

XMPP(Jabber) 聊天快速指南

2017 年 3 月

什么是 XMPP(Jabber)? 为什么推广 XMPP?

简而言之, XMPP (又称为 Jabber) 是一种开放的互联网实时通讯协议。很多流行的聊天软件都是 XMPP 的封装应用, 比如 Google Hangout、Facebook Message、AOL Chat、米聊、人人桌面和陌陌等。很多网络游戏的内部聊天用的也是 XMPP 协议。

我们推广 XMPP 是希望推动这种开放的聊天协议, 完全使用自由软件建立自由软件社群人与人之间沟通的桥梁。XMPP 配合 OTR 或 OMEMO 的端对端加密聊天, 替代传统封闭的、有隐私泄漏风险的专有软件, 同时探索社群沟通新生态。

安装 XMPP 客户端

支持 XMPP 的客户端有很多, 这里仅选取经过 BLUG 成员测试挑选之后, 最适合自由软件社群的。以下所列均为自由软件。

PC 客户端: 推荐使用 Pidgin, GNU/Linux 发行版可通过包管理器搜索“pidgin”来安装, 也可以从 <https://pidgin.im> 下载源码包编译安装。Windows 可前往 <https://pidgin.im> 网站下载二进制安装包。

macOS 客户端: 推荐使用 Adium, 可以从 <https://adium.im> 网站下载到。也可以用 Jitsi, 到这里直接下载 <https://jitsi.org/Main/Download>。

移动客户端: Android 系统强烈推荐 Conversations, 支持发送图片、语音和文件等多种格式。首先前往 <https://f-droid.org> 下载安装 F-Droid 市场, 然后更新包缓存, 之后就可以搜索并安装 Conversations 了。iOS 系统可以安装 ChatSecure, 从 App Store 上直接搜索安装即可, 支持发送图片和语音。

注册 XMPP 账号

互联网上有很多开放的 XMPP 服务, 可以通过 <https://xmpp.net> 网站查找。BLUG 服务器也开放了 XMPP 服务 blug.moe。经过我们的大量测试, 安全性较好且速度较快的有 jwchat.org、im.koderoot.net、dukgo.com 和 jabber.cat, 其他服务器账号可与我们联系。可以自由选择这些服务器注册。注册成功以后就获得了一个形如 `yourname@domain.name` 的账号。

注册方法非常简单, 以上公开的 XMPP 服务器都支持客户端注册, 只需要在添加账号时勾选“在服务器上创建此账号”或“我想注册一个新账户”, 并在服务器(或“域”)一栏填入服务器地址即可; 有的客户端(比如 Conversations)可直接输入你想注册的账号, 例如填上 `yourname@blug.moe` 就表示希望注册 blug.moe 服务器上的账号, 然后输入希望使用的密码。下图展示了 Pidgin 上如何注册和设置新账号。

特别提醒, 很多 XMPP 服务器并不支持密码找回(包括 blug.moe), 请记住并妥善保管你的 XMPP 账户密码!



Android 的 Conversations 客户端



添加好友，无限畅聊

注册成功以后就可以用新账号登录了，添加好友开始聊天吧！以上推荐的服务器都支持跨服务器加好友和聊天，例如在 blug.moe 上注册的账号可以加 xmpp.is 或其他公开服务的好友聊天。注意添加好友时需要输入对方完整的 XMPP 账号。

BLUG 也有和 IRC 聊天同步的账号 chatirc@beijinglug.club，只要加此账号为好友，就可以与 IRC 同步聊天啦！

加入群聊（多用户聊天）

还可以用 XMPP 多人聊天（“聊天室”或“讨论组”），只需要在软件里选择“加入聊天”，然后输入讨论组的账号即可。

使用端对端加密聊天保护隐私

OTR（Off The Record）端对端加密为一对一聊天增加了更多的安全性。OTR 是非对称加密，并具有否定性，即便是密钥丢失，过往的聊天记录也无法解密。类似的端对端加密方式还有 OMEMO。

有些客户端内置了 OTR 加密插件，比如 Adium、Conversations 和 ChatSecure。只要在一对一聊天界面找到形如挂锁的图标 （未加密）或“OTR”菜单，然后点选这个图标，并在弹出菜单中选择开始私密聊天（或类似的文字）即可。稍等片刻一旦私密聊天建立，图标会变成闭合的挂锁图标 （已加密），聊天界面里也可以看到相应的文字提示。Conversations 和 ChatSecure 还支持 OMEMO 加密，开启加密的方式与之类似，但要注意验证此设备是否是你亲自登录。

Pidgin 需要安装相应的 OTR 插件。GNU/Linux 发行版可以搜索并安装“pidgin-otr”包，Windows 用户前往 <https://otr.cypherpunks.ca> 下载并安装 Pidgin 的 OTR 插件。插件安装好以后，在“工具->插件”目录下找到并勾选 Off The Record Messaging。然后按“配置插件”按钮，打开对话框，按“生成”按钮以生成 OTR 密钥和指纹。之后就可以按上面类似的方法开启加密聊天了。

加密聊天建立以后，需要验证对方身份（这一步可选），可以通过保密问题或直接验证指纹的方式。注意：**OTR 是客户端对客户端的加密**，同一账户的不同客户端，指纹并不相同，因此均需要验证。

发送图片、语音和文件

发送图片、语音和文件，与客户端有很大关系。目前经过测试，Conversations 可以非常好的支持发送音视频和文件，OTR 加密启用时文件也同时加密传输。ChatSecure 也支持发送加密的图片和语音。PC 端的软件大多只支持文件传送。移动端与 PC 端之间暂时还不能传送加密的图片、语音和文件。

详细配图教程（Tutorials）

- GNU/Linux 系统使用 OTR 详细教程：<https://ssd.eff.org/en/module/how-use-otr-linux>
- Windows 系统使用 OTR 详细教程：<https://ssd.eff.org/en/module/how-use-otr-windows>
- MacOS 系统使用 OTR 详细教程：<https://ssd.eff.org/en/module/how-use-otr-mac>



Pidgin 的添加新账户设置

