配置 LDAP 同步

- LDAP 同步概述， 第 1 页
- LDAP 同步前提条件， 第 2 页
- LDAP 同步配置任务流程， 第 2 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 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。

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。 决定要将哪个访问控制组分配给用户。 对于许多部署而言，默认组即已足够。 如果您需要自定义您的角色和组，请参阅《管理指南》的“管理用户访问”一章。
- 配置默认情况下应用于新的预配置用户的凭证策略的默认凭证。
- 如果要从 LDAP 目录同步用户，请确保设置了一个功能组模板，其中包含要分配给用户电话和电话分机的用户配置文件、服务配置文件以及通用线路和设备模板设置。

注释 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 3 页	登录到 Cisco Unified 功能配置并激活 Cisco DirSync 服务。

	命令或操作	目的
步骤 2	启用 LDAP 目录同步， 第 3 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 4 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 7 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 8 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。

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 8 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**。

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。