明的帮助，请参阅联机帮助。

-
- 步骤 1** 在 Cisco Unified CM 管理中，依次选择系统 > LDAP > LDAP 目录。
- 步骤 2** 请执行以下步骤之一：

- 单击**查找**并选择现有的 LDAP 目录。
- 单击**新增**以创建新的 LDAP 目录。

步骤 3 在 **LDAP 配置名称** 文本框中，为 LDAP 目录分配唯一的名称。

步骤 4 在 **LDAP 管理员判别名字段** 中，输入具有 LDAP 目录服务器访问权限的用户 ID。

步骤 5 输入并确认密码详细信息。

步骤 6 在 **LDAP 目录同步计划** 字段中，创建 Cisco Unified Communications Manager 用于同外部 LDAP 目录同步数据的计划。

步骤 7 填写**要同步的标准用户**字段部分。对于每个最终用户字段，选择 LDAP 属性。同步过程会将 LDAP 属性的值分配给 Cisco Unified Communications Manager 中的最终用户字段。

a) 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 8 要将导入的最终用户分配给所有导入的最终用户通用的访问控制组，请执行以下操作：

- 单击**添加到访问控制组**。
- 在弹出窗口中，单击要分配给所导入最终用户的每个访问控制组对应的复选框。
- 单击**添加选定项**。

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。

注释 对于 Cisco Unified Communications Manager 9.x，您必须在**最终用户配置窗口**（**用户管理 > 最终用户**）中将最终用户分配到访问控制组。

步骤 9 在 **LDAP 服务器信息** 区域，输入 LDAP 服务器的主机名或 IP 地址。

步骤 10 如果想创建到 LDAP 服务器的安全连接，则选中**使用 SSL** 复选框。

步骤 11 单击**保存**。

验证选项

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。

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。

将客户端配置为通过 LDAP 服务器验证

如果配置使用 LDAP 凭证验证身份，您还必须配置客户端。

步骤 1 使用 `LDAP_UseCredentialsFrom` 参数更新 `jabber-config` 文件。

示例：

```
<LDAP_UseCredentialsFrom>CUCM</LDAP_UseCredentialsFrom>
```

步骤 2 如果 LDAP 服务器部署在与 Cisco Unified Communications Manager IM and Presence Service 和 Cisco Unified Communications Manager 不同的域中，则配置 `LDAPUserDomain` 参数。如果未配置此参数，默认将使用必需参数 `PresenceDomain` 的值。

示例：

```
<LdapUserDomain>example.com</LdapUserDomain>
```

通过匿名绑定验证身份

您可以将匿名绑定配置为向 LDAP 服务器验证用户身份的方式。使用匿名绑定可防止用户在 Jabber 选项菜单的帐户选项卡中输入凭证。

在 `Jabber-config.xml` 文件中，为 `LdapAnonymousBinding` 参数配置 `true` 或 `false` 值。

示例:

```
<LdapAnonymousBinding>true</LdapAnonymousBinding>
```

有关配置此功能的详细信息，请参阅 *Cisco Jabber* 参数参考指南。

手动用户验证

您可以设置服务身份验证，以便用户在 Jabber 客户端中为所需服务手动输入自己的凭证。

在没有配置服务身份验证（例如，在服务配置文件或 LDAP 服务器上）时，需手动提示用户输入自己的凭证。

用户在 Jabber 选项菜单的帐户选项卡中输入其凭证。

在客户端中启用 SAML SSO

开始之前

- 在 Cisco Unified Communications Applications 10.5.1 Service Update 1 上启用 SSO — 关于对此服务启用 SAML SSO 的信息，请参阅《*Cisco Unified Communications Applications 10.5* 版本的 *SAML SSO* 部署指南》。
- 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*》。

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。

适用于移动客户端的基于证书的 SSO 身份验证

只有 Cisco Jabber iPhone 和 iPad 版本才需要此配置。Cisco Jabber Android 版本不需要类似的配置。

要启用此功能，需在 Cisco Unified Communications Manager 和 Cisco Unity Connection 中为 iOS 配置相同的 SSO 登录行为设置。

使用 Expressway for Mobile and Remote Access 时，将 Jabber iPhone 和 iPad 版本客户端配置为使用 VCS Expressway 管理控制台中嵌入的 Safari 浏览器。有关详细信息，请参阅 <https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-guides-list.html> 处的《Cisco Expressway 安装指南》。

您无法为 Webex Messenger 启用通用标识（CI）。要启用嵌入的 Safari 以使用基于客户端证书的 SSO 身份验证连接到语音邮件时，您必须禁用 CI。

在 Cisco Unified Communications Manager 上配置基于证书的 SSO 身份验证

Cisco Unified Communications Manager 11.5 版或更高版本上支持此配置。

步骤 1 在“Cisco Unified CM 管理”中，转至系统 > 企业参数。

步骤 2 在 SSO 配置部分中，向下滚动到 iOS 的 SSO 登录行为，然后选择使用本机浏览器。

步骤 3 选择保存

在 Cisco Unity Connection 上配置基于证书的 SSO 身份验证

步骤 1 在“Cisco Unity Connection 管理”中，转至系统 > 设置企业参数。

步骤 2 在 SSO 配置部分中，向下滚动到 iOS 的 SSO 登录行为，然后选择使用本机浏览器。

步骤 3 选择保存。

执行同步

在添加目录服务器并指定身份验证方法后，您可以将 Cisco Unified Communications Manager 与目录服务器同步。

步骤 1 选择系统 > LDAP > LDAP 目录。

步骤 2 单击查找，然后选择所配置的 LDAP 目录。

LDAP 目录窗口将会打开。

步骤 3 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 随后将用户数据同步到 IM and Presence Service 数据库。

将服务配置文件关联到用户

将服务配置文件与个别用户关联

将服务配置文件与个别用户关联。

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。

查找并列用户窗口将会打开。

步骤 3 在查找用户位置字段中指定适当的过滤器，然后选择查找以检索用户列表。

步骤 4 从列表中选择适当的用户名。

最终用户配置窗口将会打开。

步骤 5 找到服务设置部分。

步骤 6 选择主群集。

步骤 7 对于电话模式部署，确保为 **Unified CM IM and Presence** 启用用户（在相关的 UC 服务配置文件中配置 **IM and Presence**）选项未选中。

对于所有其他部署，选中为 **Unified CM IM and Presence** 启用用户（在相关的 UC 服务配置文件中配置 **IM and Presence**）复选框。

步骤 8 从 **UC 服务配置文件** 下拉列表中选择您的服务配置文件。

重要事 仅限 Cisco Unified Communications Manager 版本 9.x — 如果用户仅有即时消息和在线状态功能（仅适用于项 **IM**），请选择使用默认值。Cisco Unified Communications Manager 版本 9.x 会应用默认服务配置文件，无论您从 **UC 服务配置文件** 下拉列表中选择什么。

步骤 9 选择保存。

将服务配置文件与多个用户批量关联

将服务配置文件添加到多个用户。

步骤 1 打开 **Cisco Unified CM** 管理界面。

步骤 2 选择 **批量管理 > 用户 > 更新用户 > 查询**。

查找并列出来要更新的用户窗口将会打开。

步骤 3 在 **查找用户位置** 字段中指定适当的过滤器，然后选择 **查找** 以检索用户列表。

步骤 4 选择下一步。

更新用户配置窗口将会打开。

步骤 5 对于电话模式部署，禁用即时消息和在线状态，选中为 **Unified CM IM and Presence** 启用用户的其中一个复选框。

对于所有其他部署，选中为 **Unified CM IM and Presence** 启用用户的两个复选框。

步骤 6 选中 **UC 服务配置文件** 复选框，然后从下拉列表中选择您的服务配置文件。

重要事 仅限 Cisco Unified Communications Manager 版本 9.x — 如果用户仅有即时消息和在线状态功能（仅适用于项 IM），则必须选择使用默认值。

对于仅有 IM 的用户 — Cisco Unified Communications Manager 版本 9.x 总是应用默认服务配置文件，无论您从 **UC 服务配置文件** 下拉列表中选择什么。

步骤 7 在作业信息部分，指定您要立即还是稍后运行作业。

步骤 8 选择提交。

批量预填充联系人列表

您可以使用批量管理工具（BAT）预填充用户联系人列表。

通过这种方式，您可以为用户预填充联系人列表，以便他们在首次启动客户端后自动拥有一组联系人。

Cisco Jabber 的客户端联系人列表中支持最多 300 个联系人。

过程

	命令或操作	目的
步骤 1	创建 CSV 文件，以定义您要为用户提供的联系人列表。	创建 CSV 以导入联系人列表，第 11 页
步骤 2	使用 BAT 将联系人列表批量导入到一组用户。	使用 BAT 上传联系人列表，第 11 页

创建 CSV 以导入联系人列表

CSV 文件结构

CSV 文件必须采用以下格式：

<User ID>、<User Domain>、<Contact ID>、<Contact Domain>、<Nickname>、<Group Name>

CSV 文件条目示例：

```
userA,example.com,userB,example.com,buddyB,General
```

表 1: 输入文件参数的说明

参数	说明
用户 ID	必填参数。IM and Presence Service 用户的用户 ID。最多可包含 132 个字符。
用户域名	必填参数。IM and Presence Service 用户的 Presence 域名。最多可包含 128 个字符。
联络人 ID	必填参数。联系人列表条目的用户 ID。最多可包含 132 个字符。
联系人域名	必填参数。联系人列表条目的 Presence 域名。域名格式需遵守以下限制： <ul style="list-style-type: none"> • 长度不能超过 128 个字符 • 只能包含数字、大小写字母和连字符 (-) • 不能以连字符 (-) 开头或结尾 • 标签长度不能超过 63 个字符 • 顶级域名只能包含字符，并且至少要有两个字符
Nickname	联系人列表条目的昵称。最多可包含 255 个字符。
组名称	必填参数。要添加联系人列表条目的组的名称。最多可包含 255 个字符。

使用 BAT 上传联系人列表

开始之前

创建包含联系人的 CSV 文件。

步骤 1 打开 Cisco Unified CM IM and Presence 管理界面。

步骤 2 选择批量管理 > 上传/下载文件。

步骤 3 选择新增。

步骤 4 选中选择，找到并选择 CSV 文件。

步骤 5 选择联系人列表作为目标。

步骤 6 选择导入用户的联系人 - 自定义文件作为“事务类型”。

步骤 7 选择保存以上传文件。

为 UDS 联系人搜索配置身份验证

搜索联系人时，Cisco Jabber 支持验证目录查询。Cisco Unified Communications Manager 版本 11.5 或更高版本上已配置身份验证。

步骤 1 登录到命令行界面。

步骤 2 运行 `utils contactsearchauthentication status` 命令以确认此节点上的联系人搜索身份验证设置。

步骤 3 如果您需要配置联系人搜索身份验证：

- 要启用身份验证，请运行 `utils contactsearchauthentication enable` 命令。
- 要禁用身份验证，请运行 `user-authentication disable` 命令。

步骤 4 对所有 群集节点重复此程序。

注释 您必须重置电话才能使更改生效。

启用扩展 UDS 联系人搜索

开始之前

扩展 UDS 联系人搜索仅在 Cisco Unified Communications Manager 版本 11.5 (1) 或更高版本中可用。

步骤 1 打开 Cisco Unified CM 管理界面。

步骤 2 选择系统 > LDAP > LDAP 搜索

步骤 3 要使用企业 LDAP 目录服务器执行用户搜索，选中启用企业目录服务器用户搜索复选框。

步骤 4 配置 LDAP 搜索配置窗口中的字段。请参阅联机帮助，了解有关字段及其配置选项的更多信息。

步骤 5 选择保存。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。