用户管理

Jabber ID

Cisco Jabber 使用 Jabber ID 标识联系人来源中的联系人信息。

使用用户 ID 和在线状态域创建默认 Jabber ID。

例如，Adam McKenzie 的用户 ID 为 `amckenzie`，他的域为 `example.com`，其 Jabber ID 为 `amckenzie@example.com`。

Cisco Jabber 用户 ID 或电子邮件地址支持下列字符：

- 大写字符（A 到 Z）
- 小写字符（a 到 z）
- 数字 (0-9)
- 点号 (.)
- 连字符 (-)
- 下划线 (_)
- 代字号 (~)
- 井号标签 (#)

当填充联系人列表时，客户端将使用 Jabber ID 搜索联系人来源以解析联系人，并显示“名字”、“姓氏”和任何其他联系信息。

IM 地址方案

Cisco Jabber 10.6 和更高版本支持在域处于相同的在线状态架构（例如 example-us.com 和 example-uk.com 中的用户）时用于内部部署的多个在线状态域架构模型。Cisco Jabber 支持使用 Cisco Unified Communications Manager IM and Presence 10. x 或更高版本的灵活 IM 地址方案。IM 地址方案是用于识别 Cisco Jabber 用户的 Jabber ID。

为支持多域模型，部署的所有组件都需要以下版本：

- Cisco Unified Communications IM and Presence 服务器节点和呼叫控制节点版本 10. x 或更高版本。
- 在 Windows、Mac、IOS 和 Android 版本 10.6 或更高版本上运行的所有客户端。

在以下情况下，仅部署具有多个域架构的 Cisco Jabber：

- Cisco Jabber 10.6 或更高版本经部署为所有平台（Windows、Mac、IOS 和 Android，包括基于 Android 的 IP Phones（例如 DX 系列））上组织中所有用户的全新安装。
- 在在线状态服务器上更改任何域或 IM 地址之前，Cisco Jabber 将为所有平台（Windows、Mac、IOS 和 Android，包括基于 Android 的 IP 电话（例如 DX 系列））上的所有用户升级到版本 10.6 或更高版本。

高级在线状态设置中的可用 IM 地址方案包括：

- UserID@[默认域]
- 目录 URI

UserID@[默认域]

将“用户 ID”字段映射到 LDAP 字段。这是默认的 IM 地址方案。

例如，用户 Anita Perez 的帐户名称为 aperez，且将“用户 ID”字段映射到 sAMAccountName LDAP 字段。使用的地址方案为 aperez@example.com。

目录 URI

将目录 URI 映射到**邮件**或 **msrtcsip-primaryuseraddress msrtcsip-primaryuseraddress** LDAP 字段。此选项提供独立于用于身份验证的用户 ID 的方案。

例如，用户 Anita Perez 的帐户名称为 aperez，“邮件”字段为 Anita.Perez@domain.com，使用的地址方案为 Anita.Perez@domain.com。

使用 Jabber ID 的服务发现

服务发现使用以 `[userid]@[domain.com]` 格式输入的 Jabber ID，并且默认情况下会提取 Jabber ID 的 `domain.com` 部分以发现可用的服务。对于在线状态域与服务发现域不同的部署，您可以在安装期间包含服务发现域信息，如下所示：

- 在 Cisco Jabber Windows 版本中，此操作使用 `SERVICES_DOMAIN` 命令行参数完成。
- 在 Cisco Jabber Mac 版本、Cisco Jabber Android 版本或 Cisco Jabber iPhone 和 iPad 版本中，可以使用与 URL 配置配用的 `ServicesDomain` 参数设置服务发现域。

。

SIP URI

SIP URI 与每个用户关联。SIP URI 可以是电子邮件地址、IMAddress 或 UPN。

SIP URI 使用 Cisco Unified Communications Manager 中的“目录 URI”字段进行配置。以下是可用的选项：

- 邮件
- msRTCSIP-primaryuseraddress

用户可以通过输入 SIP URI 搜索联系人并给联系人拨号。

LDAP 用户 ID

您从目录来源同步到 Cisco Unified Communications Manager 时，可以从目录属性填充用户 ID。保留用户 ID 的默认属性为 `sAMAccountName`。

用于联合的用户 ID 规划

对于联合，Cisco Jabber 需要每个用户的联系人 ID 或用户 ID，以便在联系人搜索期间解析联系人。

在 SipUri 参数中设置用户 ID 的属性。默认值为 `msRTCSIP-PrimaryUserAddress`。如果存在要从您的用户 ID 中删除的某个前缀，您可以在 UriPrefix 参数中设置一个值，请参阅《*Cisco Jabber* 的参数参考指南》的最新版本。

用于用户联系人照片的代理地址

Cisco Jabber 访问照片服务器以检索联系人照片。如果您的网络配置包含 Web 代理，则需要确保 Cisco Jabber 能够访问照片服务器。

身份验证和授权

Cisco Unified Communications Manager LDAP 身份验证

在 Cisco Unified Communications Manager 上配置 LDAP 验证，以通过目录服务器进行验证。

当用户登录到客户端时，在线状态服务器会将身份验证路由到 Cisco Unified Communications Manager。Cisco Unified Communications Manager 随后会将该身份验证代理到目录服务器。

Cisco Webex Messenger 登录验证

使用 Cisco Webex 管理工具配置 Cisco Webex Messenger 身份验证。

当用户登录到客户端时，该信息将发送到 Cisco Webex Messenger，并且身份验证令牌会发送回客户端。

单点登录身份验证

使用身份提供程序 (IdP) 和服务配置单点登录验证。

当用户登录到客户端时，该信息将发送到 IdP，一旦接受凭证，身份验证令牌就会发送回 Cisco Jabber。

用于 Cisco Jabber iPhone 和 iPad 版本的基于证书的验证

Cisco Jabber 通过客户端证书在 IdP 服务器上进行身份验证。此证书验证可让用户无需输入用户凭证即可登录到服务器。客户端使用 Safari 框架来实施此功能。

要求

- Cisco Unified Communications Manager 11.5、IM and Presence Service 11.5、Cisco Unity Connection 11.5 及更高版本。
- Expressway for Mobile and Remote Access server 8.9 及更高版本。
- SSO 已针对统一通信基础设施启用。
- 所有服务器证书均已由 CA 签署，包括 Cisco Unified Communications Manager、IM and Presence Service、Cisco Unity Connection 和 IdP 服务器。如果 iOS 设备使用 OS 的受信任授权机构，请在安装 Cisco Jabber 应用程序之前安装 CA 证书。
- 在 Cisco Unified Communications Manager 中为 SSO 配置本机浏览器（嵌入式 Safari）。有关详细信息，请参阅 *Cisco Jabber* 内部部署中基于证书的 SSO 身份验证部分。
- 在 Expressway for Mobile and Remote Access server 中配置用于 SSO 的本机浏览器（嵌入式 Safari）。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》。

您可以通过 EMM 解决方案在 iOS 设备上部署 Cisco 证书。

建议 — **Cisco** 建议使用 EMM 解决方案在 iOS 设备上部署证书。

用于 Cisco Jabber Android 版本的基于证书的验证

Cisco Jabber 使用客户端证书登录到单点登录服务器（Webex Messenger 和内部）。

要求

- Android 操作系统 5.0 或更高版本
- 已启用单点登录
- Jabber 客户端通过移动和Remote Access (MRA) 和非 MRA 部署模式得到支持。
- Jabber 始终在 Android 7.0 和更高版本上显示无效证书的通知，即使 Android OS 上已安装自定义 CA 签名的证书也是如此。面向 Android 7.0 的应用程序仅信任系统提供的证书，不再信任用户添加的证书权限。

证书部署

Cisco 建议使用 EMM 解决方案在 Android 设备上部署证书。

语音邮件验证

用户需要在 Cisco Unity Connection 上存在。Cisco Unity Connection 支持多个验证类型。如果 Cisco Unified Communications Manager 和 Cisco Unity Connection 使用相同的验证，我们建议将 Cisco Jabber 配置为使用相同的凭证。

OAuth

您可以将 Cisco Jabber 设置为使用 OAuth 协议来授权用户对服务的访问权限。如果用户登录到启用 OAuth 的环境，则无需在每次用户登录时都输入凭证。但是，如果服务器没有启用 OAuth，则 Jabber 可能无法正常工作。

如果您使用 Cisco Unified Communication Manager 12.5 或更高版本，您也可以启用 SIP OAuth。它允许 Jabber 向 SIP 自行授权，从而允许 Jabber 通过 TLS 连接到 SIP 服务。它还可让 Jabber 通过安全连接 (sRTP) 发送媒体。SIP OAuth 意味着不再需要 CAPF 注册来启用安全 SIP 和媒体。

先决条件：

- 如果部署为功能，则必须跨所有这些组件打开 OAuth 刷新令牌
- Cisco Unified Communication Manager、Cisco Unified Communication ManagerInstant Messaging and Presence 以及 Cisco Unity Connection 必须是版本 11.5(SU3) 或 12.0
- Cisco Expressway for Mobile and Remote Access 版本 X8.10 或更高版本

- 对于 SIP OAuth：Cisco Unified Communication Manager 12.5 或更高版本、Cisco Expressway for Mobile and Remote Access 版本 X12.5 或更高版本。

在配置 OAuth 之前，请检查您拥有的部署类型：

- 如果您有本地验证部署，则不需要 IdP 服务器，Cisco Unified Communication Manager 负责进行验证。
- 您可以配置或不配置 SSO 来设置 OAuth。如果您正使用 SSO，请确保将其为所有服务启用。如果您有启用 SSO 的部署，则部署 IdP 服务器，IdP 服务器负责进行验证。

您可以为您的用户启用以下服务的 OAuth：

- Cisco Unified Communications Manager
- Cisco Expressway
- Cisco Unity Connection

默认情况下，这些服务器上禁用 OAuth。要在这些服务器上启用 OAuth：

- 对于 Cisco Unified Communications Manager 和 Cisco Unity Connection 服务器，请转到**具有刷新登录流 > 的企业参数配置 OAuth**。
- 对于 Cisco Expressway，转至**通过刷新由 OAuth 令牌授权的配置统一通信 > 配置**。

当在任何这些服务器上启用或禁用 OAuth 时，Jabber 会在配置重新提取间隔内识别它，并让用户注销并登录到 Jabber。

在注销期间，Jabber 会删除缓存中存储的用户凭证，然后让用户使用常规登录流登录，其中 Jabber 首先获取所有配置信息，然后让用户访问 Jabber 服务。

要配置 Cisco Unified Communication Manager 上的 OAuth：

1. 转至 **Cisco Unified Communications Manager 管理 > 系统 > 企业参数 > SSO 配置**。
2. 将 **O-Auth 访问令牌到期计时器（分钟）**设置为所需的值。
3. 将 **O-Auth 刷新令牌到期计时器（天）**设置为所需的值。
4. 点击**保存**按钮。

要在 Cisco Expressway 上配置 OAuth：

1. 转至**配置 > 统一通信 > 配置 > MRA 访问控制**。
2. 将 **O-Auth 本地身份验证**设置为“开”。

要在 Cisco Unity 上配置 OAuth：

1. 转至 **AuthZ 服务器**并选择**新增**。
2. 在所有字段中输入详细信息，然后选择“**忽略证书错误**”。
3. 单击**保存**。

限制

Jabber 触发自动入侵保护

条件：

- 配置您的 Expressway for Mobile and Remote Access 部署以通过 OAuth 令牌（带有或不带刷新令牌）进行授权。
- Jabber 用户的访问令牌已过期。

Jabber 执行以下一项操作：

- 从桌面休眠恢复
- 恢复网络连接
- 在注销后几个小时尝试快速登录

行为:

- 一些 Jabber 模块尝试使用过期的访问令牌在 Expressway-E 上进行授权。
- Expressway-E（正确）拒绝这些请求。
- 如果特定 Jabber 客户端上有五个以上的此类请求，Expressway-E 将阻止该 IP 地址十分钟（默认）。

症状：

受影响的 Jabber 客户端的 IP 地址将添加到 HTTP 代理授权失败类别中 Expressway-E 的被阻止地址列表 。您可以在**系统** > **保护** > **自动检测** > **阻止的地址**上查看这些地址。.

暂时解决办法：

您可以通过两种方式解决此问题；您可以增加该特定类别的检测阈值，也可以为受影响的客户端创建例外。我们在此处介绍阈值选项，因为例外在您的环境中可能不实用。

1. 转至**系统** > **保护** > **自动检测** > **配置**。
2. 单击 **HTTP 代理授权失败**。
3. 将**触发器级别**从 5 更改为 10。10 必须足以容许显示到期令牌的 Jabber 模块。
4. 保存配置，此操作会立即生效。
5. 取消阻止任何受影响的客户端。

多资源登录

当用户登录到系统时，所有 Cisco Jabber 客户端都会向以下中心 IM and Presence Service 节点之一注册。此节点跟踪 IM and Presence Service 环境的可用性、联系人列表和其他方面。

- 内部部署：Cisco Unified Communications Manager IM and Presence Service。

- 云部署：Cisco Webex。

此 IM and Presence Service 节点按以下顺序跟踪与每个唯一网络用户相关联的所有已注册客户端：

1. 当在两个用户之间启动新的 IM 会话时，第一个传入消息被广播给接收用户的所有注册的客户端。
2. IM and Presence Service 节点会等待其中一个注册的客户端的第一个响应。
3. 第一个响应的客户端然后会收到剩余的传入消息，直到用户使用另一个注册的客户端开始响应。
4. 然后，节点将后续消息重新路由到此新客户端。

注释 如果用户登录到多个设备时没有活动的资源，则优先级将给予具有最高在线状态优先级的客户端。如果所有设备上的在线状态优先级相同，则优先级将分配给用户登录到的最新客户端。