XMPP 新手使用手册

2024 年 11 月 13 日版

目录

XMPP 客户端分发下载渠道问题

请不要在不可靠的分发渠道下载安装 XMPP 客户端，也不要在私有平台直接为他人分发 XMPP 客户端安装包，尽管 XMPP 客户端本体安装包是十分安全的，但如果在不可靠的分发渠道下安装 XMPP 客户端，就有可能下载到遭到篡改内置后门的 XMPP 客户端，也不要在私有平台直接分发 XMPP 客户端安装包，因为私有平台可能会篡改你分发的 XMPP 客户端安装包，本手册内置的 XMPP 客户端下载链接都是可靠分发渠道的下载链接，建议向新手分发本手册的宣传专用下载链接，如在私有平台分发本手册宣传专用下载链接，请通过 PrivateBin 免翻墙文字寄存实例分发，并设置复杂的链接访问密码和较短的链接有效时间，请勿在私有平台直接分发本手册下载链接和文件副本，否则由此产生的一切安全问题和相关责任由分发者自行承担。

PrivateBin 免翻墙文字寄存实例推荐列表:
(1) https://privatebin.arch-linux.cz/
(2) https://0.jaegers.net/
(3) https://bin.0xfc.de/
(4) https://bin.bus-hit.me/
(5) https://bin.ngn.tf/

《XMPP 新手使用手册》git 仓库免翻墙最新版下载链接(推荐链接):
https://codeberg.org/xmppjx/xmpp
（链接包含手册文件副本以及安卓客户端安装包，该链接可以免翻墙打开下载，但仅建议在手册所有源都失效的情况下使用安装包。)

《XMPP 新手使用手册》宣传专用下载链接(推荐链接):
https://zb3.org/xmppjxgh/xssysc
(基于 Firefox Send 实例和 writefreely 实例的手册免翻墙永久更新维护下载链接，相对其他链接更加下载简单一步到位，并且抗长城防火墙封锁能力更强，如其他下载链接免代理条件下打不开，可尝试打开本下载链接访问，建议用于对外宣传分发。)

请点击最新版手册下载链接查看自己当前阅读的《XMPP 新手使用手册》是否为最新版。如手册当前阅读版本并非最新版本可能会出现一系列问题，建议下载最新版本手册文件阅读。下载最新版本手册后如果也有问题，可向我们的手册教学邮箱反馈问题。

全系统自由免费浏览器下载链接:
https://rant.li/t8dvecaox6
(如手册内的链接无法正常打开，可能因为国产私有软件浏览器导致，请将浏览器更为自由免费浏览器打开链接)。

前言

我相信看到这份手册的人们一定会感到很多疑惑，比如说 XMPP 是什么？我们为什么要下载使用 XMPP?

在这里我们简单明了的介绍一下 XMPP:
XMPP 是一款类似 QQ 的即时通讯聊天平台。但它的客户端和服务端是自由开源免费的，并接受 GPL-3.0 自由软件许可协议标准及自由件社区监督，因此不存在任何软件源代码后门。并且自带现代军事级的端到端加密算法，可以保证您在合理的条件下使用它，不会被除您和交流者以外的人监视聊天内容。而且绝大部分 XMPP 服务器注册不需要提供任何隐私信息，在其上聊天可以保证隐私信息匿名安全。同时由于它的服务器架构邦联制去中心化互通互联，人人都可以自建部署服务器，因此在其上的服务器无法被任何个人和组织垄断。也无法建立中心化的言论审查机制，在上面说话无需担心被封号禁言。

更多有关 XMPP 自由邦联即时通讯的相关信息可查看:
https://xmpp.org/

https://beijinglug.club/wiki/lib/exe/fetch.php?media=xmpp-guide.pdf

XMPP
看到这里您可能已经想要下载使用 XMPP 了，但却不知道应该如何下载使用 XMPP，我们将在以下篇幅介绍 XMPP 客户端的下载链接、XMPP 各系统客户端的下载使用教程、本手册隶属的 XMPP 聊天室地址、本手册提供教学的匿名邮箱联系地址、本手册隶属的 XMPP 私人教学公号，并对这些介绍分步骤进行配图教学，保证看到这个手册的人们能够成功下载使用 XMPP。

一.安卓操作系统应该如何下载 XMPP 客户端?
我们这里推荐安卓系统下载 XMPP 客户端 Conversations，因为这个 XMPP 客户端是自由软件且具有良好的客户端稳定性、对新人友好的客户端操作难度、支持开启 OMEMO/OpenPGP (端到端加密)、现代的客户端 UI(用户界面)等等优势。

以下是 Conversations 客户端下载链接(访问免翻墙)：：
https://rant.li/g8gbqzmyf8

Conversations 客户端使用操作说明详见(访问免翻墙):
https://conversations.xmpp45.dynv6.net

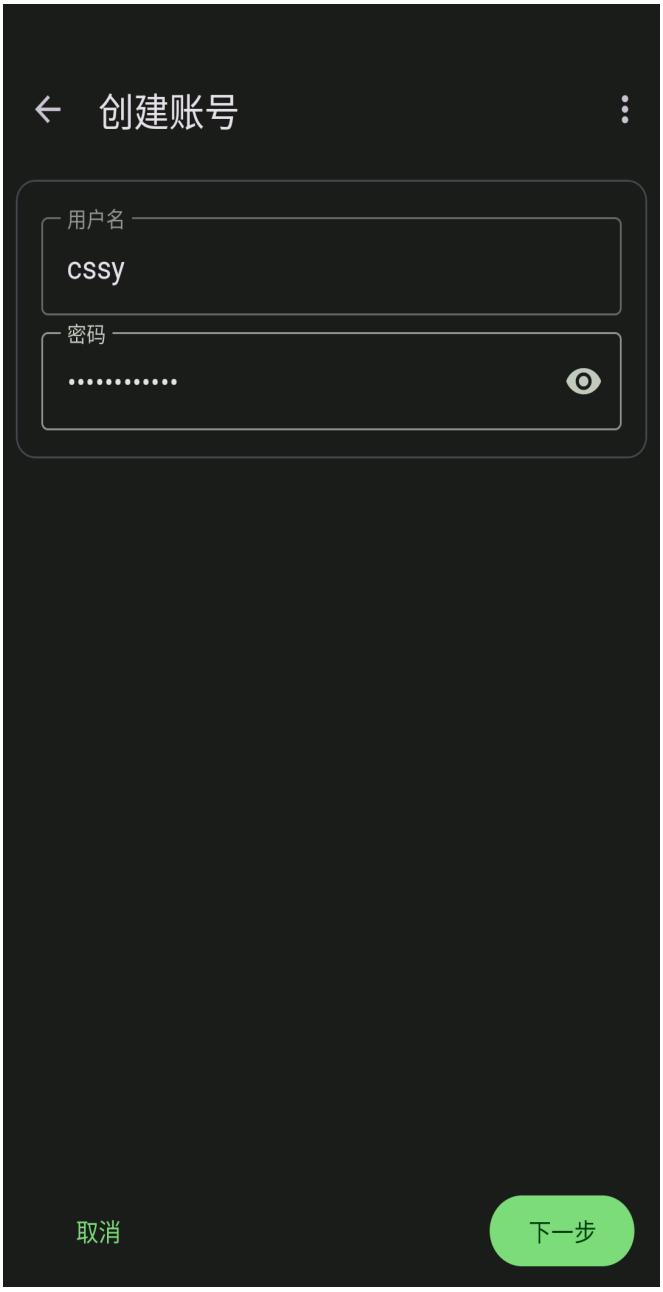
我已经下载安装好了 XMPP 安卓客户端，接下来应该怎么做?

第一步点击创建新账号

第二步点击使用 conversations.im

第三步输入一个用户名 (用户名最好只使用小写字母和数字，不要使用特殊符号和其他字符，否则可能会注册失败，并且请尽量使用具有特色的用户名，跟其他用户重名也会导致无法注册，用户名不要跟其他平台有关联，防止被有心之人通过身份关联性顺藤摸瓜。)

第四步设置一个密码并点击下一步
(点击使用 conversations.im 以后会自动生成一个密码，我们最好不要使用这个自动生成的密码，应当设置一个自己能记住的密码，防止因密码忘记丢失账号，密码长度不要太短了否则可能会注册失败，注册过程也不要退出界面做其他事情，这样也有可能导致注册失败。）

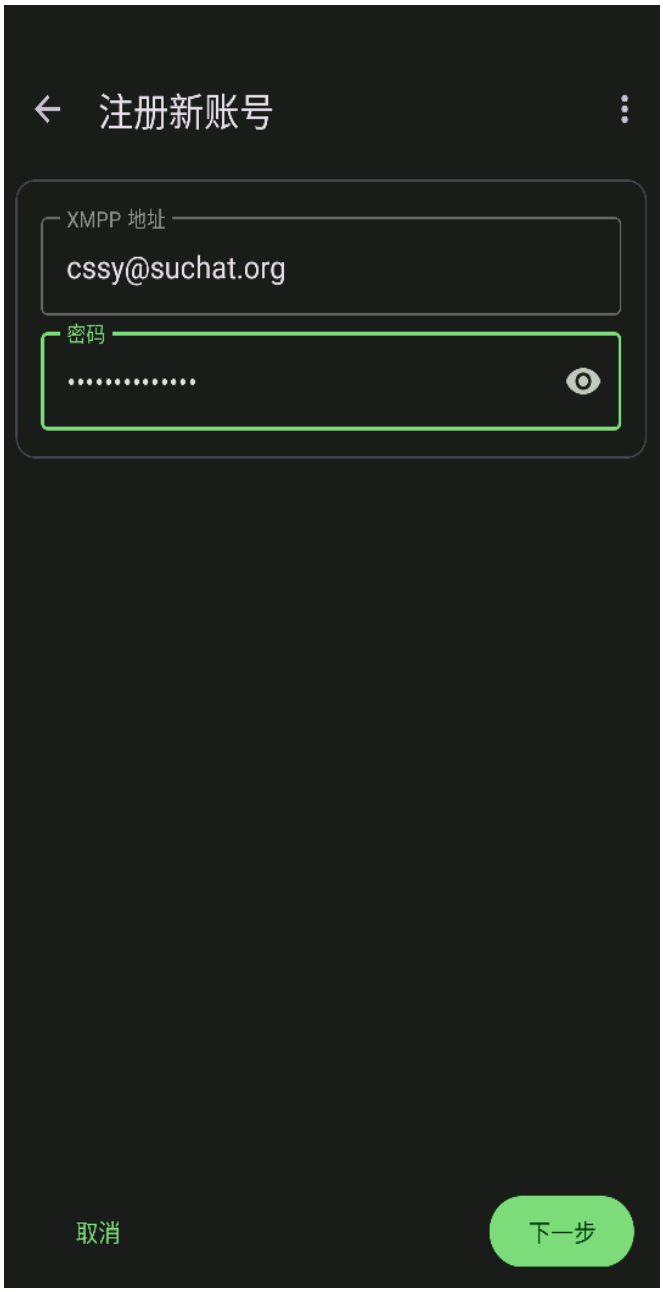


第五步通过注册验证码
点击下一步以后请等待一会，会弹出一个注册验证码弹窗，请区分验证码大小写后输入正确验证码，如果点击下一步以后未弹出验证码弹窗，请检测是否是用户名重复/不符合标准，如果不是请检查自己的网络环境是否正常，以及 conversationa.im 服务器是否被屏蔽封锁了。

第六步 如果 conversations.im 服务器被屏蔽封锁该怎么办?
我们推荐您使用翻墙代理工具尝试注册，如果不会翻墙则可以在创建新账号界面点击使用我自己的提供者，然后按照本手册推荐的注册服务器列表，按照用户名@注册服务器的格式输入用户名，并设置一个密码通过注册验证码后即可完成注册操作。
本手册的推荐注册服务器列表:

suchat.org	conversations.im	yax.im	chat.sum7.eu
yourdata.forsale	chat.sum7.eu	projectsegfau.lt	magicbroccoli.de
thesecure.biz	lsd-25.ru	macaw.me	07f.de

更多服务器列表详见：https://beijinglug.club/wiki/doku.php?id=projects:xmpp



第七步我已经完成了注册操作，应该如何加入本手册的公开聊天室?
我们十分推荐新用户加入本手册隶属的公开聊天室，那里有专门针对新人使用操作 xmpp 的教学，有着良好的聊天氛围和大量的聊天室成员，并且群公告挂了许多推荐加入的 XMPP 中文聊天室，接下来我们将教学如何加入本手册的公开聊天室。
本手册的公开聊天室地址是: xmpp 新手室@salas.suchat.org
(前缀会议室名称的 xmpp 和新手室之间没有空格，完整聊天室地址包括@salas.suchat.org 后缀服务器域名部分，否则将无法添加聊天室地址。)

1.点击右下角加号

2.点击加入公开频道

加入公开聊天室地址
如图所示复制粘贴输入 xmpp 新手室@salas.suchat.org 这段地址，并点击加入然后静待几秒刷新后即可完成操作。
(前缀会议室名称的 xmpp 和新手室之间没有空格，完整聊天室地址包括@salas.suchat.org 后缀服务器域名部分，否则将无法添加聊天室地址。)

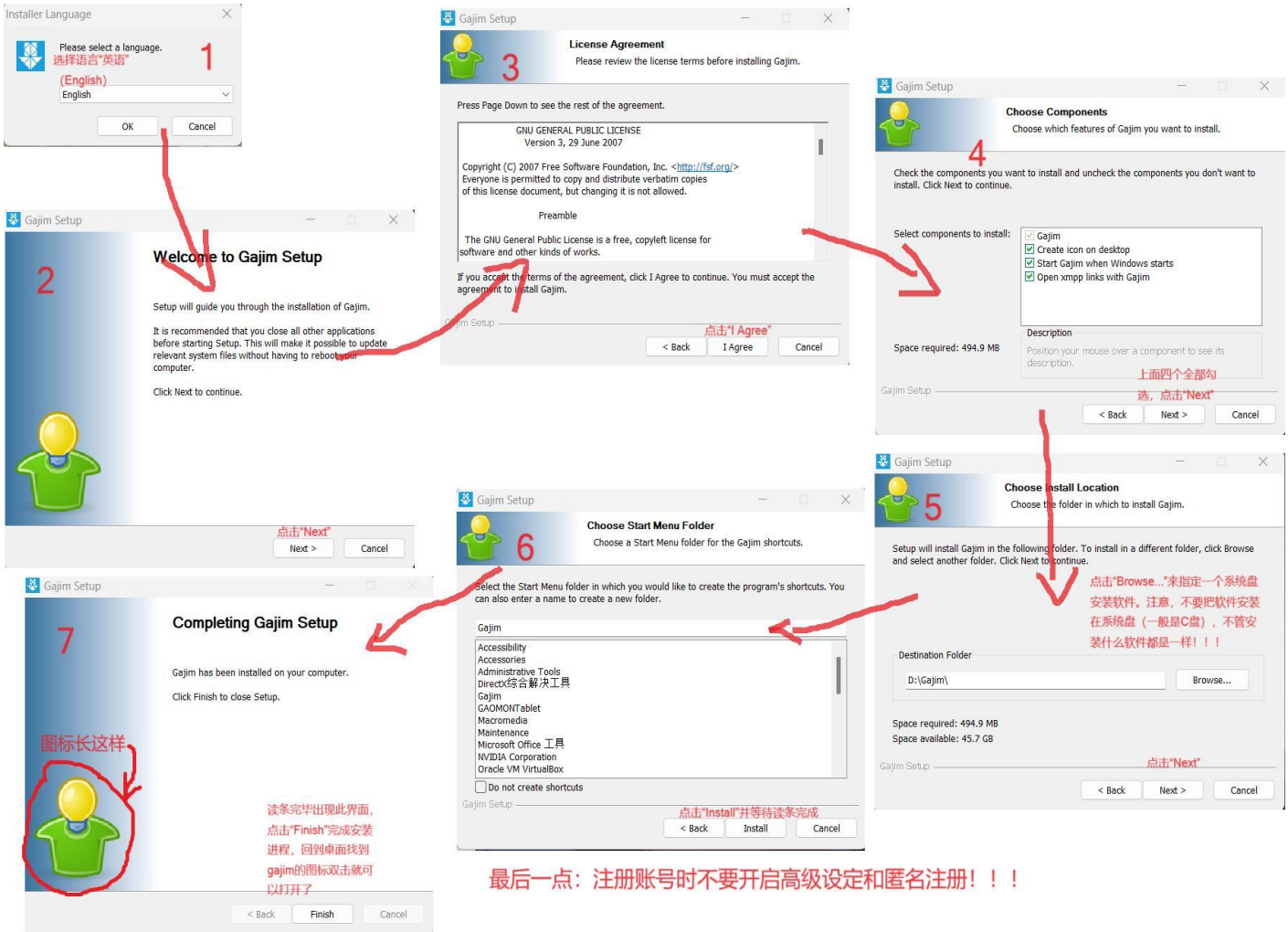
二、电脑操作系统如何下载并注册使用 XMPP?

这里推荐 Gajim 客户端，因为 Gajim 客户端同样是且自由软件对新人操作使用友好，而且客户端功能比较强大，支持 OMEMO/OpenPGP（端到端加密），接下来看看如何下载注册使用 Gajim 客户端吧。

Gajim 官网： https://gajim.org/
Win7 用户下载(32bit)：https://gajim.org/downloads/1.3/Gajim-Portable-1.3.3-32bit-1.exe
Win10 及 11 用户下载：https://gajim.org/downloads/1.9/Gajim-Portable-1.9.1-64bit.exe
GNU/Linux 用户下载：https://gajim.org/download/#linux

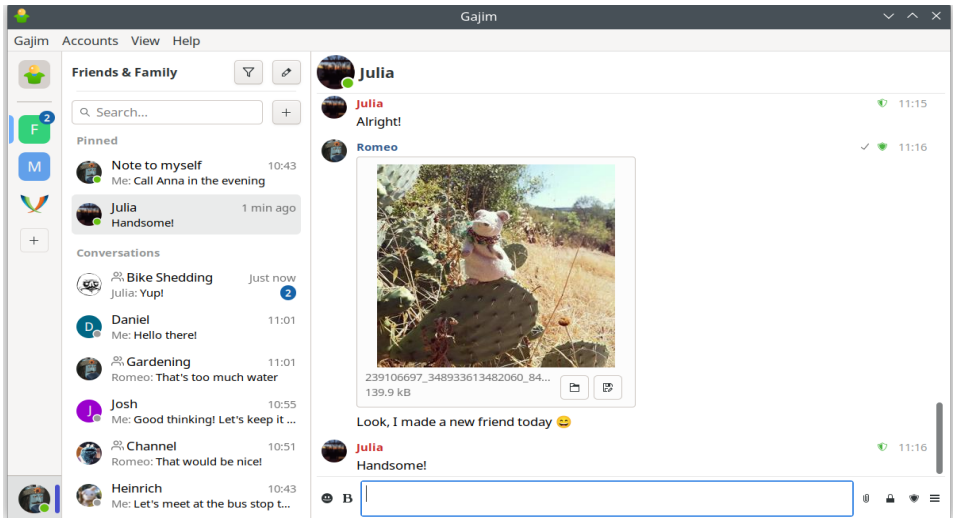
我们并不推荐在 Windows 上下载使用使用 XMPP 客户端，因为 Windows 是私有软件系统，其中嵌入了大量的私有软件（如系统应用，内核，驱动等），他们常常会违背用户的意愿来工作（如自动更新系统等）。微软公司对设备和其中的数据有随时访问和控制的权限，国内的数据也储存在被严密控制的微软中国数据中心里。在电脑上推荐使用自由软件系统 GNU/Linux。（网络安全相关知识 xmpp 平台上有很多相关聊天室和技术人员，可以加入后深入学习。）

使用教程步骤(附带步骤配图)

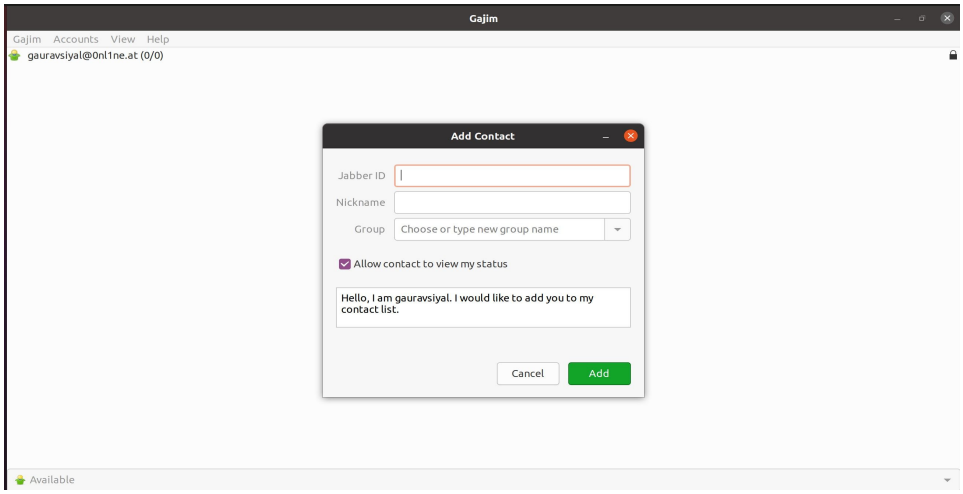


Gajim 安装教程参考（Windows）

注册步骤和 conversations 客户端类似，如果没有账户就先挑选一个服务器，输入用户名和密码注册一个 xmpp 账户。如图，第一栏添加要登陆/注册的 jid 地址，第二行填写账户密码。



登陆账户后点击顶栏中的“Accounts”（联系人）后光标移到已登陆的账户上，然后点击“添加联系人”。



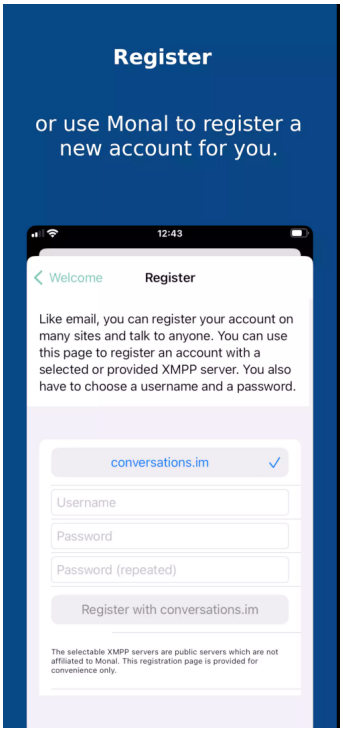
在添加联系人页面第一栏输入想添加的联系人/聊天室 jid（Jabber ID），第二行“Nickname”（昵称）可输入对其的备注（不输入默认则为其 jid 中“@”之前的部分），第三行“Group”（组）可为要添加的联系人/聊天室添加分组。比如 xmpp 新手室 jid： xmpp 新手室@salas.suchat.org
(前缀会议室名称的 xmpp 和新手室之间没有空格，完整聊天室地址包括@salas.suchat.org 后缀服务器域名部分，否则将无法添加聊天室地址。)

三、苹果 iOS/macOS 操作系统如何下载使用 XMPP 客户端?

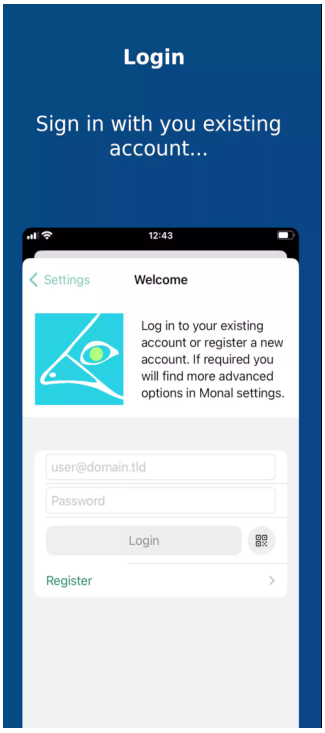
我们也十分不推荐在 iOS/macOS 上下载使用使用 XMPP 客户端，因为 iOS/macOS 也是私有软件系统，其中嵌入了大量的私有软件（如系统应用，驱动等）且使用需要注册账户。苹果公司对设备和其中的数据有随时访问和控制的权限，国内的数据也储存在被严密控制的“云上贵州”之中。手机推荐买可以解 bootloader 锁刷机的型号，刷写相对自由的第三方安卓系统，如 lineageos,divestos 等。（网络安全相关知识 xmpp 平台上有很多相关聊天室和技术人员，可以加入后深入学习。）

如果因暂时无法更换设备而临时过渡选择使用 iOS/macOS 下载使用 XMPP 客户端，推荐选择 Monal，因为这个客户端是相对自由的且功能相对比较丰富，而且 UI(用户界面)比较现代化，并且支持 OMEMO/OpenPGP（端到端加密），下面介绍如何下载使用。

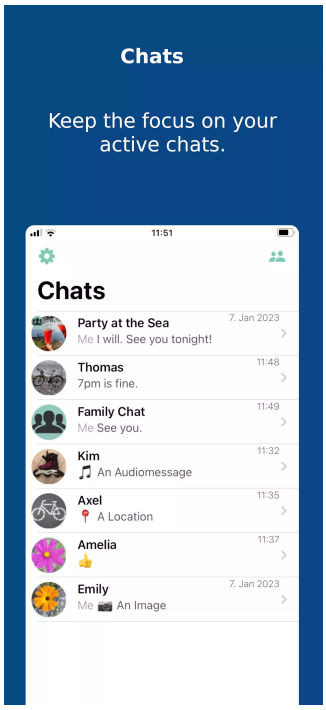
Monal 官网: https://monal-im.org/
Monal 项目地址: https://github.com/monal-im/Monal?tab=readme-ov-file
(稳定版安装需要非中国大陆 AppleID)



注册步骤和 conversations 客户端大同小异，如果没有账户就先挑选一个服务器，输入用户名和密码注册一个 xmpp 账户。如图，顶栏的“conversations.im”就是选择托管账户的 xmpp 实例，也可以选择其他实例。



已有账户直接点击“Login”,输入 jid（之前注册时设置的昵称加“@”和实例名称）与密码后点击“Login”即可登陆。



在聊天界面点右上角图标后输入用户或聊天室的 jid 就可以加入聊天了，
比如 xmpp 新手室 jid： xmpp 新手室@salas.suchat.org
(前缀会议室名称的 xmpp 和新手室之间没有空格，完整聊天室地址包括@salas.suchat.org 后缀服务器域名部分，否则将无法添加聊天室地址。)

四、我按照了手册教程操作仍不知道如何下载使用 XMPP，或是手册提供的下载链接已损坏/被封锁怎么办?

我们为了防止这种情况特地做了应对措施，请新人向我们的匿名教学邮箱发送消息，如果是无法下载需要补发客户端，请附带上您的操作系统信息和需要补发的客户端，并向我们发送一封邮件，然后耐心等待我们的邮件回复补发，如果有使用操作疑惑则应尽可能清晰，并且语句通顺的求助具体使用操作疑惑，最好附带对应截图信息向我们求助。

（请读者使用匿名邮箱联系我们的教学邮箱地址，防止使用实名邮箱联系我们暴露自己的个人信息，我们拒收一切例如 QQ 邮箱、网易邮箱等实名邮箱咨询我们的邮件消息。）

注册使用匿名邮箱的教程：https://paper.wf/xmppjxgh/ru-he-zhu-ce-shi-yong-ni-ming-you-xiang

推荐用于发送求助问题的临时邮箱地址：https://www.moakt.com/zh

xmpp 匿名教学邮箱地址： xmppjx@proton.me

五、如何安全的使用 XMPP

前言:XMPP 平台本身虽然很安全，但是使用者自身如果没有足够的安全意识，使用者的设备软件环境不安全，或是使用时没有配置 Tor 匿名代理，又或是注册了需要个人信息的服务器，或者在不可靠的下载渠道下载了被篡改的 XMPP 客户端，都可能导致使用 XMPP 的安全性大幅降低，那么我们应该如何保证安全的使用 XMPP 呢?

接下来笔者会对要注意的安全问题进行一一列举:

1.使用 XMPP 时必须注意与其他平台的身份隔离

不要使用与实名平台有关联的头像昵称账号信息，避免设置与实名平台同样或相似的账号密码(防止被撞库攻击)，避免在实名平台透露有关自己在 XMPP 上的信息，例如分享自己在 XMPP 的私人 jid 地址，或自己创建的会议室 jid 地址，以及自己在 XMPP 说了什么自己是 XMPP 上的谁，自己对 XMPP 上的什么事情印象深刻等等，还需避免在 XMPP 透露自己实名平台上的信息，例如转发自己在其他平台上的聊天记录(即使打了码也未必能保证安全)，转发带有追踪器的实名平台链接，例如 B 站的 b23 追踪器链接，转发跟自己实名平台账号有关的信息，例如自己在 B 站发的视频和蓝奏云网盘文件等等，请勿加入在实名平台建立的 XMPP 教学群，防止被有心之人关联信息顺藤摸瓜。

2.使用 XMPP 时应当配置网桥使用 Tor 匿名代理

尽管 XMPP 是匿名加密的即时通讯平台，但如果不配置匿名代理直连 XMPP，仍会对运营商暴露自己使用了 XMPP，并且在什么时候使用了 XMPP，以及使用了哪一个 XMPP 服务器的流量情况，即使运营商不会知道你是这个服务器上的某个用户，也无法知道你使用 XMPP 究竟做了什么，但仍可能会降低你使用 XMPP 的匿名性，而通过使用配置了网桥的 Tor 匿名代理，即可有效防止运营商知道你使用了 XMPP，因为 Tor 匿名代理会将您的流量数据进行三层中转加密，您的流量数据会像剥洋葱一样被加密

隐藏起来，而配置了 Tor 网桥又可以隐藏你使用 Tor 匿名代理的流量特征，让运营商不知道你使用了 Tor 匿名代理。

具体如何配置 Tor 匿名代理，可以到以下 XMPP 会议室求助:
tret9@muc.pimux.de

3.使用 XMPP 时应当使用 OMEMO/OpenPGP 加密来交换需要保密的信息

OMEMO/OpenPGP 加密是可靠的端对端加密算法，通过使用 OMEMO/OpenPGP 加密，可以让服务器和其他第三方不知道你们说了什么，保证你们的消息做到从设备端到设备端的交换，这里简单介绍一下端对端加密的原理，端对端加密又称为不对称加密，端对端加密的密钥分发者持有两个密钥一个密钥叫公钥，公钥可以大范围公开分发无需对其保密，公钥只能加密消息而不能解密消息，另一个密钥叫私钥私钥只能保管在密钥分发者本地数据，密钥分发者不能对其他任何人分发私钥，一旦私钥泄露整个密钥就作废了，假如某人想要用端对端加密向我们发消息，我们需要把自己的公钥分发给对方，对方用我们的公钥给我们发送加密消息，我们再使用私钥解密对方给我们发送的加密消息，对方想跟我们聊天也同样如此操作，在端对端加密的密钥交换过程当中，每个人都只公开了可以被公开的公钥，互相都不知道对方的私钥是什么，而服务器和第三方也只知道公钥，根本无法解密你们两方的加密消息，因此实现了真正意义上的端对端加密，这与传统的对称加密只存在一个密钥，一旦密钥泄露了加密消息就会直接泄露，并且难以安全公开大范围的分发密钥来说，不对称加密无疑是十分安全可靠的，至于在不知道私钥的情况下暴力破解可靠的端对端加密算法，即使使用量子计算机对其进行暴力破解，也往往需要投入海量的破解成本和数十年上百年的破解时间，所以应该保证只在开启端对端加密的情况下交换保密消息。

4.软件环境安全问题

即使在做到了上述的安全措施后，使用私有软件操作系统安装私有软件，仍会使我们使用 XMPP 的安全性降低，因为私有操作系统和私有软件本身也会监视我们在干什么，比较典型的现实案例就是华为系统的后台报警，QQ 每半小时一次对设备硬盘数据进行的全盘扫描，Windows 系统汇报用户的使用数据等等，如果对安全保密的程度要求足够高的话，应当使用一台更换了第三方开源自由操作系统的设备，并且不在上面安装任何一款私有闭源软件来使用 XMPP。

更换电脑开源自由系统以及了解电脑自由开源软件请在以下会议室求助:

tret9@muc.pimux.de

更换手机开源自由软件系统请在以下会议室求助:

loqgsv@conference.jabb3r.de

了解手机自由开源软件请在以下会议室求助

fotog@conference.jabb3r.de
想要联系我们？请加入我们在 XMPP 上的官方会议室吧！会议室地址：
ovimiqa@conference.conversations.im

5.XMPP 聊天时的安全问题

在发送图片前必须去除图片 EXIF 值，请尽量不要发送现实拍摄的图片，不要随便下载陌生人发送的文件附件，如客户端开启了自动下载文件附件，请在客户端内关闭这个设置，不要随便点击陌生人发送的链接，不要向陌生人透露自己的隐私信息。

建议在设置里关闭对 OMEMO 指纹的盲目信任，因为 OMEMO 指纹具有高度防伪性，交流者通过新的设备和客户端登陆账号，或删除了之前客户端储存的 OMEMO 私钥数据，重新登陆必然会产生新的 OMEMO 指纹，如开启了 OMEMO 指纹盲目信任，则不容易察觉到交流者产生了新的 OMEMO 指纹，当发现交流者 OMEMO 指纹产生变化时应对其进行身份核实，例如对其可信任的旧指纹发送 OMEMO 加密消息，若交流者能够对旧指纹发送的加密消息进行解密，则说明交流者依旧持有可信任的 OMEMO 旧指纹私钥，交流者身份及其新指纹也是可以被信任的，或通过事先制定的暗号进行核实，以确保同你聊天的人没有被他人掉包，也可以同时采取两种甚至更多的核实措施。

在公开会议室聊天时需谨慎，在那里可能存在心怀不轨的第三方爬虫窃听消息，要记住只有 Jid 私聊和私密会议室能开启端到端加密，公开会议室交流无法开启端到端加密，也无法阻止不怀好意者的窃听。

部分 XMPP 客户端使用的语音/视频通话协议，可能会通过 jingle 协议获取 ip 信息，请勿接听陌生来电或向不信任的人进行语音/视频通话，防止对方获取您的 ip 信息。

请注意同你进行保密交流的人软件环境/设备硬件安全，必须确保其操作系统是自由软件操作系统，并且其设备没有安装任何一款私有软件，其设备系统分区没有被篡改安装后门，其设备也没有被心怀不轨之徒安装窃听硬件，否则即使你做了充分的安全保密措施，并确保交流者是可以被信任的，交流者软件环境/设备硬件不安全的因素仍会使其成为不自觉的泄密者。

请勿注册无可靠证书机构颁发未过期 TLS 证书的 XMPP 用户服务器，除非你只在其上使用 OMEMO/OpenPGP 加密交流，否则你的消息极易被不怀好意之徒窃听篡改，建议只注册支持 Tor 匿名代理连接，无需提供个人信息注册的 XMPP 用户服务器，不要注册部署在中国国内和中国邻国的 XMPP 用户服务器。

应当多加利用主流 XMPP 客户端可以多开账号，且许多 XMPP 用户服务器注册账号方便的优势，注册使用几个不同身份的 XMPP 账号，并规定每个账号身份的不同用途，每个账号身份应当设置不同的头像昵称，并避免语言习惯和上下线时间与其他账号身份相似，如此操作可更大限度保护个人隐私，避免被心怀不轨之徒通过社工手段获取个人隐私信息。

不建议通过移动数据、校园网、公司网这类不安全的网络使用 XMPP 聊天，仅建议在非实名认证连接的 WiFi 的条件下使用 XMPP 聊天(例如家用 WiFi 或公共场所输入密码即连的 WiFi)，并配置随机生成的 MAC 地址+Tor 匿名代理+Tor 网桥使用 XMPP 进行聊天，因为移动数据的蜂窝网可通过基站对你目前位置进行实时定位，而校园网则会对你的流量活动情况进行管控，即使你配置了 Tor 匿名代理对流量数据进行混淆加密，并通过 Tor 网桥隐藏流量特征，后台也会对超出阈值的流量流向外国 ip 现象进行报警，如无法在不使用校园网、公司网等实名认证连接的 WiFi 条件下使用 XMPP，请选择通过移动数据+Tor 匿名代理+obfs4/webtunnel/snowflake 这类 Tor 网桥的条件下使用使用 XMPP，尽管这样 isp 可以通过蜂窝网基站对你进行实时定位，但无法得知你设备的流量活动情况，也无法得知你设备使用 Tor 匿名代理，此外保密专用机不建议插入电话卡使用移动数据，防止遭到蜂窝网基站定位、isp 或骇客的数据侵入、以及被一些网站或应用读取电话卡信息，仅建议使用自由开源操作系统的设备共享移动数据热点联网，因为私有软件操作系统的热点共享软件一般也是私有软件，会记录连接热点设备的相关信息，还可能会对连接设备进行 DHCP 中间人攻击。

本手册由 xmpp 宣传与共建联合委员会监制

该网站是手册组织的官方网站，读者如若感兴趣可以打开查看。

https://xmppjx.codeberg.page/guanwang.html