配置企业组

- 企业组概览，第 1 页
- 企业组前提条件，第 2 页
- 企业组配置任务流程，第 3 页
- 企业组部署模型 (Active Directory)，第 7 页
- 企业组限制，第 10 页

企业组概览

配置企业组时，Cisco Unified Communications Manager 会在将其数据库与外部 LDAP 目录同步时纳入用户组。 在 Cisco Unified CM 管理中，您可以在“用户组”窗口中查看同步的组。

此功能还可以帮助管理员：

- 为具有类似特征的用户设置通用功能集（例如，销售和会计团队）。
- 将消息发送到特定组中的所有用户。
- 为特定组的所有成员配置统一的访问权限

此功能还可以帮助 Cisco Jabber 用户快速构建具有共同特征的用户的联系人列表。 Cisco Jabber 用户可以在外部 LDAP 目录中搜索用户组，然后将其添加到其联系人列表中。 例如，Jabber 用户可以搜索外部LDAP目录并将销售组添加到联系人列表，从而也将所有销售团队成员添加到联系人列表中。 如果组在外部目录中更新，则用户的联系人列表会自动更新。

Windows 上的 Microsoft Active Directory 支持将企业组用作外部 LDAP 目录。

注释 如果禁用“企业组”功能，Cisco Jabber用户将无法搜索企业组或查看已添加到其联系人列表的组。 如果禁用此功能时用户已经登录，在用户注销前该组将一直可见。 用户再次登录时，该组将不可见

安全组

安全组是企业组的子功能。 Cisco Jabber 用户还可搜索安全组并将其添加至联系人列表。 要设置该功能，管理员必须配置一个自定义LDAP过滤器并将其应用到已配置的LDAP目录同步。 仅Microsoft Active Directory 支持安全组。

可允许的最多条目数

配置企业组时，请确保配置处理组的联系人列表最大值

- 联系人列表中允许的最多条目数是联系人列表条目数与已添加到联系人列表的组中的条目数之和。
- 联系人列表的最多条目数 =（联系人列表条目数）+（组中条目数）
- 启用“企业组”功能时，如果联系人列表的条目数不超过允许的最多条目数，Cisco Jabber用户就可将组添加到联系人列表。 该功能禁用时，如果超过了允许的最多条目数，则在该功能启用前用户不受限制。 如果用户在该功能启用后继续登录，将不会显示错误消息。 用户注销和再次登录时，将显示错误消息，要求用户删除过量条目。

企业组前提条件

此功能假定您已经使用以下条件配置了 LDAP 目录同步计划。 如需有关配置 LDAP 目录同步的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“从LDAP目录导入用户”一章。

- 必须激活 Cisco DirSync 服务
- LDAP 目录同步必须包含用户和组
- 必须安排使用 **LDAP 目录同步计划**配置的常规 LDAP 目录同步。

受支持的 LDAP 目录

企业组仅支持 Microsoft Active Directory。

LDAP 目录	企业组支持
Microsoft Active Directory	企业组和安全组均受支持。
OpenLDAP	Windows 上的 OpenLDAP 具有以下支持： • 仅支持 `GroupOfNames` 对象类 • OpenLDAP 不支持安全组。 • 最低版本为 2.4.42。 • 不支持 Linux 上的 OpenLDAP。

LDAP 目录	企业组支持
其他 LDAP 目录	不支持。

企业组配置任务流程

以下任务用于配置企业组功能。

过程

	命令或操作	目的
步骤 1	从 LDAP 目录验证组同步， 第 3 页	确认您的 LDAP 目录同步包括用户和组。
步骤 2	启用企业组， 第 4 页	完成此任务以使 Cisco Jabber 用户能够在 Microsoft Active Directory 中搜索企业组并将其添加到其联系人列表中。
步骤 3	更新 OpenLDAP 配置文件， 第 4 页	（仅 OpenLDAP）编辑 Windows 的 OpenLDAP 目录中的配置文件 `slapd.conf`。
步骤 4	启用安全组， 第 5 页	（可选）如果您希望 Cisco Jabber 用户能够搜索安全组并将安全组添加到其联系人列表，请完成此任务流程。
步骤 5	查看用户组， 第 7 页	（可选）查看与 Cisco Unified Communications Manager 数据库同步的 企业组和安全组。

从 LDAP 目录验证组同步

此程序用于确认您的 LDAP 目录同步是否包含用户和组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**服务器** > **LDAP** > **LDAP 目录**。

步骤 2 单击**查找**并选择要从中同步企业组的 LDAP 目录。

步骤 3 确认**同步**字段是否选定了**用户和组**。

步骤 4 在“LDAP 目录”配置窗口中完成剩余字段。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 5 单击**保存**。

启用企业组

配置系统以在 LDAP 目录同步中包含企业组。

过程

步骤 1 从“Cisco Unified CM 管理”中，选择**系统** > **企业参数**。

步骤 2 在**用户管理参数**下，将 **Cisco IM and Presence 上的目录组操作**参数设置为**启用**。

步骤 3 输入**允许在线状态信息的最大企业组大小**参数的值。 允许的范围是 1 到 200 个用户，默认值为 100 个用户。

步骤 4 从**企业组同步模式**下拉列表中配置您要定期执行的 LDAP 同步：**无**、**差异同步**、**完全同步**。

注释
请参阅企业参数帮助以获取有关配置这些字段的其他帮助。

步骤 5 单击**保存**。

更新 OpenLDAP 配置文件

如果您在 Windows 上通过 OpenLDAP 配置企业组，必须更新 OpenLDAP 目录中的 `slapd.conf` 文件。

过程

步骤 1 在 Windows 的 OpenLDAP 文件目录中，浏览到 `slapd.conf` 文件。

步骤 2 在文本编辑器中打开文件。

步骤 3 在文件中添加以下文本：

```
moduleload memberof.la
overlay memberof
memberof-group-oc groupOfNames
memberof-member-ad member
memberof-memberof-ad memberof
memberof-refint TRUE
cachesize 160000
```

步骤 4 保存文件。

步骤 5 重新启动 OpenLDAP 目录。

启用安全组

如果您要允许Cisco Jabber用户能将安全组添加至其联系人列表，请完成这些可选任务以将安全组纳入您的 LDAP 目录同步。

注释 安全组同步仅支持从 Microsoft Active Directory 同步。

注释 如果初始同步已经完成，您将无法在 Cisco Unified Communications Manager 中将新配置添加到现有的 LDAP 目录配置。

过程

	命令或操作	目的
步骤 1	创建安全组过滤器， 第 5 页	创建可同时过滤目录组和安全组的 LDAP 过滤器。
步骤 2	从 LDAP 目录同步安全组， 第 5 页	添加新的 LDAP 过滤器至 LDAP 目录同步。
步骤 3	为安全组配置 Cisco Jabber， 第 6 页	更新现有的服务配置文件以提供相关的Cisco Jabber用户可搜索和添加安全组的服务配置文件访问权限。

创建安全组过滤器

创建过滤安全组的 LDAP 过滤器。

过程

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

步骤 2 单击**新增**。

步骤 3 输入一个唯一的 **过滤器名称**。 例如，`syncSecurityGroups`。

步骤 4 输入以下 **过滤器**： `(&(objectClass=group)(CN=*))`。

步骤 5 单击**保存**。

从 LDAP 目录同步安全组

将安全组过滤器添加到 LDAP 目录同步并完成同步。

注释 如果初始 LDAP 同步已经完成，您将无法在 Cisco Unified Communications Manager 中将新配置添加到现有的 LDAP 目录配置。

注释 有关如何设置新 LDAP 目录同步的详细信息，请参阅《*Cisco Unified Communications Manager* 系统配置指南》的“配置最终用户”部分。

开始之前

创建安全组过滤器，第 5 页

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 执行下列操作之一：

- 单击“新增”以创建新的 LDAP 目录。
- 单击**查找**并选择用于同步安全组的 LDAP 目录。

步骤 3 从 **LDAP 自定义组过滤器**下拉列表中，选择您创建的安全组过滤器。

步骤 4 单击**保存**。

步骤 5 在 **LDAP 目录配置**窗口中配置任何剩余字段。 有关字段及其配置选项的更多信息，请参阅联机帮助。

步骤 6 单击**现在执行完整同步**以立即同步。 否则，当下一次预定的 LDAP 同步出现时，安全组才会进行同步。

为安全组配置 Cisco Jabber

更新现有的服务配置文件，以允许与此服务配置文件关联的 Cisco Jabber 用户从 LDAP 目录中将安全组添加至联系人列表。

注释 有关如何设置新的服务配置文件并分配至 Cisco Jabber 用户的详细信息，请参阅 *Cisco Unified Communications Manager* 系统配置指南的“配置服务配置文件”章节。

开始之前

从 LDAP 目录同步安全组，第 5 页

过程

步骤 1 在**服务配置文件配置**窗口完成其余字段的设置。 有关这些字段及其设置的帮助，请参阅联机帮助。

步骤 2 单击**查找**并选择 Jabber 用户使用的服务配置文件。

步骤 3 在**目录配置文件**下，选中**允许 Jabber 搜索和添加安全组**复选框。

步骤 4 单击**保存**。
与此服务配置文件关联的 Cisco Jabber 用户现在可以搜索和添加安全组。

步骤 5 为 Cisco Jabber 用户使用的全部服务配置文件重复此步骤。

查看用户组

您可以使用以下步骤查看与 Cisco Unified Communications Manager 数据库同步的 企业组和安全组。

过程

步骤 1 从 Cisco Unified CM 管理中，选择**用户管理** > **用户设置** > **用户组**。
此时将出现**查找并列出用户组**窗口。

步骤 2 输入搜索条件，然后单击**查找**。
此时将显示与搜索条件匹配的用户组列表。

步骤 3 要查看属于某个用户组的用户列表，请单击所需用户组。
此时将出现**用户组配置**窗口。

步骤 4 输入搜索条件，然后单击**查找**。
此时将显示与搜索条件匹配的用户列表。

如果单击列表中的用户，将出现**最终用户配置**窗口。

下一步做什么

（可选） 启用安全组，第 5 页

企业组部署模型 (Active Directory)

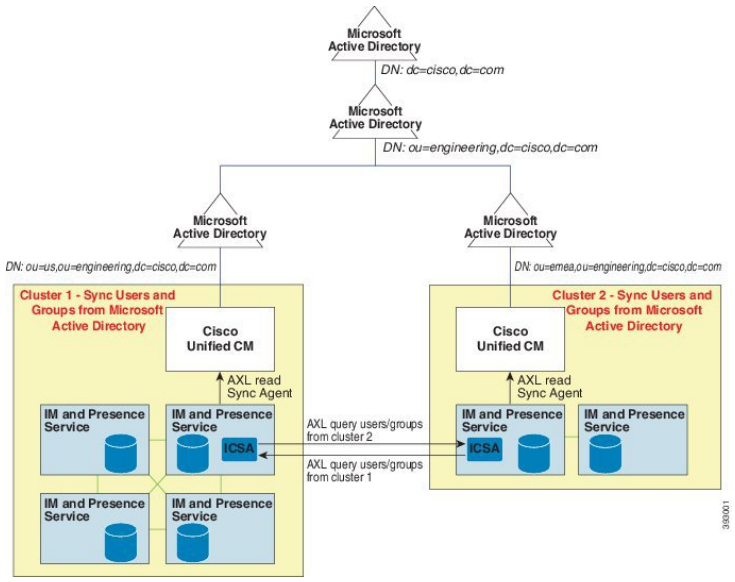
企业组功能为 Active Directory 提供了两个部署选项。

重要事项 在通过思科群集间同步代理服务同步数据之前，确保群集 1 和群集 2 具有一组唯一的 UserGroup、UserGroupMember 和 UserGroupWatcherList 记录。 如果两个群集都有唯一的记录集，则同步后两个群集都将具有所有记录的超级集合。

企业组部署模型 1

在此部署模型中，群集 1 和群集 2 从 Microsoft Active Directory 同步不同的用户和组子集。 思科群集间同步代理服务将数据从群集 2 复制到群集 1 中，以构建用户和组的完整数据库。

图 *1:* 企业组部署模型 *1*



企业组部署模型 2

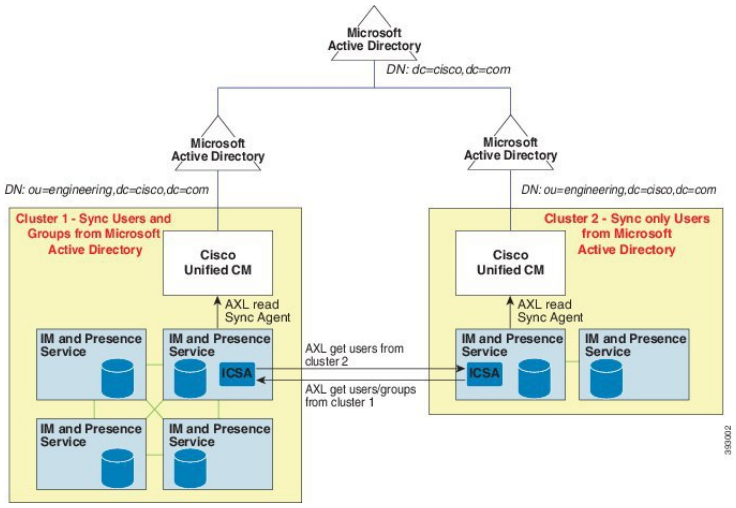
在此部署模型中，群集 1 从 Microsoft Active Directory 同步所有用户和组。 群集 2 只会从 Microsoft Active Directory 同步用户。 思科群集间同步代理服务将组信息从群集 1 复制到群集 2 中。

注意 如果使用此部署模型，请确保仅在一个群集中同步组数据。 如果不这样做，企业组功能将无法按预期工作。

您可以在 **Cisco Unified CM IM and Presence 管理** > **在线状态** > **群集间**窗口中验证您的配置。

检查群集间对等表中的**企业组 LDAP 配置**参数。 **未发现冲突**表示对等节点之间没有错误的配置。 如果发现冲突，单击“企业组冲突”链接，然后单击显示的**详细信息**按键。 这将打开“报告”窗口以显示详细报告。

图 *2:* 企业组部署模型 *2*


Microsoft Active Directory
DN: dc=cisco,dc=com
Microsoft Active Directory
Microsoft Active Directory
DN: ou=engineering,dc=cisco,dc=com
DN: ou=engineering,dc=cisco,dc=com
Cluster 1 - Sync Users and Groups from Microsoft Active Directory
Cisco Unified CM
AXL read Sync Agent
IM and Presence Service
IM and Presence Service
ICSA
IM and Presence Service
IM and Presence Service
AXL get users from cluster 2
AXL get users/groups from cluster 1
Cluster 2 - Sync only Users from Microsoft Active Directory
Cisco Unified CM
AXL read Sync Agent
IM and Presence Service
ICSA
IM and Presence Service
393002

企业组限制

表 *1:* 企业组限制

限制	说明
阻止所有人	当 Cisco Jabber 用户在其 Cisco Jabber 策略设置中启用“阻止所有人”功能时，会阻止其他 Jabber 用户查看或与阻止的用户交换即时消息和在线状态，除非他们是阻止用户的联系人列表中的联系人。 例如，Cisco Jabber 用户 (Andy) 已在其个人 Jabber 设置中启用阻止所有人。 以下列表分解了 Andy 的阻止设置如何影响其他 Jabber 用户，这些用户可能包括也可能不包含在 Andy 的个人联系人列表中。 除了设置阻止功能之外， Andy 的个人联系人列表中： • 包括 Bob — 由于 Bob 在 Andy 的个人联系人列表中，尽管设置了阻止，但他仍然可以发送即时消息和查看 Andy 的在线状态。 • 忽略 Carol — 由于设置了阻止，Carol 不能查看 Andy 的在线状态或发送即时消息。 • 将 Deborah 作为个人联系人。 然而，Deborah 是 Andy 列为联系人的企业组成员 — Deborah 被禁止查看 Andy 的在线状态或向 Andy 发送 IM。 请注意，尽管 Deborah 在 Andy 的联系人列表中是企业组成员，但他仍然无法查看 Andy 的在线状态，也无法向 Andy 发送即时消息。 有关企业组联系人行为的其他详细信息，请参阅 CSCvg48001。
与 10.x 群集的群集间对等	版本 11.0(1) 及更高版本支持企业组。 如果同步组包含来自 10.x 群集间对等的组成员，则较高群集上的用户无法查看 10.x 群集中的同步成员的在线状态。 这是由于 11.0(1) 为企业组同步引入的数据库更新造成的。 这些更新不是 10.x 版本的一部分。 为了保证驻留在较高群集上的用户可以查看驻留在 10.x 群集上的组成员的在线状态，较高群集上的用户应手动将 10.x 用户添加到其联系人列表中。 手动添加的用户没有在线状态问题。
多级分组	组同步不允许多级分组。
仅组同步	当用户组和用户出现在同一搜索库中时，不允许进行仅组同步。 相反，用户组和用户都是同步的。

限制	说明
最大用户组数量	您可以将 Microsoft Active Directory 服务器中的最多 15000 个用户组同步到 Unified Communications Manager 数据库。 每个用户组可以包含 1 到 200 个用户。您可以在 **Cisco Unified CM IM and Presence 管理** > **系统** > **服务参数**窗口配置具体数量。 数据库中的最大用户帐户数不能超过 160,000。
用户组迁移	如果用户组从一个组织单位移到另一个组织单位，必须先对原始单位执行完全同步，然后对新单位执行完全同步。
本地组	本地组不受支持。 仅支持从 Microsoft Active Directory 同步的组。
未分配给 IM and Presence Service 节点的组成员	未分配给 IM and Presence Service 节点的组成员显示在联系人列表中，并且状态气泡显示为灰色。 但是，在计算联系人列表中允许的最大用户数时会考虑这些成员。
从 Microsoft Office Communication Server 迁移	从 Microsoft Office Communication Server 迁移期间，在用户完全迁移到 IM and Presence Service 节点之前，企业组功能不受支持。
LDAP 同步	如果您在同步过程中更改 **LDAP 目录配置窗口**中的同步选项，现有同步不受影响。 例如，如果您在同步过程中将同步选项从**用户和组**变更为**仅用户**，用户和组同步仍会继续。
通过边缘的组搜索功能	本版本提供通过边缘的组搜索功能，但尚未经过全面测试。 因此，无法保证完全支持通过边缘的组搜索。 预计未来版本中会实现对此功能的全面支持。
思科群集间同步代理服务定期同步	如果在外部 LDAP 目录中更新了组名称或组成员名称，则只有在思科群集间同步代理服务定期同步之后，信息才会在 Cisco Jabber 联系人列表中更新。 通常情况下，思科群集间同步代理服务同步每 30 分钟进行一次。
通过 LDAP 配置中的不同同步协议同步用户和用户组	如果用户和用户组作为同一同步协议的一部分同步到 Cisco Unified Communications Manager 数据库，同步后，Cisco Unified Communications Manager 数据库中的用户和组关联也会按预期更新。 但是，如果用户和用户组作为不同同步协议的一部分同步，则在第一次同步后，用户和组可能无法在数据库中关联。 数据库中的用户和组关联取决于同步协议的处理顺序。 如果用户在组之前同步，则这些组可能在数据库中不可用于关联。 在这种情况下，您必须确保在与用户的同步协议之前安排与组的同步协议。 否则，在组同步到数据库之后，用户将在下一次手动或定期同步后与组关联，并将同步类型设置为“用户和组”。 仅当协议同步类型设置为“用户和组”时，系统才会映射用户和相应组的信息。 .

限制	说明
已测试企业组的 OVA 信息	**测试的场景** 在具有两个群集（群集 A 和群集 B）的群集间部署中： 从 Active Directory 同步的 160K 用户中，群集 A 为 IM and Presence Service 启用了 15K OVA 和 15K 用户。 在 15K OVA 群集上，每个用户经过测试和支持的平均企业组数量为 13 个企业组。 从 Active Directory 同步的 160K 用户中，群集 B 为 IM and Presence Service 启用了 25K OVA 和 25K 用户。 在 25K OVA 上，每个用户经过测试和支持的平均企业组数量为 8 个企业组。 名录中经测试和支持的用户个人联系人与用户名册中来自企业组的联系人的总和小于或等于 200。 **注释** 在具有 2 个以上群集的环境中，这些号码不受支持。
导出联系人列表	在使用**批量管理** > **联系人列表** > **导出联系人列表**来导出用户的联系人列表时，联系人列表 CSV 文件不包含他们在 Jabber 客户端中的企业组的详细信息。

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。