配置 LDAP 目录

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 Unified Communications Manager 数据库。 您还可以在导入时配置您的最终用户。

注释 Unified Communications Manager 支持 LDAPS（通过 SSL 的 LDAP），但不支持通过 StartTLS 的 LDAP。 确保您将 LDAP 服务器证书作为 Tomcat-Trust 上传到 Unified Communications Manager。

有关受支持的 LDAP 目录的信息，请参阅《*Cisco Unified Communications Manager* 和 *IM and Presence Service* 的兼容性值表》。

LDAP 同步会通告以下功能：

- **导入最终用户**—您可以在初始系统设置期间使用 LDAP 同步将用户列表从公司 LDAP 目录导入 Unified Communications Manager 数据库。 如果您已预先配置了功能组模板、用户配置文件、服务配置文件、通用设备和线路模板等项目，可以将配置应用到您的用户，并在同步过程中分配配置的目录号码和目录 URI。 LDAP 同步过程将导入用户和用户特定数据列表，并应用您设置的配置模板。

注释 一旦发生初始同步，您将无法编辑 LDAP 同步。

- **计划的更新**—您可以将 Unified Communications Manager 配置为按计划的时间间隔与多个 LDAP 目录同步，以确保定期更新数据库且用户数据为最新。

- **验证最终用户**—您可以将系统配置为针对 LDAP 目录而不是 Cisco Unified Communications Manager 数据库验证最终用户密码。 LDAP 验证使得公司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。 此功能不适用于 PIN 或应用程序用户密码。
- **针对思科移动和远程访问客户端及终端的目录服务器用户搜索**—即使在企业防火墙外部运行，您也可以搜索公司目录服务器。 启用此功能后，用户数据服务 (UDS) 将充当代理，并将用户搜索请求发送到公司目录，而不是发送到 Unified Communications Manager 数据库。

最终用户的 LDAP 验证

通过 LDAP 同步，您可以将系统配置为针对 LDAP 目录而不是 Cisco Unified Communications Manager 数据库验证最终用户密码。 LDAP 验证使得公司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。 此功能不适用于 PIN 或应用程序用户密码。

目录服务器用户搜索思科移动和远程访问客户端及终端

在以前的版本中，当具有思科移动和远程访问客户端（如 Cisco Jabber）或终端（如 Cisco DX 80 电话）的用户在企业防火墙外部执行用户搜索时，结果基于存储在 Cisco Unified Communications Manager 数据库中的用户帐户。 数据库包含本地配置或从公司目录同步的用户帐户。

在此版本中，即使在企业防火墙外部运行，思科移动和远程访问客户端及终端现在也可以搜索公司目录服务器。 启用此功能后，用户数据服务 (UDS) 将充当代理，并将用户搜索请求发送到公司目录，而不是发送到 Cisco Unified Communications Manager 数据库。

可通过此功能实现以下结果：

- 无论地理位置如何，都提供相同的用户搜索结果 — 移动和远程访问客户端及终端可以使用公司目录执行用户搜索；即使它们在企业防火墙之外连接也不例外。
- 减少 Cisco Unified Communications Manager 数据库中配置的用户帐户数量 — 移动客户端现在可以搜索公司目录中的用户。 在以前的版本中，用户搜索结果基于数据库中配置的用户。 现在，管理员不再需要仅为用户搜索而将用户帐户配置或同步到数据库。 管理员只需配置由群集提供服务的用户帐户。 减少数据库中的用户帐户总数可缩短软件升级所需的时长，同时提高数据库的整体性能。

要配置此功能，您必须启用 **LDAP 搜索配置**窗口的**启用用户搜索企业目录服务器**，并配置 LDAP 目录服务器的详细信息。 有关详细信息，请参阅配置企业目录用户搜索 ， 第 7 页程序。

LDAP 同步前提条件

先决任务

从 LDAP 目录导入最终用户之前，请完成以下任务：

- 配置用户访问权限

- 配置凭证策略
- 配置功能组模板

对于您希望将其数据同步到您的系统的用户，请确保他们在 Active Directory 服务器上的电子邮件 ID 字段是唯一的条目或留空。

LDAP 同步配置任务流程

执行以下任务以从外部 LDAP 目录提取用户列表并将其导入 Cisco Unified Communications Manager 数据库。

注释 如果您已同步 LDAP 目录一次，仍可以从外部 LDAP 目录同步新项目，但无法在 Cisco Unified Communications Manager 中将新配置添加到 LDAP 目录同步。 在这种情况下，您可以使用批量管理工具和菜单，例如“更新用户”或“插入用户”。 请参阅《*Cisco Unified Communications Manager* 批量管理指南》。

过程

	命令或操作	目的
步骤 1	激活 Cisco DirSync 服务， 第 4 页	登录到 Cisco Unified 功能配置并激活 Cisco DirSync 服务。
步骤 2	启用 LDAP 目录同步， 第 4 页	在 Unified Communications Manager 中启用 LDAP 目录同步。
步骤 3	创建 LDAP 过滤器， 第 4 页	**可选**。 如果希望 Unified Communications Manager 只同步公司 LDAP 目录中的一部分用户，请创建 LDAP 过滤器。
步骤 4	配置 LDAP 目录同步， 第 5 页	配置LDAP目录同步的设置，例如字段设置、LDAP 服务器位置、同步计划以及访问控制组、功能组模板和主分机的分配。
步骤 5	配置企业目录用户搜索， 第 7 页	**可选**。 配置系统以用于企业目录服务器用户搜索。 请遵照此程序配置系统中的电话和客户端，以对企业目录服务器而不是数据库执行用户搜索。
步骤 6	配置 LDAP 验证， 第 9 页	**可选**。 如果要使用 LDAP 目录进行最终用户密码验证，请配置 LDAP 验证设置。
步骤 7	自定义 LDAP 协议服务参数， 第 9 页	**可选**。 配置可选的 LDAP 同步服务参数。 对于大多数部署而言，默认值已足够。

激活 Cisco DirSync 服务

执行以下程序可在 Cisco Unified 功能配置中激活 Cisco DirSync 服务。 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。

过程

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**。

启用 LDAP 目录同步

如果要将 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。

注释 如果您已同步 LDAP 目录一次，仍可以从外部 LDAP 目录同步新用户，但无法在 Unified Communications Manager 中将新配置添加到 LDAP 目录同步。 您还不能向基础配置项目（如功能组模板或用户配置文件）添加编辑。 如果已经完成一个 LDAP 同步，并且想要添加具有不同设置的用户，则可以使用批量管理菜单，例如“更新用户”或“插入用户”。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 系统**。

步骤 2 如果您希望 Unified Communications Manager 从 LDAP 目录导入用户，选中**从 LDAP 服务器启用同步**复选框。

步骤 3 从 **LDAP 服务器类型**下拉列表中，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**下拉列表中，选择您希望 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。

步骤 5 单击**保存**。

创建 LDAP 过滤器

您可以创建 LDAP 过滤器以将 LDAP 同步范围限制为 LDAP 目录中的部分用户。 将 LDAP 过滤器应用于 LDAP 目录时，Unified Communications Manager 只会导入 LDAP 目录中与过滤器匹配的用户。

注释 您配置的 LDAP 过滤器必须符合 RFC4515 中规定的 LDAP 搜索过滤器标准。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 过滤器**。

步骤 2 单击**新增**以创建新的 LDAP 过滤器。

步骤 3 在**过滤器名称**文本框中，输入您的 LDAP 过滤器的名称。

步骤 4 在**过滤器**文本框中，输入过滤器。 过滤器最多可包含 1024 个 UTF-8 字符，且必须括在括号中 ()。

步骤 5 单击**保存**。

配置 LDAP 目录同步

此程序用于将 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 Unified Communications Manager 数据库，以便其显示在“最终用户配置”窗口中。 如果您具有带通用线路和设备模板的设置功能组模板，可以将设置自动分配给新预配置的用户及其分机。

提示 如果要分配访问控制组或功能组模板，则可以使用 LDAP 过滤器将导入限制为具有相同配置要求的用户组。

过程

步骤 1 从 Cisco Unified CM 管理中，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 目录配置**窗口中，输入以下内容：

a) 在 **LDAP 配置名称**字段中，为 LDAP 目录分配唯一的名称。
b) 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。
c) 输入并确认密码详细信息。
d) 在 **LDAP 用户搜索空间**字段中，输入搜索空间详细信息。
e) 在**用户同步的 LDAP 自定义过滤器**字段中，选择**仅限用户**或者**用户和组**。
f) （可选）。 如果要将导入限制为满足特定配置文件的部分用户，请从**适用于组的 LDAP 自定义过滤器**下拉列表中选择 LDAP 过滤器。

步骤 4 在 **LDAP 目录同步计划**字段中，创建 Unified Communications Manager 用于同外部 LDAP 目录同步数据的计划。

步骤 5 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 Unified Communications Manager 中的最终用户字段。

步骤 6 如果您正在部署 URI 拨号，请确保分配用于用户主目录 URI 地址的 LDAP 属性。

步骤 7 在**要同步的自定义用户字段**部分，输入具有所需 LDAP 属性的自定义用户字段名称。

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：

a) 单击**添加到访问控制组**。
b) 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。
c) 单击**添加选定项**。

步骤 9 如果要分配功能组模板，从**功能组模板**下拉列表中选择模板。

注释 只有在最终用户第一次未显示时，才会将用户与所分配的**功能组模板**同步。 如果现有**功能组模板**被修改且为关联的 LDAP 执行了完全同步，则修改内容不会更新。

步骤 10 如果要对导入的电话号码应用掩码以分配主分机，请执行以下操作：

a) 选中**应用掩码到同步的电话号码以为插入的用户创建新线路**复选框。
b) 输入**掩码**。 例如，如果导入的电话号码是 8889945，则掩码 11XX 会创建一个主分机 1145。

步骤 11 如果要从目录号池分配主分机，请执行以下操作：

a) 选中**如果未根据同步的 LDAP 电话号码创建新线路，请从池列表分配一条新线路**复选框。
b) 在 **DN 池开始**和 **DN 池结束**文本框中，输入要从中选择主分机的目录号码范围。

步骤 12 （可选）如果要创建 Jabber 设备，请在“Jabber 终端预配置”部分中，从下列下拉列表中选择一个所需的 Jabber 设备进行自动预配置：

- 适用于 Android 的 Cisco 双模 (BOT)
- Cisco Dual Mode for iPhone (TCT)
- Cisco Jabber 平板电脑版 (TAB)
- Cisco Unified Client Services Framework (CSF)

注释 **写回到 LDAP** 选项可让您将选中的主目录号码从 Unified CM 写回到 LDAP 服务器。 可用于写回的 LDAP 属性包括：**telephoneNumber**、**ipPhone** 和 **mobile**。

步骤 13 在 **LDAP 服务器信息**部分，输入 LDAP 服务器的主机名或 IP 地址。

步骤 14 如果想使用 TLS 创建到 LDAP 服务器的安全连接，则选中**使用 TLS** 复选框。

注释 有时，当我们在重启 tomcat 后尝试通过安全端口同步用户时，用户无法同步。 您必须重新启动 Cisco DirSync 服务才能成功同步用户。

步骤 15 单击**保存**。

步骤 16 要完成 LDAP 同步，请单击**立即执行完全同步**。 否则，您可以等待预定的同步。

注释 在 LDAP 中删除用户时，他们会在 24 小时后自动从 Unified Communications Manager 中删除。 此外，如果为以下任何设备将已删除用户配置为移动用户，则这些非活动的设备也将自动删除：

- 远程目标配置文件
- 远程目标配置文件模板
- 移动智能客户端
- CTI 远程设备
- Spark 远程设备
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS 集成移动 (基本)
- 运营商集成的移动
- 适用于 Android 的 Cisco 双模

配置企业目录用户搜索

此程序用于配置系统中的电话和客户端，以对企业目录服务器而不是数据库执行用户搜索。

开始之前

- 确保您选择用于 LDAP 用户搜索的主、辅和第三服务器均可通过网络连接到 Unified Communications Manager 订阅方节点。
- 依次选择**系统** > **LDAP** > **LDAP 系统**，从 **LDAP 系统配置**窗口的**LDAP 服务器类型**下拉列表配置 LDAP 服务器的类型。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 搜索**。

步骤 2 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 3 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 4 单击**保存**。

注释 要在 OpenLDAP 服务器中搜索表示为会议室对象的会议室，请将自定义过滤器配置为 (|(objectClass=intOrgPerson)(objectClass=rooms))。 这将允许 Cisco Jabber 客户端按名称搜索会议室并拨打与聊天室关联的号码。

如果 OpenLDAP 服务器中针对会议室对象配置了 **givenName**、**sn**、**mail**、**displayName** 或 **telephonenumber** 属性，会议室将可搜索。

目录服务器 UDS 搜索的 LDAP 属性

下表列出了**启用企业目录服务器用户搜索**选项启用时，UDS 用户搜索请求使用的 LDAP 属性。 对于这些类型的目录请求，UDS 充当代理并将搜索请求中继到公司目录服务器。

注释 UDS 用户响应标记可以映射到其中一个 LDAP 属性。 属性映射取决于您从 **LDAP 服务器类型**下拉列表中选择的选项。 从**系统** > **LDAP** > **LDAP 系统配置**窗口访问此下拉列表。

UDS 用户响应标记	LDAP 属性
userName	• samAccountName • uid
firstName	givenName
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail
directoryUri	• msRTCSIP-primaryuseraddress • mail

UDS 用户响应标记	LDAP 属性
department	• department • departmentNumber
manager	manager
title	title
pager	pager

配置 LDAP 验证

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。 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。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**系统** > **LDAP** > **LDAP 验证**。

步骤 2 选中**对最终用户使用 LDAP 验证**复选框以使用 LDAP 目录进行用户验证。

步骤 3 在 **LDAP 管理员判别名**字段中，输入具有 LDAP 目录访问权限的 LDAP 管理员的用户 ID。

步骤 4 在**确认密码**字段中，输入 LDAP 管理器的密码。

步骤 5 在 **LDAP 用户搜索库**字段中，输入搜索条件。

步骤 6 在 **LDAP 服务器信息**部分，输入 LDAP 服务器的主机名或 IP 地址。

步骤 7 如果想使用 TLS 创建到 LDAP 服务器的安全连接，则选中**使用 TLS** 复选框。

步骤 8 单击**保存**。

下一步做什么

自定义 LDAP 协议服务参数，第 9 页

自定义 LDAP 协议服务参数

执行此程序可配置自定义 LDAP 协议的系统级设置的可选服务参数。 如果不配置这些服务参数，Unified Communications Manager 将应用 LDAP 目录集成的默认设置。 对于参数说明，在用户界面中单击参数名称。

您可以使用服务参数自定义以下设置：

- **协议的最大数**—默认值为 20。
- **主机的最大数**—默认值为 3。

- 主机出现故障时的重试延迟（秒）—主机故障的默认值为 5。
- **HotList** 出现故障时的重试延迟（分钟）—hostlist 故障的默认值为 10。
- **LDAP** 连接超时（秒）—默认值为 5。
- 延迟同步开始时间（分钟）—默认值为 5。
- 用户客户映射审核时间

过程

步骤 1 从 Cisco Unified CM 管理中，选择**系统** > **服务参数**。
步骤 2 从**服务器**下拉列表框中，选择发布方节点。
步骤 3 从**服务**下拉列表框选择 **Cisco DirSync**。
步骤 4 配置 Cisco DirSync 服务参数的值。
步骤 5 单击**保存**。

LDAP 目录服务参数

服务参数	说明
协议的最大数	您可以配置的 LDAP 目录最大数。 默认设置为 20。
主机的最大数	您可以出于故障转移目的配置的 LDAP 主机名最大数。 默认值为 3。
主机出现故障时的重试延迟（秒）	主机出现故障后，Cisco Unified Communications Manager 在重试与第一个LDAP服务器（主机名）的连接之前延迟的秒数。 默认值为 5。
主机列表出现故障时的重试延迟（分钟）	主机列表出现故障后，Cisco Unified Communications Manager 在重试每一个配置的LDAP服务器（主机名）之前延迟的分钟数。 默认值为 10。
LDAP 连接超时（秒）	Cisco Unified Communications Manager 允许建立 LDAP 连接的秒数。 如果无法在指定的时间内建立连接，LDAP 服务提供程序将中止连接尝试。 默认值为 5。
延迟同步开始时间（分钟）	Cisco DirSync 服务启动后，Cisco Unified Communications Manager 延迟启动目录同步过程的分钟数。 默认值为 5。

将 LDAP 同步的用户转换为本地用户

将 LDAP 目录与 Cisco Unified Communications Manager 同步时，对于 LDAP 同步的最终用户，除非将 LDAP 同步用户转换为本地用户，否则无法编辑**最终用户配置**窗口中的任何字段。

要在**最终用户配置**窗口中编辑 LDAP 同步字段，请将用户转换为本地用户。 不过，如果执行此转换，当 Cisco Unified Communications Manager 与 LDAP 目录同步时，最终用户不会更新。

过程

步骤 1 在 Cisco Unified CM 管理中，选择**最终用户** > **最终用户管理**。

步骤 2 单击**查找**并选择最终用户。

步骤 3 单击**转换为本地用户**按键。

步骤 4 在**最终用户配置**窗口中进行更新。

步骤 5 单击**保存**。

将 LDAP 同步用户分配给访问控制组

执行此程序将 LDAP 同步用户分配给访问控制组。

开始之前

必须配置 Cisco Unified Communications Manager，将最终用户与外部 LDAP 目录同步。

过程

步骤 1 在 Cisco Unified CM 管理中，依次选择**系统** > **LDAP** > **LDAP 目录**。

步骤 2 单击**查找**并选择配置的 LDAP 目录。

步骤 3 单击**添加到访问控制组**按键。

步骤 4 选择您要应用到此 LDAP 目录中的最终用户的访问控制组。

步骤 5 单击**添加选定项**。

步骤 6 单击**保存**。

步骤 7 单击**执行完全同步**。

Cisco Unified Communications Manager 会与外部 LDAP 目录同步，并且同步的用户会插入到正确的访问控制组中。

注释 仅当您第一次添加访问控制组时，同步的用户才会插入到所选的访问组中。 执行完全同步后，您添加到 LDAP 的任何后续组将不会应用到同步的用户。

集成 LDAP 目录以在 XMPP 客户端上搜索联系人

这些主题介绍如何在 IM and Presence Service 上配置 LDAP 设置，以允许第三方 XMPP 客户端的用户从 LDAP 目录搜索和添加联系人。

IM and Presence Service 上的 JDS 组件负责处理第三方 XMPP 客户端与 LDAP 目录的通信。 第三方 XMPP 客户端发送查询到 IM and Presence Service 上的 JDS 组件。 JDS 组件向已配置的 LDAP 服务器发送 LDAP 查询，然后将结果发送回 XMPP 客户端。

您在执行此处介绍的配置之前，请先执行将 XMPP 客户端与 Cisco Unified Communications Manager 和 IM and Presence Service 集成的配置。 请参阅与第三方 XMPP 客户端应用程序集成相关的主题。

图 *1:* 集成 *LDAP* 目录以在 *XMPP* 客户端上搜索联系人的工作流程

下面的工作流程图显示了集成 LDAP 目录以在 XMPP 客户端上搜索联系人的简要步骤。

下表列出了集成 LDAP 目录以在 XMPP 客户端上搜索联系人所需执行的任务。 有关详细的说明，请参阅相关任务。

表 *1:* 集成 *LDAP* 目录以在 *XMPP* 客户端上搜索联系人的任务列表

任务	说明
配置 XMPP 客户端的 LDAP 服务器名称和地址	如果在 LDAP 服务器与 IM and Presence Service 之间启用了 SSL 并且配置了安全连接，请将根 CA 证书作为 xmpp-trust-certificate 上传到 IM and Presence Service。 **提示** 证书中的主题 CN 必须与 LDAP 服务器的 FQDN 匹配。
配置 XMPP 客户端 LDAP 搜索设置	必须指定可让 IM and Presence Service 对第三方 XMPP 客户端成功执行联系人搜索的 LDAP 搜索设置。 您可以指定一个主要 LDAP 服务器以及最多两个备用 LDAP 服务器。 **提示** 也可以打开从 LDAP 服务器检索 vCards 的功能，或者允许 vCards 存储在 IM and Presence Service 的本地数据库中。
打开 Cisco XCP 目录服务	必须打开 XCP 目录服务，以允许第三方 XMPP 客户端的用户从 LDAP 目录搜索和添加联系人。 **提示** 在为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置之前，不要打开 Cisco XCP 目录服务；否则服务将停止运行。

LDAP 帐户锁定问题

如果针对您为第三方 XMPP 客户端配置的 LDAP 服务器输入错误的密码，并在 IM and Presence Service 上重新启动 XCP 服务，JDS 组件将会多次使用该错误密码尝试登录 LDAP 服务器。 如果将 LDAP

服务器配置为在几次尝试失败后锁定帐户，则 LDAP 服务器将在某个时候锁定 JDS 组件。 如果 JDS 组件与其他连接到 LDAP 的应用程序（这些应用程序不一定在 IM and Presence Service 上）使用相同的凭证，这些应用程序也将被 LDAP 锁定。

要解决此问题，请配置一个单独的用户，使其具有与现有 LDAP 用户相同的角色和权限，并仅允许 JDS 以此辅助用户的身份登录。 如果您针对 LDAP 服务器输入错误的密码，LDAP 服务器将只锁定 JDS 组件。

为 XMPP 客户端配置 LDAP 服务器名称和地址

如果选择启用安全套接字层 (SSL)，请在 LDAP 服务器与 IM and Presence Service 之间配置安全连接，并且将根证书机构 (CA) 证书作为 cup-xmpp-trust 证书上传到 IM and Presence Service。 证书中的主题通用名称 (CN) 必须与 LDAP 服务器的完全限定域名 (FQDN) 匹配。

如果您导入证书链（从根节点到信任节点的多个证书），则会导入链中的所有证书，叶节点除外。例如，如果 CA 对 LDAP 服务器的证书进行签名，则只需导入 CA 证书，无需导入 LDAP 服务器的证书。

即使 IM and Presence Service 与 Cisco Unified Communications Manager 之间的连接是 IPv4，您也可以使用 IPv6 连接到 LDAP 服务器。 当 IPv6 对 IM and Presence Service 节点上的企业参数或 ETH0 禁用时，如果为第三方 XMPP 客户端配置的外部 LDAP 服务器的主机名是可解析的 IPv6 地址，该节点仍可执行内部 DNS 查询并连接到外部 LDAP 服务器。

提示 您可以在 **LDAP 服务器 - 第三方 XMPP 客户端**窗口中为第三方 XMPP 客户端配置外部 LDAP 服务器的主机名。

开始之前

获取 LDAP 目录的主机名或 IP 地址。

如果使用 IPv6 连接到 LDAP 服务器，请先在企业参数及 Eth0 上为每个 IM and Presence Service 节点启用 IPv6，然后再配置 LDAP 服务器。

过程

步骤 1 选择 **Cisco Unified CM IM and Presence 管理** > **应用程序** > **第三方客户端** > **第三方 LDAP 服务器**。

步骤 2 单击**新增**。

步骤 3 输入 LDAP 服务器的 ID。

步骤 4 输入 LDAP 服务器的主机名。

对于 IPv6 连接，可以输入 LDAP 服务器的 IPv6 地址。

步骤 5 在监听 TCP 或 SSL 连接的 LDAP 服务器上指定端口号。

默认端口为 389。如果启用 SSL，请指定端口 636。

步骤 6 指定 LDAP 服务器的用户名和密码。 这些值必须与您在 LDAP 服务器上配置的凭证匹配。

有关此信息，请参阅 LDAP 目录文档或 LDAP 目录配置。

步骤 7 如果要使用 SSL 与 LDAP 服务器通信，请选中**启用 SSL**。

注释 如果启用了 SSL，则输入的**主机名**值可以是 LDAP 服务器的主机名或 FQDN。 使用的值必须与安全证书 **CN** 或 **SAN** 字段中的值相匹配。

如果必须使用 IP 地址，则此值还必须在证书上用于 **CN** 或 **SAN** 字段。

步骤 8 单击**保存**。

步骤 9 在群集中的所有节点上启动 Cisco XCP 路由器服务（如果此服务未运行）。

提示

- 如果启用 SSL，XMPP 搜索联系人的速度可能较慢，因为 IM and Presence Service 建立 SSL 连接后，设置 SSL 连接设置时要进行协商、数据加密和解密。 这样，如果用户在您的部署中广泛执行 XMPP 联系人搜索，将会影响总体系统性能。
- 在上传 LDAP 服务器的证书后，可以使用证书导入工具检查与 LDAP 服务器主机名及端口值的通信。 选择 **Cisco Unified CM IM and Presence 管理** > **系统** > **安全** > **证书导入工具**。
- 如果为第三方 XMPP 客户端更新 LDAP 服务器配置，请重新启动 Cisco XCP 目录服务。 选择 **Cisco Unified IM and Presence 功能配置** > **工具** > **控制中心 - 功能服务**以重新启动此服务。

下一步做什么

继续为 XMPP 客户端配置 LDAP 搜索设置。

为 XMPP 客户端配置 LDAP 搜索设置

必须指定可让 IM and Presence Service 对第三方 XMPP 客户端成功执行联系人搜索的 LDAP 搜索设置。

第三方 XMPP 客户端在每次搜索时连接到 LDAP 服务器。 如果无法连接到主服务器，XMPP 客户端会尝试第一个备份 LDAP 服务器，如果该服务器不可用，它将尝试第二个备份服务器，以此类推。 如果当系统故障转移时正在进行 LDAP 查询，下一个可用的服务器将完成此 LDAP 查询。

（可选）您可以打开从 LDAP 服务器检索 vCard 的功能。 如果您打开 vCard 检索：

- 公司 LDAP 目录会存储 vCard。
- 当 XMPP 客户端搜索自己的 vCard 或某个联系人的 vCard 时，将通过 JDS 服务从 LDAP 检索 vCard。
- 客户端无法设置或修改自己的 vCard，因为它们未获得编辑 LDAP 目录的授权。

如果打开从 LDAP 服务器检索 vCard 的功能：

- IM and Presence Service 将 vCard 存储在本地数据库中。
- 当 XMPP 客户端搜索自己的 vCard 或某个联系人的 vCard 时，将从本地 IM and Presence Service 数据库检索 vCard。

- 客户端可以设置或修改自己的 vCard。

下表列出了 XMPP 客户端的 LDAP 搜索设置。

表 *2: XMPP* 客户端的 *LDAP* 搜索设置

字段	设置
LDAP 服务器类型	从该列表中选择 LDAP 服务器类型： • Microsoft Active Directory • 通用目录服务器 - 如果要使用任何其他支持的 LDAP 服务器类型（iPlanet、Sun ONE 或 OpenLDAP），请选择此菜单项。
用户对象类	输入与您的 LDAP 服务器类型对应的“用户对象类”值。 此值必须与在您 LDAP 服务器上配置的“用户对象类”值匹配。 如果您使用 Microsoft Active Directory，则默认值为 user。
基本上下文	输入与您的 LDAP 服务器对应的“基本上下文”。 此值必须与以前配置的域和/或 LDAP 服务器上的组织结构相匹配。
用户属性	输入与您的 LDAP 服务器类型对应的“用户属性”值。 此值必须与在您 LDAP 服务器上配置的“用户属性”值匹配。 如果您使用 Microsoft Active Directory，则默认值为 sAMAccountName。 如果使用 Directory URI IM 地址方案，且 Directory URI 映射到 mail 或 msRTCSIPPrimaryUserAddress，则必须在用户属性中指定 mail 或 msRTCSIPPrimaryUserAddress。
LDAP 服务器 1	选择主 LDAP 服务器。
LDAP 服务器 2	（可选）选择备份 LDAP 服务器。
LDAP 服务器 3	（可选）选择备份 LDAP 服务器。

开始之前

为 XMPP 客户端指定 LDAP 服务器名称和地址。

过程

步骤 1 选择 **Cisco Unified CM IM and Presence 管理** > **应用程序** > **第三方客户端** > **第三方 LDAP 设置**。

步骤 2 在字段中输入信息。

步骤 3 如果要使用户能够请求其联系人的 vCard 和从 LDAP 服务器检索 vCard 信息，请选中**从 LDAP 建立 vCard**。 如果希望客户端能够在用户加入联系人列表时自动为用户请求 vCard，则将此复选框保持不选中状态。 在这种情况下，客户端从本地 IM and Presence Service 数据库检索 vCard 信息。

步骤 4 输入构造 vCard FN 字段所需的 LDAP 字段。 在用户请求联系人的 vCard 时，客户端使用 vCard FN 字段中的值显示联系人在联系人列表中的姓名。

步骤 5 在“可搜索 LDAP 属性”表中，将客户端用户字段映射到相应的 LDAP 用户字段。

如果使用 Microsoft Active Directory，IM and Presence Service 会填充表中的默认属性值。

步骤 6 单击**保存**。

步骤 7 启动 Cisco XCP 路由器服务（如果此服务未运行）

提示 如果更新第三方 XMPP 客户端的 LDAP 搜索配置，请重新启动 Cisco XCP 目录服务。 选择 **Cisco Unified IM and Presence 功能配置** > **工具** > **控制中心 - 功能服务**以重新启动此服务。

下一步做什么

继续打开 Cisco XCP 目录服务。

打开 Cisco XCP 目录服务

必须打开 Cisco XCP 目录服务，允许第三方 XMPP 客户端的用户从 LDAP 目录搜索和添加联系人。 在群集中的所有节点上打开 Cisco XCP 目录服务。

注释 不要打开 Cisco XCP 目录服务，直到您为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置。 如果打开了 Cisco XCP 目录服务，但没有为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置，该服务将启动，然后再次停止。

开始之前

为第三方 XMPP 客户端配置 LDAP 服务器和 LDAP 搜索设置。

过程

步骤 1 选择 **Cisco Unified IM and Presence 功能配置** > **工具** > **服务启动**。

步骤 2 从“服务器”菜单中选择 IM and Presence Service 节点。

步骤 3 选择 **Cisco XCP 目录服务**。

步骤 4 单击**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。