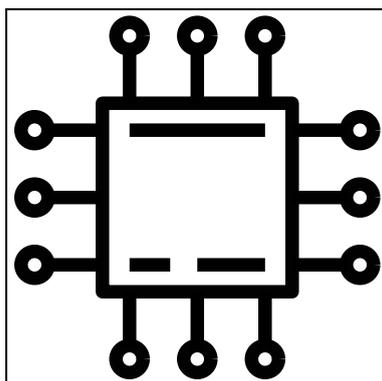


社会主义XMPP高级用户使用说明书

(2024年01月05日版)

此书已经完成了编写计划，不会频繁地有新的的重要内容更新。



此书由金星革命委员会编著

<https://shzyly.bitbucket.io/>、<https://shzyly.rf.gd/>

1. 基本设计
 1. 初识XMPP
 2. XMPP地址和XMPP链接（基本设计）
 3. 元数据
 4. 对话（基本设计）
 5. 会议室
2. 具体使用
 1. XMPP身份
 2. 对话（具体使用）
 3. 会议室详述
 4. 可选的XMPP客户端软件
 5. 公共服务器及查找
 6. 注册和登录时可能出现的问题
 7. 使用中可能出现的问题
 8. 高级屏蔽名单
 9. 专业房主说明
 10. XMPP的未来
3. Conversations章节
 1. Conversations介绍及下载
 2. 注册与登录
 3. Android权限问题
 4. “对话选项”界面和“联系人与群聊”界面
 5. 对话界面
 6. 添加联系人及联系人详情界面
 7. 群聊详情界面
 8. XMPP身份管理界面
 9. 疑难解答
 10. 关于原版的说明
4. Gajim章节
 1. Gajim介绍
 2. 下载与安装
 3. 通用设置
 4. 注册与登录
 5. 添加联系人
 6. 开启对话项
 7. 对话界面
 8. XMPP身份选项
 9. 联系地址设置
 10. 疑难解答
5. Psi章节
 1. Psi介绍
 2. 下载与安装
 3. 设置
 4. 注册
 5. 登录
 6. 查找服务

7. 添加会议室和联系人
8. 会议室界面
9. 普通私信
10. 高级屏蔽名单
11. 注销
6. Converse的介绍
7. Dino的介绍、下载、安装
8. 附录
 1. 附录: TLS加密
 2. 附录: OMEMO加密
 3. 附录: 第三方会议室搜索引擎
 4. 附录: 反馈错误信息实例
 5. 附录: 周边技术问题
 6. 附录: 周边疑问
 7. 附录: 供新手尝试的服务器地址列表

初识XMPP

XMPP



XMPP的徽标

XMPP是一套世界通用的通信标准，是一套用于机器程序之间的稳定通信规则（其计算机术语为“协议”），遵守此规则的应用程序们可以顺利地一起对话。

- “Tried and tested. Independent. Privacy-focused.”（已经历练。独立，注重隐私。）
- “No one owns XMPP. It's free and open for everyone since 1999.”（没人私有XMPP。自从1999年起它就免费公开给所有人了。）

它不属于专利，属于公有领域。难以受到资产阶级政府的控制。

XMPP的公共服务器由世界各地的志愿者们架设，提供免费且没有歧视的服务。它不依赖于中央服务器，公共服务器们可以和其它公共服务器建立通信，也就是说，并不会因为一个公共服务器无法使用而导致很多人断联。

XMPP的软件，无论服务器软件还是用户端软件，由志愿的开发者们创造。有许多不同的用户端软件，用于不同的操作系统。

XMPP的全称是“Extensible Messaging and Presence Protocol”，本说明书给出的参考翻译为“组件式在线通讯协议”。正如它的名字一样，它的功能都是可装卸的组件；再加上它的开放性，它很容易扩展功能。但是，它本身有标准化工作，因此不至于无法在现实中广泛通用。

它的每一条功能标准都有格式如“XEP-#####”的编号，不过普通用户需要在意的编号很少。

XMPP的革命所需属性

一般用途

XMPP是用于机器程序之间通信的，因此它的实际作用范围远不只聊天；但XMPP的主要用途还是普通交流。

家人、朋友、学生、同事之间的相互通信：这就是它最基本的应用了。就是最简单的通信，发送文字，打个电话。生活中不可缺少的应用。

自由交流：无论你是革命派还是反动派，它不会妨碍你交流，不需要避讳任何敏感字词。它诚实地告诉你你的消息是否发送成功，不用担心想发送的消息被屏蔽，让你的发言成为很轻松的事情。

找新朋友：当它普及起来后，用它来找朋友就会很容易。因为它兼有私密的设计和公开的设计。你可以通过搜索引擎搜索公开的群聊，找到各省市县镇乡村庄的人，找到不同兴趣爱好的人们。

宣传：开个记者会或辩论会不在话下，甚至还可以再带成百的观众。

干地下工作：不管你认为“地下工作”是褒义还是贬义，你都不可否认它确实“适合干地下工作”。

机器程序之间的指令：配合程序可以用来传送非直接文字形式的信息。例如，它可以用来远

程控制设备，可以用来让两个人远程下棋。

可普及性

革命要选择的通讯方式必须要有可普及性。没有可普及性的通讯方式不能用来从事公开的政治活动。

可普及性也是一个代表属性，因为它和许多属性有关——易用性、功能性、稳定性……。

不受言论审查

有屏蔽字词会把整个互联网平台的交流氛围搅乱。革命派必须有固定的为革命服务的词汇，不能接受词语概念上的妥协。我们必须说大白话。

轻便

这里的“使用成本”既指服务器软件的运行成本，也指客户端软件的运行成本。

服务器的建设成本和运营成本低，可以服务特别多的用户。考虑到要搞波及人数很多的革命，而且还是跨国界的世界范围的革命，也就是说，它的用户数量一定要无比庞大，那么这种轻便的条件就是必要的。这使得它经得起经济萧条。

客户端占用的运行内存和处理器资源很少，极大地降低了使用成本。

开放和分立的程序架构设计、国际化

开放意味着人人都可以搭建公共服务器；分立意味着没有相互依赖的合作方，也就不会因为一个环节的瘫痪而无法使用。因此，它经得起政治动荡。

革命要选择的通讯方式不能局限于某个国家或某一片地区，也不能局限于某一种语言，不能对用户有歧视，而应该是人人都能正常使用的。我们本来就是国际主义者。国际化不仅是社会主义革命所要求的；而且也是自然而然的，因为这种工具本身无恩无怨无情，把它设计得本身对人有这种歧视的话就很容易把用户（也就是说包括我们）的手脚束缚住。

资本主义集团的通讯方式很难做到这一点，因为它们总是以金钱利润为导向，也随声附和各国法律规定和（无论真假的）舆论倾向，对不同的地区或不同的语言有不同的服务策略。用户数量变化无论增多或减少都可能劣化服务质量和用户体验。政治局势动荡、市场经济危机更是它们难以承受的。

有为了开放和公开而设计的功能

这让人们便于以可追溯的虚拟身份从事宣传和公开活动，革命家们必要的功能。

这也让它对零散的，缺乏教员引导的新学习XMPP的人更友好，它们能很轻松找到别人，从而开始体验XMPP的交流。

有匿名性的功能设计

所有从事地下工作的人们都需要这一特性。

它和政治身份没有关联，不需要电话号码，甚至不需要电子邮箱。

加上可以多端在线的特点，还可以轻易做到多个人用同一个虚拟身份，使得对虚拟用户的政治身份猜测更加困难。

是否公开自己的政治身份信息，是用户自己决定的事情。

免费公益，非商业性质

这一点当然很重要，毕竟我们是为无产阶级的革命服务的。

国际标准

XMPP是一套国际标准。

它的通信规则不会轻易变化，因此也就不会导致因为通信规则快速变化而让使用旧设备或旧

软件的人们出现各种难以排查原因的通信问题甚至断联，这也方便了教程的编写和更新工作，方便教学工作。

这决定了它的服务端软件和用户端软件的程序很容易公开，因此这种通信方式也就无比得可信。

它本身，无论设计目的还是设计成果，就是个成套的、系统的、完整的规则。它不需要资本主义集团的其它技术支持，对用户很诚实。

信息传输安全性

这里说的“安全性”有两种因素：不被篡改和不被窃听。这是互联网服务的标准配置。

主动加密可以避免被窃听消息内容，同时帮助确保消息传输不出差错。端到端加密确保了只有目标收信端可以解读消息。

爱憎分明的设计

或者说它的设计简单粗暴。它没什么用来调和人与人之间的矛盾冲突的设计，例如没有如下小资产阶级般的设计：

- 黑名单有名额限制。
- 在对方回复前，你只能发送一条消息。
- 字词检测和屏蔽。虚假的“评论发送成功”反馈。
- 不经同意地远程删除别人已经收到的消息。
- 自动添加并应用花里胡哨的社交功能。

爱憎分明的设计是很有用的，也正符合我们的做派。我们可不喜欢和立场混乱的人们交流。

XMPP地址和XMPP链接（基本设计）

XMPP地址包括两种：用户地址（XMPP身份标识）、会议室地址。用户地址和会议室地址不相同。

XMPP地址是在全世界范围内的定位符，也是收信地址，独一无二。

要在XMPP地址或XMPP链接前后添加其它文字时，为了避免程序识别错误，请在它们前后添加空格。或者，让它们各自独占一行也可以。

XMPP有个不标准的旧名叫“Jabber”，目前因为历史遗留还在广泛使用。XMPP地址也被称为“JID”——“Jabber ID”（“Jabber Identity”）。

用户地址

每个虚拟用户有一个通用的XMPP身份标识。XMPP身份标识的格式为：

“XMPP身份号码@其所属的用户服务器地址”。

XMPP身份号码不支持大写英文字母，以及程序和规则占用的一些符号。

用户地址可以扩展：

“XMPP身份号码@其所属的用户服务器地址/登录点标识”。

可以用来将消息发送到不同的登录点，对方的所有登录点不一定会同步，但基本不需要这么做。只有在线传输文件不能多个登录点同时接收，必需一个对方的登录点标识。

会议室地址

会议室地址格式为：

“会议室门牌号码@其所属的群聊服务器地址”。

会议室门牌号码不支持大写英文字母，以及程序和规则占用的一些符号。

有一个XMPP身份就可以创建会议室，门牌号码自选。群聊服务器一般不欢迎别家的用户创建会议室。

会议室地址可以扩展：

“会议室门牌号码@其所属群聊服务器地址/占座名”。

在加入会议室时可以用来填写加入时的占座名。也用作室内私信的收信地址。

XMPP链接

XMPP链接基于XMPP地址，用于被视为用来执行快捷操作的按钮。有三种形式：

- xmpp:XMPP身份号码@其所属的用户服务器地址?message
- xmpp:会议室门牌号码@其所属的群聊服务器地址?join
- xmpp:服务器地址?register

前两者用来添加联系地址。注意，手动输入地添加联系地址时填写XMPP链接的话可能出错。

如果联系地址的链接没有后缀，那么用户端软件通常会视它为一个用户地址链接，而非会议室地址链接。同时可以添加“?……”的格式来附带其它信息。

去中心化设计

XMPP的服务器是不需要中央服务器的。公共服务器可以相互连接，使不同服务器的用户可以相互通信；服务器也可以独自运作，且不会因此而缺失功能。

整个XMPP服务器将不同的功能分配到不同的地址，也可以只提供一个功能。地址常见形式

如下（假设服务器的基础地址是“soviet.union”）：

- 用户服务器地址为“soviet.union”，和基础地址相同。
- 群聊服务器地址为“conference.soviet.union”。
- 文件寄存服务器地址为“upload.soviet.union”。

如果一个服务器只提供群聊功能，那么它往往会用基础地址作为群聊服务器地址。

每个XMPP身份都绑定服务器地址，都只由一个用户服务器托管，无法转移到其它用户服务器。

由于每个公共服务器都可以替你送信到另一个公共服务器，所以这类似于每一个公共服务器都是一个XMPP专用代理网络连接服务器。XMPP并不是专门用来通过互联网封锁的工具——它不会让你的其它网络流量通过它，而且换服务器用不会转移存储在旧XMPP身份上的数据。不要依赖它可以换服务器使用的特点来把它当作通过互联网封锁的工具，除非你并不和几个人相互认识或交流，也不想用它当稳定的联系方式。

元数据

元数据的交互大多需要XMPP地址，少数需要共享在线状态。这些元数据皆存储在服务器上。

注册

要获取一个XMPP身份号码，需要向服务器提供的信息至少要有：你想要的XMPP身份号码、你想设置的密码。其它的都不是XMPP规定所必需的，除非服务器要求。一般说来，一个公共服务器要得再多点，多的也就只会是：你的电子邮箱地址、服务器给你的一条防机器滥用的验证码。不会向用户索要任何政治身份信息（……除非有哪个国家的执政党使用XMPP来为政治服务，因此影响了一些XMPP服务器。）

登录、修改登录密码、注销，都只需要提供用户XMPP地址和正确的密码。

登录点标识

XMPP支持多个登录点同时在线，不论设备型号，不论软件名称，不论登录点标识。

每个在线的登录点都有一个登录点标识，格式常常是“用户端软件名称.非一次性的随机号码”，由用户端软件决定。登录点标识对服务器而言意义不大，通常，登录点下线后，服务器就会忘记对应的登录点标识。

不能同时上线两个标识相同的登录点。因此，要实现多端在线，只应该用密码登录的方式，而不要简陋地使用备份文件恢复的方式。备份文件恢复只能用于迁移数据，而不能用于完全复制登录点并同时在线。

获得了自己共享的在线状态的联系人可以看见自己的登录点标识，以供别人了解自己在用的登录点以及用户端软件。如果用户端软件允许，就可以自由修改。

联系人名单

也许有人管它叫“通讯录”（“contact”）。

XMPP用户有自己的联系人名单，所有被添加到联系人名单里的用户即为联系人。是否添加一个联系人，由自己决定。

对联系人可以共享自己的在线状态。这不仅需要己方发送，还需要对方接收。对方不接收是不行的。

通常，添加联系人后会自动执行共享在线状态的操作，因此对方会得知自己已经被哪个用户添加了联系人。用户可以得知对方的在线状态共享情况。

联系人名单记录联系人的XMPP地址，可以对联系人进行分组（一个联系人可以属于多个分组），给联系人起称呼，添加笔记。

一些公共服务器拒收非联系人消息，来防止服务器和用户受到骚扰。配合黑名单或白名单时，联系人名单也可以用来记录敌人的地址。

仅自己可见。

个人地图

也许有人管它叫“书签”（官方术语“Bookmark”）。

个人地图记录的每一项记录会议室地址、你对会议室的称呼、加入会议室时的默认占座名（仅一条）、准入口令、“是否要在登录后自动加入”记号。

仅自己可见。

除了“是否要在登录后自动加入”记号外，个人地图里有没有哪个地址不影响任何事情。

其存储的项目有排序，但用户端软件们往往会自己按照名称字符顺序排列。

屏蔽名单

屏蔽名单记录拒绝通信的地址。屏蔽一个用户地址后，此地址就完全无法和你通信。但这不影响室内私信，也不影响群聊消息，因为这些消息来自不同的地址。

可以屏蔽会议室地址，使自己无法进入那个会议室。可以屏蔽整个用户服务器地址，使属于此域名的所有用户都无法和自己通信。

分为屏蔽名单（XEP-0191）和高级屏蔽名单（XEP-0016）。

在线状态

和其它用户相互添加联系人并贡献在线状态后就可以相互看到在线状态；与此同时，可以相互看到对方的最后在线时间点，以判断对方是否弃用了这个XMPP身份。

除了基础的在线状态外，还有四种更具体的在线状态：

- 空闲（chat）：我对着屏幕发呆，很闲，来找我聊聊吧。
- 暂离（away）：去上个厕所什么的，应该过不了多久就回来。
- 远离（xa, eXtended Away）：跑远了，不知道什么时候能回来。
- 忙碌/勿扰（dnd, Do Not Disturb）：忙着呢，请勿打扰。

在对用户端软件搁置不管时，可以对联系人公布**挂机时间点**（Idle Time），也就是最后一次操作用户端软件的时间。再次操作时，或者下线时，此信息便失效。

在线状态也可以附带自定义信息。如果用户端们软件长久保存它，而不是下线后就忘记，而且还会展示在交流界面上，那么你可以把它当成个性签字（自我介绍或宣传语）来用。群聊也支持显示这个。

电子名片

用户可设置一个通用网名，可以置空。

用户的虚拟肖像也可以置空。最保证支持的图像格式为PNG。

可填其它信息，只要自己愿意。

电子名片有一项旧标准（XEP-0054）和一项新标准（XEP-0292）：

- 除了虚拟肖像以外，它们的内容不互通。
- 旧电子名片有了XMPP地址就可以查询，通过室内占座地址也可以查询。
- 新电子名片可以设置陌生人是否可以查询【通用网名和虚拟肖像】、【电子名片里的其它信息】。

电子名片可以通过用户XMPP地址来查阅，但电子名片内容不包括用户的XMPP地址。

注销

注销操作请求服务器删除和你的XMPP身份直接相关的所有内容（包括共享的在线状态），无法再登录。此操作只需要对应的登录密码。

服务器信息

用户可以查询服务器信息：服务器软件的名称，有哪些服务项目以及它们的地址，群聊服务器上的露天会议室，服务器支持哪些功能标准。

要查询，只需要登录一个XMPP身份。公共服务器也会允许别家服务器的用户查询自家服务器上的信息。

对话（基本设计）

对话通道

对话通道×3：普通私信、会议室、室内私信。

普通私信：用户地址作为收信地址，允许离线消息，支持音视频通话，可用主动加密。

会议室：会议室地址作为收信地址，允许离线消息，不能音视频通话，满足条件可用OMEMO加密。

室内私信：室内网名作为收信目标，必须双方在场，不能音视频通话，主动加密不一定能使用。

“会议室”、“频道”、“房间”、“群聊”，这四个概念在XMPP里都是一个意思，没有差别。只是有的被用作学术语，有的被用作通俗叫法。

加密

对文字消息，支持的被动加密方式是“TLS”；支持的主动加密方式是“OMEMO”；参阅附录可具体了解它们。

音视频通话所用加密是“DTLS-SRTP”。

文字消息

回执：收信用户端收到消息时向发信者返回“已收到消息”的信号。

“已读”信号：用户可以发送“已读”信号来告知对方自己知悉了哪些消息。

“正在输入文字”信号：用户可以发送“正在输入文字”的信号，以告知对方自己正在撰写消息。

反馈错误：发送失败的消息有反馈错误信息供排查技术原因。如果是收信服务器拒收了，收信服务器会返回拒收原因；如果是发信服务器发送失败，发信服务器会返回错误信息。

用户收回（Retract）：用户可以远程收回自己已经发送的消息。

主持删除（Moderate）：主持在会议室里可以任意删除人员已经发送的历史消息，同时可以对室内人员们提供自编写的理由。

更正消息：发送者试图用一条新消息替代上一条已经发送出去的消息，有时限。

音视频通话

一对一的音视频通话的前提条件可能有两个用户相互共享在线状态。多人音视频通话需要会议室设置为锁门+小桌。

音视频通话会优先让两个用户直接连接（这会相互暴露IP地址）；如果直接连接未能成功，那么服务器会负责代理传输。

文件在线传输与寄存

在线文件传输仅支持一对一，需要双方都在线，且无法使用主动加密。服务器通常会亲自递送，也可能只负责引路。

寄存服务器对单文件有最大体积限制，会通过XEP-0363只告诉用户端软件，未进行主动加密的寄存文件将有一个通用的HTTP下载链接。

历史消息存档（管理）

用户服务器存档用户消息。用户可以拒绝服务器存档这些消息；拒绝后，用户消息只能收到一次，无法向服务器再索要一次。

群聊服务器为用户存档群聊的公开历史消息，和用户服务器互不干涉。此设置由房主决定。

三个选项是：

- 从不保存：用户服务器不为你存档任何消息。
- 仅联系人：用户服务器只为你存档你和你的联系人之间的普通私信。
- 全部：除了联系人列表里的以外，也包括来自非联系人的消息和室内私信。

你可以对一些地址设置特例。

消息被存档与否，决定于消息被收信服务器接收时你的历史消息存档设置。如果某条消息已经存档了，那么修改设置至“从不保存”也不会删除它。如果你不在线，那么，无论这条设置如何，只要服务器为用户配置的待收消息存储条数没达到上限，服务器就会寄存别人发送给你的消息，等到你上线时发给你一次后再删除。

会议室

占座名

用户的每一个会议室的每一个在场登录点都有一个室内网名（占座名）。室内网名不能与其它在场用户重复。成员名单可以为用户预留一个占座名，不允许它人使用。

一个在场用户的每一个不同的占座名都会被算作占了一个座位，这会影响会议室的占座数以及空闲座位数（如果会议室内的座位数有限的话）。

在一个登录点修改占座名时不会同步修改其它在场登录点的占座名。

封禁名单

会议室的封禁名单和用户屏蔽名单功能相同。

六大状态设置

以下设置项都是可以在进入会议室之前就获知的。而且它们可以任意组合，互不冲突。

露天或地下

露天（Public Room）：服务器在露天会议室列表里公布会议室地址。【参考直译：公开】

地下（Hidden Room）：服务器不公布会议室的地址。【参考直译：隐藏】

锁门或敞门

锁门（Members-Only Room）：只有成员能进入。【参考直译：仅允许成员】

敞门（Open Room）：允许游客进入。【参考直译：开放】

大桌或小桌

大桌（Semi-Anonymous Room）：成员名单只有管家和房主可以看到，在场人员的XMPP地址只有主持能看到。【参考直译：半匿名】

小桌（Non-Anonymous Room）：所有在场人员都可以看到成员名单和在场人员的XMPP地址。【参考直译：非匿名】

开幕或闭幕

开幕（Moderated Room）：遵循参与等级。【参考直译：受主持的】

闭幕（Unmoderated Room）：所有在场人员都可以自由发言。【参考直译：无主持的】

口令守卫或门神守卫

口令守卫（Password-Protected Room）：对每个想进去的人问口令（密码）【参考直译：密码保护的】

门神守卫（Unsecured Room）：会议室不设入口密码。【参考直译：不受保护的】

棚屋或砖屋

棚屋（Temporary Room）：会议室没人在场时，就会被立刻拆除。【参考直译：临时】

砖屋（Persistent Room）：当会议室里没有人在场时，会议室仍会存在。【参考直译：持续】

六条信息设置项

会议室名称：给所有人看的信息项。露天会议室还会将此项公布在服务器的露天会议室列表里。

会议室介绍（描述）：专门给室外人员看的信息项。露天会议室将此项公布在服务器的露天会议室列表里。可以用于招揽人。

会议室语言：给所有人看的信息项。会议室交流用的自然语言。语言相同，才好交流。它对室内说什么语言没有电子程序上的影响。这项只有按照标准填写语言的英文简写才合规有效，写全称则不合规。（汉文为“zh”，简体汉文为“zh-CN”。）

会议室话题（公告板）：只给在场人员看的信息项。

会议室门画：给所有人看的信息项。作为辅助阅读会议室列表的图标。

是否对室外公开在场人员的占座名：专门给场外人员看的信息项。室内的在场人数则是有了地址就可以获知的，不受此设置影响。

群聊人员术语概览

管理等级×5：**房主、管家、会员（议员）、游客（访客、观众、听众）、流寇。**

参与等级×4：**离场、旁听（旁观、参观、看戏）、与会（参会）、主持（主席）。**

合称归类×2：**成员、人员。**

合称归类

成员：房主+管家+会员。

人员：成员名单上的所有人+在场游客。（也可以说是“在场的+缺席的”。）

管理等级

也许有人管它叫“归属关系”（官方术语“Affiliation”）。

房主（Owner）：对房间有完全的管理权。参与等级必然是主持。独有编辑房主名单、编辑管家名单、更改会议室设置的权力。

管家（Administrator）：用于辅佐房主管理。可以编辑会员名单和封禁名单。默认的参与等级是主持。

会员（Member）：默认的参与等级是与会。

游客（None）：不在成员名单上，也不在封禁名单上的人。默认参与等级是旁听。

流寇（Outcast）：被封禁的人。无法进入会议室。无法获得会议室的详细信息。流寇名单是单独和成员名单分开的。

如果在一个群聊服务器上有创建会议室的权限，那么对一个不存在的门牌号码执行XMPP规定的加入操作会直接创建这个会议室并成为房主，此时会议室的设置就是群聊服务器设置的默认值；如果没有此权限，那么此操作对一个不存在的门牌号码就会无效。

参与等级

也许有人管它叫“角色”（官方术语“Role”）。

离场（None）：离场者不接收会议室消息，无法和会议室互动。这个参与等级必然不被记录。它不算是个正式的参与等级。

旁听（Visitor）：无**公开发言权**（官方术语“Voice”）。

与会（Participant）：有**公开发言权**。

主持（Moderator）：主持有**公开发言权**；可以看到在场人员的用户XMPP地址；可以更改会议室话题；可以授予和撤销**公开发言权**；可以删除历史消息；可以将人员移出会议室。

调整参与等级不会同时变动管理等级；调整管理等级通常会将其参与等级归为对应管理等级的默认值。

群聊服务器可能永久保留人员的在场参与等级；也可能不保留，此时每次加入会议室时参与等级为对应管理等级的默认值。

只有人员在场时，它的参与等级才能被调整。

单独调整参与等级时可能仅对被操作的在场占座名有效，此时被操作用户的其它在场占座名则在下次加入时才应用新参与等级。

旁听可以按键来给主持们发送索要公开发言权的请求，如果群聊服务器支持此操作的话。

一个登录端下线时，此登录端会离开所有的会议室。

操作通知

以下操作会产生室内通知给所有在场人员：

- 会议室设置被修改，但不是修改了“大桌/小桌”项。
- 修改了“大桌/小桌”项。直接通知此具体修改。
- 修改了会议室公告板。
- 会议室被解散。此通知是一次性的，解散后试图加入时不会这么显示。
- 以下操作涉及占座名，其不在场或在场状态被隐藏时不会通知：
 - 用户被踢出和被封禁。
 - 用户修改占座名占据了一个新座位。
 - 一个占座名加入时和离开时。
 - 技术问题迫使用户离开。

XMPP身份

XMPP地址和XMPP链接（补充）

有的用户端软件不需要用户自己分辨用户地址和会议室地址，它们会在正式添加联系地址前直接访问对应的地址，通过服务器的回应来判断它是哪一种地址，这种设计也可以防止用户添加无法联系的地址。

XMPP身份号码和会议室门牌号码支持汉字，汉字是合规的，但有的服务器不一定支持。在这方面不支持汉字的服务器通常只支持小写英文字母、阿拉伯数字、一些常用符号，也不支持其它语言的字符。以下字符是不合规的：“”、“'”、“<”、“>”、“&”、“/”、“:”、“@”、“ ”（ASCII空格）。

XMPP和其它服务完全无关。例如，它和电子邮件服务无关，XMPP不能和电子邮箱收发信息。

有时你会在会议室里看到两个人员有真正相同的用户XMPP地址，但它们却有不同室内网名和虚拟肖像。这是因为那个人员在一个登录点更改了室内网名和虚拟肖像，且其它登录点没有同步使用新室内网名，而用户端软件在大桌的会议室里可能是根据室内网名来缓存虚拟肖像的（这种设计是为了在它们离场的时候也能在历史消息记录里显示保存的虚拟肖像。）

考虑到在不同操作系统上使用的兼容性，请不要在要注册的XMPP身份号码里添加操作系统在文件位置路径上不允许的符号。例如，如果你要使用Microsoft Windows操作系统，那么就不应该在XMPP身份号码里添加ASCII里的问号“?”。

设计得差的用户端软件不会自动识别并去掉XMPP链接的前后缀，还会给错误的联系地址打开一个对话框。所以请记得在输入添加联系地址时，手动去掉构成链接的前后缀。

有的用户端软件会提供把XMPP地址做成HTTP链接的选项，实际上它并不算是XMPP链接，HTTP地址实际上指向一个网页，其很可能包含用户端软件自己的宣传内容。它的兼容性不好，通常不要分享HTTP地址。

注册（补充）

两种可能的注册方式：注册和登录在各个设计得好的用户端软件都通用，但并不是所有的服务器都允许在用户端软件注册，一些服务器只允许在网页端注册。试着使用网页浏览器访问服务器的地址到达服务器的官方网站。如果网站上说不允许直接注册，而且也没有直接提供网页端的注册入口的话，那么你就得去用户端软件请求注册，然后它就会告诉你网页端注册的地址。

不要过于依赖用户端软件直接注册：公共服务器很难保证长期允许在用户端软件直接注册（“in-band registration”）。例如，如果服务器有想让注册的用户提前知道的提示信息，那么它就只会允许在网页端注册，XMPP的注册功能不适合用来展示和阅读大量文字。

电子邮箱重置密码：在网页端注册可能会获得更多功能。最常见的就是服务器网站允许用户预留电子邮箱地址，用来在忘记密码的时候用它重置密码。

XMPP连接和HTTP连接不同：存在互联网封锁时，你能否使用网页浏览器顺利地直接访问服务器的官方网站，和你能否使用XMPP用户端软件正常地使用其服务器注册和登录，可能没有直接关系。因为XMPP连接和HTTP连接并不相同。

注册表单：有的用户端软件会直接将服务器提供的注册表格递给注册用户看，这种情况的兼容性最好，用户可以最清楚地了解服务器有什么注册要求。有的用户端软件还会请求获取本地语言的注册表单，看服务器有没有准备翻译过的表单了。如果表格文字是读不懂的外语……那么就比较糟糕。有图片验证码时，表格往往还会提供验证码链接，供用户端软件显示不了验证码的注册者复制链接到网页浏览器访问来获取验证码图片。

注册要提供的信息：许多公共服务器只须要提供想要的XMPP身份号码和想设置的密码就可以注册，也许再加个防机器滥用的验证码，也许再加个电子邮箱地址，不会再多了。如果服务器要用户的政治身份信息或隐私信息，那么这种服务器不可信的，或者是指定人群专用的；总之，普通用户不该在这种服务器上注册使用。

注册连接滞留时限：在用户端软件注册时，获取表单后，如果你在注册的步骤滞留太久，服务器可能会中断连接。有的公共服务器允许在注册步骤滞留的时间并不长（网站注册一般不会有此设计），所以要提前想好你要设置的XMPP身份号码和密码。

XMPP身份号码支持多种字符：如果你愿意的话，注册时积极地试一试汉字和符号，如果注册失败，那么还是得用最基本的字母和数字组合，或者换一个公共服务器注册。

“用户名”：由于XMPP身份号码不少被人们直接当网名用，因此它也被叫作“用户名”，但是在同一服务器里终究不能重复，且注册后就不可直接改变了。

XMPP身份号码复杂度：如果将自己的XMPP身份号码设置得太长难以记忆（例如十五个随机组合的小写英文字母，这就已经太复杂了），那么，不管你是否记得住这个身份号码，你的XMPP身份号码给其它人带来的初始信任都会更低。

密码复杂度：有的服务器会拒绝太短或字符种类太少的密码。良好的密码要有十个或以上数量的字符，并应该兼有多种字符（大小写英文字母、数字、符号）。同时，不应该将密码设置为和你在其它地方使用的其它密码相同。（一般来说，设置的密码越是有规律性，越是存在有自然语言意义的字符组合，就越容易被视为弱密码。这只是额外提醒，很少有公共服务器的检查细致到这个地步。）

验证码复杂度：验证码可能会简单得只有人人都认识的数字或英文字母（请记得区分大小写来填），也可能会五花八门：

- 有的公共服务器使用当地语言文字做验证码，这种服务器是无法向绝大多数人推荐的。
- 有的验证码是算术题。
- 有的验证码让你从一些字符中去掉一部分。
- 有的验证码故意让字符处于边缘，只显示一半。
- 有的验证码是整行歪的，可能会因有些字符出界而无法完成验证。

如果一个服务器在注册时不需要验证码，那么此服务器很有可能因为被从事网络攻击的机器程序滥用而被其它服务器列入拒绝通信的黑名单，进而影响你和其它服务器的通信；当然，服务器也有可能以后添加验证码门槛。

耐心点：只要你成功获取了服务器的注册表单，那么你和服务器的连接就是正常的。提交注册表单后的等待时间应该不超过半分钟。

停止接纳新用户：如果一个公共服务器内的注册用户已经够多，为了不降低给已有用户的服务质量，它可能会停止接纳新注册用户。已经停止接受注册的服务器是不应当被推荐的。

多次注册：你可以注册获得多个XMPP身份号码。但请不要像网络攻击一般为自己注册过多，这是违背互联网精神的。

独立的联系方式：如果服务器不提供电子邮箱重置密码或者类似的功能，那它就是一种独立的联系方式。也就是说，有以下特点：

- 你可以完全地将它送给一位朋友，也就是替别人注册了一个XMPP身份。
- XMPP身份标识和密码是仅有且必需的登录凭证。
- 如果你失去了另一种联系方式（互联网除外），那么它不会受影响。

注意敏感字词：如果你在XMPP身份号码里或网名里加入对一些人具有冒犯性的内容，那么那

些人就很可能在一见到你，在你“什么都还没说”时就拒绝和你通信，甚至将你加入公共的参考封禁名单。如果服务器管理员能直接读懂你的冒犯性言语并惹怒了它，它自然会封禁你。例如，服务器管理员可能会不允许使用类似于“admin”（英语单词“管理员”“administrator”的简写）这样的内容当XMPP身份号码，它们可能认为这有被用来诈骗别人的登录密码的危险性。

见鬼的“匿名注册”：XMPP服务器可能允许“匿名注册”（更好的叫法应该是“临时注册”），这在语言表达上和应用程序上都有所矛盾。这个“名”指的是你的XMPP身份号码，而不是指政治身份信息；普通注册本来就是不需要政治身份信息的。“匿名注册”给你一个临时的XMPP身份号码，服务器在你保持离线一小段时间后就注销它，没什么特别方便或特别有用的。“匿名注册”的用户交流诚意往往更少，而且会占用一些XMPP身份号码取值范围，也可能被滥用并给这些号码以及服务器留下不好的历史遗留问题，所以通常公共服务器更可能不允许这么做。

邀请注册：用已有的XMPP身份向服务器请求再注册一个号码。这在平时基本没用，只有服务器对注册有较严格的限制时才有用；但不受人工监管的机械程序地邀请还是可能会导致服务器遭到滥用和用户遭到垃圾骚扰。

请推荐：对新手而言，组织内的同志推荐服务器很重要。

登录

登录只需要XMPP地址和密码。这也就意味着钓鱼网站有效果，用户必须学会辨别钓鱼网站。参考“周边技术问题”章节的“钓鱼网站问题”条目。

第一次登录时，服务器很可能会给你发送一条欢迎消息。常常是外语。不用回复，也无法回复。还可能带你去服务器的一个会议室，如果语言不通，那么最好退出会议室，并删除对应的个人地图项目（保存的会议室地址），避免尴尬。

只要你登录成功了，那么所有的文字信息都是由服务器当邮递员传送的。如果是两个不同服务器的用户之间通信，那么这两个邮递员都参与递信。唯有下载寄存的文件是和各个服务器直接连接，因此下载异服务器的寄存文件是否成功和你能否成功连接自己的服务器没有关系。如果你的服务器无法连接一个异服务器的会议室，那么这是服务器和服务器之间的连接问题或服务策略问题，此时你使用代理网络连接也是没用的（你所成功登录的服务器本身就算是个变相的代理连接服务器了）。你只能在那个会议室所属的服务器上或其它服务器上再注册一个新的XMPP身份，看看能否连接那个服务器的会议室。

如果一些用户端软件提供“隐身登录”选项，请不要选择它。无论是从整个通讯系统的功能配合和程序设计上，还是从社会交际上讲，“隐身”这个在线状态都是大矛盾，自然而然地被废弃了。保守派们自然地喜欢这个并将此视为用来调和社交矛盾的东西，但这实际上只会让人们的交流更加闷气更加难受。拒绝隐身状态符合革命派爱憎分明的优点。

普通用户不应当在意“服务器名/主机名”和“端口”（两个计算机术语）这种登录时的高级选项。不要启用它们。无视它们，置空或保持默认值即可。

更改密码

修改密码只需要密码，很方便，所以泄露密码是很危险的。

更改密码后，所有其它的登录端都会无法登录。但有的用户端软件会死心眼儿地不断用原来的密码尝试登录，对服务器造成网络攻击，这会导致服务器拒绝和你通信；所以也要及时修改那些用户端软件的登录密码。

注销

手动注销：如果你用的服务器支持手动注销的话，那么在XMPP上这个操作常常是一瞬间的事情，没有“反悔期”的概念，不可撤销。如果是自己的重要XMPP身份，就要小心注销按钮，

不要手贱。泄露密码是很危险的，你的XMPP身份可能会被别人注销。

自动注销：服务器通常会自动注销很久没有登录过的XMPP身份。不手动注销可以有效避免一些历史遗留问题（例如注销后立刻有另一个人注册此号码的情况）。公共服务器有的自动注销期限短者有的为三个月，长者有的为两年。

在本地删除：在自己的设备上删除XMPP身份的同时常常会删除所有的本地存储聊天记录。如果服务器没有为你存储聊天记录，你也没有备份的话，那么你就会彻底丢失它们。在本地删除不影响服务器的存储信息，用户可以再次登录。

防冒充：有的公共服务器会封存被注销的XMPP身份号码一段时间，阻止别人注册此号码以防止别人冒充以前的用户。但大多数公共服务器没有这种功能。普通用户想要废弃某个XMPP身份时，要做的仅仅是停止登录，等待服务器自动注销。

注销后，所有其它的用户端软件都会无法登录，但有的用户端软件会死心眼儿地不断用原来的密码尝试登录，对服务器造成网络攻击，这会导致服务器拒绝和你通信；所以要及时停止让它们尝试登录，并删除本地遗留下来的废弃的XMPP身份。

不同服务器的注销反应并不同：

- 注销直接成功，并发给用户端软件注销成功标准回应。
- 服务器的服务政策不允许手动注销。停止登录，让它以后自动注销吧。
- 服务器有自定义的注销成功的反馈信息，但是用户端软件错误地认为注册失败了。
- 服务器注销完毕了，但是没给用户端软件回信；用户端软件等了很久后才告诉用户说“操作超时”（“未成功”）。
- 用户端软件在发现注销成功后可能不给任何反馈信息。可能在表现上只是删除了本地存储的用户数据。

不管怎样，只要用户无法再用密码登录，那么就是注销成功了。

主动注销前应当考虑以下问题：

- 是不是有应该保存的历史消息或以后还要再联系的地址等等没有保存？毕竟用户端软件们在注销时通常会一并删除本地存储的用户数据。
- 是不是应该通知一些人“我要注销号码了”？毕竟注销操作只会提醒联系人们说“对方已停止共享在线状态”，而不是“对方已经注销了号码”。
- 会不会有某个已经知道我这个XMPP地址的人等我注销后注册这个XMPP地址以冒充我。
- 是不是应该通知会议室房主或管家，让它们在成员列表里删除我的用户地址？
- 如果要更换一个新的联系地址，是不是应该先告知自己的新联系地址。毕竟来自旧联系地址的这种通知是一种能证明新联系地址是我的凭证。
- 我是个名人吗？我注销会造成什么负面影响？
- 我有后悔症吗？后悔症会不会发作？

多端在线（补充）

每个登录点都有自己的通用登录点标识，格式通常为“用户端软件名称.随机字符串”，随机字符串常常是此登录点第一次登录时就随机生成并固定下来的。有些用户端软件允许用户自己修改，没有特别目的请不要这么做。汉字可能会导致运行不正常，若求稳定，请只使用ASCII字符。

一个XMPP身份可以很容易地被多个人合作一起使用，因此你可能看到有的虚拟用户有性格、谈吐、举止不同的，“人格分裂”的表现。

多身份在线

这是用户端软件可以提供的功能，而非XMPP标准规定的。好的XMPP用户端软件都允许多个XMPP身份同时登录在线。XMPP本身对此没有限制，也无法限制，它不会分辨是不是一个人在同时使用多个虚拟身份。公共服务器也基本不会严格限制哪个人这么做。

可以使用多个虚拟身份，有的用来和近距离认识的人实名交谈，有的用来和远方网友匿名交谈。但是自己在使用多个虚拟身份时要分得清自己在用哪一个XMPP身份，自己在和谁说话。可以同时只上线一个虚拟身份，手动下线其它的，来防止这种错误。

网名（补充）

严格地说，XMPP身份号码不属于网名，但当你没有设置网名时，它通常会被作为网名来用。

你可以为自己设置一个通用网名，它在别人的视角里会代替被作为临时网名的XMPP身份号码。

在会议室里，你可以单独设置你在会议室里的网名，不同的登录点可以设置不同的名称（这会导致室内私信通道也针对不同的登录点），每一个室内网名都在会议室里单独占一个在场座位，管理等级变化时会同步，参与等级则并不如此。

对联系人而言，你可以设置你对联系人的称呼，这只显示在你的视角里。

通常，联系人在你视角的显示名称的优先级为：己方给对方设置的自定义显示名称>联系人自己设置的网名>联系人的XMPP身份号码。

通常，会议室名称显示优先级为：自己给会议室设置的标签名>房主自己设置的会议室名称>会议室的门牌号码。

室内网名也有字符种类限制，但一般比XMPP身份号码和会议室门牌号码更宽泛。

有的群聊服务器允许的室内网名不长，很可能导致加入会议室失败。要避免这种冲突出现，那么在进入会议室时使用一个很短的网名，并试着慢慢改长，直到你接受的长度。也有的群聊服务器允许的室内网名很长，都可以当宣传板了。

如果你给自己起的网名在日常交流中跟容易遇到，因此用户端软件时常在别人本意没有提到你时对你发出通知提醒的话，你可以给自己的网名前面或后面添加不常见的符号。

虚拟肖像

选择一个虚拟肖像发布是个好主意。这非常有助于帮助别人一眼分辨谁是谁。不然，有些用户在长长的联系人列表找人时，以及在群聊中读消息时，就只能仔细看网名甚至地址来分辨人。

虚拟肖像的长宽比是不限制的，但大多用户端软件们选择使用正方形。

虚拟肖像可以发布任何格式的电子图片。但实际应用中你用的用户端软件 and 用户服务器可能会为了考虑兼容性而对此有所限制（例如，请不要用虚拟肖像的位置存储大型图片），也得其它人用的用户端软件能正常显示才有用：

- PNG格式是XMPP标准保底支持的格式。也是我们最建议使用的格式。
- JPEG格式特别通用，肯定没问题。
- WebP格式的优越性已经受到广泛认可，软件们肯定愿意支持它。
- SVG格式图片如果设计得很棒就会体积小又特别精美。它普遍占用较多处理器资源，如果设计不够好或内容过于丰富再加上图像显示程序不小心的话还可能会占用太多运行内存。也许有些用户端软件尚未考虑它，或者不会考虑它。
- AVIF格式在位图中则占用很多运行内存和处理器资源。不过作为小型的虚拟肖像的话，是可以接受的。
- 其它的图像格式就不要考虑了。

有的用户端软件在无法获取或无法显示别人的虚拟肖像时会采用显示名称的前一两个字符作为临时显示的虚拟肖像，并根据显示名称和界面背景明暗模式来算出一种背景颜色。

在大桌会议室里，会议室设置可以阻止查询别人的电子名片，这同时也会导致与会和旁听看不到别人设置了虚拟肖像。

除了电子名片里有虚拟肖像之外，其它的功能标准也有虚拟肖像。因此，有的人的确设置了虚拟肖像，但却不在电子名片里。因此，在大桌会议室里不是主持时，会出现有些人设置了虚拟肖像但你却看不到的情况。

在大桌会议室里，不是主持时，别人以前发过消息，但现在离场或改占座名了，此时，如果你的用户端软件不为历史消息的室内网名保留过去的虚拟肖像的话，你的用户端软件就不会再在历史消息里显示它们的虚拟肖像；如果你的用户端软件为历史消息的室内网名保留过去的虚拟肖像，那么当另有一人更改室内网名来冒充前人时，你的用户端软件就可能会为前人的历史消息显示后人的虚拟肖像。

对话（具体使用）

添加联系地址（补充）

尽管用户端软件自动分辨联系人地址和会议室地址是可能的，但在添加联系地址时仍然有必要自己手动区分。不要在添加会议室联系地址的输入框里输入用户地址；也不要往添加用户联系地址的输入框里输入会议室地址。

有的公共服务器对自己的用户拒收陌生人消息，未向对方分享自己的在线状态在这种服务器上会导致对方无法向自己发送消息。相互分享在线状态了，才算是相互信任了，才会允许更多交互操作。

XMPP联系人名单可以起到仅记录的作用，但用户端软件们（或加上服务器们）基本都会设计成添加一个联系人后就让对方获知并自动请求共享在线状态。

如果你认为对方刻意地或无意地忽视了你发送过去的添加联系人申请或共享在线状态的请求，或者可能你自己忽视了“请求被拒绝”的通知，你可以取消请求共享在线状态，并重新请求共享在线状态，这会再发送过去一次请求。

添加一个纯服务器地址作为联系地址是可行的，但这不是一个普通用户地址，给服务器地址发消息常常无效或没有多少实际作用。服务器管理员基本用普通的XMPP用户地址作为联系地址。服务器地址常常被用来发布服务相关的通知，对新注册的用户打个招呼或发些提示或请求走一个敷衍的法律流程。给服务器地址发送消息时，也许它是会接收的，但不一定会给你发送任何回执。你是不是此服务器的用户也影响着此服务器地址是否会拒收你的消息。

如果要创建一个会议室，首先得确保在对应的群聊服务器上有创建会议室的权限。不过这个过程很简单，大多公共服务器会兼具用户服务器和群聊服务器，其用户服务器上用户在其群聊服务器上有权创建会议室，而且用户端软件通常会自动查找到与用户服务器对应配套的群聊服务器。（如果创建时要求手动填写群聊服务器地址的话，那么你就要手动查找用来创建会议室的XMPP身份所属的用户服务器是否有配套的群聊服务器，服务器也可能不提供群聊服务器。）公共群聊服务器一般不会给予别人的用户服务器的用户以创建会议室的权限，但一个会议室完全可以通过编辑房主名单来做到使它没有任何一个房主属于自家的用户服务器。

有些服务方（不一定是XMPP服务方）提供用来和其它非XMPP的通讯协议或平台通信的转接桥，只需将转接桥的地址视为XMPP联系地址来添加就可以使用。由于不同通讯平台的功能设计不同，转接桥会有兼容性问题 and 功能性问题。使用转接桥接入另一个通讯平台的基本原理是在那个通讯平台上创建一个和自己的XMPP身份对应的虚拟身份，伪装成一个属于那个通讯平台的普通的、正常的虚拟用户。这会带来很多问题，例如不知道那一端的服务器的服务策略如何，不知道不用时会保留还是会注销那一端创建的虚拟身份。XMPP标准没有关于转接桥这种东西的规定。只有提供转接桥的服务方才对转接桥的设计和效果负责。

加密（补充）

用户端和服务器之间有TLS加密。

主动加密使得只有交流的用户之间可以直接读取信息。这保障了信息安全。

由于有被动加密和主动加密之分，所以有些人说的“未加密”有所歧义。它们常常是指没有端到端的主动加密，而不是指用户端和服务器之间连被动加密都没有。

在线传输文件（非寄存）无法使用主动加密，需要加密时只能手动加密（例如使用“7z”打包文件格式）。

如果两个通信端能用的加解密方式不一致，那么就只能用无主动加密的消息来对话。当有的人着实要用老旧的软件来用XMPP，因此不支持你想用的加密方式时，请自行考虑关闭主动加密

来和对方通信。

文字消息的主动加密除了OMEMO外还支持OpenPGP和OTR，但都不是我们建议使用的：

- OTR是一种老旧过时的落后加密方式，请忘了它。许多用户端软件不再支持这个加密方式了，服务器也不一定会支持。如果用这个加密方式，别人很可能因为自己的用户端软件不支持而无法接收并解读你的加密消息，或者甚至服务器根本就不支持。
- OpenPGP操作复杂，学习量大，有太多的衍生问题，也不作介绍。

文字消息（补充）

文字消息是它的基本功能。虽然可以像电子邮件一样写标题，但通常这是不必要的，大多用户端软件也不支持这个。

用户收回和主持删除只能确保还没有收到这个消息的人在获取历史消息时得不到它。对已经收到的人则会发出请求删除的信号，它们是否删除终究还是它们决定的。如果别人收回或删除了一条已发送消息，但你的用户端软件的功能尚不支持此功能，那么你可能会收到一条提示信息说明此事。

它有更正已发送消息的功能，常用于发送的消息中有错别字的情景。由于历史消息存档系统不记录哪些是更正后的消息，所以只有在场人员才知道哪些消息是被更正了的，获取历史消息的用户则会看到原文和订正文分别显示。

文字消息的发送结果有三种之一：发送成功、发送失败、不确定：

- 收到用户的回执时为确定发送成功。
- 确定发送失败时的情形有例如服务器明确拒收消息，填写收信服务器地址不存在（因此无法抵达）等。
- 不确定的情况，即为发送操作已经执行，可没有收到收信用户的对应回执，也没有检测到其它错误。不同的用户端软件对发送结果不确定的消息的显示不相同，有的和发送成功的消息作相同地显示，有的则区别对待它们。

有向服务器举报垃圾信息的功能，在提交对方XMPP地址的同时还可以附带说明信息。但这个功能的作用很小，小到让人质疑——人们可以轻松发送主动加密消息，服务器管理员无法看到谁说了什么，难以作决断；而且这还会牵扯到个人恩怨以及社会问题。很明显，在对社会不负责任的无名小卒泛滥的，和政治身份完全无关的交流平台上的话，我们基本可以忽视这个功能了。

文件传输与寄存（补充）

关于文件传输的速度。寄存的文件的上传和下载速度直接决定于用户端和寄存服务器的连接速度。在线传输则更麻烦点，服务器可能为你传递数据，也可能只给你引个路而让你和对方直接连接；如果是服务器为你传递文件，通常异服务器的在线传输速度会比同服务器的在线传输更可能更慢。

服务器有单文件寄存体积限制，会通过对应的功能标准信息项告知用户端软件，但总寄存体积限制和寄存期不会直接告知，需要去官方网站查看服务策略。

绝大多公共服务器都提供文件寄存功能，但由于XMPP并不是专门为了寄存文件而生的，所以大多公共服务器的文件寄存体积并不大。一般来说，文件寄存体积限制越狭小，公共服务器就能承载更多的用户数量和更多的消息存量。如果要寄存的文件体积超出了服务器允许的体积，可以使用互联网上的其它的免费又不需要注册的打开即用的文件临时寄存服务，这常常会更加方便好用。

寄存常常是更好的选择，不仅速度快，而且还能让多个人同时下载。在线文件传输则只能一对一，还需要双方都在线，速度还更可能更慢。

如果寄存的文件体积超过了总体积限制，就会把最早的文件删除。不要用公共XMPP服务器的寄存方式来大量传输文件，很可能你在大量传输过程中前面的文件因为超限就自动被服务器删除了。

如果寄存文件没有使用主动加密，那么它的下载链接就是通用的HTTP链接，任何获得链接的人都可以使用网页浏览器获取（即使它们完全不使用XMPP）。同时，XMPP不能保证文件名被完全保留，有的寄存服务器会重置文件名，给要传输的文件打包可以避免这种情况。

寄存的文件的下载由用户和文件寄存的服务器直接连接，而文字消息（包括寄存文件的下载链接）由你的服务器当邮递员为你送达。所以不同服务器的人为你发送一个寄存的文件时，如果你的上网环境存在污染或障碍，就可能会出现你无法下载的情况。实际上这属于周边技术问题，请参考“周边技术问题”章节的“上网环境阻碍问题”条目。

有些公共服务器允许寄存的文件体积确实很小，但这正是XMPP作为即时通讯服务（而非文件寄存服务）的特点，对革命派而言，这还能算是一种优点。这种特点确保了XMPP的公共服务器压力小，因此有大规模普及的基础可能性。而那些资本主义的商业服务，随着用户数量增长，它们早晚得要求用户验证政治身份，早晚要降低服务质量，早晚要投放商业广告，早晚要宰熟客，早晚不小心来一次泄露用户政治身份信息，等等。

关于寄存文件的文件名是否保留，或者添加什么前后缀（例如时间、来源）等便于分类和排序的信息，其影响因素有你的文件寄存服务器是怎么配置的，还有你的用户端软件是怎么设计和配置的。

历史消息存档（管理）（补充）

有的公共服务器承诺存多少天或多少条。有的公共服务器则不承诺。

承诺存多少条的更可能是专用服务器，不是给用于一般交流用途的普通用户用的，或者说，每天收信数少的用户可以使用。

作为即时通讯，它不会像电子邮箱那样永久存储历史消息并让用户自己管理分配给自己的空间。一般而言，公共服务器最少应该存一个星期，存两个星期（或半个月）算较好，存一个月（或四个星期）的算很好，存三个月的话那太慷慨了，还有的给存一年。通常，如果它们存得久，它们能服务的用户数量就会少。

有的公共服务器则不承诺，可能是随心搭建的服务器或刚刚建成的空闲容量很大的服务器，看着来，先尽可能多存。用户数量将影响这一服务策略。

你设置了存档非联系人消息，再加上你的用户服务器存档历史消息特别久，这种情况可能会导致在你上线一个新的登录点时获取到太多过去已久的历史消息（也要看你的用户端软件本身的设计如何），你都不一定记得这些人和事。

如果你过于依赖服务器为你存档久远的历史消息，而没有自己保留存档的习惯，那么你应该清楚：如果你习惯用主动加密的消息，那么一旦你丢失了解密密钥，即使你获取了历史消息，也无法解读它们了。

用户端软件通常会有防止获取过多历史消息的设置，不会一次性获取所有能获取到的历史消息，否则很可能会包括大量非常久远因此对用户没什么用的消息（如果服务器的历史消息存档期限确实很久的话），或者对使用计费流量互联网的用户造成不必要的损失。对每个对话项可能只获取一定数量或一定期限的历史消息。对会议室而言，也许是最近的一些消息，也许是上次离开后面的一些消息。如果不想错过会议室里的消息，就考虑逗留在会议室里，不要离开。

对话通道（补充）

室内私信通道是按照室内网名送信的。

在会议室里，公开发言权和室内私信权是两种东西。

室内私信通道很特别，用户端软件们对它有两种设计：

- 将室内私信和公开消息放到同一个对话界面里，当你想临时和一个用户使用私信交流时，它会非常方便；但当你想和它交流很多时，依赖室内私信通道就会影响阅读公开消息，因为这些室内私信会和公开消息穿插起来。
- 将室内私信通道作为单独的对话选项，不和公开消息放在一起。这方便做到在不添加为联系人的前提下交流大量信息，但一旦对方修改室内网名，或一方离场，这个对话项就废弃了。
- 不同的这种设计通常也会影响保存消息记录时是合并保存的还是分开保存的。如果是合并保存的，那么在分享消息记录文件时就要留意这一点。

请求授予公开发言权

没有公开发言权的最常见情况是：在一个开幕且敞门的会议室里，有个人第一次进入此会议室。会议室的房主、管家、主持人和这个新来的都不是朋友，甚至不认识，因此成员名单里没有它。而且，会议室没有设置【默认给未经手动更改权限的人公开发言权】。

以下是请求获取公开发言权的办法：

- 如果你有哪个朋友和主持也是朋友，你可以请它做媒来请求主持为你授予公开发言权。
- 如果会议室允许旁听发送室内私信给主持，那么你可以自己来发消息请求主持授予你公开发言权。
- 如果用户端软件和会议室都允许旁听者按键请求授予公开发言权，那么也可以这么做。这会向所有在场主持都发送操作通知。
- 如果会议室有诸如“想获取公开发言权，请在室内网名前添加某符号”此类的规定，你可以照做，并等待主持为你授予公开发言权。
- 如果会议室公告板或信息板上有主持的用户XMPP地址，那么就可以用普通私信联系。
- 要是以上办法都不行，那么只要没有隐藏旁听在场状态的话，你可以修改室内网名来向它们传递信息。修改室内网名会产生一条室内通知，期望主持的用户端软件支持且没有隐藏此通知吧，或者主持会时不时地查看在场列表的话也可以。

套用的交流插图 (sticker)

有的服务器（不一定是XMPP服务器）会提供可套用的交流插图。这些插图在多次接收的时候不会多次下载，因为这些交流插图并不是以用户上传的文件的形式存在的，而是直接访问存储套用插图的服务器提供的图片链接而得到的。这些图片链接是否还能够访问并获取内容也是由对应的服务器决定的。

这种东西对处于互联网封锁之中的用户而言比较麻烦。

消息互动反应

当你发送一条消息时，别人可以对这条消息发表反应。结果就像在贴文平台上的一条贴文下面显示褒贬各有多少数量一样。

但这个功能还没有很好地普及，最好不要依赖此功能。

会议室详述

占座名（补充）

有的用户端软件的有些修改占座名的操作会同步修改个人地图里记录的默认占座名。有的用户端软件在本地记录加入会议室所要使用的占座名，而并不随时应用个人地图记录的默认占座名。

六大设置状态（补充）

补充形象的说明。

露天或地下

露天：在公共大地图上标出会议室的位置，让大家都找得到。服务器在露天会议室列表里公布会议室地址。别人有了地址进而可获知会议室名称、介绍、门画、设置状态、公布的占座数。用于认为人多热闹且喜欢人多热闹，欢迎各种人加入的情况。第三方的搜索引擎也可能会收录你的会议室地址的名称、描述介绍、地址，让其它人可以很方便地搜索到。

地下：会议室在地下，能减小被其它人发现的可能性。服务器不公布会议室的地址。但会议室的地址仍然可以被用户们泄露，别人仍然可以按照获得的地址精准找到会议室并试图加入。

锁门或敞门

锁门：游客有了地址也无法进入；只有成员能进入。别人看不到会议室的公告板、消息、人员电子名片。会议室露天或地下都是次要的，锁不锁门才是外人能不能进来的关键。由敞门改成锁门后会立刻将所有的游客撵走。

敞门：允许游客进入。这并不决定它们是否有公开发言权或私密发言权。请牢记敞门区别于锁门的核心作用——带观众，给人看。你想在此说的就是想给人看的，而且是所有人都能看的，全世界都能看的，包括敌人，包括战友。

大桌或小桌

大桌：房主特别支持匿名活动，与会和旁听看不到别人的身份证。（成员名单只有管家和房主可以看到，在场人员的XMPP地址只有主持能看到。）因此，在场人员变更面具或名牌可以起到伪装的效果，可以轻松地装成一个与会者和旁听者以前没见过的人；只有主持才能看透它们的表皮，才知道它们到底是谁。这是一种试图调和立场冲突的人们之间的矛盾的做法，也是一种人与人之间信任不足的直接象征。宽大的桌子，离得远的座位，让它们得以保持“安全距离”。

“我昨天见到了这个名字，但是今天我再来的时候，我不知道这个名字是原来的人，还是另一个人占用了这个名字冒充了此人……即使我不离开，可它一离场，再回来时，我同样也无法100%确定出去的和进来的是同一个人了。我也不知道主持会不会泄露我的身份证，我都不确定有几个主持，更别说对主持们追究责任了。”（对政治身份而言，这已经达到了九成的匿名了，再匿就太危险了。）

小桌：房主期望所有人以各自身份的荣辱来为自己的言行负责，要求公开成员名单和在场人员的身份证。（所有在场人员都可以看到成员名单和在场人员的XMPP地址。）任何人的表皮都没有好的伪装作用。小桌子可以拉近我们的距离，方便我们察言观色。成员不在场时，也可以按照它们身份证上的信息来联系它们。在锁门的会议室里，小桌是信任的象征；在敞门的会议室里，小桌则是对捣蛋鬼们的一种限制措施，但同时对于会议室里的主要人员也有了政治素养要求，至少要愿意以固定身份来活动，还要能抵抗敌人那直达的和间接的言语攻击。（这种情况下公开的只是XMPP身份标识，而不是现实政治身份信息。只能说是“相对的无匿名”而已，它仍然可以说是一种匿名。）

提醒：在大桌会议室里，XMPP身份标识不明时，你还无法分辨哪些人是正式的XMPP用

户，哪些人员是在借助网桥从其它通讯平台接入。

开幕或闭幕

开幕：会议开始了，遵循参与等级。谁能发言，谁该闭嘴，全部由主持们决定。对敞门的会议室而言，几乎必须用开幕模式，否则容易受到捣蛋鬼的垃圾信息攻击。

闭幕：会议没有开始，现在只是个普通的公共交流场所，因此发言不受管理，在座的各位想说啥就说啥。（所有在场人员都可以自由发言。）只有确保没有捣蛋鬼进入会议室时，闭幕模式才是有意义的——一种情况是锁门会议室，不过很明显会议室锁门的话基本也就不用管开幕闭幕了；另一种情况是，服务器对注册用户和连接的其它服务器有严格的素质要求，确保不受任何捣蛋鬼入侵，因此敞门会议室的房主们就不用自己防捣蛋鬼了，用闭幕模式可以让别人一来就可以公开发言。

口令守卫或门神守卫

口令守卫：门口里面有个守卫，对每个想进去的人问口令（密码），没有提示，没有具体问题内容，知道密码的人就算过了这一关。如果锁了门且没有钥匙，那就不用问口令了。口令不是很安全，会议室里有不信任的人时就没有很好的效果，因为密码可能被泄露并公布。密码只能稍微限制人员的来源，其效果的不确定性很强。这是不建议设置的，因为它是不论参与等级地限制所有人的；而且，在修改口令后，所有人在下次加入时都要输入新口令。

门神守卫：没有守卫问口令。会议室不设入口密码。只有会议室对外公布的信息能影响外人的加入意愿。如果要禁止游客进入的话，应该用锁门。

棚屋或砖屋

棚屋：只要有人在，它就撑得起来。要是人都走了，一点风雨、一只野鸡都能把它压倒。（会议室没人在场时，就会被立刻拆除。）

砖屋：经得起风吹雨打。（当会议室里没有人在场时，会议室仍会存在。）空置的砖屋遗留太多会空占很多门牌号码，干扰其它人获取高质量的露天会议室搜索结果和挑选门牌号码地创建会议室。可是，基本上，只要将会议室用于长期的一般交流，那么就on应该将会议室设置为砖屋。因为：

- 用一个会议室的人少时，很可能出现没人在场的情况。
- 即使是人多时，服务器断线也会导致所有人被迫离场，会议室被删除。
- 更严重的情况是，如果你在对应服务器上有创建会议室的权限的话，加入会议室的操作命令对不存在的会议室能起到创建新会议室的作用（如果用户端软件没有在加入之前事先检测会议室是否存在并阻止用户加入空会议室的话）。在会议室被意外删除后可能会出现别人抢先加入鸠占鹊巢的情况。

可以将用户端软件们设计的【创建】操作理解成：执行XMPP规定的加入操作，并调整由此产生的会议室设置为砖屋等。

如果用户端软件设计了如上的【创建】操作，那么用户端软件们设计的【加入】操作也许是这样的：在执行XMPP规定的加入操作前，先检测此会议室是否存在。若不存在，则用户端软件拒绝【加入】（因此此“加入”完全不会创建一个新的空会议室）。

通常服务器们会自动删除长期没有任何活动迹象的会议室，不必因为遗留下一个砖屋而太担心在其它人的搜索结果中产生干扰项。有的服务器会封存被主动拆除的会议室的门牌号码一段时间，期间不允许再次占用。

本说明书中对会议室所说的“解散”和“拆除”是一样的意思。

管理等级（补充）

“国王”管理等级：管理服务器的人。在所有会议室里显示为房主，且不可被更改管理等级。（“国王”并不是XMPP标准里特别规定的名词，只不过我们用这个来形象表达。）国王是服务器的管理者，是所有属下会议室的房主。国王平时不在会议室的成员列表里显示，所以会议室有可能在没有任何对应的授权操作的情况下突然出现一个新的房主。这是国王串门来了。如果语言互通，那就好说话；如果语言不通，那就尴尬。

参与等级（补充）

参与等级的具体管理稍显复杂，不过一般不需要那么特殊的权限管理操作（针对一般用不着的操作的说明和想当然的规则已淡化显示）：

- 房主的在场参与等级必然是主持，其它所有人的在场参与等级都可以被任意调整。
- 只有房主和管家可以授予和撤销别人主持。管家对其它管家只能设置主持，而不能撤销。管家的主持只有房主能撤销。
- 只有参与等级是主持时，才可能将人员的参与等级在旁听和与会之间直接调整。不主持的管家要将人员的参与等级在旁听和与会之间调整时，只能先将人员的参与等级设为主持，再在撤销人员主持时选择设为旁听或与会，以做到间接调整。
- 主持无法对管理等级大于自己的人员将参与等级从与会降低至旁听。
- 主持将旁听和与会设为离场时，要求主持的管理等级大于或等于被操作方。主持将主持设为离场时，要求操作方是房主或管家且管理等级大于被操作方。

由于有“管理等级”和“参与等级”两种分类，所以用户端软件们设计的在场人员列表里很可能分类不同，请注意区分。

在保存人员参与等级的群聊服务器上，那么参与等级就能发挥更多作用。例如：

- 你没有很信任的人在场，又迫切地需要人来帮你管理公开发言权，又担心管家有过大的权力；那么，你可以仅设置主持。
- 一个敞门的会议室里有许多游客，它们想偶尔发言，却又不是常客或对会议室交流不重要。你不想这些不重要的人把成员名单挤得太长，就可以给它们公开发言权，而无需成员列表里记录它们。当更改会议室为锁门的时候，它们会直接被排除在外，而不用重新审查成员列表看看哪些不重要的闲人该进来却进来了。
- 非主持人的管家可以编辑会员名单，同时看不到在场人员的用户XMPP地址到底是多少。但是，如果有两个管家，它们就可以相互授予主持人的参与等级。

关系状态

XMPP标准并没有规定这些关系状态，但介绍这些会方便我们的语言表达。

关系状态×4：**出席、缺席、在场、无关。**

出席：是成员，且到场了。

缺席：是成员，但没有到场。

在场：到场了。

无关：不是成员也不是流寇，也不在场。

在XMPP的群聊里，人员到场和离场都会记录对应的时间，作为通知信息发送给所有在场的人。在实际应用中，这种信息的意义不大，严重地干扰交流，人们通常会手动关闭显示这种信息。因为：

- 上线和下线这两种基本的操作会进出会议室。
- 人流量越多，那么到场离场的信息就越多。
- 有的用户所处的无线网络环境信号强度不够好，导致经常掉线并重新连接。

- 有的用户的手机节电设置使用户端软件时常掉线并重新连接。

自愿性

XMPP的会议室对用户没有强制的归属关系。只要用户有进入某个会议室的权限，那么去不去以及在不在那个会议室就是自愿的，想来就来，想走就走。

用户和会议室之间在程序设计上没有被动的必然绑定关系。以下情况都是可能的：

- 你从来没有去过一个会议室，也不知道它存在，但是你却被这个会议室的房主或管家调整了管理等级（无论被调整成哪一种），在这以后你还是没有去过这个会议室，也还是不知道它存在。
- 你在一个会议室里是最活跃的，和大家积极交流。但是长年累月过后，你在这个会议室里的管理等级仍然只是个游客，参与等级仍然只是与会。会议室的成员列表从来没有存储过你的XMPP地址。

即使别人将你设为房主或管家，那也只是它期望你能帮它管理会议室；你去不去帮忙，以及去了是否参与管理工作，由你自己的意愿决定。别人将你设为会员，也只是它期望你能去进行交流；别人授予你公开发言权，也只是它允许你发言；你去不去，以及去了是否发言，由你自己的意愿决定。

其它常见功能

- 限制会议室座位数。
- 按照参与等级隐藏人员的在场状态，无视管理等级地起作用。此时，涉及隐藏人员占座名的操作通知不会产生；隐藏人员也无法接收室内私信；无法通过在场人员列表对它们操作。
- 室内私信开关。以及按参与等级来限制旁听发送室内私信至的人员范围。
- 授权与会修改公告板。
- 允许旁听按键请求授予公开发言权。限制按键请求公开发言权的频率。
- 在开幕模式下，设置未被手动调整过参与等级的人员的默认参与等级。
- 在大桌会议室里是否允许人员查询它人的电子名片，这会影响到是否能看到别人设置的虚拟肖像。在小桌会议室无效，小桌会议室里是必然能看到它人设置的虚拟肖像的。如果想在大桌会议室里也轻松告知别人自己的用户XMPP地址，那么可以写在电子名片里。
- 允许会员执行“邀请”操作，否则就只有房主和管家可以邀请。邀请操作可以对不在场的用户发送让对方进入会议室的请求（无论被邀请者管理等级如何）。在敞门会议室里谁都可以执行邀请操作；当在锁门的会议室给非成员发送邀请时，被邀请者还会获得会员的管理等级。实际上，在锁门会议室里对外人授予会员权限才是“邀请”操作的主要作用，因为别人不一定能收到邀请通知。如果别人没有收到邀请通知，就只能把会议室地址发给它们，请它们主动加入。即使允许了会员执行邀请操作，会员仍没有吊销其它会员的权限。
- 禁止旁听在会议室里展示自定义在线状态。
- 允许旁听当场更改室内网名。（这个作用很小，只能防止在场时更改，不防止加入时更改。）
- 室内个人标签功能（“hat”）。这个很有用，和虚拟肖像、室内网名附在一起用来表达每个人在会议室负责什么职位。但是，此功能没有在用户端软件普及，所以请忽视。
- 人类验证码。游客在每次进入会议室时都需要输入验证码。这会给它们造成颇大的麻烦。由于用户端软件的支持性问题，它们可能无法识别并显示验证码，用户得用网页浏览器访问验证码链接才可以看到验证码。面向新手时不建议设置这个。
- 是否存档会议室的历史消息。如果取消存档，那么在实际应用中就会造成严重的问题：发送消息时只有在场的人们能确定收到，不在场的人们将无法在到场时得知之前人们都说了什么。如果取消存档，就只适合开办有组织性的、约定时间的会议了。取消存档往往是对人员

不够信任的表现。

- 限制刚进入会议室的人员可获取的历史消息数量。

“【占座名】因技术原因被移出”室内通知

这个通知很常见。最常见的原因是用户掉线了，没有正常地给服务器发送下线指示：

- 在手机上走出无线路由器网络范围且没有接入其它网络通道时，会这样。
- 用操作系统命令杀掉客户端软件的进程，或者客户端软件执行退出命令时不给服务器发送下线指示的话，也会这样。
- 在其它群聊服务器的房间里在场时，自己用的服务器不发指示地掉线的话，也会这样。

会议室设置表单

Room title	<input type="text" value="会议室名称(对室外公开)"/>									
Room description	<input type="text" value="会议室介绍(专门给室外看)"/>									
会议室交流所用的自然语言的英语简写(对室外公开) Natural Language for Room Discussions	<input type="text" value="zh"/>									
Make room persistent	<input checked="" type="checkbox"/> 砖屋✓/棚屋×									
Make room public searchable	<input checked="" type="checkbox"/> 露天✓/地下×									
Make participants list public	<input checked="" type="checkbox"/> 对室外公开占座数和占座名									
Make room password protected	<input type="checkbox"/> 口令守卫✓/门神守卫×									
Password	<input type="text" value="口令守卫的口令(准入密码)"/>									
Maximum Number of Occupants	<input type="text" value="200"/> 座位数限制									
Present real Jabber IDs to 大桌/小桌	<input type="text" value="Moderators Only"/> 主持/全员									
Roles for which Presence is Broadcasted 显示哪些参与等级的人员在场状态	<table><tr><td>Moderator</td><td>主持</td><td><input checked="" type="checkbox"/></td></tr><tr><td>Participant</td><td>与会</td><td><input checked="" type="checkbox"/></td></tr><tr><td>Visitor</td><td>旁听</td><td><input checked="" type="checkbox"/></td></tr></table>	Moderator	主持	<input checked="" type="checkbox"/>	Participant	与会	<input checked="" type="checkbox"/>	Visitor	旁听	<input checked="" type="checkbox"/>
Moderator	主持	<input checked="" type="checkbox"/>								
Participant	与会	<input checked="" type="checkbox"/>								
Visitor	旁听	<input checked="" type="checkbox"/>								
Make room members-only	<input type="checkbox"/> 锁门✓/敞门×									
Make room moderated	<input checked="" type="checkbox"/> 开幕✓/闭幕×									
Default users as participants	<input type="checkbox"/> 给未被手动操作者公开发言权									
Allow users to change the subject	<input type="checkbox"/> 允许与会修改话题 (公告板)									
Allow users to send private messages	<input checked="" type="checkbox"/> 允许非房主人员使用室内私信									
允许旁听向哪些参与等级发送室内私信 Allow visitors to send private messages to	<input type="text" value="Moderators Only"/> 禁止/仅主持/全部在场人员									
Allow users to query other users	<input checked="" type="checkbox"/> 大桌时允许查阅人员电子名片									
Allow users to send invites	<input type="checkbox"/> 锁门时允许会员带外人加入									
Allow visitors to send status text in presence updates	<input checked="" type="checkbox"/> 允许旁听显示在线状态信息									
Allow visitors to change nickname	<input type="checkbox"/> 允许旁听当场更改室内网名									
Allow visitors to send voice requests	<input type="checkbox"/> 允许旁听按键请求公开发言权									
Allow subscription	<input type="checkbox"/> 非标准功能，请不要启用。									
Minimum interval between voice requests (in seconds) 允许的请求授予公开发言权按键频率(秒数)	<input type="text" value="1800"/>									
XMPP URI of Associated Publish-Subscribe Node	<input type="text" value="置空，不要在意"/>									
Enable hats	<input type="checkbox"/> 人员标签 (未普及功能)									
Make room CAPTCHA protected	<input type="checkbox"/> 游客每次进入都得输入验证码									
Exclude Jabber IDs from CAPTCHA challenge	<input type="text" value="一种自定义验证码设置"/>									
启用书记(服务器端会议室历史消息存档) Enable message archiving	<input checked="" type="checkbox"/>									

(服务器软件“Ejabberd”)会议室设置示例

其中“Default users as participants”（“默认用户为与会”）的意思是：从未被手动更改过在场参与等级的人，设其在场参与等级为与会，否则为旁听。这也就意味着，新来的人直接就有公开发言权。（更改会议室设置后，不会立刻对目标对象们生效，而是到它们下次加入会议室时生效。）调整管理等级时会自动将其参与等级归为对应管理等级的默认值，这也算是手动更改，其在场参与等级会被记录，此设置便不再对其生效。

会议室设置选项由服务器决定并提供，而非由用户端软件提供。因此：

- 你的服务器提供的设置选项很可能和例图不同，可能差别很大。
- 服务器可以给予不同语言文字的表格：这要看服务器是否准备了你本地语言文字的表格（可能有翻译错误），以及你的用户端软件是否支持获取对应语言文字的表格。
- 同一个服务器同一个用户在用各个用户端软件访问时获得的会议室选项是一样的，只有描述的语言文字种类可能有差异。
- 对同一个会议室，服务器自家的房主和别家的房主获得的会议室设置表单可能不同。例如，非本服务器的房主可能无权调整会议室的“棚屋/砖屋”设置，或者获取不到这个设置项。

支持完整地获取会议室设置表格的用户端软件有Gajim、Psi(+)、Dino、Converse。每一个创建会议室的新房主都应该完整地检查一遍会议室的设置表单。

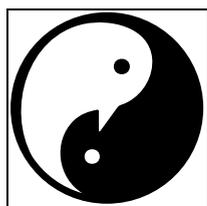
可选的XMPP用户端软件

本页中推荐的软件，都是开源程序代码的。如同Android，由全世界的志愿者们共同创造，不被任何一个国家私有。

如果有哪个用户端软件不在此页里，那就是不推荐的；即使它们曾经在这一章节出现过，现在也不再被推荐了；不被推荐的用户端软件要么是不开放、不符合标准、不适合新手，要么就是太老旧有严重的功能缺陷。

网页端

请记住网址，看好网址，小心骗取XMPP身份标识和登录密码的假网站。



converse.js

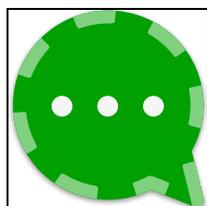
<https://conversejs.org/fullscreen.html>

一些公共服务器的网站上也提供这个组件。在许多公共服务器的网站上可以找到它。

比较简陋，但至少可以让你修改会议室设置。

有的我们并没有推荐的网页XMPP用户端软件会在它的服务器上保持登录状态，而不是在关闭网页浏览器后就下线。不用时不手动下线会给造成一些困扰，例如有人明明在会议室里占了一个座位，对其发送消息也收到了回执，但它就是没有回应。它也可能吓到自己，因为它有一个无法有效地删除的（网页端的）OMEMO密钥，再加上自己又不明白为什么会多一个。

Android



Conversations

<https://conversations.im/>

https://f-droid.org/zh_Hans/packages/eu.siacs.conversations/

最低支持Android 5.0。

Conversations很稳定，更新速度慢。它有很多衍生品，如果要使用本说明书未推荐的衍生品，那么首先你应该已经是个高级用户，能自己解决遇到的本说明书未提供支持的问题。



革命通讯器C

Conversations的改版。其翻译和引导对汉语新手很友好。这也是我们为使用Android系统的同志们首要推荐的。对其它的用户端软件，你基本都要小心错误翻译。

到金星革命委员会的官方网站可获取其源文件包和安装包。



Monocles
Chat

https://f-droid.org/zh_Hans/packages/de.monocles.chat/

最低支持Android 6.0。

Conversations的衍生品。功能多点，但程序差错也可能会多。

它可以编辑联系人的标签，它的自定义标签实际上是联系人分组，好好利用这一点。

Microsoft Windows 用户

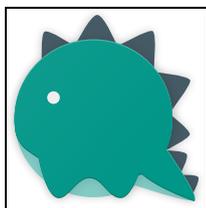


Gajim

跨平台：Windows端和MacOS端。

<https://gajim.org/download/>

功能够多。日常使用。



Dino

Windows端。

<https://github.com/LAGonauta/dino/releases>

功能简陋，但不算糟。可以为桌面端补充音视频通话功能。



Psi

跨平台：Windows端和MacOS端。

<https://psi-im.org/>



Psi+

跨平台：Windows端和MacOS端。

<https://psi-plus.com/>

非日常使用，仅用于补充其它用户端软件没有的或损坏的功能。

iOS 用户



Monal (IM)

跨平台：MacOS端和iOS端。

<https://www.monal-im.org/>

<https://apps.apple.com/us/app/monal/id317711500>



Siskin IM

<https://siskin.im/>

<https://itunes.apple.com/us/app/tigase-messenger/id1153516838>

我们并没有推荐过使用iOS设备。对普通用户而言，iOS基本没有离线安装包的概念，下载安装软件完全依赖于服务商，安装软件的自由程度和可安装的软件的运行的兼容性比Android设备差太多了。

Monal和Siskin的运行都不一定稳定。看着来，那个好用就用哪个。

iOS归属Apple公司控制，Apple是个服从中国法律的资本主义公司，禁止了一种用于音频通话的程序组件，因此从中国服务区下载到的Monal和Siskin无法使用音频通话功能。

iOS的条件对使用XMPP不是那么友好，这是不得不承认的。而且，中国服务区的iOS用户（以后）不被允许下载安装XMPP软件是可能的吗？是可能的。有的高级用户会购买美国服务区的APPLE用户身份使用，这样就可以下载安装中国服务区不允许的软件（包括代理网络连接软件）了。

Mac OS用户



Gajim

跨平台：Windows端和MacOS端。

Mac OS可以用但安装不方便，官方没有直接提供的安装包。

<https://gajim.org/download/>



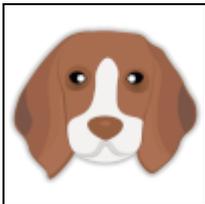
Monal (IM)

跨平台：MacOS端和iOS端。

<https://www.monal-im.org/>

<https://apps.apple.com/app/id1637078500>

MacOS平台的Monal无法使用音频通话功能。



Beagle IM

<https://beagle.im/>

<https://apps.apple.com/us/app/beagleim-by-tigase-inc/id1445349494>



Psi

跨平台：Windows端和MacOS端。

<https://psi-im.org/>



Psi+

跨平台：Windows端和MacOS端。

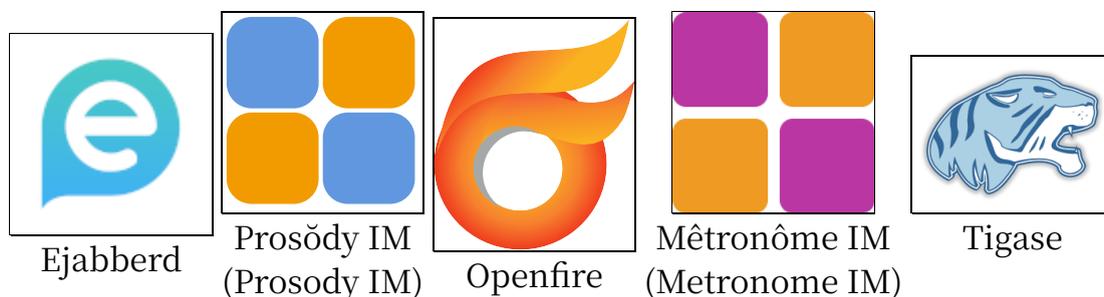
<https://psi-plus.com/>

非日常使用，仅用于补充其它用户端软件没有的或损坏的功能。

公共服务器及查找

服务器软件

本节并不是教用户搭建服务器，本说明书没有编写教搭建服务器内容的计划。但我们以政治活动为目的，有些“独特”的需求，用户仍然有必要认识服务器端软件，以尽可能地做到注册一个身份后就不用再更换。



服务器软件	公共服务器数量	群聊功能性	XEP-0016
Ejabberd	多	丰富	支持
Prosody IM	多	插件	没有
Openfire	少	丰富	支持
Mètronôme IM	少	插件	支持
Tigase	少	丰富	支持

鉴于后三个服务器软件的公共服务器建设数量少，新手可以忽视它们。

读者要了解不同服务器软件对群聊功能的默认配置，因为许多公共服务器的运营者在服务器运行起来后就不再多精心调整配置功能了，因此你可以直接参考服务器用的什么软件来猜测它的群聊服务器对房间提供了哪些供用户调整的配置选项。

“Ejabberd”服务器是给新手推荐的选择，本说明书编写过程中的实践测试也主要基于Ejabberd。要注意的一些事情是：

- 21.07及以前的旧版本会公布所有房主的XMPP地址在会议室信息板上。不过它支持XEP-0016，对高级用户而言，所以这并无大碍。
- 22.10版本开始保留会议室人员的在场参与等级。好好利用这一点。
- 23.04版本开始支持主持删除历史消息。
- 23.10版本开始支持会议室成员名单预留占座名，开始支持XEP-0421（会议室人员标识。在一个会议室内，每人一个，互不相同。无论大桌还是小桌，无论怎样改占座名，它都不会变。它可以用来查看是否有人冒充了另一个人。推荐的客户端中只有Dino支持这个。）
- 从22.10版本到23.01版本有严重的程序差错：只要曾经被授予过公开发言权，那么作为流寇可以加入会议室，作为非成员可以加入锁门会议室。所以请考虑避开这两个版本。如果使用这两个版本，那么就只适合用于不驱逐任何人的敞门会议室；对敌人不要放到封禁列表里，不给它们公开发言权就好。
- 它的会议室设置表单的汉语翻译有严重的错误，且留在了很多版本号里：
 - “设置房间只接收主持人”应为“使房间受到管理”（开幕模式，启用公开发言权管理）

- “允许访客发送声音请求”应为“允许旁听者按键请求授予公开发言权”

“Prosody IM”是插件式的，由服务器管理员决定安装哪些功能组件，所以很难猜测某个它搭建的服务器的功能设计到底如何。因为许多公共服务器的运营者在服务器运行起来后就不再多精心调整配置功能了，所以被配置得功能丰富的公共服务器很少，它的群聊服务器的房间的功能设置常常选项不多，缺乏必要的防垃圾信息的功能选项，不适合创建使用敞门会议室。这是我们抛弃它的一个重要原因。更严重的原因是它移除了高级屏蔽名单功能，这直接导致了它的用户服务器不适合用来从事政治活动，不该在上面注册用于一般交流用途的虚拟身份。也就是说，它只适合用来提供锁门的会议室。如果你要带两百个以上的活跃XMPP用户加入一个锁门会议室，你可以考虑使用它，它运行的公共服务器很可能不会限制座位数；其它用途就算了。

“Mêtronôme IM”是“Prosody IM”的改版，它们有所相像。

你在“专业房主说明”章节可以看到，如果要隐藏旁听的在场状态的话，那么你可能就需要会议室能够不设最大座位数限制了，因为你无法通过在场列表获得它们的地址，因此你无法对多到致使会议室将要满场的人进行封禁（以腾出更多座位给更多愿意活跃参与的人们）。面对这种情况，Openfire和Tigase可以帮到你。

公共服务器列表网站

要自己寻找公共XMPP服务器地址的话，可行的做法例如：打开你的网页浏览器，使用英文搜索引擎搜索“(free) (public) XMPP servers (list) (for everyone)”之类的关键词。注意你需要的是公共服务器地址而不是搭建服务器的软件（许多英语文章将“server softwares”简称为“server”）。如果你不懂外语，那么最好让其它同志帮忙。也可以让其它同志推荐服务器。甚至可以直接要一对XMPP身份标识和密码来登录。

除了专门检测服务器是否在运行的网站以外，仅收录服务器地址的网站不保证及时把停止运营的服务器地址删除。

我们在此例出一些收录XMPP服务器的网站地址。

“<https://providers.xmpp.net/>”：

- 这里提供了一些服务器地址并作了评级，由好到差为从A到D。
- 虽然它是XMPP官方网站提供的列表，但这种评价对我们这种专门从事政治活动的用户而言参考意义不大。
- 点击导航栏里的“Overview”按钮可以纵览它们的特性并按照你想要的条件来排序。

“<https://xmpp-servers.404.city/>”：

- 这里提供一些服务器地址。这个网站反对“<https://providers.xmpp.net/>”的偏见，并不特别推荐任何服务器地址，尝试不对它们作分类和评价。
- “Satellites”意为“同一个服务器的不同域名”，意思是说那些服务器地址都属于同一个服务方，或者甚至同一个实体服务器（也就是说，有相同的服务器功能配置，有相同的公共运行资源占用率）。
- 这个网页不是活跃更新的，一些下线已久的服务器地址没有被删除。

“<https://www.freie-messenger.de/en/xmpp/server/>”：

- 你可以在这里找到一些公共服务器，连带它们的属性。
- 这个网站的原生语言是德语，不保证其它的语言有良好的翻译。
- 如果整个表格的宽度超出了你的屏幕显示宽度，请调小网页浏览器显示内容的缩放率。

“<https://the-federation.info/protocol/20/>”：

- 你可以在这里找到一些公共服务器，它的列表展示那些公共服务器是否开放注册，以及它们属于哪个国度，其服务器软件是什么。
- 虽然表格的“Name”列大多数都是域名，但一些是服务器名字，你需要点击才能看到其域名。
- 它并不是个专门为XMPP用户服务的网站。
- 它列表里的Prosody服务器好多啊……

“<https://list.jabber.at/>”：

- 这里提供一些公共服务器地址，连带一些服务器直接的注册入口链接和服务策略链接。
- 有的服务器已经下线很久了都没有被删除地址，看起来这个网站的更新不活跃。
- 有些域名属于同一个服务器，但是并没有归类。

“<https://jabberworld.info/servers/>”：

- 这个列表只是检测一些服务器信息使用，而非专门给新人推荐的公共服务器列表。很多地址都是不能用的。
- 似乎只有服务器软件及其版本号、在线时间记录这两条信息是准确的，请不要直接参考其它参数。新用户可以用网页内搜索的方式来查看一个公共服务器的服务器软件是什么（请将较长的服务器地址截取前面的部分）。将鼠标光标放到服务器软件图标上可以查看版本号。（它对Ejabberd服务器用Ejabberd的老徽标而非新徽标。）
- 红底色的行是已经停止运行的历史服务器。也可能是在检测的时候服务器恰好临时掉线。留意网页底部的列表更新时间，只要它没有太久不更新，就有参考价值。

“<https://compliance.conversations.im/old/>”：

- 它不是专门给新人推荐的公共服务器列表。
- 这里检测一些服务器的功能标准运行状况，作为列表显示出来。它不会频繁到每天检测，只能反映大概可能的情况。
- 它的检测并不是十分准确，要具体了解，还是得注册对应的服务器并测试功能。
- 点击导航栏里的“Servers”按钮可以输入服务器地址来检测，但它不会任意收录服务器地址的检测记录。

“<https://xmpp.love/>”：

- 它有随机列出服务器地址的设计，然而它并不是专门给新人推荐的公共服务器列表。
- 点击该网站网页底部的“Next”按钮以请求再随机列出一些。
- 这里提供一些参考信息，“INBAND”（In-Band Registration）意为允许从用户端软件注册。
- 准确吗？不一定。应该把它当成是给一些闲得没事做的用户随便访问网址闲逛互联网（看看有什么穷乡僻壤的网站和XMPP服务器）用的。

连接状况检查

这个网站可以帮助你按照地址检查公共服务器的连接情况：“<https://connect.xmpp.net>”

/'。

也可以在一个正常的服务器上登录上线，并按照地址查询其它公共服务器的内容，看是否有正确的回应。

查询服务器的服务项

登录一个XMPP身份，就可以按照地址查询各个公共服务器的服务项。这种做法主要用来查询群聊服务器上的露天会议室。

只要那些服务项的地址作出了正确的回应（在用户端软件查找结果中不被打叉），那么就是正常可用的。但是，对待来自不同服务器的用户的查询时，公共服务器只有群聊服务器地址保证作出回应。像是寄存服务地址就不一定对不同服务器的用户作出回应了。要确认那个服务器的其它服务项是否能用，就应该用被查询服务器自家的XMPP身份再查询一次。

对服务器地址可以查询它的软件名称及版本号。要注意的是，服务器的软件版本号不一定是正式发布版本的版本号，它可能有多余的后缀，或者是随机数，这通常意味着它是更细化的版本号，它可能更新得很频繁（也许两到四个星期就掉线更新一次）。

功能实现

大多功能的实现需要服务器和用户端软件都支持才可以。

服务器可以选择提供哪些功能。公共服务器基本不会被刻意设计得功能异常。

由于XMPP的功能都是组件式拼装起来的。因此，特别核心的，主要的功能很容易普及；而那些次要的功能，甚至不符合标准的功能，就不是所有的用户端软件支持的了。依赖没能普及的功能和不符合标准的功能会无法和其它用户正常交流，甚至会造成妨碍，用户应当考虑这一点。

它的规则是稳定的。因此某个服务器软件更新或某个用户端软件停止更新都不会严重影响使用；参考资料文件也较久有效适用。

服务策略

不同的公共服务器有不同的服务策略，它能影响很多事情。通常，你能在服务器的官方网站上看到它们，不过很多公共服务器并不会仔细考虑并公布太多的细节。以下是示例。

影响重要的

- 文字消息存档期限或条数。
- 寄存的单文件体积限制、总文件体积限制、存档期限。
- 是否设多复杂的注册验证码以阻止被网络攻击者滥用注册。
- 注册是否要电子邮箱地址。
- 是否有网站。（有的公共服务器根本不设网站。）
- 服务器是否已经满载，因此不再接收新用户。（允许寄存的文件体积越大，服务器就越容易不堪重负。）
- 是否和被滥用（过）的服务器联系。
- 群聊服务器提供哪些房间设置选项，这种不同尤其见于插件式的服务器软件上，不同服务器的差别有可能不小。

常见且基本不会限制到普通用户的

- 离线时待接收消息存档条数上限。
- 每天允许发送的消息条数（一般特别多，能达到这一限制的大多是广泛发布垃圾信息的机器程序）。
- 单用户最多同时登录的端数。
- 是否有防垃圾设计（例如拒绝传递用户的非联系人消息。如果对室内私信有干扰交流的防垃圾设置，请考虑相互添加联系人）。

- 是否允许手动注销，以及未登录自动注销的期限。
- 第一次登录时的欢迎消息或提醒消息（基本是服务器本地的语言）；创建会议室时的提示消息；服务策略变更通知以及临时下线维护更新的通知（少见）；让新注册的用户走个敷衍的法律流程（少见）。
- 是否有供本服务器的用户交流的总会议室，以及是否第一次登录后自动加入。
- 消息传递失败时的反馈错误信息描述。
- 支持哪些功能标准。
- 是否强制用户使用TLS加密连接，以及强制使用哪个版本的TLS。
- 是否和TLS加密有问题的服务器联系。

不常见的

- 有的服务器不提供群聊服务，有的服务器只提供群聊服务（不提供XMPP身份）。
- 不和其它公共服务器联系。（专用服务器可能很多，但毕竟人们很少会介绍这些不能随意使用的给公众。）
- 自动注销不保存任何联系地址的XMPP身份。
- 首次发消息以及请求共享在线状态时，要求访问网址处理验证码。（对新手不友好。）
- 注销后封存号码一段时间。
- 使用邀请注册制以防止被滥用式地大量注册。

异常服务器

有的服务器网站有模有样，但它连同XMPP服务器都已经停止维护。它们的XMPP服务器可能还能用，但TLS问题会导致一些用户端软件限制使用它，其它公共服务器也可能会拒绝和TLS有问题的服务器连接。

有的服务器看似运作良好，TLS加密证书也没有过期，但是它们的管理员确实把它们丢在一边置之不理了。这种服务器一般是没有名气的，如果你让这个服务器出名了，它就可能会因为用户数量太多以及对网络攻击的防御配置不够好而瘫痪，直到服务器管理员发现并着手处理这个情况。

有的服务器的确可能一时出现严重的问题，不能正常使用。如果你在用正确的密码尝试登录时服务器反馈“未被授权”，那么你可以怀疑是服务器出现了问题，而不是你的错。

有的服务器为了防止大量注册的滥用行为，而限制了服务器每单位时间允许的注册量，这实际上不是好做法。

有的服务器保留着直接注册功能，而这个功能是坏的。给注册表单，但提交表单无法通过。

如果怀疑自己试图出去的加密消息没有发送成功，请记得用无主动加密的消息来测试，看看有没有反馈错误信息。

有的服务器只允许在网站注册，但却是注册其它服务才一并注册XMPP。我们希望用户专注于学习XMPP，所以在这里不建议涉足杂七杂八的服务。

有的服务器的服务策略明确地拒绝激进政治活动。

非普通互联网的服务器地址

可能你会发现一些服务器地址以“.onion”、“.i2p”结尾。它们不是普通互联网的。这涉及更多的原生问题和更多复杂的衍生问题，本说明书决定不作介绍，也不建议普通用户去接触它们。

使用这些服务器地址需要用有这种后缀的XMPP用户地址。如果你试图用普通互联网的XMPP用户地址发送消息给这种特殊地址，具体结果决定于你的服务器的配置是否考虑了这种东西，是否支持这种东西。大多公共服务器不考虑这种东西。

垃圾信息问题

垃圾信息问题是这种和政治身份无关的互联网平台必然存在的问题。你可能会收到你完全不需要的各种各样的垃圾信息：非联系人发来的商业广告；对我们这种从事政治活动的人而言，敌人的文字消息骚扰和电话骚扰可能更多。

如果你收到了垃圾信息，这说明那些发送垃圾信息的人已经获知了你的XMPP用户地址。面对这种情况，最好的办法是启用高级屏蔽名单功能。如果你的服务器不支持此功能，那么你将处于被动局面，那么你应该后悔选择了这个服务器，并更换一个公共服务器注册使用。

服务器的以下要素可以减小用户收到垃圾信息的可能性：

- 服务器拒绝为自己的用户传递来自非联系人的消息、音视频电话请求。（不过服务器可能只拒绝传递不同服务器的。）若想正常交流，就需要相互添加为联系人，且收信方将在线状态成功共享给了发信方。（如果你善用高级屏蔽名单功能，那么这一点可以忽略。）
- 服务器拒绝和TLS加密证书过期的服务器联系。（TLS加密证书过期通常意味着服务器缺乏监管，也就很有可能大量用来捣蛋的XMPP身份。）
- 服务器针对被滥用的公共服务器有屏蔽名单。不过常常很难做到发现被屏蔽的服务器恢复正常并解除对它的屏蔽。

大量地将想要屏蔽的地址添加到屏蔽名单内属于下策。对我们这种从事政治活动的用户而言更是如此。

如果你执意要使用不支持高级屏蔽名单的用户服务器，你想寻找有防垃圾信息设计的服务器，那么应该优先试试那些有精心设计的网站的，甚至向注册者要电子邮箱地址的公共服务器。通常它们对服务器更可能配置得拒收非联系人消息。

防垃圾信息设计可能会误伤室内私信（例如同时包含两条网页链接的消息），不过服务器会明确表示拒收。

XMPP的用户越多，必然导致公共服务器们更多地要求用户们通过网站注册并配置复杂验证码。这是理所应当的，毋庸置疑的。而且，这种做法是可以抑制进行垃圾信息攻击的用户的，不能说“别的公共服务器不阻止滥用注册，我也就没必要滥用过量注册了。”。

实时屏蔽名单

XMPP社区有一种叫作“实时屏蔽名单（Real-Time Block List, RTBL）”的东西，它们会实时地添加一些让人们不满意的虚拟用户的XMPP地址（一般是倒垃圾信息的虚拟用户）进去，供房主们甚至服务器管理员们自愿使用。

有些公共服务器提供公用的辅助用机器程序号码。如果要使用，只需邀请它到自己管理的会议室，并授予管家资格。要注意的是：

- 它们大多都不公布有哪些XMPP地址在名单里，原因便是其中会包含不良信息。同时它也会因此而无法让公众看到是否有误伤和不公正的封禁。
- 它无法阻止刚刚注册登录后第一次来倒垃圾信息的敌人。
- 如果会议室真的有哪个信任的人喜欢到处撒野，它也会有误伤的可能性。甚至，正常用户可能会因“遭到捣蛋鬼举报+败官判决”而被加入到名单里。
- 只要它不是你的，那么它的规则就基本是别人定的。它设计得好不好，决定于别人。例如，如果设计得不好，那么就可能有此情景：当你因为它误伤严重而想移除它时，却无法给它下命令让它撤销它执行的所有错误操作。
- 它是资本主义自由化的，没有严格且统一的规则。只要是开放公共使用的，那么无论是谁定制规则还是谁在用，都很难让大多数人满意。如果有多种列表，那么了解不同列表的规则也是很费劲的事情。只有限制使用范围，在某一领域专门设计使用时才能达到更理想的效

果。

- 它也可能会有明确的服务策略，因为它也是对公共服务器资源的占用形式。

如果某一整个公共服务器应用实时屏蔽名单的话，那么它的不确定性就更大，尤其是对我们这种从事政治活动的人们而言。这种公共服务器将不那么适合用于稳定通讯。

介绍邀请制

介绍邀请制是一种很好的方法。它可以防止不怀好意的陌生人干扰。拉帮结党的时候可以用介绍邀请制，有熟人介绍，这会增加初始的信任度，减少筛查工作量，省心省力。

有的服务器使用介绍邀请制（这里不是说那种程序功能），这种服务器不能随意注册，但也不会产生倒垃圾信息的用户。这种服务器的组建方会有较强的组织性，甚至会对新注册用户有政治审查。

如果只是个人搭建的公共服务器的话，那么大多就只是注册者自我介绍，服务器管理员处理不了多少邀请，更不会在意你的意识形态。联系服务器管理员，告诉它你想注册的XMPP身份号码，它就会为你开放一次注册。不要刻意去打探服务器管理员的好恶，用就是了。

筛选适合革命使用的服务器的步骤

如果你只想当无名小卒，不想当活动家，更不想当革命家，那么你随便找一个能注册登录的服务器就可以。

至于找适合革命使用的服务器，那就不简单。新手直接使用信任的同志已经筛选过的，为你推荐的服务器的地址就好。参考附录。

1. 先拿到许多服务器地址，优先从为新手推荐服务器的网站摘录。不要去那些检测站随意摘录服务器地址。
2. 筛除Prosody服务器，因为它不支持XEP-0016。
3. 筛除已经停运的服务器。
4. 筛除软件版本太老的服务器。（不会判断的话，可以忽略这一点。）
5. 筛除完全不允许注册的服务器。
6. 测试注册。是否受互联网封锁，是否能直接连接，这完全不是考虑因素！在受互联网封锁的环境中请使用代理网络连接进行测试。
7. 能在用户端软件直接注册吗？如果可以，那么更适合不懂外语的新手。
8. 注册的验证码是不是包含外语？如果包含外语，那就不要推荐注册了。
9. 注册是不是要电子邮箱？如果要，那就不要推荐（很可能不懂电子邮箱的）新手注册了。
10. 留意TLS证书是否过期或不受信任。
11. 检查允许寄存的文件体积，不宜太大，越大越不稳定。
12. 查找服务，看看其它服务项（群聊房间、寄存文件）是否有效。
13. 它的网站是不是有模有样的？是不是积极和用户对话的？是不是积极更新的？如果是，那么更可能是维护良好且长期运行的公共服务器，也就是适合用来公开发言和活动的公共服务器。
14. 留意服务方的服务策略及其变动。同时无视所有的“请遵守道德和法律”的套话。
15. 对新手而言，服务方最好专注于XMPP，而不要把一些其它的服务或分享内容放在首位。
16. 如果一个服务方有多个服务器地址，那么只选一个就好，不要重复推荐给别人。

注册和登录时可能出现的问题

如果你的注册直接成功了，可以直接跳过这一章阅读。

未找到服务器

你所输入的地址所对应的服务器没有上线或不在线，或者它确实存在而且运行正常，但你的设备和用户端软件所处的互联网环境没能找到它。

如果某个服务器曾经存在，但是下线了，那么其上的所有XMPP身份和会议室都将无法访问。若要访问，只能的等待服务器再次上线。

试试使用通用代理网络连接访问服务器，或者换一个服务器（注册并）登录。

连接服务器花费时间太长

使用代理网络连接。或者换一个服务器地址注册使用。

违反服务策略

如果注册前没有连接过服务器的话……可能你索要的XMPP身份号码是不是包含不被允许的词汇？例如对服务器管理员有冒充的可能性的词汇？

服务器暂停接受注册时也会这么显示。可以去它的网站看看有什么通知。

登录时出现这种情况，基本是因为自己执行了过多的异常操作请求，被服务器视为网络攻击而被禁止了。例如连续多次使用错误的密码试图登录。一种可能的原因是：你有多个同时在线的登录点，你在其中一个登录点向服务器请求修改了密码，但没有先让其它登录点下线，因此其它登录点的用户端软件在多次或者甚至不断地尝试用错误的密码发送登录请求。有的服务方提供多个服务器地址，这些服务器的屏蔽记录可能是一样的。你可以等几个小时，半天，或一天，也许更久，看看服务器有没有原谅你。

“用户名不合规”

遇到这种问题时，许多新手并不是刻意地想往XMPP身份号码填写栏输入不允许的字符（例如空格、大写英文字母），而是误把此填写栏当成了XMPP地址填写栏，因此输入了不允许的字符“@”。

未授权/“号码和密码不匹配”

可能提交的用户身份标识和密码同服务器上的记录不匹配。可能是XMPP身份号码不对，也可能是密码不对，服务器地址输入错误也是有很小的可能的。

- 如果是用户身份号码不对，那就是说服务器上没有记录这个用户身份号码。可以是这个身份号码没有被注册，也可以是曾经被注册过，但是被注销删除了。检查用户身份号码，不要输入错误。
- 如果是密码不对。检查密码，不要输入错误。如果确定用户身份号码已经被注册了，且密码是正确的，那么就可能是别人窃取了密码，并登录后修改了密码或注销了。如果服务器在注册时提供了填写电子邮箱的选项，且你填写并提交了电子邮箱地址，那么你可以试着去网页端访问服务器，请求重置密码。

如果你丢失了密码，无法登录，也不能通过电子邮箱来重置密码的话，那么你的这个XMPP身份号码就彻底不可用了，你只能等待它因为太久没有上线而被服务器自动删除，才可以再注册这个身份号码。如果你忘记了你的XMPP身份号码或服务器地址，结果也是一样。

也可能是因为你还有额外的注册步骤。例如如果服务器要求提交并验证电子邮箱，而你只是提交了电子邮箱地址，却没有验证，那么你的XMPP身份无效就是当然的。

当你连续尝试注销，第二次时这么显示，就意味着已经注销成功了。

服务器产生异常也会导致这种情况。

网页端注册的验证码问题

有些服务器依赖第三方的验证码组件，你能访问这个网址并不意味着你能也访问（这个网站引入的）来自其它网址的内容。在网页端注册时，请留意网页的加载状态，如果长时间没有完全加载完毕，那么可能丢失了注册过程必需的验证码组件。此时你应该使用代理网络连接。

使用中可能出现的问题

未主动加密的消息发送失败

未主动加密的消息发送失败后会有反馈信息（可能是外语），助你排查技术原因。不同服务器软件及版本的反馈信息的描述可能会不同，尤其是在服务器有自定义功能设计的情况下。为了减小篇幅，以及照顾不懂外语的新手，此处告诉你一些高准确率快速排查的办法——检查反馈错误信息的关键词。具体实例详解请见附录。

“**DNS**”或“**domain**”：添加的联系地址中，服务器地址错误。

“**timeout**”：同上。

“**connection refused**”：同上。

“**connection closed**”：对面服务器坏了。

“**certificate**”：收信服务器因你用的服务器的TLS证书有问题而拒绝联系。

“**policy**”：你用的服务器拒绝和收信服务器联系。很可能对方服务器被滥用过。

“**strangers**”：收信服务器拒收非联系人消息。只有对方请求并获取了你共享的在线状态后你才可以成功发送。

“**privacy list**”：你的高级屏蔽名单没有允许和这个地址通信。

“**service unavailable**”：目标收信用户不存在，或者它的黑名单或白名单没有允许和你通信。

“**offline message**”：收信人离线时的未接收消息数满了，存不下更多了，得等它上线。

无法发送加密消息

无法发送加密消息的可能性包括所有未主动加密的消息发送失败的可能性。如果你的收信用户地址不正确，那么连同未加密消息也会无法发送。请先试试未主动加密的消息能否被发送，如果也发送失败，检查反馈给你的出错信息，然后参考“未主动加密的消息发送失败”条。

如果纯服务器地址（不含“@”字符）给你发送了消息，那么就会有和服务器的对话选项及其对话界面。它不是一个真正的XMPP用户地址，无法获取对方的加密所需凭证，也就无法给它发送主动加密的消息。

无论发送什么类型的加密信息（全手动加密除外），都需要自己的客户端软件和双方服务器都支持才可以。有其中一条因素不支持，就会导致无法发送加密消息。

如果还是有问题，检查你所使用的服务器的功能状况，看看服务器是否支持XEP-0060和XEP-0163（必须）；XEP-0384（OMEMO）；XEP-374（OpenPGP）、XEP-0378（OTR）。

关于OMEMO的更具体原因，请查看附录的OMEMO章节。

找不到远程服务器

这个服务器不存在，或没有上线，或你的服务器连接不上对面的服务器。也可能是你输入了一个错误的服务器地址。

“远程服务器超时（未作出正确的响应）”

请求已成功发出，但较长时间没有收到正确的回应。这个服务器存在，但它可能不是一个XMPP服务器（检查你添加的联系地址是否有误），也可能是个配置损坏的服务器，也可能是个拒绝和你用的服务器连接的服务器。

被强调的未加密信息

有的未主动加密的消息在对话界面会被强调“未加密”。这并不是说连被动加密都没有，而

是由双方发送的消息的主动加密状态决定的。如果双方都使用主动加密，或都不使用主动加密，那么就不会强调。如果一方发送主动加密的信息，另一方发送没有主动加密的信息，那么未加密的信息的收信方的界面里就会强调对方的消息没有加密。这属于用户端软件的设计。

信息送达的延迟时间较长

可能是因为你和服务器的连接不稳定。试试切换你的网络环境。

如果确定你和你用的服务器连接一切正常，那么原因就是你用的服务器和目标收信服务器的连接速度慢了，这是使用代理网络连接也无益的，普通用户能尝试的唯一办法只有更换服务器。

在使用无线网络连接时进入存在信号干扰环境中的话也会出现这一情况。此时要么拆除信号干扰源，要么离开信号干扰范围。

消息一直处于“正在发送”或“等待发送”的状态

首先确保你和你用的服务器的连接状态是正常的，确保互联网连接稳定，确保你处于“在线”状态。曾经有身处存在人为干扰信号的无线网络环境的用户报告过此情况。

在此之上问题还在的话，那么可能是目标收信服务器的服务策略拒绝和你用的服务器通信，但目标收信服务器在操作上只是忽视，而不明确地拒绝收信。此时对方试图给自己发信的话会有对应的反馈错误信息。面对这种情况时，解决办法是更换一个公共服务器来联系对方。（有的用户端软件在建立对话项前先尝试对方服务器的连接，连接成功后才建立对话项，可以避免遇到这种情况。）

下载文件速度慢

你可以复制对应的下载链接，到网页浏览器里访问来下载（主动加密文件除外），也可以使用多线程下载工具来下载，也可以使用代理网络连接。

看不到其它用户的虚拟肖像

这和挺多因素有关的：

- 其它用户必须设置了虚拟肖像。
- 需要服务器支持。（一般没问题。）
- 需要用户端软件支持获取并显示虚拟肖像。（一般没问题。）
- 其它用户的XMPP地址是否明确也是个重要的影响因素。如果是在大桌会议室里，那么此会议室应当允许人员查询别人的电子名片。
- 其它用户使用的图像格式不被用户端软件支持。

服务器的相互连接问题

除了下载寄存的文件是用户和目标服务器直接连接以外，剩下的文字信息全部由你使用的服务器当邮递员来传递。登录成功后，只要添加的联系地址存在且正确，目标服务器也在线，如果还是无法成功连接目标服务器的会议室或用户，那么可能性如下：

- 目标服务器的服务策略拒绝连接你用的服务器。（可能的原因例如：你的服务器曾经被从事网络攻击的人们滥用，被目标服务器列入了通信黑名单。）
- 你的服务器或目标服务器所在的国家存在互联网封锁。
- 你的服务器或目标服务器按照服务策略本来就不和其它服务器联系，只为属于自己的用户服务。

用户无法解决这种问题，只能更换一个服务器使用，看看能不能连接到目标服务器。

特别的“被盗号”情况

当一位虚拟用户注销了自己的身份号码后，很快就有另一个人注册并登录了这个号码。这时就出现了XMPP身份换人的情况，且原主人和新主人都不知道发生了什么。新主人可能因为原主

人的虚拟身份号码被原主人的联系人们记录了，而在自己的对话选项界面刚注册登录就会出现联系人选项。如果不想这种尴尬的事情发生，考虑不主动在服务器上注销身份号码。服务器们通常会自动注销过了半年一年太久没有登录的身份号码。

还有一种情况。会议室的用户地址都是临时的，和显示名称有关。你和甲用会议室的临时私聊通道聊了一会儿，后来甲主动离开了会议室或下线了，因此甲的群内显示名称不再被占用，允许它人使用。乙在会议室里把显示名称改为甲之前和你交流用的名字，并给你发送消息，那么你以为和你说话的是甲，实际上和你说话的是乙。如果你可以看到不同的虚拟肖像，那么你自然能直接察觉到异常。

特别的“走错门”情况

你按照互联网上别人分享介绍的会议室地址加入了一个会议室，但是里面的人员、内容、氛围，都跟引路的网友介绍的不同。这很可能是因为你所读到的地址分享条文是多年前发布的了，而在此期间，这个会议室地址的人们解散了，并有了另一队人们又注册了这个会议室门牌号，占用了这个地址。当然了，会议室不拆，但里面的人都已经换了一遍，都不知道那个分享者当时分享会议室地址时的初衷，也会有类似的效果。门是没有走错的，但是人见错了。

加入会议室时看不到消息和会议室公告板

你的高级屏蔽名单启用了宽松屏蔽模式，没有允许和这个群聊服务器通信。

我忘记了我的登录密码

如果现在你还有已经记录了密码的，可以直接登录的客户端软件：

- 也许你的客户端软件修改密码操作的设计不要求用户输入当前登录密码，你可以在登录后直接向服务器请求修改登录密码。
- 也许你可以方便地找到你的客户端软件明文存储的密码，但这样做的客户端软件太傻了，任何一个设计正常的客户端软件都不会明文存储密码。

如果你的服务器网站提供预留电子邮箱地址用来在忘记密码时恢复XMPP号码的功能，且你预留了电子邮箱地址，那么你可以通过它来修改密码。

没有其它方法了。因忘记登录密码而遭到恶果向来是活该的事情。忘记密码意味着你没有认真对待学习和使用XMPP的事宜，这会降低人们对你的信任。

翻译问题

这个问题在资本主义开源界几乎是无人不知。即使这样，还是很严重。小心错误翻译！

例如：“Idle Time”（挂机时间点）中“Idle”（“空闲”）的修饰对象是机器，而不是用户。它的意思是机器的最后被操作时间，而不是用户开始空闲的时间。

有些翻译吓到了一些XMPP用户，因此产生了典型的XMPP笑话：

- “错误：违反政策”（错误：违反了服务器的服务策略）
- “错误：用户名不合法”（错误：所填写的XMPP身份号码的格式不合XMPP规定）
- 谣言的产生过程：“某人的XMPP地址暴露了！”（事实）→“某XMPP用户的地址暴露了！”（歧义）→“某XMPP用户被定位了！”（谣言）

怎么办？要么就怪这些用户不读说明书、没见识；要么怪这些用户太胆小（因此有被害妄想症，夸大危险性）；要么就怪翻译者和转述者。

高级屏蔽名单（过滤规则列表）

个人防火墙。主要用来屏蔽陌生人的联系请求。（如果你使用的服务器有自己的防垃圾信息设计，那么服务器的决定优先。）功能标准编号是“XEP-0016”。推荐的客户端软件中对此功能有良好支持的客户端软件只有Psi(+).

基础设计

- 由用户编辑，可以有多张，至少要有一张。
- 必须有一张被设置为默认启用项，每一个登录点在上线时都会应用它。各登录点可以设置自己的使用项，如果不支持此功能，就会用默认使用项。
- 每张高级屏蔽名单包含至少一条通信过滤规则。
- 服务器可能会给你安排一个名称固定的高级屏蔽名单，在你把它更改名称后还是会再出现一个这个名称的名单。
- 你可以新建一张高级屏蔽名单，但是根本不启用，不让它产生任何效用，把它当成一个让服务器为你存储的纯地址簿来作记录和查阅。（但是客户端软件不一定给你设计方便搜索条目和排序条目的功能。）

每条通信过滤规则都有四个组成因素：筛选类别、筛选参数、应对决策、过滤项：

- 筛选类别包含四种，择一：地址（XMPP身份标识或服务器地址）、组别（联系人分组）、在线状态共享情况、其余全部（尚未决定如何处理的通信）。
- 关于筛选参数：
 - 筛选类别“地址”和“组别”的筛选参数由用户自由填写，每条规则填一项；
 - “在线状态共享情况”有四种，择一：双方皆成功共享、只有己方成功分享在线状态给对方、只有对方成功分享在线状态给己方、无（双方皆未成功共享）。
 - “其余全部”没有筛选参数。
- 应对决策有两种：允许通信、拒绝通信。
- 过滤项有四种，至少要选择一项：消息、元数据请求、传出状态、传入状态。

对公共服务器而言：和某个地址联系时，如果列表里的规则没有决定允许或拒绝，则被视为允许通信；如果对某个条目选择“应对决策”为“允许”但过滤项不是全部的话，实际上结果等于允许和此条目的全部通信。

过滤规则是将条目排序作为优先级顺序决定做法的。如果和某个地址的通信已经被前面的规则决定允许或拒绝了，那么后面的规则对它就毫无影响。

拒绝过滤项“消息”会同步使别人的音视频通话和加入会议室的邀请无效化。

黑名单的基础

XEP-0016（高级屏蔽名单）是基于XEP-0191（屏蔽名单）的。如果不手动调整高级屏蔽名单，那么它就只会发挥黑名单的作用。所有在黑名单内的项目也会在高级屏蔽名单内作为一条被拒绝所有通信的项目。

具体应用

如果你想在XMPP平台当一个名人，例如一个有名的领袖，那么你就一定会需要此功能。在实际应用中把它当白名单功能使用时，首先要有的条目是：

- 允许来自你自己的用户XMPP地址的所有通信，以正常使用自己给自己发送消息的功能。
- 查找自己用的服务器的服务项，允许来自所有服务项的地址的所有通信，至少要包括群聊服务器地址和文件寄存服务器地址。（允许和群聊服务器地址通信是没有问题的，邀请加入会议室的通知消息来源于用户地址，而非群聊地址，所以会议室不会于你不在场的时候主动

打扰你。)

- 要加入某个群聊，就允许和对应的群聊服务器地址的所有通信。

在这些设置的基础之上，当白名单使用有两种模式：

- 一种水火不侵，刀枪不入的模式，我们管它叫“严格屏蔽模式”。这种模式下不会收到陌生人的消息和它们添加联系人的请求，自己发送添加联系人的请求时也会受阻。在实际应用中，专门用来管理大型会议室，平时不和陌生人交流，用于非常有名气的人。
- 一种只屏蔽陌生人消息的模式，我们管它叫“宽松屏蔽模式”。这种模式下可以相互添加联系人并共享在线状态，但只有在此之后才能接收对方的消息。在实际应用中，只是用于一般防垃圾信息。如果用户变得出名了，光是收到的大量添加联系人的请求就已经造成了不小的打扰的话，那么还是得用严格屏蔽模式。

如果要用宽松屏蔽模式，那么就在名单最后添加一个对没有共享在线状态的地址只拒绝消息的过滤规则。（不要添加到前面，因为你和会议室们是根本不会有共享在线状态的，这么做会拒绝和会议室通信。）

如果要改成严格屏蔽模式，那么就把屏蔽其它通信的那条规则的过滤项改为全部^①。

①『要屏蔽添加联系人的请求的话，必须同时拒绝“元数据请求”、“传出状态”、“传入状态”三项。如果你不想你的联系人看到你的在线状态和登录点信息，那么你可以对联系人拒绝“传出状态”和“传入状态”，但你要承担联系人误认为你的XMPP身份已被废弃而因此删除联系方式的可能性。拒绝“元数据请求”过滤项的同时会阻止你查询其它服务器的服务项和它的旧版电子名片。』

在使用严格屏蔽模式时，为了方便添加联系人，就要专门设置一个允许通信的联系人分组，添加联系人时放到这个分组里。如果对方也用严格屏蔽模式，那么对方也需要这么做。

你不应该将非XMPP用户的地址添加到联系人分组里。要允许和群聊服务器地址通信，就得在高级屏蔽名单里填写那些地址。如果你的活动范围跨很多群聊服务器，那么会使得高级屏蔽名单长一点，但这是值得的。

不要和用户服务器地址允许通信，因为这么做等于允许和那个服务器的所有用户通信。只有在你相信那一整个服务器都没人会骚扰你的情况下才能这么做。

宽松屏蔽模式配置示例

说明	筛选类别	筛选参数	应对决策	过滤项
别把自己给堵死了	地址	我自己的XMPP地址	允许	全部
	地址	我所属的服务器的群聊服务地址	允许	全部
	地址	我所属的服务器的文件寄存服务地址	允许	全部
不屏蔽群聊服务器	地址	群聊服务器地址1	允许	全部
	地址	群聊服务器地址2	允许	全部
	地址	群聊服务器地址3	允许	全部
允许通信的分组	组别	为严格屏蔽模式准备的分组的名称	允许	全部
屏蔽其它	在线状态共享情况	无	拒绝	消息

专业房主说明

锁门会议室

锁门会议室很好管理。如果不使用OMEMO加密，那么新手房主也能很好掌控。使用OMEMO加密时就需要有了解OMEMO的房主作撑场面的技术员。

如果成员们相互信任，那么就用小桌；否则就用大桌。

如果成员们相互信任，那么还可以允许会员直接执行邀请操作；否则就要求先向房主和管家介绍，经过允许。

如果成员们组织性不强，那么就不要再改成敞门了，要用敞门会议室就应该另建一个新的。

只要成员们组织性强，那么它就是最适合革命派的交流区，也是用来干地下工作的不二之选。

想省心？创建会议室并调整设置为锁门+大桌，只带认识的人进去，这不会让你失望的。如果你管理敞门会议室累了，也请随时记得改成锁门会议室。

一般兴趣爱好交流的敞门会议室

用于缺乏组织性，缺乏纪律性，立场不明确，信仰不坚定，明天不确定，只要遵守不多的规则就给别人公开发言权的会议室。例如把革命派、口头“革命派”、改良派混在一起的左派会议室。（甚至还会有泥潭派，加上一些不务正业只是来测试自己能否通过审核且通过了的人。）那么，只有些普遍的规则和会议室配置要说。

人们相互的信任不足，或者大多不擅长用XMPP的情况下——用大桌。

如果想让会议室被尽可能多的人知道，那么就要设置为露天。甚至还要考虑第三方公共搜索引擎的收录条件。

一般应当对室外公开在场人员数量和室内网名。这样，室外人员可以猜测室内是否活跃，它们也可以判断会议室是不是废置的空会议室。室外人员跑到一些被废弃的空会议室会重置空会议室的自动删除计时，让它们感到尴尬；如果跑到隐藏全部人员在场状态的会议室，那么遭遇就更难确定。

在会议室里会有这样的常见规则，即使它们不一定要在会议室里成文地说明：

- 禁止外语、禁止无关的商业广告、禁止超长的文字信息、禁止倒垃圾信息。
- 禁止非标准汉语、禁止暗语。
- 禁止人工智障（“AI”，Artificial Idiot）机器程序。
- 禁止冒充其它人。
- 不要频繁修改室内网名和虚拟肖像。
- 当会议室座位快达到服务器规定的上限的时候，长期空占位置不积极参与互动的人要被封禁。除非房主和管家确实喜欢有这种人占着位置保持满场状态来防止会议室里活跃的人太多，因而看不过来数量过多的消息。
- 不要带偏话题，尤其是在房间创建的目的本来就是专门讨论某个话题的情况下。如果一群人熟悉起来了，关系好了，难以避免地想讨论各种其它的话题，那么一起创建或加入另一个专门服务其它话题的会议室是个好办法。
- 在多人同时讨论一个话题时，甚至仅仅是在只有两个人交流的声音时（因为有别人中途加入讨论的可能性），明确地指明每条消息是发给谁的，以防止阅读理解发生串线。越是认真地辩论，就越是应该如此。
- 如果你所在的会议室被管理得很好，没有臭虫活跃，你喜欢这个会议室；那么，就给任职的房主、管家、主持更多一点的尊重。

- “给你公开发言权并不是主持的政治义务。”，用来讲道理地拒绝捣蛋鬼。

基本的防垃圾信息配置：

- 开幕模式。新来的不能直接有公开发言权。
- 禁止旁听对非主持发送室内私信。最好禁止它们对所有人发送室内私信。
- 在此之上：
 - 会议室规定，想获取公开发言权的人要给室内网名添加特殊字符并等待授予。此时不可以隐藏旁听的在场状态。
 - 会议室公告板上公布主持的XMPP用户地址，联系主持以请求授予公开发言权（主持应当会使用高级屏蔽名单功能）。此时可加以隐藏旁听的在场状态，这么做可以防止有人使用室内网名、虚拟肖像、自定义在线状态信息来骚扰。所选群聊服务器最好没有或可以不设最大座位数限制——如果周围的XMPP用户数量很多的话。
 - 隐藏旁听的在场状态有所代价，主持会因此难以确定那些联系自己的陌生人是不是真的在会议室里。如果不在，也就意味着联系自己的人要么是已经被会议室封禁的，要么就不是专门来索要公开发言权的（而是来搞其它名堂，例如骚扰）。可以禁止旁听当场修改室内网名来阻止它们通过用修改室内网名产生室内通知的方式进行骚扰。

如果遇到以下情形之一：

- 会议室声名远扬，或者周边的XMPP用户太多，因此想参与交流或成为成员的陌生人太多，而主持人力不足，或者想限制群聊规模增长速度。
- 垃圾信息泛滥到敌人不遗余力地专门攻击主持。

那么还有最强对策——邀请介绍制：“要想获得公开发言权或会员权限，就需要已有成员介绍和邀请。介绍邀请人为自己的邀请介绍负责。”主持人可以不再接纳没有任何朋友关系的陌生人。邀请介绍制平时也可以使用。

对欢迎各种人的公共服务器而言，会议室的封禁功能的意义很少。因为，锁门会议室肯定用不着封禁；公共服务器的敞门会议室又欢迎所有人加入，注册易如翻掌，被封禁后可以换虚拟身份加入。要用封禁的情况只有三种：

- 群聊服务器设置了会议室座位数上限，要坐满了，于是封禁一些空占座位没什么用的人，腾出更多位置给活跃的人。
- 有个名人，你要明确地对它表示敌对，于是通过封禁它来做到这一点。
- 会议室决定显示旁听的在场状态，但有旁听通过占座名、虚拟肖像、自定义在线状态信息来进行骚扰。

对其它令人讨厌但不严重的人而言，通常只需要撤销它的公开发言权和成员身份。

如果骚扰者太多，或者会议室将要满场的话，那么应该考虑将会议室改为锁门，连续地封禁不一定是个好办法。无论是骚扰者，还是占座位只为了旁听的人，它们被封禁后仍然可以再注册一个XMPP身份过来。

立场混乱的敞门会议室

“欢迎各种人”？“不限立场”？、“想说什么就说什么”？就差再讲一个“平等”了？那么，你将站在群魔乱舞的主持台上，要准备好受各种气；或者准备随时脱身，不要勉强自己。

你要做的只是阻止两种几乎每个会议室都要阻止的人：

- 机械程序式地发垃圾信息的人。
- 习惯说外语的人。

自己决定筛选力度：你可以看谁顺眼，就给谁公开发言权；也可以去私信试探一下它们。

立场分类的敞门会议室

一种接纳多种立场，却又不让场面太轻易地失控的会议室，它要求与会们立场明确。这种会议室稍显“有序”，适合开办辩论会。

房主将立场进行分类，示例：

- 革命派（社会主义者）（如果不想恶心的口头“革命”派混入，那么就强调它的革命性。）
- 改良派（面对更严重的资本主义政策时，嘴上说“不要”，身体却很诚实的人。）
- 保守派（资本主义者。）
- 保皇派（明目张胆的资本主义者。）
- 泥潭派（见人叫“同志”，见鬼叫“太君”。）
- 国家主义者（必须明确效忠于哪个国家，并愿意对其各种政策作明确的解释。如果只是说“效忠于某国”，那是假的国家主义者。）
- 民族主义者（尽量不要设置这个，因为有混合民族这种鬼东西鬼概念存在，它们会搞得一团糟。）
- 宗教信徒（尽量不要给具体宗教分类，或者干脆不要设置这个。）
- 自认立场混乱（根据需要设置或不用。）
- 中立派（“中立”派）（这个是不应该设置的，否则前功尽弃，会议室会变得一团糟。要给个拒绝它们的理由的话，例如经典的：“中立派（“中立”派）不会对任何人表示支持或反对，也不会打扰任何人，当然也包括主持。”）

主持优先让它们自己认领自己的帽子，每人仅一顶。为每个类别设置一个代表字符，例如革命派用“⚡”，让它们编辑自己的室内网名，在最前面添加对应的符号，然后再给它们公开发言权。对派系分类产生争执时，主持应该自己对冒充者作决断。

不进一步管控公开发言权的话，这种会议室就容易出现七嘴八舌，流程混乱，交流不畅的情况。如果想让辩论变得正式且更有序，就要有辩论会主持，每方只派一名代表，每次只允许两个人公开发言，轮流阐述立场和相互提问。对自觉守规矩的人员不用撤销公开发言权。

如果想让辩论更精彩，那么考虑以下操作：

- 室内网名必须有语言意义，且一旦确定后，禁止更改。或者干脆使用小桌。亦即要求它们以固定的身份发言。
- 禁止过快地连续变换立场。这种人是不可信的。
- 禁言休息期。理由可以是“主持不一定能彻夜看管控场”。要做到这一点的话，请挑选一个保留参与等级记录的群聊服务器，授予公开发言权时不要设置会员。到了该休息的时间后，会议室逐客锁门；休息完毕再开放。（如果它们自己愿意再另外创建会议室来彻夜长谈，那也是一件值得高兴的事情。）
- 禁止收回已经发出的消息。（基本只是规则上禁止。群聊服务器基本允许收回。）
- 定期发布历史交流记录存档文件，给查阅提供便利。

立场单一的敞门会议室

这是一种大大简化政治审核的方法。虽然形式上简单，但准备起来并不简单。

你不想立场混乱的人们以及立场敌对的人们来干扰交流；却又想招揽一些立场相同的陌生人（因此敞门），或是把交流内容给公众看（因此敞门）。

于是，你把能够筛选到相同立场的人的信条都写在会议室公告板上。规定，凡是想获取公开发言权的，都得秉承那些信条。在室内网名前添加指定字符来请求授予公开发言权。

凡是获取了公开发言权的，无论它们是真的秉承那些信条，还是假心假意，它们都得按照信

条所写的作派来发言。如果它们违反，自然就要被封禁。

也许你还需要到周边的会议室逛逛，看看是不是有些贱货在另一个会议室又秉承另一套冲突的信条。

“很简单？”不：

- 信条要言简意赅，不宜冗长。
- 信条要限制明显，这样能够将各种没有思想武装自以为是的人劝退，也能防止得以参与交流的人们不发生严重的信仰冲突。
- 确保你不会被一个无名来客轻易地用让你认为无可匹敌的理论砸碎你的这些信仰。
- 不要轻易更改，如果你轻易更改，那么这个会议室就会损失原本的意义；改得越多越频繁，那么损失得就越多。

问问题式政治审核的敲门会议室

这是审查员可以根据别人的回答来随机应变的政治审核方法，也是费劲的政治审核方法。

负责审查的主持调整高级屏蔽名单至半屏蔽模式，并将用来审查的XMPP用户地址公布在会议室公告板上。提供多个主持的联系地址不一定是个好主意，更应该多个人合作用同一个专门用来审核的（而非个人日常交流使用的）XMPP身份。以免一个请求发言的人同时联系多个主持，造成工作精力浪费；如果以后要停止审核机制，这也防止了它们的个人XMPP身份因为公务带来的历史遗留问题而妨碍到普通交流使用。

让想获取公开发言权的人们添加审查员为联系人并相互共享在线状态，成功后便可开始问问题，根据被审查者的回答来决定它们是否应该被授予公开发言权。

为了减少打扰数量，可以在会议室公告板上写上基本立场要求。

如果有人按键式请求授予公开发言权，就用室内私信告诉它们“想获取公开发言权，就请按照会议室公告板说的来做”。

为了减少收到离线垃圾信息的可能性，以及照顾审查员的休息，可以在会议室公告板上写上审查工作进行的时间段。不到点不接受任何添加联系人的请求。

审核问题应该是不固定的，以防止捣蛋鬼和不务正业的人们故意试错。审核问题也应该是尖锐的，这样能高效地击退思想不合格的人们，避免浪费更多精力。

为了增加敌人骚扰的难度，以及增加试错地参与审核的难度，你可以只允许和某几个注册有复杂验证码的用户服务器通信（甚至既有复杂验证码还要电子邮箱验证的），把这些服务器地址放到会议室公告板上。

可以要求每个要申请公开发言权的人必须要在室内网名中添加符号，以妨碍专门用大量XMPP身份试图在通过联系人申请后骚扰审查员而非真心想获得公开发言权的敌人，这样一来，谁对谁灌垃圾信息还不一定呢。（确认发现室内旁听里有敌人后，也可以用室内私信反骚扰它们，不过这么做的意义和效果很可能不大。尤其是不要泄洪式地发大量重复的信息以试图攻击，这对公共服务器而言是不敬的行为。）

请记住，邀请介绍制是最安全的手段，是从头到尾都可以使用的手段，是情况最严重时能用的最后手段。必要时就该放弃接纳陌生人，不要勉强。

给社会主义初学者们的敲门会议室

如果我们无暇去教社会主义初学者们，那么我们就只能给它们导读以及书本看，即使提供具体提问的解释，也是自助查阅的。这么做的好处是：那些写在纸上的理论言辞是经过深思熟虑的，不是临时思考的结果，因此写得很清楚；而且有效防止假初学者们浪费我们的精力。

当我们有人力精力时，就可以给社会主义初学者们创建这样的会议室。这个“社会主义初学

者”是可以打引号的。因为我们在给真正的社会主义初学者组建敞门会议室的同时，也给那些假的社会主义初学者，以及敌人，也创建了一个供旁听的敞门会议室。

政治委员们当主持来决定给哪些人授予公开发言权：

- 排除掉纯历史故事爱好者、纯理论爱好者、旧书旧物的收藏家和商人、纯经济学者、纯技术爱好者、口头“革命”派。
- 对请求公开发言权的社会主义初学者们，仔细检查它们的态度和社交胆量。如果它们的态度不好，甚至直接表示敌对，那么就不要再给它们公开发言权。如果它们的社交胆量太差，那么也不该给它们公开发言权，我们做不到专门给它们治疗社交恐惧症，也不可能低声下气地求别人革命；应该先让口头“革命”派们或改良派们带它们相处一段时间，它们的会议室规则很宽松，也“心平气和”，肯定融洽，说不定连教XMPP的事情都省了。
- 严格地将会议室里的组织内革命者和外来社会主义初学者区分开，会议室人员的室内网名应全部带有前缀符号用来区分它们。让那些初学者们自己给自己明确的定位，不允许初学者们叫“同志”。如果它们明知故犯，那么无论它们说的“同志”是谁，以及是否是革命派，它们的捣蛋行为都已经确定无疑了。
- 对组织以外来的革命者而言，只要来搞些其它名堂，不是来认真地参与学习，就不应当接受，因为无法统一行动，无法服从相同的纪律，会导致教学会议室因无法顺利执行教学任务而变成普通的左派交流会议室了；同时也会无意义地增加政治委员的审核工作量。

“向维希巴洛分子宣战，让一切调和主义分子、“观点捉摸不定的”人和优柔寡断的人见鬼去吧！！宁要好梨一个，不要烂梨一筐。宁要两三个积极肯干和忠心耿耿的人，不要十个暮气沉沉的人。”——1903年01月16日《致伊·瓦·巴布什金》，《列宁全集》汉语第二版增订版第44卷第304页。

地理行政区分类的敞门会议室

这是一种辅助激化社会矛盾的会议室。它不需要限制政治立场。主要作用只是传递信息，让人们联络起来。这可以有一个很简单的理由：“互帮互助”。

对思想腐朽的人们而言，只能从大到小，由远及近来进行。例如，先招揽整个国家的XMPP用户，人数多到一定数量后，就按照不同的行政区，例如省，缩小范围划分到不同的会议室。接着就是市、县、乡、镇、村、庄。优先组建人口多且密集的行政区的会议室，除非恰好它们的用户数量尚少。

对有组织有纪律的人们而言，则可以由小到大，由近及远。

当XMPP用户越来越多，甚至让人发现越来越近时，人们便可以畅所欲言，自由地交流，就可以有各种各样的一起交流兴趣爱好、艺术文化、风土人情的群体。想了解某个地区的民情，就去那里的会议室看看它们都讨论些什么。

不需要从一开始就限制政治立场。交流的人们多起来后，自然会自愿地按照不同的政治信仰来扎堆。

一旦信息流通起来，那么就能看到很多叫苦不迭的保守派，记住，我们不是个人英雄主义者，不是它们的挡箭牌，不是它们的救世主，不是支持可持续剥削的。它们应该自己发现真理，自己学会斗争，自己来决定自己的生死存亡。

一种简单的检查一个陌生人是否是当地人的办法是：让它们拿手机访问检测访问者IP地址的网站（只要你所处的国家不提供公共的代理网络连接服务），并发送带有现在时间的截图。这种会议室的政治性强，而且一开始就是为了政治目的服务，因此，要优先为当地人服务，不能将其它行政区的没用的无名小卒设为会员。从一开始就要想办法去尽可能地确保每一个参与的人在室内都只有一个XMPP身份有公开发言权，确保每一个获得会员权限的人确实是当地人。甚至要确

认它们能以固定身份活动，无名氏们只能被用作过渡；到了活动家多的时候，它们肯定不能再受欢迎。

如果要求没有这么严格，那么恐怕你这个会议室实际上只是个平平无奇的全国人民交流会议室。如果你要将这种会议室转化成这种地方行政区的会议室，那么你就必须态度明确地把很多以前欢迎过的又胆小又话多的捣蛋鬼们撵出去了。

付费成为会员的会议室

有些人要求付费才能授予权限，这样的人可能是有实体组织性，也可能只是个陌生人交流会议室的房主。这种做法可能是商业服务，也可能只是一种阻碍捣蛋鬼加入的方法。

这种制度的小资产阶级气味浓重。思想腐朽的人们愿意为了随波逐流、从众扎堆而付这个代价。

议会制的敞门会议室

房主因无暇参与管理，或者没有做决策的果敢，因而设置了很多管家。这些管家也同样缺乏组织性和纪律性，或者甚至意识形态严重冲突。如果它们保持冲突，那么管理工作就是完全不正常的；如果它们求同存异，那这就成了议会制会议室，尽管这样的会议室管理也很混乱，但对那些思想腐朽只想找个集体聊聊天的人们而言，算“很好”了。

如果一个会议室失去了房主，或者说房主等同于不存在（或者说是“白占了一个座位”），那么管家们可以发挥会议室的剩余功能。（但这样的会议室就不应该长期正式使用了，应该另建一个，除非它们不需要会议室来继续正经事务。）这样的会议室往往就会成为议会制会议室。因为，如果它们的意识形态契合，且在同一组织内共事的话，那么会议室就本应该有多个房主，而不是多个管家。

群英会模式会议室

其设置是敞门+小桌，说它是“群英会”的原因有：

- 只有会用高级屏蔽名单的高级用户才能顺利避免此会议室带来的垃圾信息危险性。也就是说，会议室里基本只有这种人才能长久存留。这是技术上的英才。
- 明知会公开自己的XMPP用户地址，还愿意加入的人们，基本是愿意以固定身份公开发言的。这种人不躲躲藏藏；更可能立场明确；值得敬佩。如果它们是名人，那么这种公布XMPP用户地址的做法还可以让人们确认它们不是冒牌货，而确实是其本人。
- 既然是敞门的，那么就心知肚明会议室里的内容也是给敌人看的。而且，参与的人们的虚拟身份是不掩藏的。这是胆识的表现。

对成员们不信任的来访游客在面对此情景时比用大桌时更倾向于注册使用一个临时的XMPP身份来加入。

无书记的敞门会议室

不启用会议室消息存档。这相当于没有书记的语音会议，话音一落，不在场的就无法获知这句话说的是啥，因为没有历史记录可供查询。

一般来说，不用书记是对人员们不信任的表现。房主想让人员们说的话尽可能少地被更多人知道。这可能是因为房主无法对与会者的言论负责，不想或无法多费心监管发言；也可能是房主在试图促使别人创建它们自己主管的会议室。

广播站

完全防止垃圾信息的会议室。只能看只能听，却不能对其造成任何影响。很简单：

- 隐藏旁听的在场状态。所选群聊服务器最好没有或不设最大座位数限制——如果周围的XMPP用户数量很多的话。

- 敞门+开幕+大桌。
- 禁止旁听向任何人发送室内私信。
- 邀请信任的同志们加入，参与广播发言。
- 如果广播站里的主持和与会全都是完全屏蔽所有陌生用户的名人，那么还可以用小桌。

假面舞台

一种管理不直白明确，适合用来说黑话胡话，散播传言的会议室。很简单：

- 隐藏全部会议室人员的在场状态。所选群聊服务器最好没有或不设最大座位数限制——如果周围的XMPP用户数量很多的话。
- 敞门+开幕+大桌。
- 用编辑成员列表的方式来调整公开发言权。（参与等级严格按照对应的管理等级默认值来，不独立调整参与等级。）
- 正常运作这种会议室对成员之间的信任有着极高的要求，有任何一个内奸都能产生很严重的捣蛋恶果，接收陌生人公开发言基本等于毁掉这个会议室。

在这种会议室里，看不到谁到场离场，看不到谁修改了室内网名，也看不到它们的虚拟肖像，谁都看不到消息是哪个XMPP身份发的。哪些来自不同室内网名的消息是不是同一个人发的，也没人能确定。哪些来自同一个室内网名的消息是不是好几个人发的，也没人能确定。

有什么样的人在里面，由审查员决定。说不说什么话，由参与者们决定。信不信什么话，由人们自己决定。

管理规则变动

能保证规则不轻易变化的会议室很少。如果你想以一个固定身份活动并想获得好名声的话，就不要轻易作不变会议室规则的承诺，尤其是在自己没有控制局面的能力时。

很多时候管理策略是要变动的，例如一个很常见的因素——累了，不想再为太多贱民操劳了。如果你不是因有政治任务而管理这个会议室，那么你可以完全抛弃这些不属于义务的事情；如果你有政治任务在身，我们也会说“身体是革命的本钱”。

如果要有目的地创建一个为某种群体服务的会议室，但为了临时的目的而要招揽许多以后肯定不欢迎的人进入。那么，从一开始，甚至从开始之前就要做好对付它们的准备。例如，你要记下哪些人是你以后不欢迎的，把它们和你信任的人区分开，不要混淆。你可以明摆着地或者找各种理由地撤除它们的成员资格以及公开发言权，或是封禁它们，由你决定。

敞门会议室防范“浪费运行资源”攻击

这不是指针对服务器的浪费运行资源攻击，而是指对房主、管家、主持的“浪费运行资源”攻击。

这种攻击存在于很多场景：

- 有许多人添加你为联系人，请求你共享在线状态；甚至在此之前就给你发消息，打音视频电话（如果你用的服务器允许，而且你也没有启用白名单功能的话）。它们还可能问你各种各样的政治问题，但即使你回答了很多，它们也只是抛出更多的问题，而在政治态度以及信任程度上没有期望的变化。它们也都不提供什么帮助，对它们也都问不出什么有帮助的信息，徒增你的麻烦。这些人往往是没有固定身份的，不想让众人认识并影响别人。
- 你的会议室为了防捣蛋鬼倒垃圾信息而禁止陌生人发言。但是，有许多人请求并获取了公开发言权，但它们却不说什么，不想和人们认识，不和人们分享好东西，避免牵扯它人，试图掩藏自己，把这个世界当戏看。

它们在在场列表里甚至连同成员列表里空占了一个位置，妨碍你翻阅找到想找的人。

这种人，有可能只是它们自己想这么做。另一种可能更严重，可能有人专门注册使用多个号码来从事这种浪费运行资源攻击。

敞门会议室里防范这种浪费运行资源攻击的做法，就是定制并公布严格执行的严苛规则，还可以提供自助服务：

- 如果它们违规，就直接撤销公开发言权；如果它们长久保持静谧，也应该适时地撤销它们的会员资格和公开发言权。
- 对信任不够深的人只授予公开发言权，而保持其游客的管理等级，省得把成员列表排得太长，以后要是锁门的话也方便把它们排除在外。
- 陌生人们想了解什么，就预先告知它们或预先拒绝回答。

有许多XMPP身份在成员名单里。但是随着时间的推移，有些XMPP身份被弃用了。这些被弃用的XMPP身份会纯粹地增添网络流量消耗和削弱管理效率。对锁门+小桌的会议室而言，它在接收新登录点的过程中可以发现被弃用的XMPP身份，因为无法获取（被服务器自动地或用户主动地）注销了的XMPP身份的OMEMO密钥，报错会通知这一点。其它类型的会议室就不方便了，主持需要添加所有成员为联系人并相互共享在线状态，并每隔几个月就检查一次联系人列表，看看哪些XMPP身份被弃用了。

废置会议室

如果你有一个人数很多的会议室，或者你已经把某一个会议室宣传出去了，但是现在又想废置它；那么，直接解散并不是一个好主意，这会导致严重的历史遗留问题。因为：

- 会议室被解散后，可能会有个人立刻再刻意创建这个会议室。这种情况有以下风险：
 - 解散时不在场的人们收不到解散的通知，如果它们再次加入时这个会议室已经被再次创建了，因此可以顺利加入，它们就可能不会发现会议室（被原来的房主）解散过。
 - 新房主谎称是原来的房主将会议室转让给了它；或者谎称自己就是原来的房主；或者谎称自己和原来的房主本来就是共同管理这个会议室的。以及各种各样的新房主捣蛋的情况。
- 如果一个用户在某个群聊服务器上有创建会议室的权限的话，那么加入会议室的操作对一个不存在的门牌号码会直接创建这个会议室。这也就是说，可能会有些人只是想加入原来的会议室，但是意外地成为了那个门牌号码的房主，而且随后还可能有更多其它原来的人也试图加入这个会议室。
- 新来的人试图加入会议室时，如果发现会议室不存在。它就会对给它宣传这个会议室的人降低信任，或对这个会议室原来的房主降低信任。

如果要废置的话，那么房主应该留出足够的时间让大家知道。必要把废置或解散的计划通知信息放到会议室公告板上。（如果在互联网的其它地方宣传过此会议室，那么还要考虑把预告信息放在会议室的描述信息里，以及名牌里和门画里。）不要发条用来通知的消息后就立刻解散，毕竟解散后这条消息就在服务器上被删除了，只有当时在场的可以收到。和会议室系统发出的解散通知一样，是一次性的。如果会议室里那些人获取成员资格或公开发言权的经历并不轻松，那么轻易解散对房主名声造成的负面影响更大。

为了防止有别人占用门牌号码，不要解散。同时，为了防止会议室人员滞留在会议室里，可以为会议室设置一个没有人知道的口令（可以连你自己都不知道），使得任何人在下次加入时都要输入口令。同时，记得确保会议室是砖屋。服务器管理员或服务器软件会清除太久没有任何人进入的会议室，到那时候不用担心历史遗留问题，因为人们会把这个会议室忘记。

如果你确定要拆除会议室的话……

考虑主动通知，可以最大限度地减少误会，减少历史遗留问题。

如果一个会议室被解散了，或你离开后不想再加入它了，请在个人地图里删除它，否则“登录后自动加入”标记可能会让你再次创建或加入此会议室。在解散前也请提醒原来的人员们从个人地图里删除它。

发布你的敞门会议室地址

既然设立一个敞门会议室，那么就考虑发布你的会议室地址。注意以下事项：

- 你可以将会议室地址放在自己的网站、书文、其它交流平台的个人信息内。
- 在互联网的其它地方发布时，还要考虑在那里也更新会议室状态的事务，例如会议室是不是满员了，还收不收更多外人，负责人有没有更换，等。
- 如果你要在其它会议室里发布，那么注意事项就是要经过别人同意；不要连续发布多次；如果和其它会议室的负责人是好朋友的话就干脆在公告板上挂友情链接。
- 如果你的会议室有政治审核，那么你可以考虑公布用来审核的用户地址来代替公布会议室的地址，记得要善用高级屏蔽名单功能。（如果你的会议室是锁门的，却还想要招陌生人，那么就只能公布审核员的用户地址。）

XMPP的未来

这算是后事交代章节。如果说明书编写组长期没有再更新说明书，那么请参考此章节并观察现状来决定是否继续使用XMPP。

像是：公共服务器越来越少地允许用户端软件直接注册，而是越来越多地要求识别复杂验证码或要求提供电子邮箱；对通讯管控严格的国家会将XMPP连接阻拦掉，甚至还会加以阻止下载安装用户端软件。这些都不需要多加强调。

重要的只有一件事，那就是XEP-0016。

- 2017年05月：在技术文档中开始被标为“Deprecated”（意为“不赞成使用”）。
- 2017年10月：服务器软件“Prosody IM”版本0.10.0移除了此功能。
- 2020年07月：用户端软件“Gajim”版本1.2.1移除了此功能。

此功能是理论家们和活动家们必需的，而革命必需很多理论家和活动家，哪怕这些理论家和活动家是敌对派别的。即使不考虑政治因素，那么对普通用户而言，这些事件也像是斩断了它们的一条臂膀一样，从此以后它们很难自行抵御垃圾信息攻击。

在它被标为“不被赞成”时，没有更好的用来替代的功能标准。甚至六个整年后，都没有任何可替代它的功能出现。

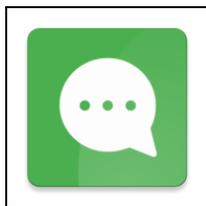
目前而言，还有一半的公共服务器（也就是“Ejabberd”运行的公共服务器）支持此功能，用户也可以使用用户端软件“Psi(+)”来完整地发挥此功能的效用。

如果哪一天Ejabberd移除了此功能，那么XMPP将不再适合为革命服务，不再适合任何政治活动，所有的理论家和活动家都应该在自己用的服务器用的软件跟进到对应版本前离开XMPP平台。更准确地说，是任何想以固定身份活动的人都应当离开。在那以后，XMPP平台上将会充斥着不为自己的言行负责的无名小卒们，也没人能保证谁的身份不被有效地冒充。

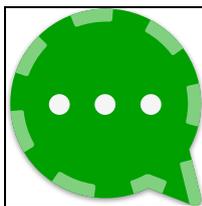
Conversations介绍及下载

介绍

本Conversations章基于的版本号是2.13.0。



启动图标



标准图标

Conversations是一个用于Android端的开放源代码的XMPP通信协议的用户端软件。它的功能不算很齐全，但已经满足了基本的通讯需要。

它支持的最低Android版本为5.0。而为Android 5.0开发的应用软件在往后的系统版本上都可以正常运行。所以，它能在所有2015年及以后开始设计生产的Andorid手机上正常运行。

Conversations的功能有以下不足：

- 注册时而不支持服务器自定义的表单，所以无法直接注册一些服务器。用户应当优先在其它用户端软件注册或在服务器的官方网站上注册。
- 无法获取会议室的设置表单，因此创建会议室后无法马上开始精心调整会议室设置。新手用户应当依赖其它熟练的房主而不应当自己创建会议室并带太多人进去。
- 当收到别人邀请加入房间时，Conversations会自动接受并加入。

Conversations在其它方面的不足：

- 翻译不够好。
- 对新手用户缺乏说明指导。
- 对新手过于“友好”，使用了一些不够明确的概念来简陋化XMPP。局限于此，将无法成为高级用户。

下载

打开网页浏览器，访问此网址：“https://f-droid.org/zh_Hans/packages/eu.siacs.conversations/”。

直接使用你的网页浏览器的页内查找文字功能，搜索“armeabi-v7a”，点击“armeabi-v7a”徽标下面的“下载APK”就可以下载了。



改版

考虑到Conversations的状况，于是我们发布了一个改版，名叫“革命通讯器C”（“revolution.messenger.c”）。



革命通讯器C的徽标

该用户端软件更改自Conversations，作了以下更改：

- 调整了翻译文字，添加了引导说明，以使得它对新手很友好。
- 崩溃报告程序无效化。
- 修改了徽标。
- 修改了一点界面颜色。
- 修改了说明页。
- 其它程序相同。

访问金星革命委员会的官方网站可获取此软件及其源文件包。

这些章节将用革命通讯器C来演示，文字篇幅将大大简化。涉及的内容主要是程序而非翻译和指导文字时，我们仍会使用“Conversations”这个名字。Conversations用户在界面文字和操作上不明白时，也可以来参考。

当前的最新版本是2.13.0.3，其安装包的MD5校验码是“4c81ccd0242216e05ba42f70b603f64b”。

注册与登录

revolution.messenger.c  



为了社会主义革命，加入XMPP吧！

欢迎使用“革命通讯器C”。

组织内负责为你发放此软件的同志应该也为你发放了一本《社会主义XMPP高级用户使用说明书》（版本号至少应为2024年01月05日版）。遇到问题时也可以询问组织内的XMPP指导员。

请记住，XMPP本身不是通过互联网封锁的工具，它不代理下载HTTP链接文件。当你无法下载别人分享的HTTP链接文件时，以及当你因处于互联网封锁环境中无法连接服务器时，你仍然需要使用代理网络连接。

请告诉别人不要使用旧版本的革命通讯器C。

[创建新的XMPP身份号码](#)

[登录一个XMPP身份](#)

首次打开后的界面

如果你留有先前用Conversations或革命通讯器C备份的虚拟用户的备份数据文件，你可以点击右上角的选单来恢复。



选择你想使用的XMPP服务器。

你组织里的XMPP指导员应该有给你推荐使用的服务器。

除了可以用原软件默认推荐的公共服务器地址“conversations.im”以外，说明书的附录给出了不少推荐尝试的服务器地址。

用来注册和登录的XMPP身份标识像这样：“XMPP身份号码@所属用户服务器地址”。例如“lenin@soviet.union”。你可以把XMPP身份号码当网名用，但一旦正式使用，就不能轻易更改了。

XMPP身份号码使用小写英文字母和数字的兼容性最好，汉字和符号则不一定支持，大写英文字母则完全不支持。

密码建议设置10位字符左右或更长，最好兼具大小写英文字母、阿拉伯数字、符号，有的服务器拒绝用过弱的密码注册。

如果验证码有英文字母，请区分大小写来填。

[使用服务器“CONVERSATIONS.IM”。](#)

自己填选一个服务器地址

选择要注册的服务器

如果你选择“使用服务器“conversations.im”，那么请将生成的随机密码改成你要设置的密码。

填写

Conversations的注册流程很特别，它是直接提交注册表单，而不是先向服务器要注册表单，等待服务器同意后再填写表单。它只是模板地支持XMPP身份号码、密码、图片验证码三种元素。因此，有的公共服务器是它不能正常注册的。

注意，只要注册失败了，不论原因是什么，上面的一栏都会显示为红色，这有一定误导性，这并不是说你那一栏填写错误。

Conversations也不会把注册时的服务器反馈信息原般地给注册者呈现，而是自己根据情况判断并反馈。因此，它会有许多错误的反馈信息。

如果点击“下一步”后没有任何反应，按钮没有变灰，那么检查你的互联网连接。

添加虚拟肖像

注册成功后会自动登录。添加号码并登录成功时没有虚拟肖像的话，通常会提醒你添加一张。到了这一步，就是说你登录成功了。

Android权限问题

它可以使用以下Android系统的权限：通讯录、位置信息、存储、话筒、相机。

通讯录：它可以读取系统通讯录里存储的联系人的XMPP地址。如果你用不着或不会用这个功能或系统通讯录，可以拒绝这个权限。

位置信息：发送位置信息的功能依赖第三方服务，它很可能效果不够好甚至无法正常起作用，不如拒绝这个权限，放弃这个功能。

存储：这是下载文件和备份数据所必须使用的。

话筒：语音通话需要用到它。

相机：视频通话和扫描二维码需要用到它。

它会使用距离传感器，在音频通话期间当手机靠近耳朵时用来自动灭屏。

也请留意以下事项：

- 取消Android对它的电池优化，确保它在后台正常运行。因为它是个要随时接收信息的即时通讯软件，不是每一刻钟或更长间隔才连接一次互联网的电子邮箱客户端软件。它的耗电量很少，如果你的系统耗电量多，你应该考虑问题出在其它因素上。
- 允许它在后台保持运行（即使是灭屏时），确保它不被杀后台运行进程。（有些资本主义衍生的Android管这个叫作“自启动”。）也请确保它的后台进程不因运行内存被满占而被杀掉。
- 请不要设置灭屏时切断路由器网络连接。

“对话选项”界面和“联系人与群聊”界面

它有“对话选项”界面和“联系人与群聊”界面。如果你现在有对话项，那么“对话选项”界面就是最外层的界面；如果没有，那么“联系人与群聊”界面就是最外层的界面。



“对话选项”界面



添加联系地址

要关闭某个对话选项，按住对应的选项并左滑或右滑。你也可以在对话界面的选单里关闭，这样更麻烦。

有其它用户邀请你去会议室时，Conversations收到后会自动加入而没有“接受”和“拒绝”的选择，也不会显示是谁邀请了你，对话选项里会多出邀请来源的会议室。

有人添加你为联系人后，对话选项界面会出现一个没有任何消息内容的新对话项。

不论你在Conversations上有多少个XMPP身份，所有的对话选项都会放在一起。注意区分是哪个XMPP身份的。但联系人列表和群聊列表只显示属于已经启用了的XMPP身份的项目。

进入对应的对话项后，其选单可以将对话项置顶。被置顶的对话项将在对话选项界面显示一个五角星徽标。

当加入或退出一个会议室时，会同步修改个人地图里的“是否要在登录后自动加入”记号。

对话选项界面的放大镜图标用来搜索本设备上已经记录的消息。联系人列表与群聊列表的放大镜图标用来搜索已经记录的联系人和会议室地址。

在对话选项界面点击右下角的对话气泡图标可到“联系人与群聊”界面。在联系人列表与群聊列表界面点击右下角的加号按钮来添加联系地址。

二维码扫描按钮用相机镜头扫描二维码获取XMPP地址，不支持读取本地图片。

创建露天会议室时，你只需要输入自定的会议室的门牌号码（也可以当会议室名称使用），群聊服务器的地址由创建时用的XMPP身份决定。

创建地下会议室时，Conversations不支持自定义会议室门牌号码，而是会生成随机的号码。如果创建者所属的服务器没有群聊服务器，那么Conversations会尝试查找并使用其它其它XMPP身份所属的服务器的群聊服务器。

关于“查找露天会议室”选项，你可以在高级设置页里选择使用第三方公共搜索引擎来查找，或是在你自己使用的服务器提供的群聊服务器上查找。这个第三方公共搜索引擎见于附录。



“联系人”界面

在联系人列表与群聊列表按住对应的选项可以打开操作选单。

有的联系地址的号码会有些字符显示为红色，这本意是帮助区分容易和英文字母或数字混淆的字符，但在程序设计上有差错，导致一些汉字也显示为红色。

对话界面



对话界面

要注意，Conversations不会先向联系地址所属的服务器发送请求来检测有效性。无论添加的联系地址是否有误，它都会打开一个对话项。

这是对话界面。右下角是发送按钮（编辑框为空时可能为其它，可在设置里调整）。发送按钮不为灰色时意为发现对方在线。

上方有更多功能：音视频通话、主动加密选项、发送文件或地理位置、更多选单。

相互添加为联系人，并共享了在线状态后，就会出现音视频通话的按钮。不过Conversations不支持多人一起音视频通话。

分享地理位置功能很可能是用不了的，请忽视它。

按住消息，和头像，将有对应的选项。自己在使用时试一试。

按住消息时，有以下操作：

- 你可以按住正在传送的文件所对应的消息，来取消传送；如果已经寄存到服务器上了，就无法取消了。
- 用系统“分享”选单来和向其它应用软件传递内容。
- 使用引用格式复制到输入框。
- 更正。
- 如果消息发送失败，那么就有（服务器传回的或本地发现的）出错信息供你排查原因。

在会议室内按住别人的头像时，如果你能看到它的XMPP地址，那么就有发送普通私信的选项，而没有发送室内私信的选项；如果你看不到它的XMPP地址，那么就相反。在会议室详情页的人员列表里这么操作也行。

在普通私信对话界面，点一下头像会进入详情页。在会议室对话界面，点一下别人的头像可以发送一个公开呼叫标识。被呼叫的用户收到消息时会有提醒。一个问题是，它使用冒号而非逗号，这会让新手误以为这是在引用某人说的话。

发送的室内私密消息和公开消息显示在同一个界面，因此不仔细看私信标识的话容易混淆。

里面打勾的盾牌图标意为此消息已主动加密。

如果收到了收信用户的回执，那么发送出去的消息会打勾。

搜索历史消息时，如果目标历史消息过去太久了，Conversations将不会展示它的前后文。

在选单里选择“邀请联系人”时，如果面对的是单个用户，那么会在服务器上创建一个新的会议室（地下+锁门+小桌）。

Conversations收到文件时，用户在下载前无法获知文件名。所以请考虑告知别人自己发送的是什么文件，以及有多大。以供别人判断自己是否需要此文件。

接收的文件的存储位置即为Android系统预置的文件夹里：

- 文档：……/Documents/Conversations/
- 图片：……/Pictures/Conversations/
- 视频：……/Movies/Conversations/
- 如果在上面没有找到你下载的文件，其它的放在“下载”文件夹里：……/Download/Conversations/

针对这个改版，把路径里的“Conversations”改成“revolution.messenger.c”。

添加联系人及联系人详情界面

Conversations不支持主动和一个陌生地址联系，只有“添加联系人”操作才能主动打开新的对话项。如果对话选项界面多出来一个陌生用户，那么就是对方给你发送了消息或添加了你为联系人。你可以也添加对方为联系人。



共享在线状态成功

你没有添加对方为联系人时，此界面会有一个“添加联系人”的按钮。

添加联系人后会有两个共享在线状态的选项。它们在达成前和达成后会显示不同的文字。

点击分享按钮可以将对方的地址链接复制到剪贴板或获得用于添加联系人的二维码：

点击联系人的虚拟肖像可以将其XMPP地址添加到设备系统的通讯录（而非XMPP的联系人列表）。但这涉及一些额外的周边技术问题，我们决定不作介绍。

当你们之间发送了第一条OMEMO加密消息后，在这个界面就可以相互看到对方的OMEMO指纹。

当你们之间发送了媒体文件后，在这个界面就可以看到这些媒体文件历史。

如果你错误地把一个会议室地址当成联系人添加了，或者错误地把一个联系人地址当成会议室添加了，那么请删除这个联系地址，按照正确的方式重新添加地址，并手动清除残余的错误消息记录。

如果你在调整在线状态共享时发现无法达成共享，那么可能你在另一个与Conversations相同或类似的软件也登录着你这个XMPP身份。你应该那些登录点暂时下线它，或者用其它的用户端软件来调整在线状态共享。

群聊详情界面

← 会议室详细信息

教学会议室

成员名单只有房主和管家可以看到；在场人员的用户XMPP地址只有主持人可以看到。管家可修改话题(公告板)。

XEP-0313: 消息存档管理 有效

教学会议室@conference.draugr.de

教

[邀请人加入](#) [查看人员列表的1位人员](#)

教学号码2
房主(主持)

只在被提到时通知

你正在使用这个XMPP身份查看并执行操作：
教学号码2@draugr.de

群聊详情界面（房主视角）

点击右上角的选单按钮可以启用“高级模式”。“高级模式”是应该启用的，这不会带来什么危险性，而且能让用户获取更详细的信息和更多的常用操作选项。

启用“高级模式”后：

- 多显示一条服务器的功能属性。
- 可对用户执行更多的管理等级操作。
- 在公开群聊里可以设置“使频道受到管理”（开幕）。
- 展示人员的参与等级（但仍不支持单独调整参与等级）。

锁门+小桌的会议室详情界面没有分享地址的按钮，只能去个人地图列表找到它的所在地，而且不允许复制。你会发现Conversations对待锁门小桌会议室和对待其它的不同。

关于人员列表，Conversations是把成员列表和在场列表合在一起的。不过，只有锁门+小桌时才能看到离场人员；大桌时，房主和管家理论上是可以看到哪些人离场的，但在Conversations中不能。

按住人员列表里的人员项目可以调整它们的权限；或者给在场人员发送室内私信。

Conversations在确定会议室设置条件不允许用户邀请其它人进入会议室时，不显示“邀请人加入”按钮。但在显示此按钮时，不一定能成功邀请：例如，如果用户是会员，会议室是锁门的，那么此按钮就不一定奏效，请让房主或管家来邀请其它人加入。

Conversations不支持获取完整的会议室设置表单，支持调整的会议室设置没几条重要的。不要依赖它来调整。当需要完整地调整设置表单时，用其它用户端软件吧。

Conversations不支持解除封禁流寇。

针对“锁门+小桌”的会议室，Conversations支持以下选项：

- “允许任何成员修改主题（公告板）”
- “允许任何成员邀请其它人”

针对非“锁门+小桌”的会议室，Conversations支持以下选项：

- “使（会议室所有人员的）XMPP地址对所有人可见（小桌）”
- “允许任何成员修改主题”
- “使频道受到管理（开幕）”（要先启用高级模式，才能显示此选项）

所以，当房间设置是“锁门+大桌”时，Conversations可以改成“锁门+小桌”。但是反之则不行。

XMPP身份管理界面



可以同时登录多个XMPP身份，例图中只有一个。点击上方的添加XMPP身份按钮可以再注册或登录一个。

旁边的滑动按钮是“启用/禁用”XMPP身份。这和“下线”选项一样。

“删除XMPP身份”的选项可以在自己的设备上删除这个XMPP身份记录的信息，也可以同时向服务器请求注销号码。（服务器拒绝注销时，Conversations会崩溃一下。）

右上角的选单里有从备份文件恢复的功能，可以恢复在设置页里备份的虚拟用户数据。注意这个功能只能用来迁移，而不得用来复制并让两个端同时上线使用。

点击一个XMPP身份，可以查看详情页。按住一个XMPP身份可以打开对它操作的选单。



点击叹号气泡按钮编辑自己的自定义在线状态信息（仅在此登录点显示）。这会显示在其它用户视角中你的联系人详情界面里。

在点击分享自己的XMPP链接时，会添加带有OMEMO指纹信息的后缀。如果你尚没有阅读附录对OMEMO的介绍，那么最好去掉后缀再分享。点击分享按钮后，你可以在你的一堆系统“分享”功能选项中选择“复制”；你也可以手动打字来告诉别人自己的XMPP地址。

“屏蔽列表”选项让你查看并管理拒绝联系的地址。

“服务器信息”让你查看服务器支持的功能标准。

如果要修改你的密码，请不要直接在图中的输入框里修改，因为那是本地存储的用来登录的密码，只有在密码被其它登录点修改了的时候才用得着。“修改密码”选项让你向服务器发出修改密码的请求。（后来的版本中在遇到“未授权”之前不再允许修改本地用来登录的密码，以防新手误操作。）

点击自己的虚拟肖像可以添加、更换、删除。

你可以看到自己的OMEMO指纹。最上面的OMEMO指纹（OMEMO身份）是你这个登录点所使用的，下面的OMEMO指纹是这个XMPP身份在其它登录点所使用的。Conversations会自动请求服务器删除太久没见活动的OMEMO密钥。

随处可达的设置选项页基本是只在这个用户端软件上通用的，不针对具体哪一个XMPP身份，少数涉及具体XMPP身份的会有明显表现。“高级设置”里的内容有的算是平常的设置，同时不建议调整你不理解的选项和本册子没有介绍的选项。由于改版里设置页的注释说明已经很充分了，我们就不放插图了，也不需要更多说明。

疑难解答

我们在革命通讯器中为不少反馈错误信息写入了良好的说明和提醒，用户在使用过程中遇到错误时直接就可以知道是怎么回事以及该怎么做。本说明书不想再对原版Conversations用户照顾太多了。

“注册失败”

它的可能性很多，因为没有将服务器反馈的失败原因显示给用户。新手面对此情景时，更换一个服务器来注册常常是最便捷的解决办法。

可能有以下原因：

- XMPP身份号码长得荒唐或包含不支持的字符。
- 输入的验证码错误。
- XMPP身份号码已被占用。
- 密码太弱。
- 服务器要求填写的注册表单含有Conversations不支持的元素。
- 服务器只支持在网页端注册，或只支持邀请制注册，或者已经停止接受注册。
- 服务器异常。

无法发送OMEMO加密消息

对新手而言，如果是新添加的联系地址，没有任何历史消息，那就先发送无主动加密的消息，看看是否出错；如果出错，查看反馈错误信息并据此排查原因。确定收信地址没错的话，再参考说明书附录对OMEMO的介绍。

如果确定OMEMO加密本应该正常，但就是无法获取OMEMO密钥，请试着关闭此对话项，并在联系人列表中重新打开。

“你被封禁了”

除了“会议室的房主或管家禁止了用户进入会议室”这种确实如此的情况以外，以下情况会导致出现这个错误的反馈信息：

你在一个你并没有创建会议室权限的群聊服务器上试图加入一个不存在的会议室。这个意思通常是说：你在按照一个错误的会议室地址试图加入。

有的会议室已经解散了，但是用户当时不在场，没有收到解散操作时发送的通知，后来查看时就会这么显示。此情景的本意应当是：“此会议室不存在，且你在此服务器上没有创建会议室的权限，因此无法和此地址联系”。

可能是创建会议室失败。这可能是设置的门牌号码的问题。一般来说，门牌号码对字符的支持可能性次序为：小写英文字母、数字>汉字等非ASCII字符>“-”、“_”等各种符号，对大写字母完全不支持。

服务器的群聊服务器不可用。有的服务器提供群聊服务器地址，但却是坏的，不能用。创建会议室后会到对话界面并显示这种错误的反馈信息。Conversations于此创建一个公开频道时，尽管会自动发现并填写群聊服务器地址，但是下一步会直接进入群聊界面并显示“你被封禁了”，并附带一个短暂的浮动通知说“你加入了一个已经存在的频道”后消失。信息会发送失败，错误信息反馈为“Conference room does not exist”。（在这种情况下试图在此服务器上创建私密群聊会有浮动通知反馈“创建群聊失败”。）你可以通过查看你使用的服务器里有没有露天会议室来判断群聊服务器的可用性。

“远程服务器超时”/远程服务器超时未作出正确的响应。

对面服务器拒绝连接时，如果有服务器自定义的反馈信息的话，Conversations是不显示

的。例如，对面服务器因你使用的服务器的TLS证书有问题而拒绝连接时，在Conversations端只会这么显示。

在上传文件时遇到 “open failed: EACCES (Permission denied)”

请换一个文件管理器软件来选择文件。或者更新你的Conversations版本。

不断显示 “需要密码才能进入该群聊”

输入正确的密码后仍然显示。这看起来是Conversations的一个程序设计差错。可以关闭对话框，再重新打开。

不断显示 “联系人请求在线状态订阅”

如果即使在你开始分享在线状态后，对话界面还是一直显示对方请求共享在线状态的提醒；那么这说明对方曾经请求过共享在线状态，但是后来又取消了（拒收共享在线状态），因此无法成功共享在线状态。这算是Conversations的一个程序设计差错。

获取历史消息时缺失消息

Conversations有个特别的程序设计。如果有一个会议室，距离你上一次进入已经很久了，于是有特别多你还没有获取的历史存档消息。当你再次进入会议室时，你就会一次获取很多历史消息，但Conversations把数量限制在了最早的750条；不过可以离开会议室后重新加入来再继续获取750条。但如果你在你获取历史消息的过程中，会议室里有人发送了一条新信息，那么获取历史消息的进程会立刻被打断，且无法再继续获取那些缺失的历史消息。除非清空此会议室本地存储的历史消息记录，然后可以手动回翻来重新获取服务器的存档消息。所以，如果使用此用户端软件，且你很在意自己存档某个会议室里的消息，请考虑随时留在会议室里，不要错过太多消息。

关于原版的说明

特别概念

Conversations有两个特别的概念：“公开频道”和“私密群聊”。“公开频道”指的是露天+敞门+大桌的会议室；“私密群聊”在创建按钮上指的是地下+锁门+小桌的会议室，然而在识别已有的会议室时，只要不是锁门+小桌，就被视为“公开频道”。Conversations对二者有区别地对待，例如无法复制“私密群聊”的XMPP地址，只能照着会议室地址簿里显示的手打。例如给用户的调整选项不同。

“Free”版和“Play Store”版的区别

你可以简单地把它们理解成“免费版”和“自愿付费版”。本说明书建议使用“免费版”，也以此作指导说明。“自愿付费版”算是给开发者和运营者的捐助形式的一种。它们区别如下：

- “Free”版独立地运行，不需要依赖其它应用软件。“Play Store”版则和资本主义公司“Google”的“Play Store”服务有关联，只有用户的操作系统内置了“Play Store”的组件，并能连接到这个互联网服务，并进行付费操作，才能发挥这个版本的独特效用。
- “Free”版的通知信息由自己生成。而“Play Store”版的通知消息则可以由“Google”服务和组件负责。同时因此它们的通知设计和设置方式并不同，这还和Android系统版本有关，也许你会讨厌“Google”组件的通知设计，也许你会喜欢。至于“Google”这个服务的有效性、服务策略及其变化的可能性等问题，问“Google”，我们不对此负责，也无法对此负责。
- 在“Play Store”版上使用非Conversations推荐的其它XMPP服务器时，你用的XMPP服务器是否能和专门负责推送通知服务器正常连接，就得你自己去确定了。如果你选择一个不支持对外推送通知的XMPP服务器（不支持XEP-0198和XEP-0357），你就无法收到“Google”组件的通知消息。
- 购买了“Play Store”版后，你将能通过“Google”服务和组件获得自动更新软件版本的服务，并可以获取测试版Conversations。
- 由于“Google Play Store”那鬼怪般的软件发布服务策略，开发者被迫为自愿付费版删除了查找露天会议室的功能。

很复杂，是吧？如果你想避免这些麻烦，“Free”版是很好的选择。如果你对“Play Store”版很感兴趣，并想了解更多，那么本介绍对你而言很可能不够准确，你应该自己去试一试，我们不对“Play Store”版负责。

Gajim介绍



Gajim的徽标

Gajim是用于Microsoft Windows操作系统上的XMPP用户端软件，功能丰富，用于日常使用。

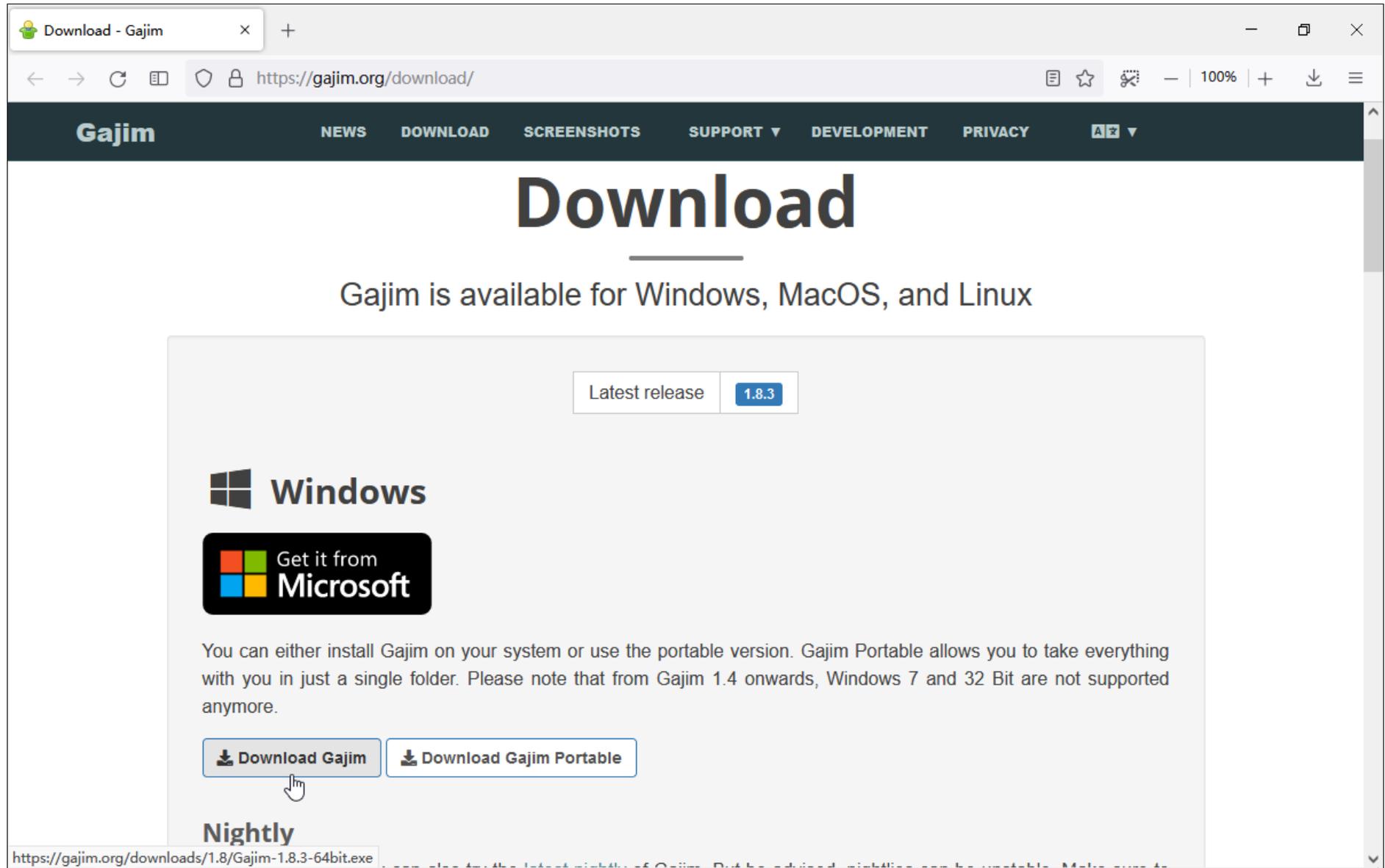
一些属性：

- 一些命运是由Python及Python官方决定的。最后支持Microsoft Windows 7的版本是1.7.3。请使用Microsoft Windows 10，不应该再用7或更老的版本了。
- 依赖更新，有些旧版本程序差错较多。请随时更新，不要使用旧版本。
- 截至1.8.3版本时，音视频通话功能已经废弃很久了。请使用Dino来补充此功能。
- 因GTK界面的原因，在收到大量超长的垃圾信息攻击时会卡死，无法抵御。
- 它只会请求获取英文的会议室设置表单，不过这在一定程度上是好事。不会遇到错误翻译。
- 在群聊里，当有人的OMEMO密钥无法获取时，Gajim会直接忽视它，而不告诉你没能获取谁的密钥。
- Gajim拒绝使用TLS证书过期的公共服务器。个人签名的证书可以手动信任，过期了的话仍然不行。

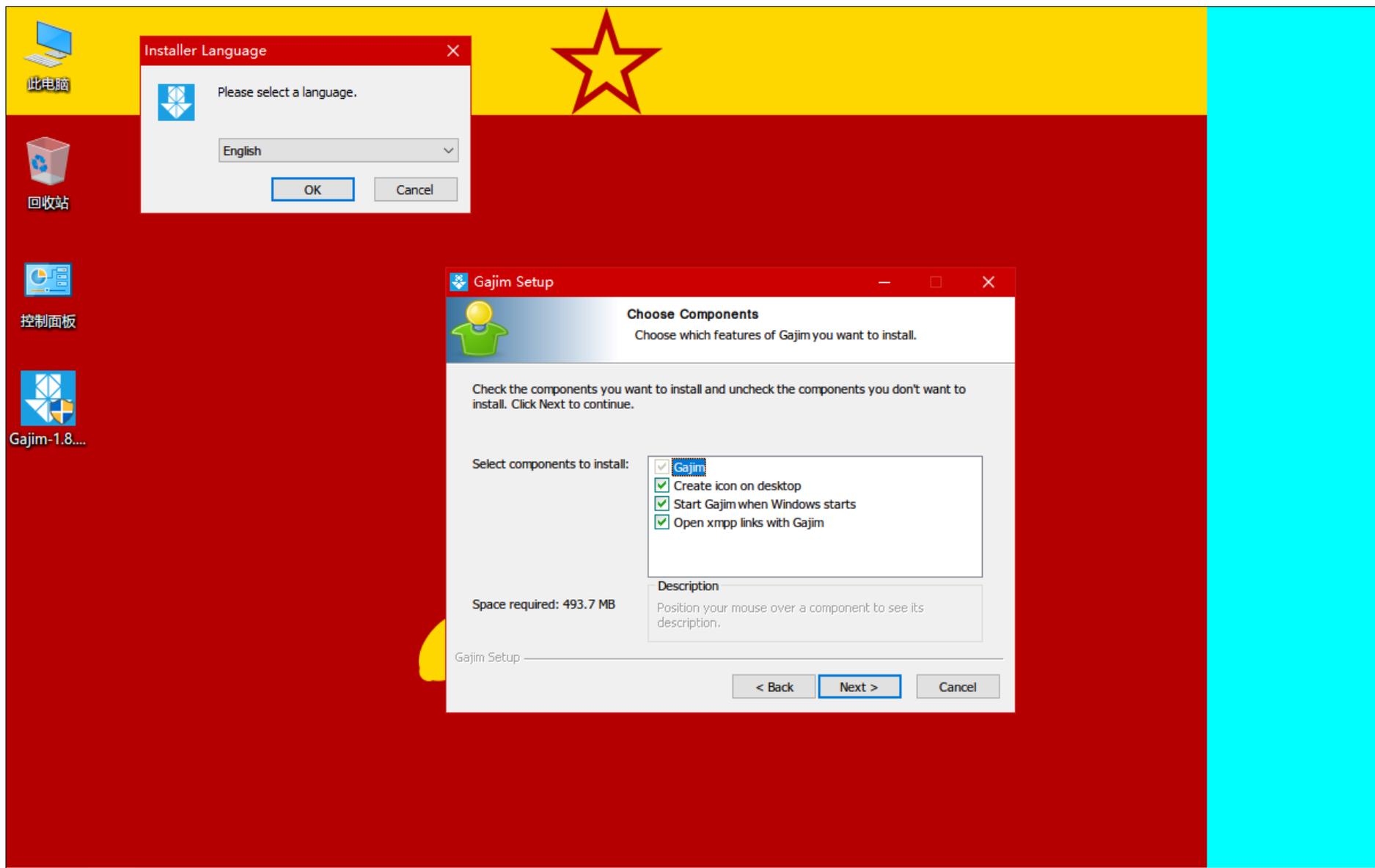
本Gajim章演示使用的版本号是1.8.3。

下载与安装

打开网页浏览器，访问此网址：“<https://gajim.org/download/>”。如下图。



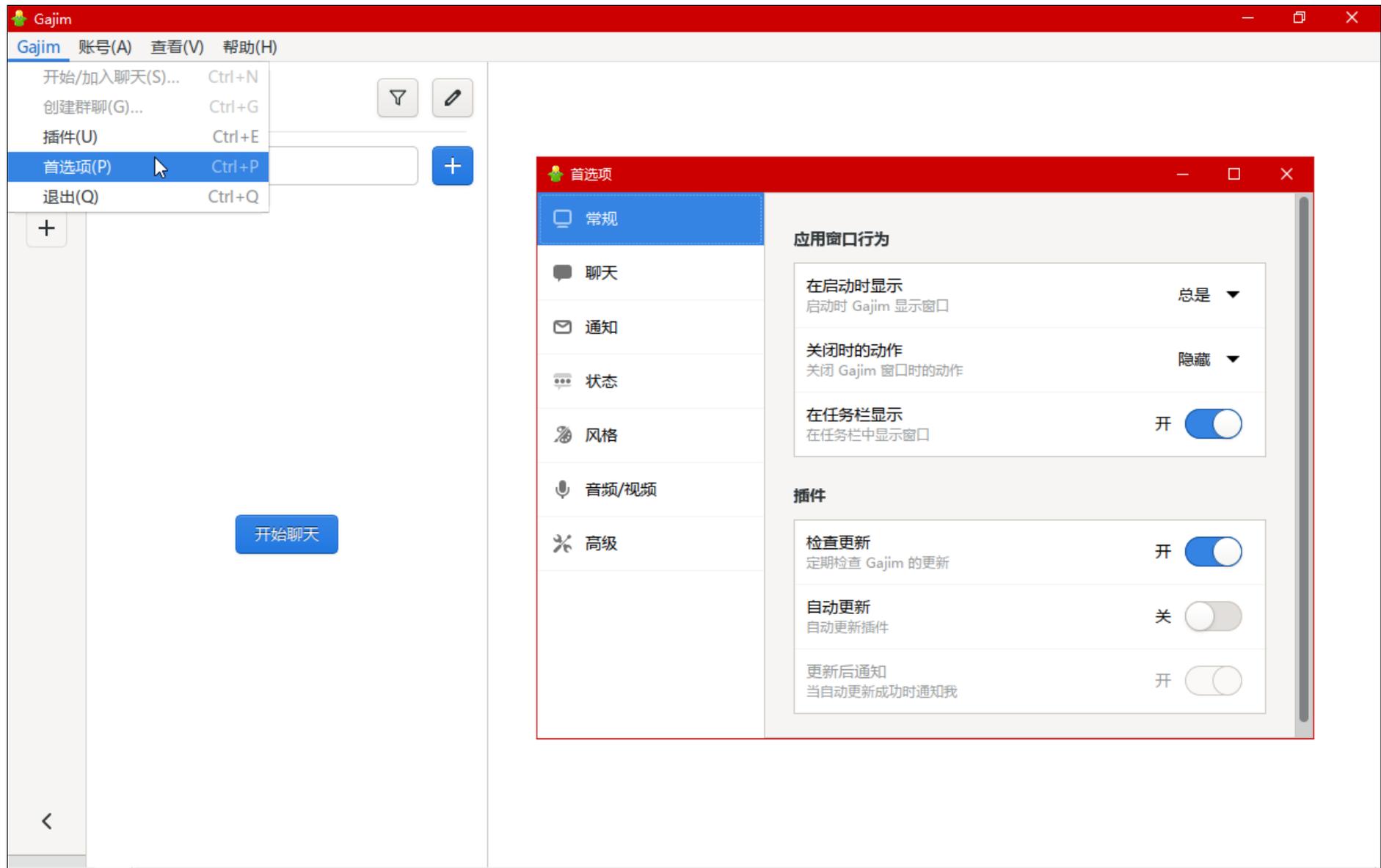
点击“Download Gajim”按钮就可以下载一个最新版本的离线安装包。



软件本身有汉语翻译，只有安装界面没有汉语，选择英文就好。

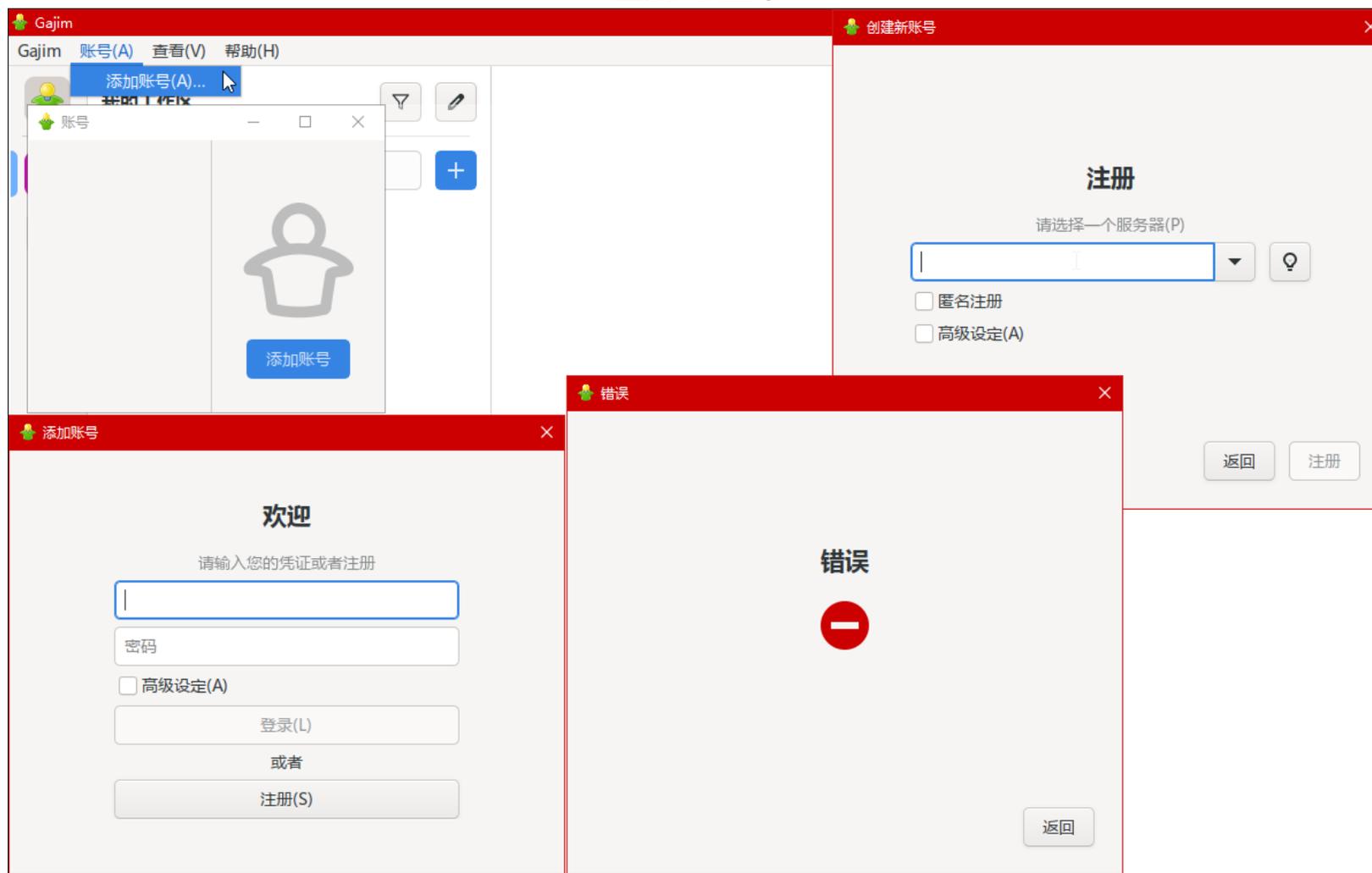
你可以一路点击“Next”按钮直至安装。也可以沿途选择是否添加桌面快捷方式，是否让它开机自己启动，是否在让系统关联XMPP链接到Gajim，以及安装到哪个位置。

通用设置



这是通用设置界面。建议调整的设置是：拼写检查 \times ；消息回执 \checkmark ；直接消息（在私人群聊中偏好直接消息） \times ；显示话题 \times 。插件没有什么需要下载的。有的附加组件年久失修，却没有移除。

注册与登录



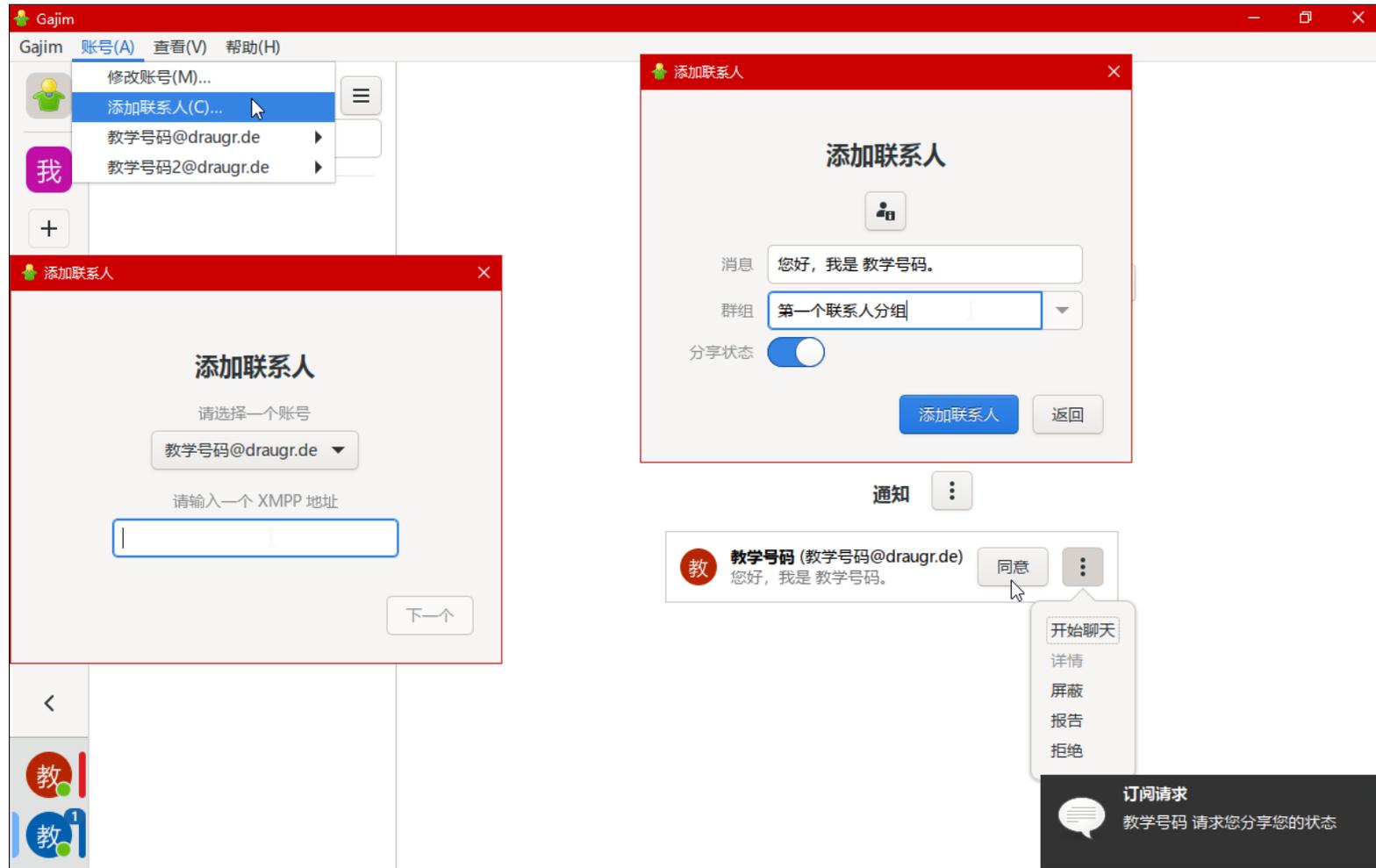
不要“匿名注册”，不要“高级设定”。原因已经在前面的章节说过了。

注册时提供的服务器地址列表对我们而言没什么参考意义。

你有可能遇见完全没有任何反馈信息的错误，这应该是Gajim的程序差错，而不是服务器的差错，请连续重试直到成功，或者换用另一个客户端软件“Dino”。

如果你添加的XMPP身份号码里含有Microsoft Windows不允许文件名里出现的字符（例如“?”），那么Gajim就会因此崩溃。

添加联系人

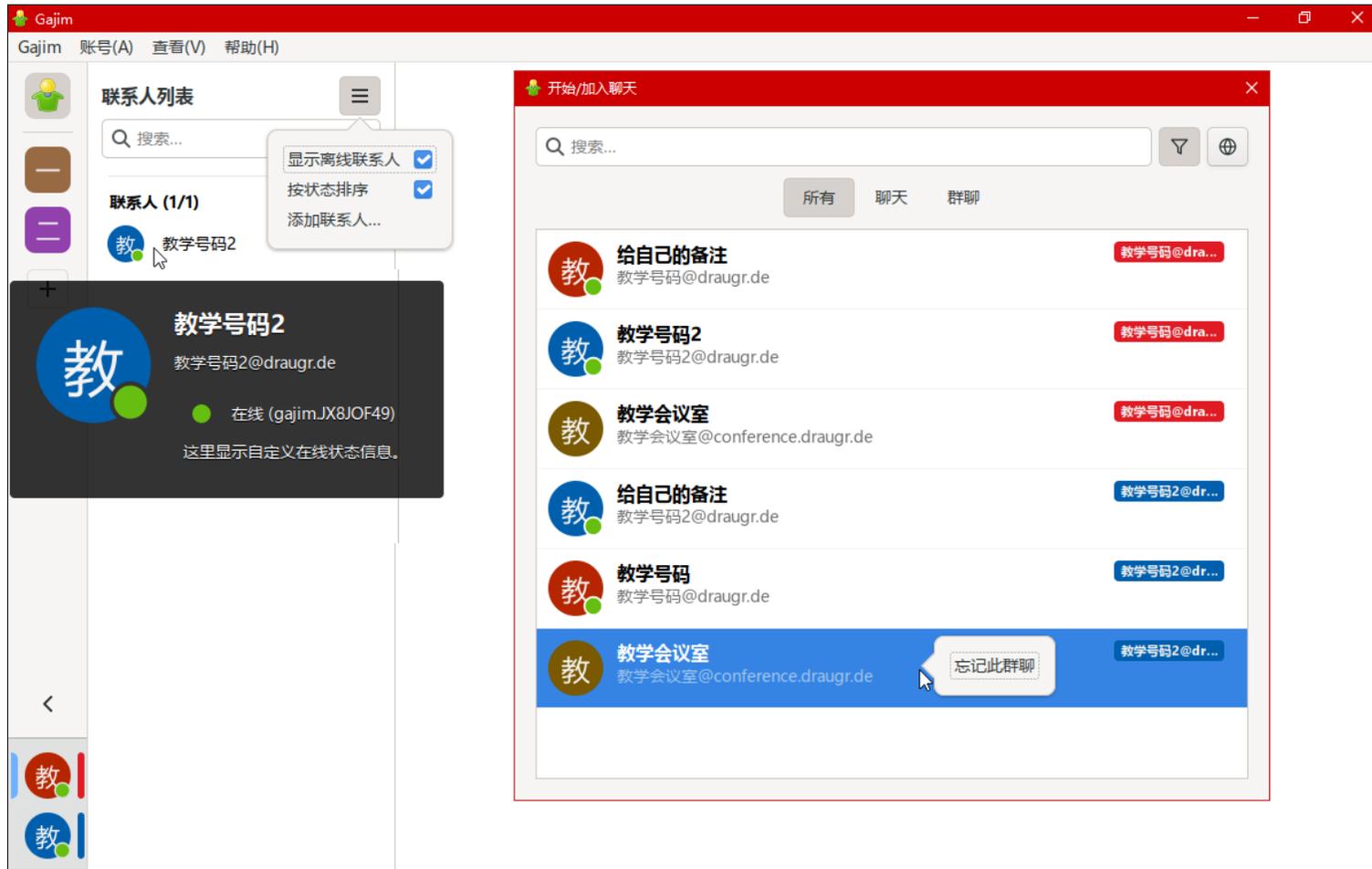


在左下角点击选择XMPP身份可以进入XMPP身份界面，XMPP身份界面的左栏是联系人列表，右栏是基础信息、设置按钮、在线状态、常驻通知。

要添加联系人，可以通过导航栏，也可以通过联系人列表上方的选单按钮。添加联系人时，可以顺着添加联系人的请求一起发送过去一条消息，同时选择一个联系人分组（要新建一个分组，就直接填写分组名）。对方收到请求后会出现右下角的弹出通知，以及常驻通知。

Gajim的通知不是通过Windows通知系统来发送的，所以你只能在Gajim中调整通知。如果你不想弹出通知遮挡屏幕内容，那么你可以在通用设置里关闭显示通知，这不会关闭通知音效。

开启对话项

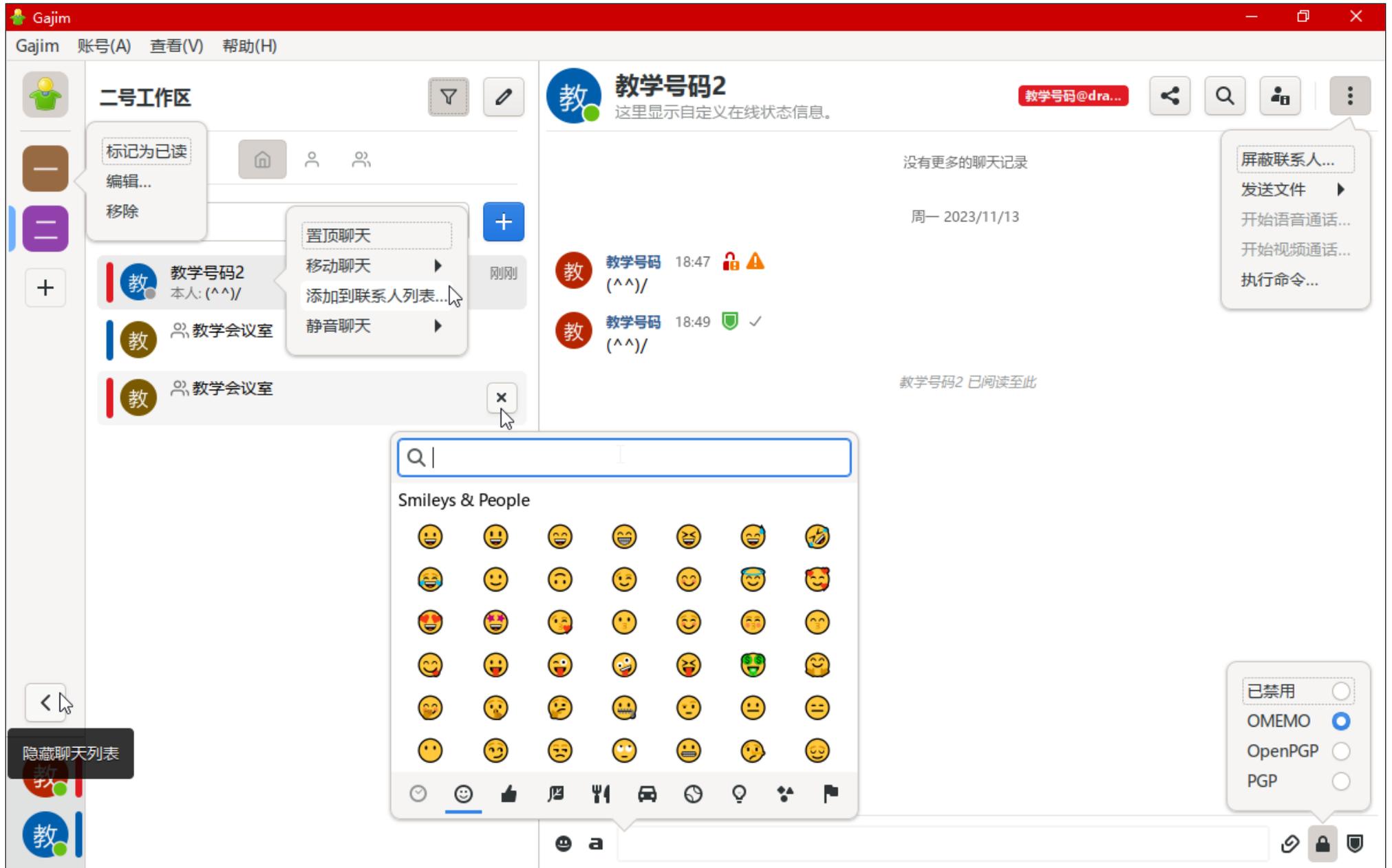


要开启一个对话项。你可以在联系人列表里双击联系人，以及在导航栏选择“Gajim”→“开始/加入聊天”。右侧的XMPP地址是对应的操作选项所属的XMPP身份，也是执行操作所用的XMPP身份。联系地址的排序优先级是：所属的本地XMPP身份>联系人和会议室之分>联系地址的名称。右键单击会议室选项可以在个人地图中删除此记录，同时Gajim会离开此会议室并删除本地存储的对应消息记录。筛选功能提供的筛选项分为：所有、联系人、群聊。点击经纬线按钮会启用内置的第三方搜索引擎（见附录）来搜索。

对陌生人打开对话项时，Gajim不会自动发送添加联系人的请求。如果添加一个群聊地址，那么它会自动记录到个人地图里。当加入或退出一个会议室时，会同步修改个人地图里的“是否要在登录后自动加入”记号。

Gajim会先检查添加的联系地址的所属服务器是否能及时作出正确的回应，然后再决定是否添加。

对话界面



四个纵栏是从左到右的归属关系，在左边的栏可以打开右边的内容。

左上角的Gajim图标按钮所达的界面用来调整所有已经启用的虚拟用户的在线状态和自定义在线状态信息，以及接收Gajim的更新通知。

最左边侧栏中间部分是本用户端软件的本地分类功能（而不是XMPP标准的功能），叫作“工作区”，用户可以自己将不同的对话项拖动到不同工作区的图标以把它们分开。点击笔形按钮，或者右键单击工作区图标选择“编辑”，可以修改工作区的名字、徽标、代表颜色。

左数第二栏是已经打开的对话项中在当前工作区的部分。当启用多个XMPP身份时，各个项目会显示其所属的虚拟用户代表颜色，以便分辨归属关系。最左栏有个针对第二栏的展开收起按钮。

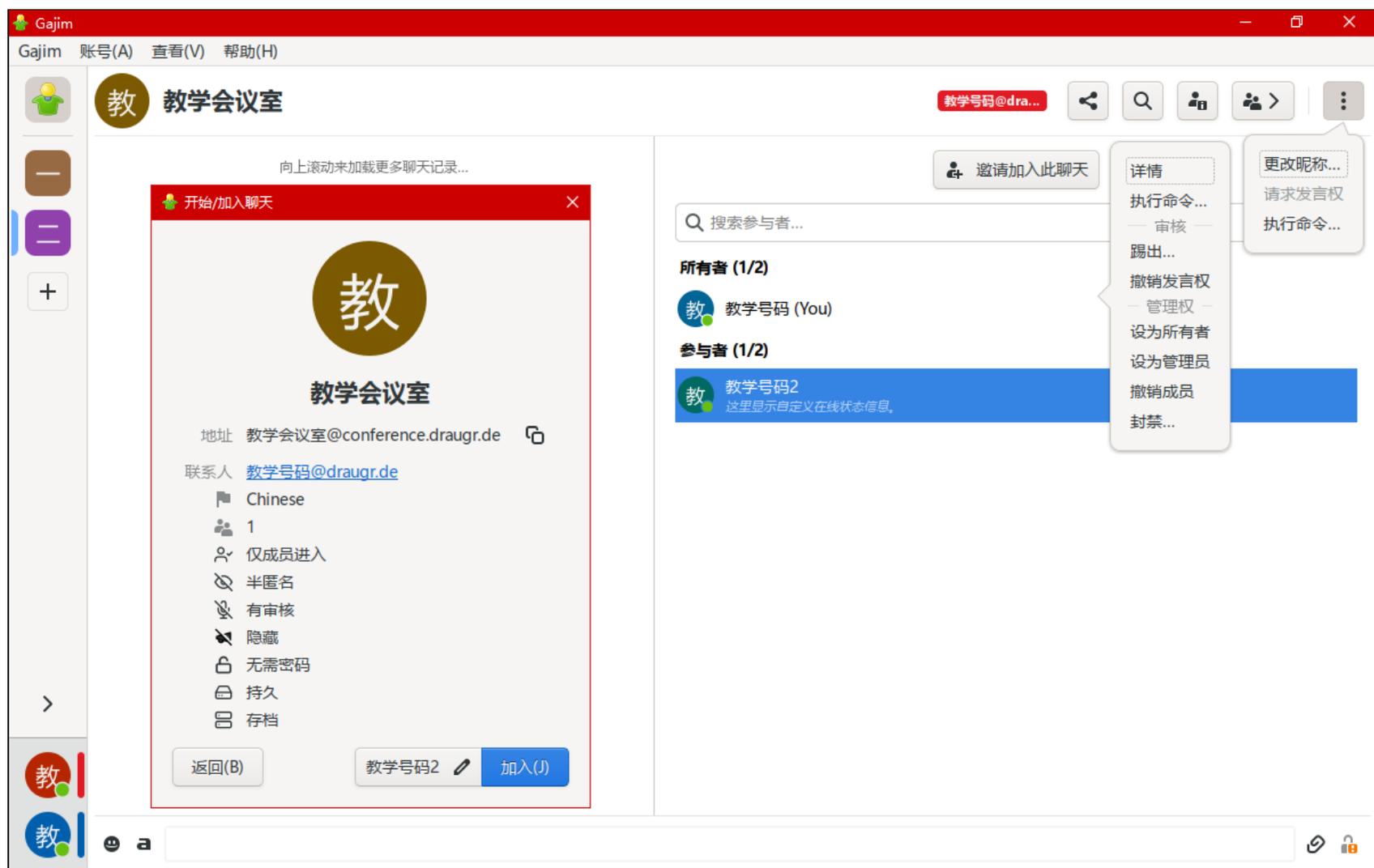
如果有哪个对话项不是联系人，你可以右键单击对应的对话项来添加联系人。

第三栏是对话界面。上方的按钮是“分享（联系地址）”、“搜索聊天记录”、“联系地址详情以及针对设置”、“更多选单”。

发送失败的消息会出现感叹号标识，将光标移动到警告感叹号标识上会告诉你反馈错误信息。红色的空锁图标表示没有主动加密，绿色盾牌图标表示有主动加密。打勾表示收到了用户回执。

对话界面的下方是表情符号（输入英文单词以搜索）、格式化显示文字、发送信息的文字输入框、发送文件、主动加密选项（OMEMO已经集成，其它的需要下载安装插件）、主动加密具体配置（启用主动加密后才会有）。

点击第三栏的放大镜按钮启用第四栏的聊天记录搜索，可以按照日期筛选，也可以扩大搜索范围至包括其它联系人和群聊的全部记录。



在加入会议室之前，Gajim会先向你呈现会议室的属性信息，在这里选择加入时的占座名时也会同步修改个人地图里记录的默认占座名。群聊对话界面上方有在场人员列表的展开收起按钮。右键单击室内人员可以进行管理。不过这个选项框的来源指向会错位。

Gajim将室内私信作为单独的对话选项，而不和室内公开消息放在一起，在对话选项的名称后面会添加括号并写入会议室的名称以表达它是个室内私信通道。于在场人员列表里双击人员会打开室内私信对话项，如果要使用普通私信，请使用对方的XMPP地址来开启一个新的对话项。

在会议室对话界面里点击右上角的三点按钮可以临时修改室内网名，而不会同步修改到个人地图里。

XMPP身份选项

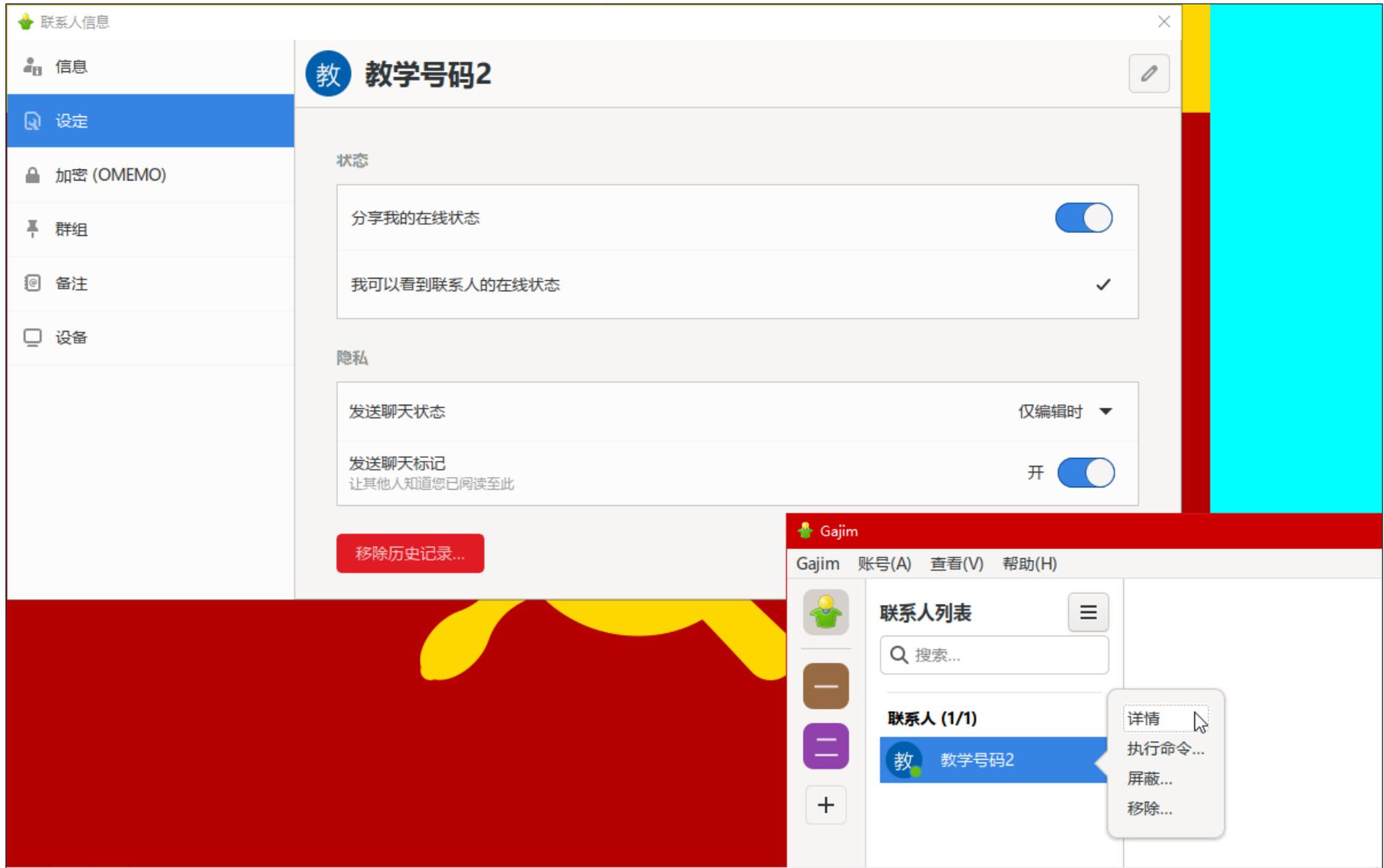


要按照服务器地址查找服务内容，那么就在“账号”选单里，选择要用来查询的XMPP身份→“寻找服务...”，你就可以看到你的服务器提供的服务项的地址了。手动更改地址可以查询其它公共服务器的内容。双击群聊服务项就可以查看服务器上的露天会议室列表。Gajim在浏览群聊服务器的露天会议室列表时有展示上的程序差错；而且执行确认操作时会不经进一步获取并显示会议室信息地直接加入会议室，要小心。

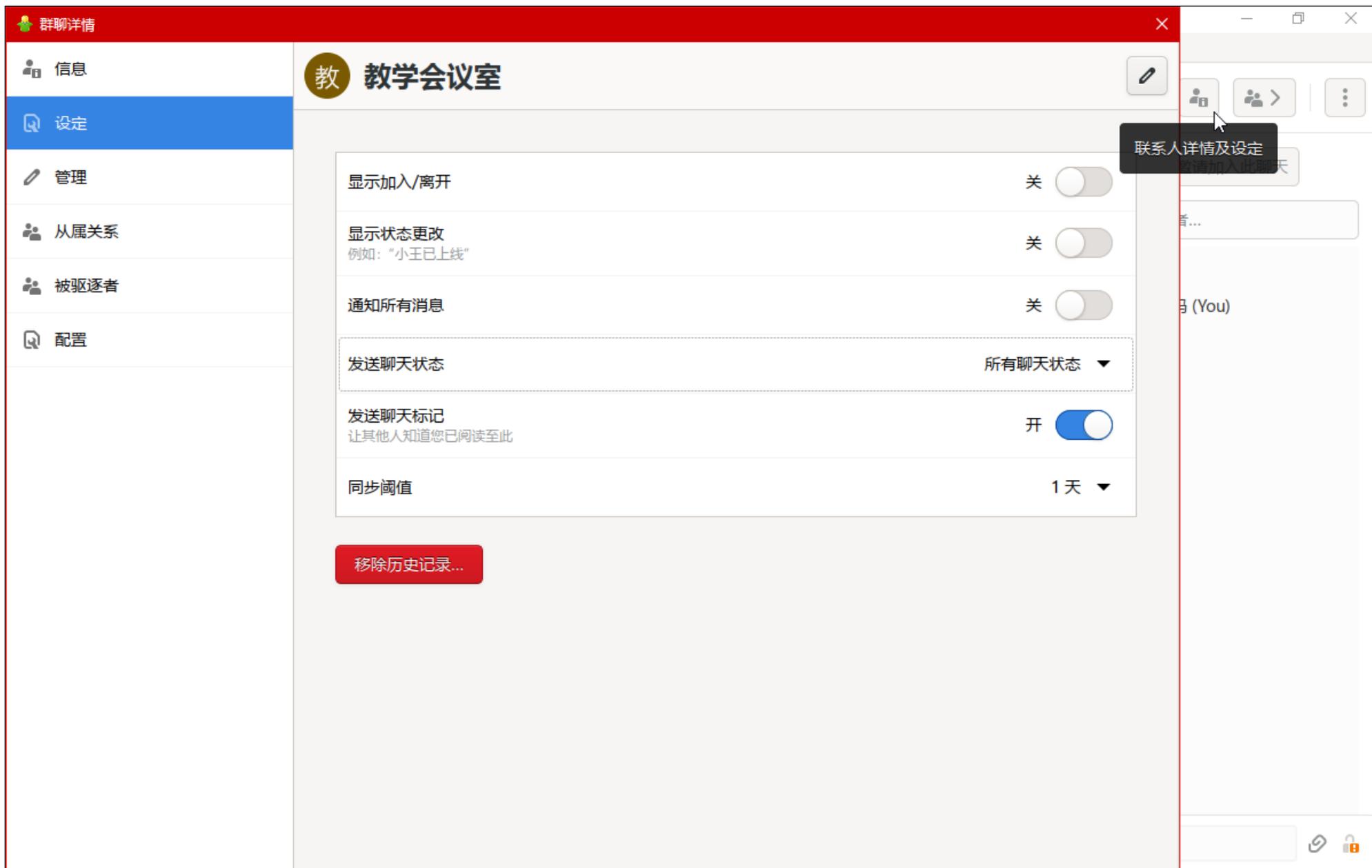
选择“个人资料”就可以编辑你的电子名片，修改通用网名和虚拟肖像，以及内容的可见性。

点击“修改账号”或工具图标就可以对XMPP身份调整各自独立的设置。有些设置在其它地方。

联系地址设置



联系人详细信息页也可以在联系人列表里打开，在这里可以编辑备注名，共享在线状态，决定是否发送编辑状态和回执，调整所属分组，查看备注信息，查看对方的在线登录点信息。



在会议室详细信息页里可以编辑备注名，查看会议室属性信息，调整一些基本的聊天选项。左栏的后四项全部是会议室设置，如果你有权限的话就能用。

疑难解答

程序上的问题

- 如果你的互联网连接不稳定，Gajim可能会出现假在线现象：此时你的在线状态不为离线，但获取不了新消息，也手动调整在线状态也无响应。只能关闭再重开。请不要使用不稳定的代理网络连接。
- 如果创建会议室Gajim误认为你没有调整会议室设置的权限，请重新加入。
- 在室内私信被禁用的会议室里发送私信时可能不会收到“室内私信被禁用”的反馈错误信息，这是Gajim的程序差错。

重置

软件数据保存位置为“C:\Users\你的系统用户名\AppData\Roaming\Gajim”。如果你找不到“AppData”文件夹，请在文件管理器中设置“显示隐藏的项目”，或者手动输入它到访问路径里。如果你在使用过程中遇到了完全无法使用的崩溃问题，你可以考虑把数据库删除或挪走，以重置Gajim。

（添加联系地址时）“该地址不可达”

这等于“远程服务器超时”，参考通用章节的“使用中可能出现的问题”。

怎么关闭进入系统桌面时自动启动？

Gajim软件本身没有这个设置，而是由系统设置决定的。要取消的话，请打开任务管理器，到“启动”标签页，禁用Gajim。

Psi介绍



Psi的徽标 Psi+的徽标

Psi是可用于Microsoft Windows端和Mac OS端的XMPP客户端软件。Psi+是它的开发版。

如果只是用于一般交流，且你使用Microsoft Windows 10，那么Gajim是更好的选择。但针对一些Gajim所没有可是为我们所需的功能，以及程序差错，我们需要Psi(+)来作补充。

使用Psi的原因有：

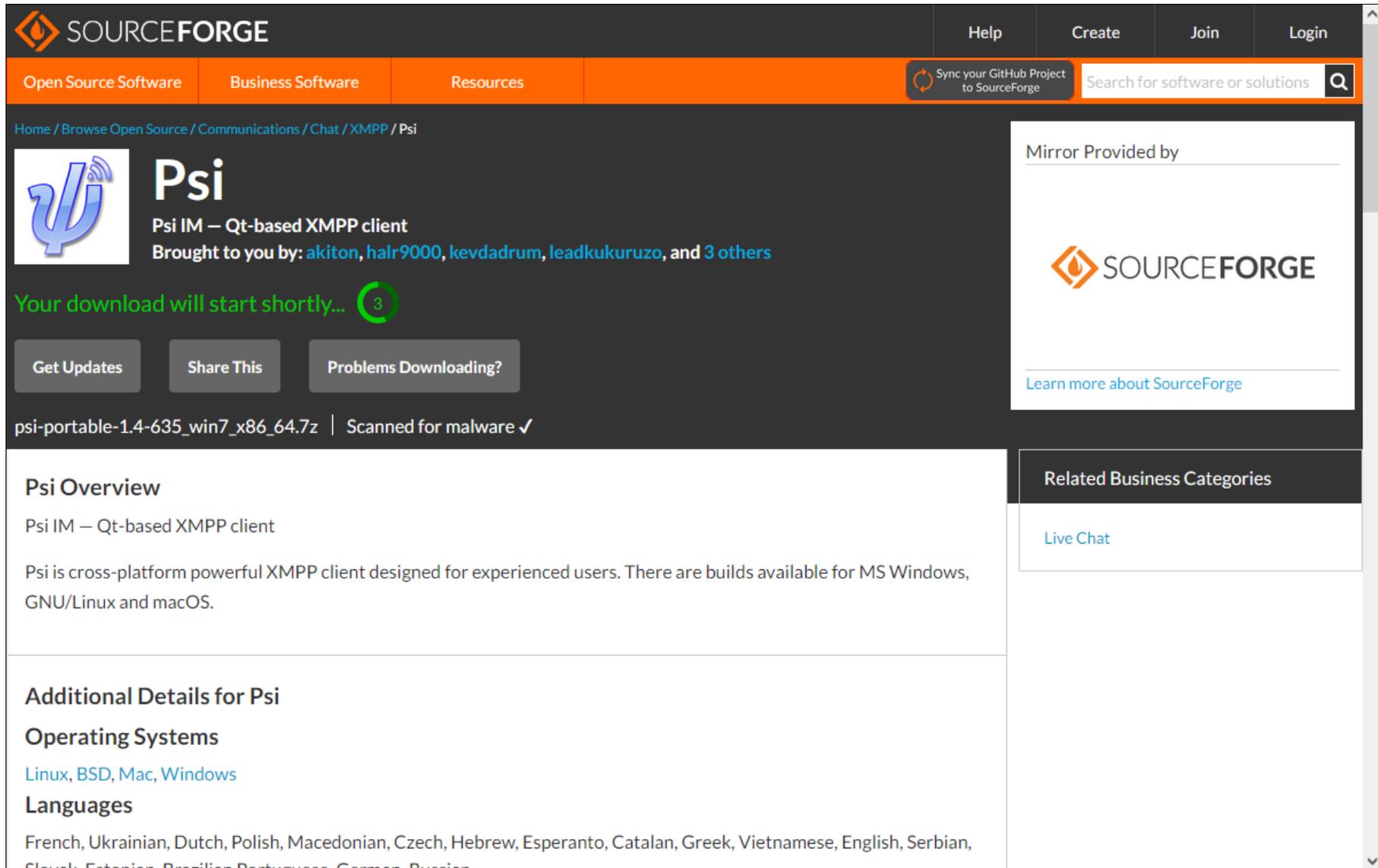
- 它支持很有用的XEP-0016功能。而Gajim于1.2.1版本移除了此功能。这是我们推荐它一个重要原因。
- Gajim对计算性能和处理器的利用率都很低，容易卡死。而Psi作为C++开发的软件，它在面对冗长的垃圾信息攻击时不会卡顿，可以处理这种紧急情况。
- 它会请求获取汉语翻译的会议室设置；而Gajim只会请求获取英文的。
- 它对调整人员的管理等级和参与等级有完备的支持。Gajim则不支持单独设置“主持”这一参与等级。
- 它可以在会议室里直接看到别人都在使用什么客户端软件，而Gajim不支持。这一特点对XMPP指导员很有用。如果你想创建只欢迎一种客户端软件的用户参与交流的会议室的话，它也有用。
- 可以通过查询电子名片来获取人们的最后在线时间。如果你想大量删除弃用了XMPP的联系人，这会有用。
- 有了Psi：如果你是Microsoft Windows 7 × 64的用户，你不会只能用老旧的且程序差错多的Gajim 1.7.3；如果你是Microsoft Windows XP用户或Microsoft Windows 7 × 32用户，你还可以比较顺利地用上XMPP！不过，如果你还在用Microsoft Windows 7，那么你真的该换Microsoft Windows 10 × 64了，让技术员同志给你安装一个省心的简洁版吧。

它们的开发已经近乎停滞了，因此维护不够良好，有些历史遗留问题。我们不得不推荐特定的版本，而不建议下载使用官方网站上的版本。我们为Windows 7用户和Windows XP用户推荐一个Psi 1.4的版本，为Windows 10用户推荐一个Psi+ 1.5的版本。Psi 1.4适合在Windows 7和Windows XP系统上运行，在Windows 10上运行容易崩溃。Psi+ 1.5版本在发送图片上有严重的程序差错，所以更不能用于日常交流了。

本章在Windows 10系统上使用Psi来演示（这和Psi+有些许不同），在实际使用中不必这么做。

下载与安装

请Microsoft Windows用户直接在以下链接中按照系统版本来选择下载：[Windows XP用户](#)、[Windows 7 ×32](#)、[Windows 7 ×64](#)、[Windows 10 ×32](#)、[Windows 10 ×64](#)。



SOURCEFORGE Help Create Join Login

Open Source Software Business Software Resources

Sync your GitHub Project to SourceForge Search for software or solutions

Home / Browse Open Source / Communications / Chat / XMPP / Psi

 **Psi**
Psi IM — Qt-based XMPP client
Brought to you by: [akiton](#), [hair9000](#), [kevdadrum](#), [leadkukuruzo](#), and 3 others

Your download will start shortly... 3

Get Updates Share This Problems Downloading?

psi-portable-1.4-635_win7_x86_64.7z | Scanned for malware ✓

Psi Overview
Psi IM — Qt-based XMPP client
Psi is cross-platform powerful XMPP client designed for experienced users. There are builds available for MS Windows, GNU/Linux and macOS.

Additional Details for Psi
Operating Systems
[Linux](#), [BSD](#), [Mac](#), [Windows](#)
Languages
French, Ukrainian, Dutch, Polish, Macedonian, Czech, Hebrew, Esperanto, Catalan, Greek, Vietnamese, English, Serbian, Slovak, Estonian, Brazilian Portuguese, German, Russian

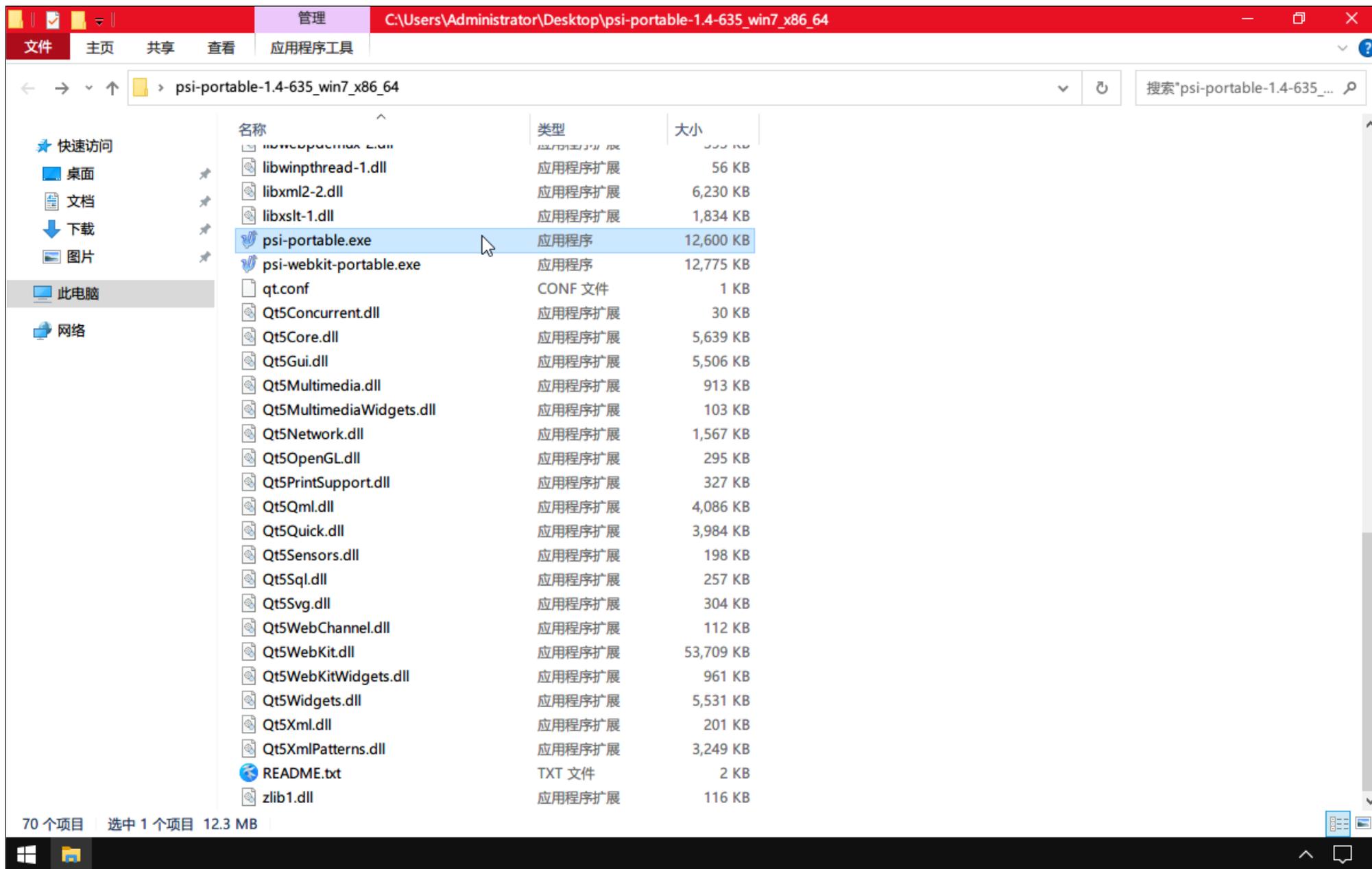
Mirror Provided by

 SOURCEFORGE

[Learn more about SourceForge](#)

Related Business Categories
[Live Chat](#)

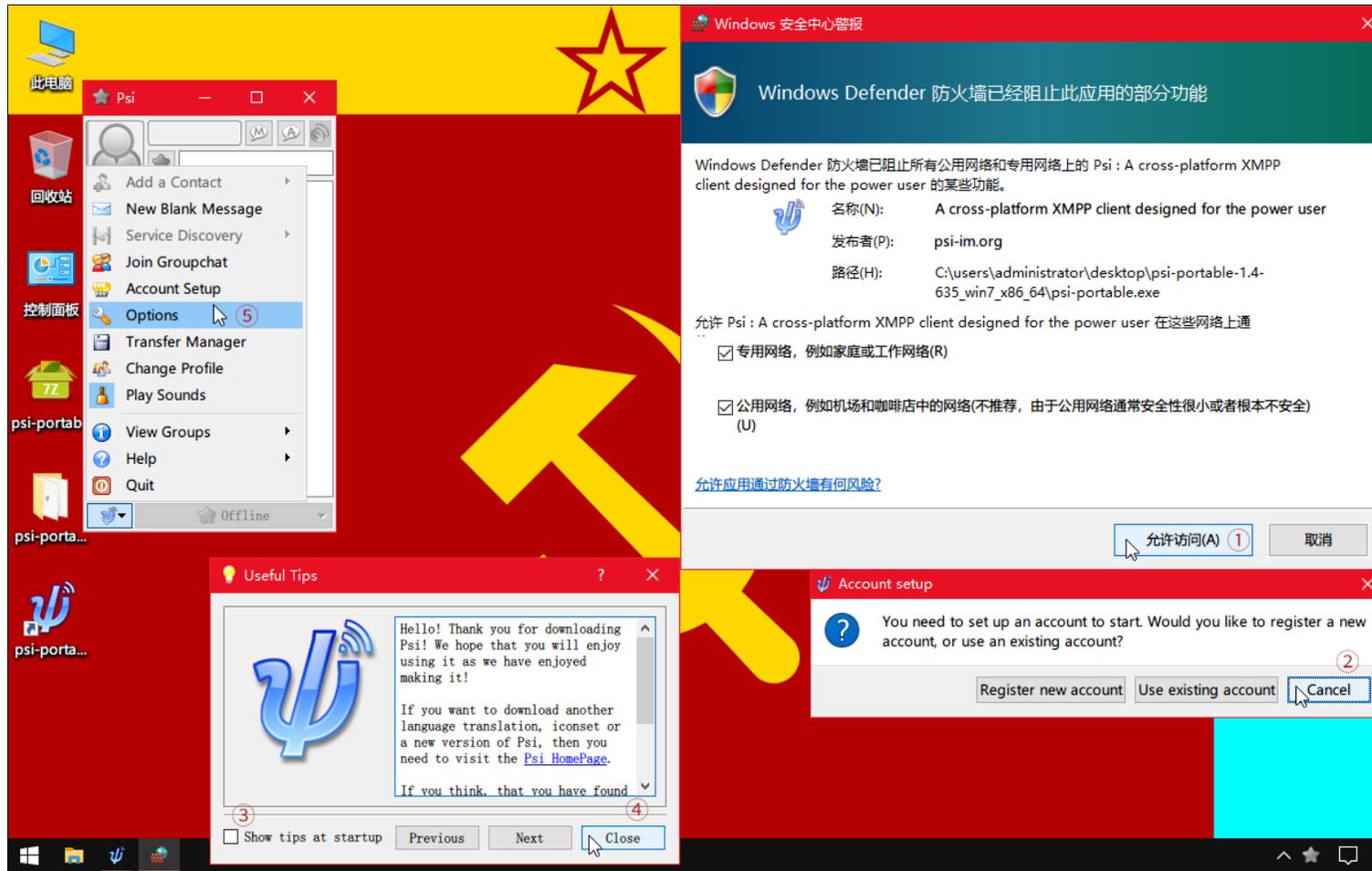
等待五秒后会开始下载。如果下载速度慢，你可以使用代理网络连接，或者向其它同志索要安装包。



针对Psi，解压到你想要安装到的位置，启动“psi-portable.exe”即可。针对Psi+，请不要选择安装“Web Engine”项，此项无法使用输入法软件来打字。

设置

启动“psi-portable.exe”。

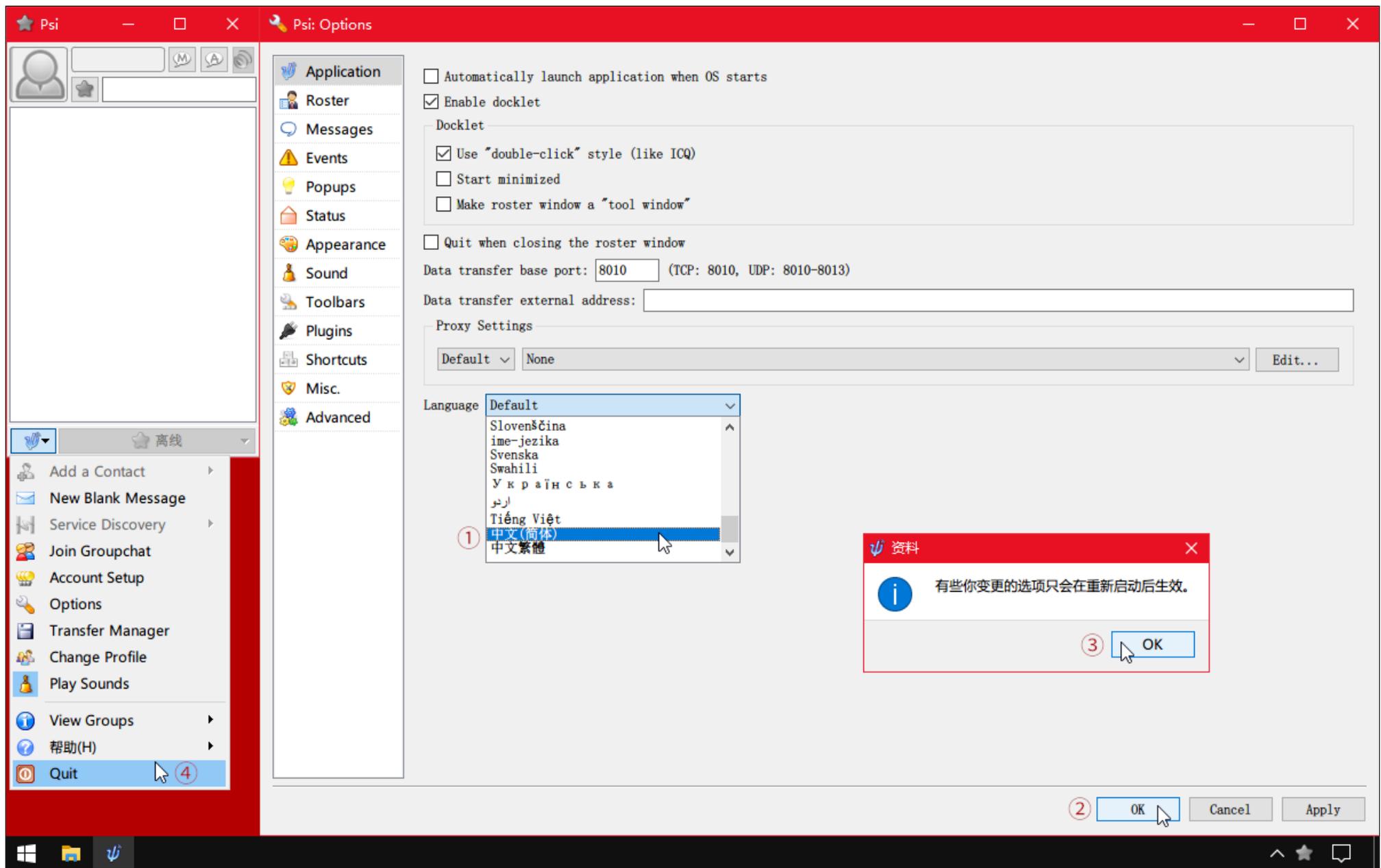


关于是否让Windows Defender防火墙允许它访问局域网的问题。请将两者都勾选，点击“允许访问”。

“Account setup”对话框提醒你注册或登录一个号码。而我们得先设置界面语言。直接关闭，点击“Cancel”或“X”叉号。

“Useful Tips”是零散提醒，它没什么用。取消勾选“Show tips at startup”来禁止在启动Psi的时候显示它，再点击“Close”或“X”叉号。

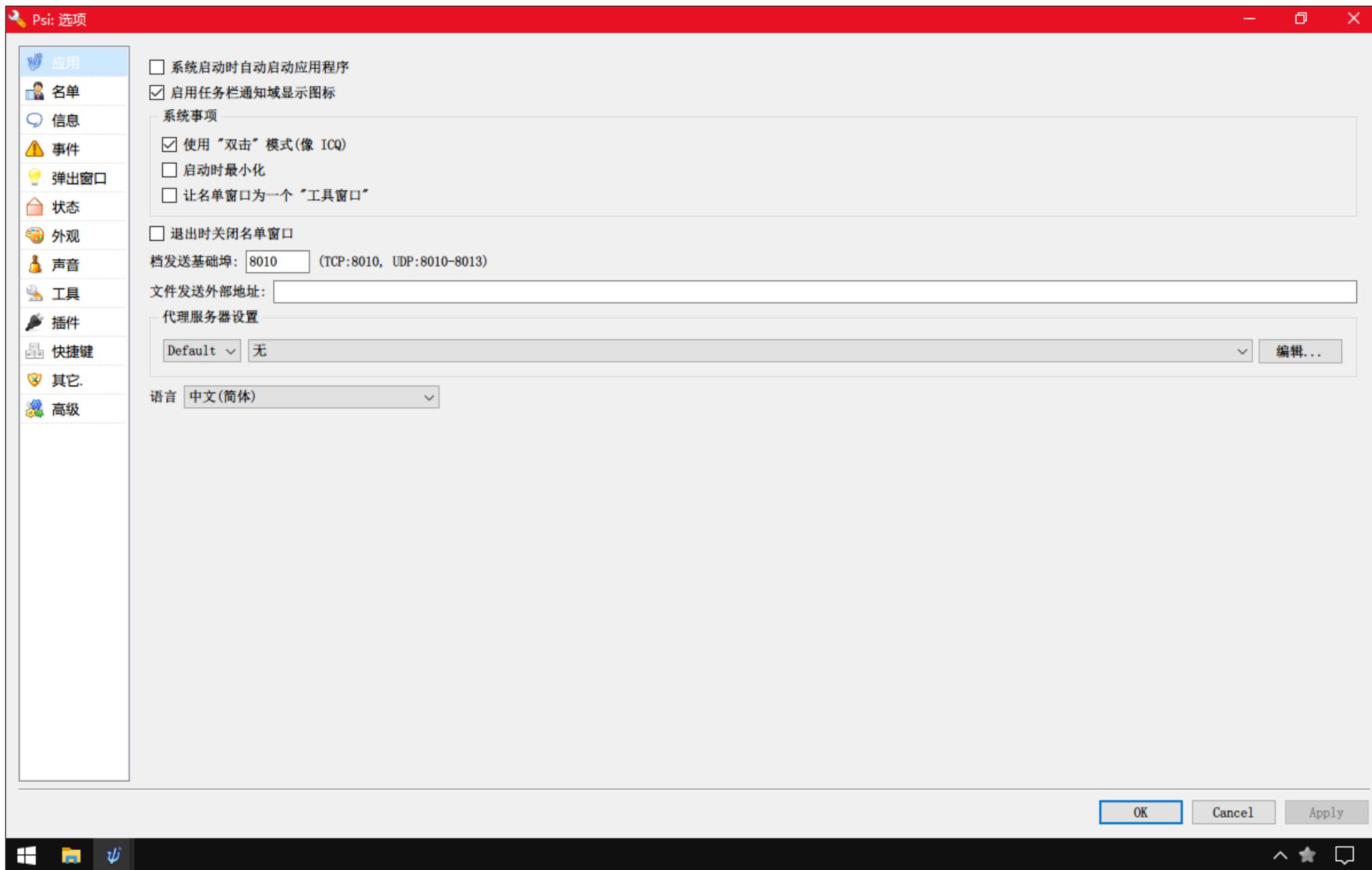
到主窗口左下角的按钮打开选单，点击“Options”，开始设置语言。



在“Application”类，选择“Language”选项为“中文(简体)”。再依次点击两个“OK”按钮。到主选单点击“Quit”选项退出。等待几秒，重新打开Psi。



又是虚拟身份号码设置提醒，再次关闭，点击“Cancel”或“x”叉号。在主选单中选择“选项”。我们得先进行一些设置，它才能变得好用。



设置界面概览 (EPUB版里为连环动图)

建议的设置如下。

名单：

- 花名册：×禁用滚动；√客户（端）：所有客户端图示
- 群聊：×禁用滚动；√头像

信息：

- Common：√使用卷标模式：根据自己的兴趣设置吧。一般说来，如果你喜欢同时看多个窗口的话，选择“使对话和MUC分开”；如果你习惯整个屏幕就一个程序，选择“使MUC，聊天和名单在一个窗口”。
- 对话：删除对话窗口内容：从不
- 输入：×启用拼写检查

外观：你可以为界面设置你喜欢的字体。注意，不是所有人都喜欢阅读花哨的字体，花哨的字体不利于截图分享。同时，只有黑白分明的点阵字体有最好的显示效果，其它的都显示得不好看。如果你想改善其它字体的显示效果，你应该安装一个叫作“MacType”的软件，但是我们尚没有在我们的网站写它的配置教程。

快捷键：联系人清单中的快捷键→打开对话与所选择的联系人。删除此快捷键。

插件：启用必要的“HTTP Upload Plugin”和“Image Preview Plugin”，不要启用“Image Plugin”。至于“OMEMO plugin”，要知道这个插件有问题，不是很好用：①收到一条加密消息后，自己会自动切换到加密模式；②一旦在加密模式下发送了文件，在重启Psi之前就不能再发送未加密的文件了；③对有些条件符合的联系人无法发送加密消息。所以建议不要启用。

除了“高级”标签页以外的，我们都设置完了，现在点击右下角的“Apply”，应用设置。

高级选项，双击对应选项的左侧可以直接更改是否（“true”，译为“真”，为“是”；“false”，译为“假”，为“否”）：options.muc.show-joins: false（禁用在会议室里显示谁来了谁走了，因为会有太多这种信息干扰阅读消息。）

完毕，现在再次退出，并重新打开Psi。

注册

The screenshot illustrates the registration process in Psi XMPP client, with numbered annotations (1-9) highlighting key steps and elements:

- 1:** The 'Psi: 添加账号' (Psi: Add Account) dialog box, where the user selects '注册新账号' (Register New Account).
- 2:** The 'Psi: XMPP 账号' (Psi: XMPP Accounts) list, showing a table with columns for '名称' (Name), '服务器' (Server), and '状态' (Status).
- 3:** The '注册新账号' (Register New Account) checkbox in the 'Psi: 添加账号' dialog.
- 4:** The '添加(A)' (Add) button in the 'Psi: 添加账号' dialog.
- 5:** The 'draugr.de' server name entered in the '注册账号' (Register Account) dialog's server field.
- 6:** The '下一个(N)' (Next) button at the bottom of the '注册账号' dialog.
- 7:** The 'User:' field containing '教学号码' (Teaching Number) in the '注册账号' dialog.
- 8:** The '下一个(N)' (Next) button at the bottom of the '注册账号' dialog.
- 9:** The 'OK' button in the '成功' (Success) dialog box, indicating successful registration.

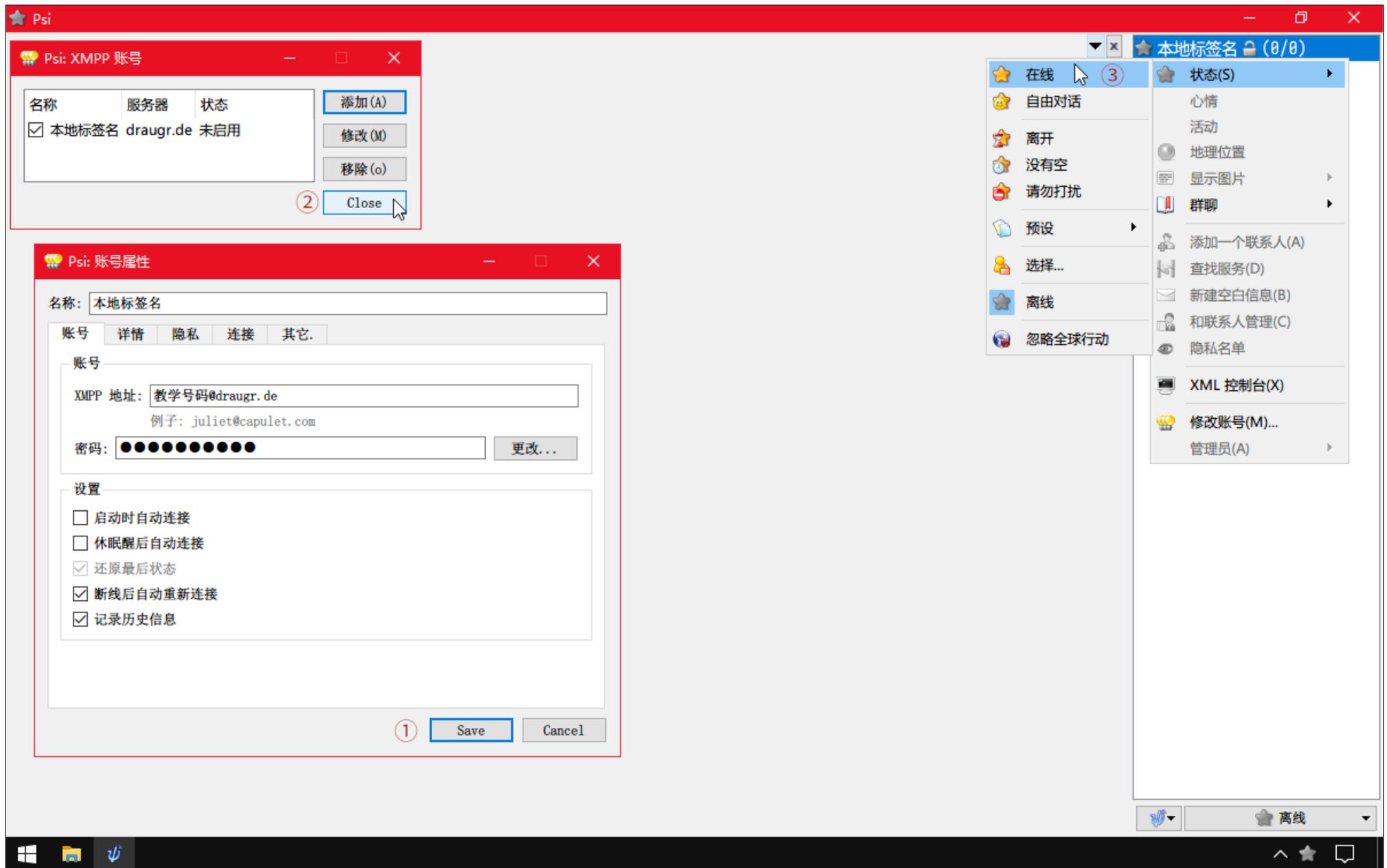
Additional elements shown include the '账号设置' (Account Settings) dialog, a '服务器错误' (Server Error) message, and the Psi main menu.

你可以直接点击自动弹出的“账号设置”对话框里的“注册新账号”或“使用现有的账号”，也可以从头开始操作。

1. 在主选单中选择“账号设置”。
2. 进入本地的XMPP身份管理窗口。点击“添加”。
3. “Psi:添加账号”窗口里的“名称”只是在本地软件给你自己看的，用于在同时使用多个号码时分辨哪一个。如果你要注册一个新的号码，那么就要勾选“注册新账号”，否则下一步就是登录操作。
4. 输入要注册号码的服务器地址。（现在你可以看到翻译差错了，“下一个”实际上应为“下一步”。）
5. 输入你要使用的XMPP身份号码和密码、验证码。
6. 注册成功。（图中附带了一个服务器因嫌用户操作太慢而停止接待注册的错误信息。）

如果你要向服务器请求修改登录密码的话，Psi(+)可能会有问题，考虑用其它用户端软件来修改。

登录



除了XMPP地址和密码以外，不需要其它设置。点击“Save”来保存。关闭XMPP身份管理窗口。

在主窗口右键单击你的本地标签名，调整状态为“在线”。

底下的按钮也可以用来上线，不过那是全局上线，会让所有启用的XMPP身份都上线。

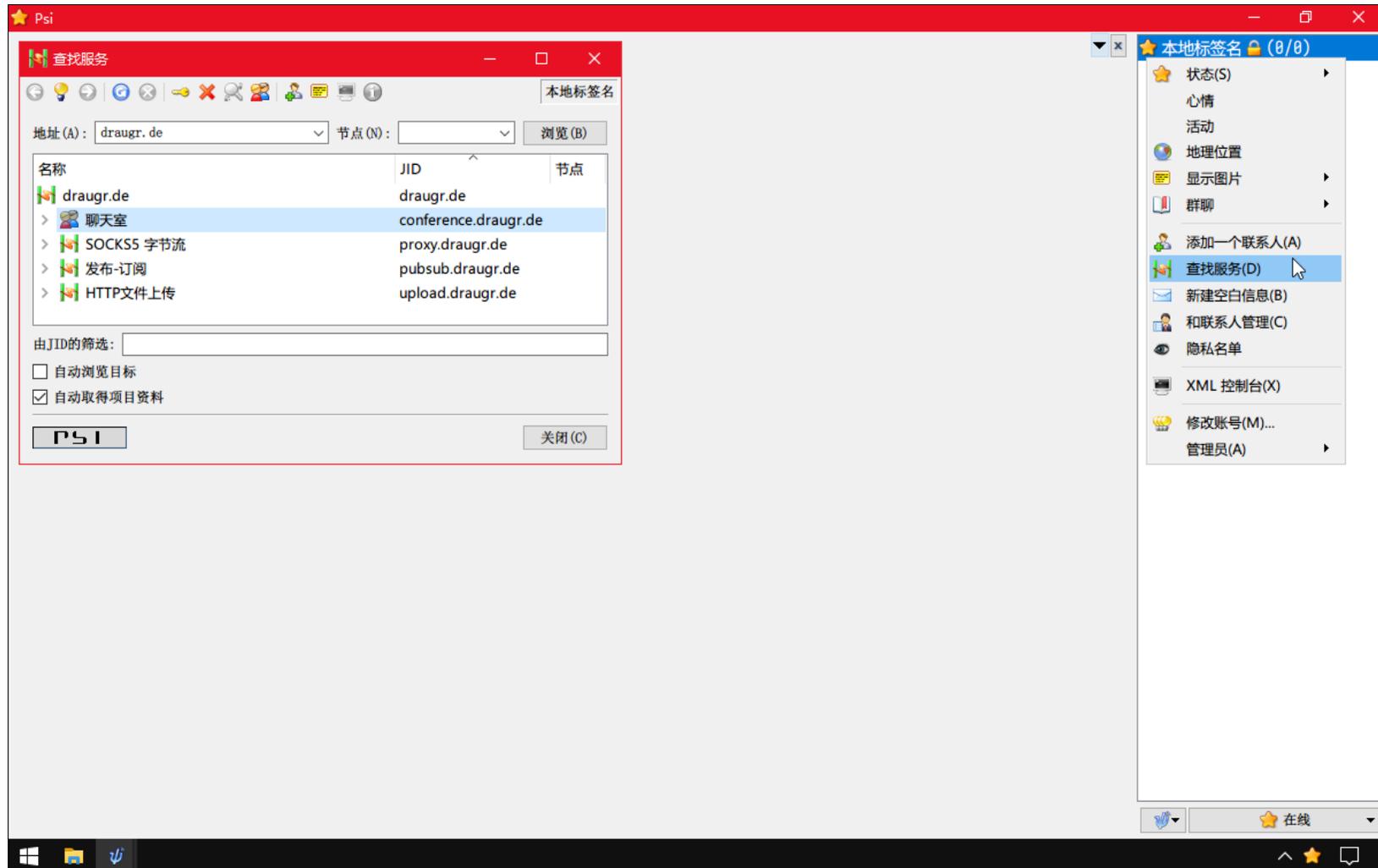
Psi+在新添加的虚拟用户第一次登录后的自动加入会议室时会出现问题，自动批量加入会议室操作会是加入同一个会议室。退出Psi+后重新打开并上线，以后就不会有这个问题。

如果你是使用已有的号码来登录，那么，在登录操作后，请等待它获取联系人信息和加入个人地图里设置了自动加入的的会议室。当Psi(+)批量加入会议室时进行操作容易导致它崩溃退出。如果你不想自动加入所有会议室的话，可以在高级设置里将“options.muc.bookmarks.auto-join”设为“false”，禁用Psi每次上线时自动加入会议室，省去这个过程。

如果登录密码填写错误了。请不要在登录失败后弹出的密码错误对话框里修改登录密码，这么做无效，这是个程序差错。请到设置界面的XMPP身份管理窗口里修改登录密码。

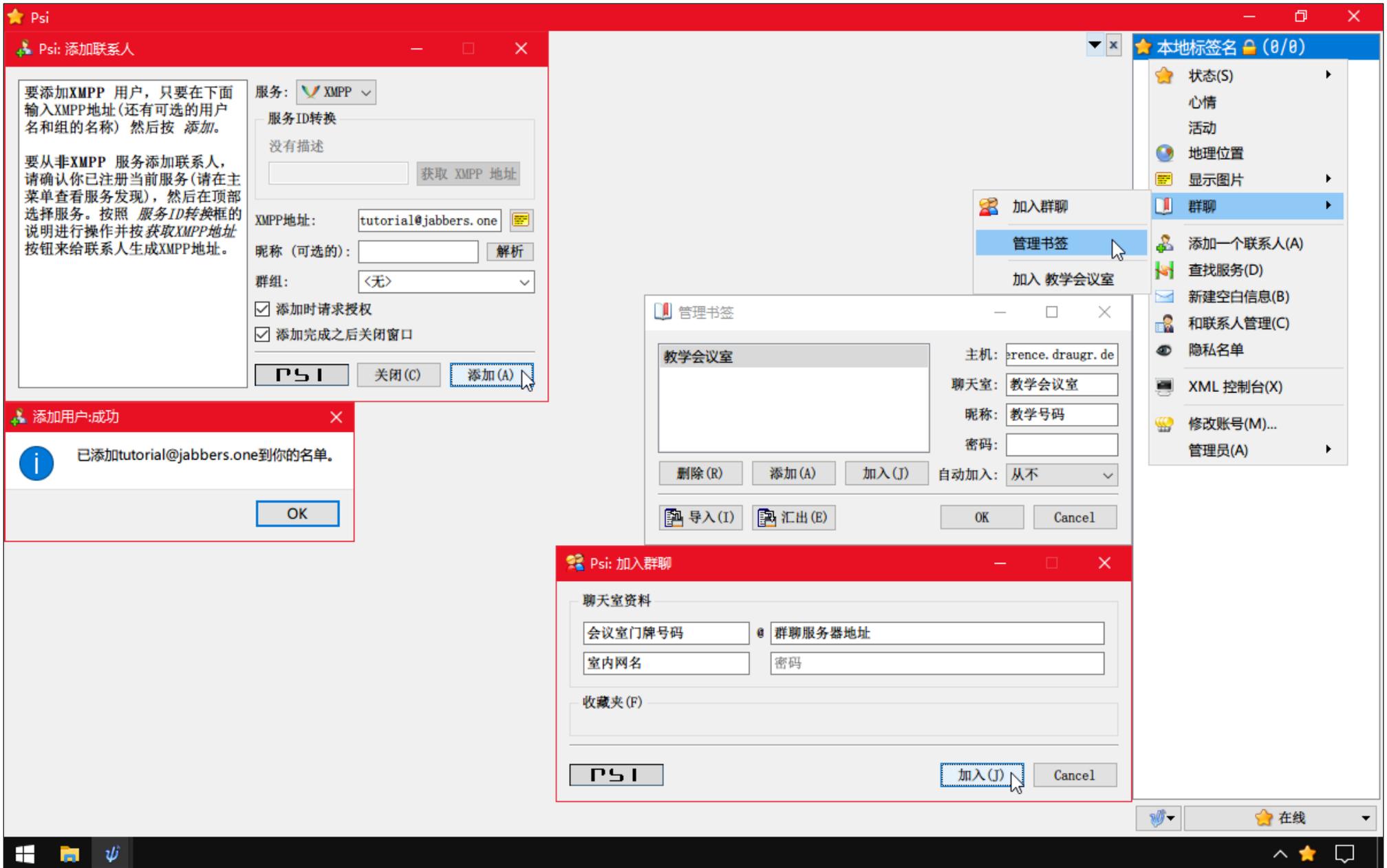
查找服务

加入会议室得知道群聊服务器的地址。使用“查找服务”功能可以找到不同服务器的不同服务的连接地址，可以让你找到你的服务器上都有哪些露天会议室，可以让你查询服务器软件信息。



注意小窗口左下角的“PSI”标识，你会在很多地方遇见它。如果Psi在执行什么正在等待服务器响应的操作，那么它会显示动画，据此可以判断操作执行情况。如果动画停止了却没有得到期望的结果，那么就是操作执行失败了。如果它长时间不停止，那么用户应当视为失败并停止执行此操作。

添加会议室和联系人



“群聊”选项的子选项有“加入群聊”和“管理书签”两个操作，剩下的都是加入你个人地图里的会议室加入选项（如果你已经有了记录的个人地图项目的話）。

要加入群聊，需要分开输入群聊服务器地址和会议室门牌号码，还有你要用的室内网名。至于密码，如果你要加入的会议室不需要密码，那么置空就好。

如果你要创建一个会议室，那么也是通过“加入群聊”操作，如果你输入的门牌号码不存在，那么就会自动创建这个会议室。留意新建的会议室的设置，你大概需要手动将会议室设置成砖屋。

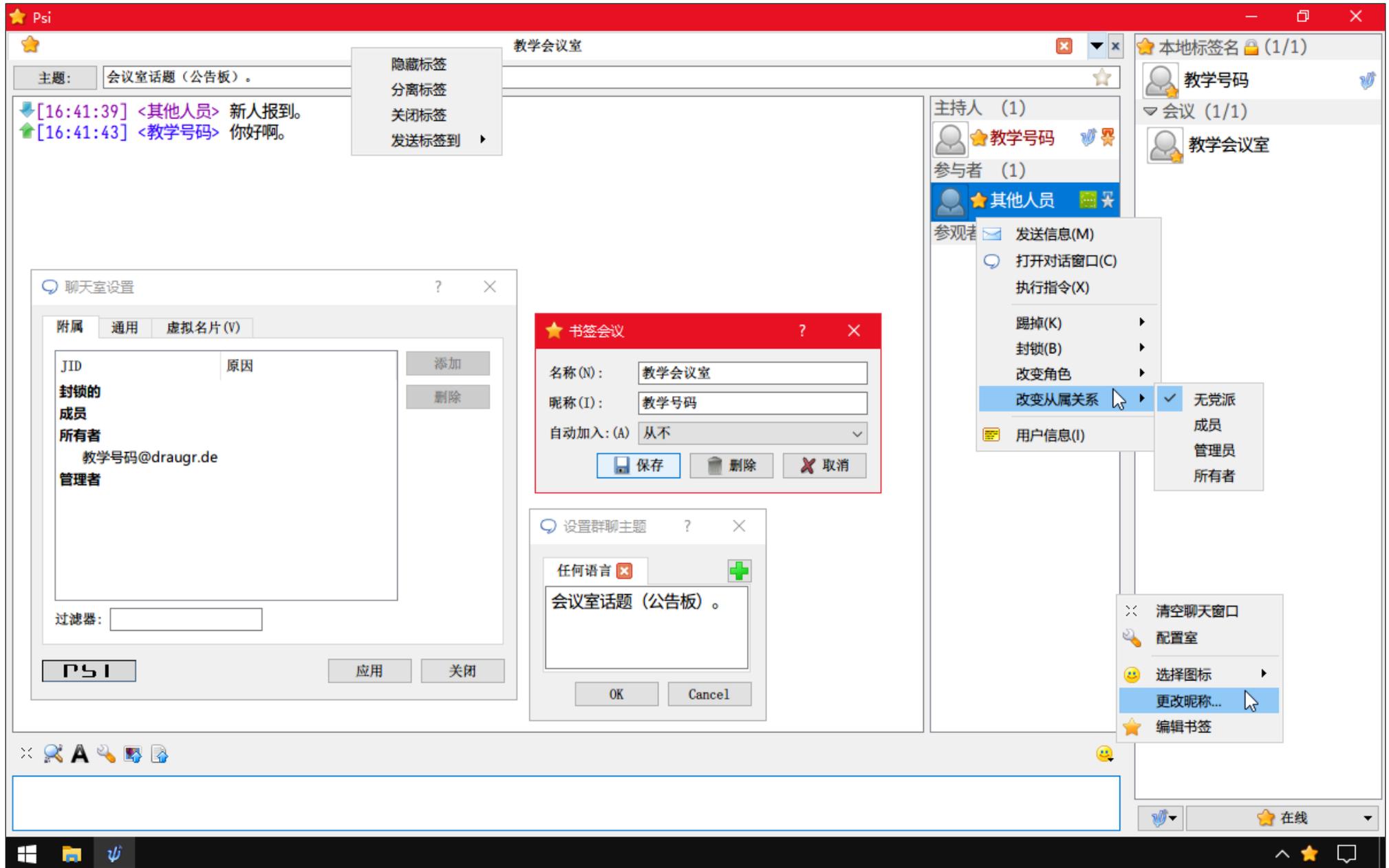
有时候个人地图里记录的会议室名称是空白，在“管理书签”窗口里双击就可以编辑显示名称。

要添加一个联系人，直接输入完整的XMPP地址。“添加时请求授权”意为请求对方给自己分享在线状态。当在联系人之间提到“授权”时，就是指分享在线状态。

在添加联系人之前，你可以点击电子名片图标按钮来获取对应地址的（旧版的）电子名片。

如果你使用Psi加入了一个隐藏了你在场状态的会议室，那么此时其它用户端软件再进入此会议室就会不正常。

会议室界面



图中左下角的按钮分别是：清除窗口消息、查找消息、设置字体格式、更改会议室设置（如果你是房主的话）、发送图片（必要启用的插件）、寄存文件（必要启用的插件，和前一个是同一个插件）。

在会议室设置里，点击“通用”标签可以获得的会议室的设置。

右下角的按钮用来添加表情符号，但选项不多。右键单击它就有更改室内网名的选项。

左上角的“主题:”按钮用来修改会议室公告板（话题），如果你有权限的话，就能修改成功。

左上角的五角星图标的明暗状态告诉你这个对话项是不是管用。如果是灰色的，那么就无法通信。灰色时，原因有各种，例如服务器掉线、你离线、联系地址错误……。

标签页中间是会议室的名称。调整标签页的位置选项里，“发送标签到”意为“合并标签到（某标签所在窗口）”。

标签页最右侧的叉号也是关闭当前会话项，关闭会议室的会话项会离开会议室。旁边的三角形图标按钮纵向展示已经打开的会话项，用于切换会话项。

主题栏右边的五角星为灰暗色时，意为此联系地址不在你的地址簿里，你可以点亮来添加它到个人地图。点亮后，再次点击可以编辑这个个人地图项。

如果你有权限，那么你可以对其它人员调整管理等级（“从属关系”）和参与等级（“角色”）。

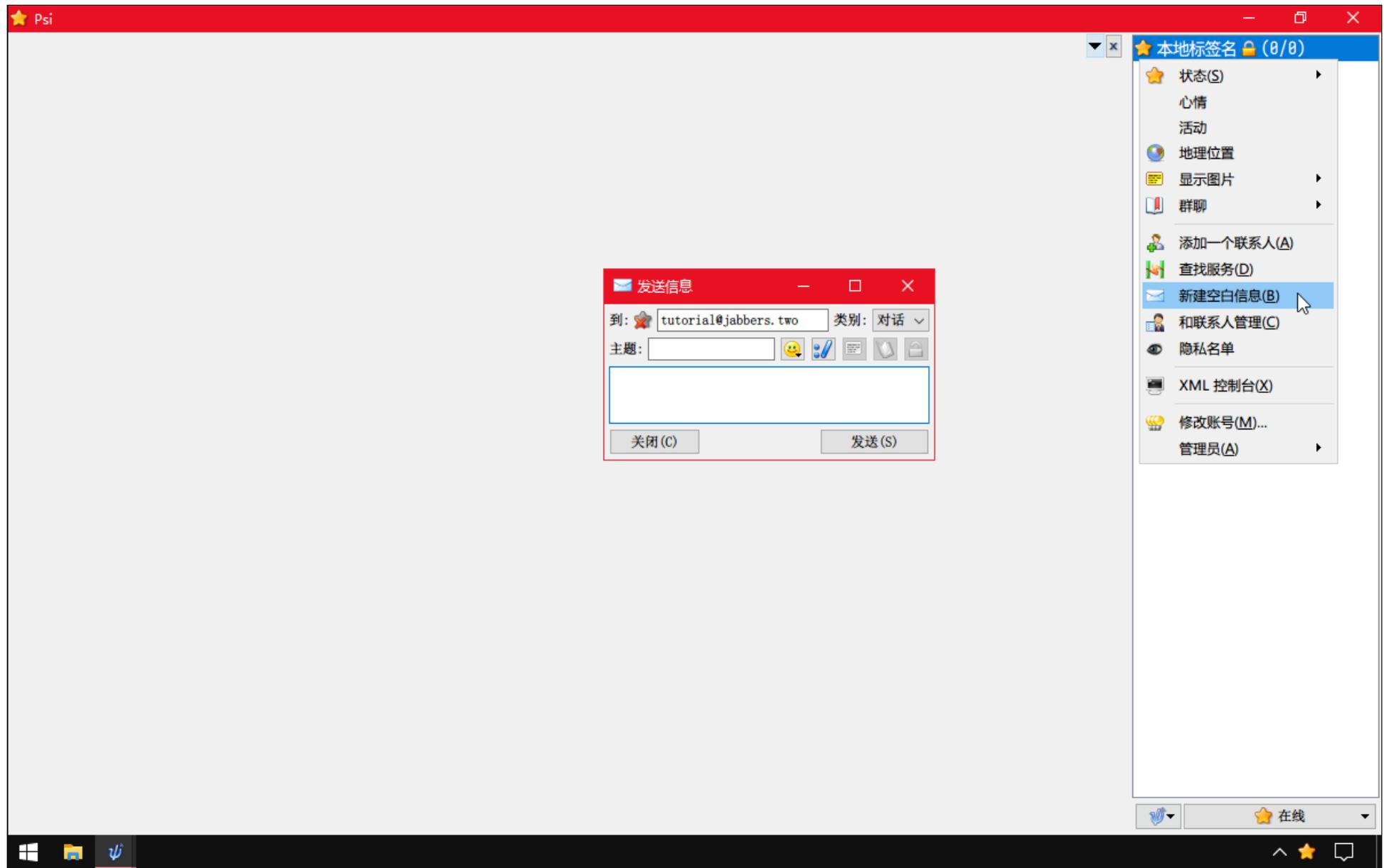
你可以查看会议室的人员都在用什么用户端软件，即使你无权得知它们的XMPP地址。

接收到的信息在左侧显示为蓝色向下的箭头，发送成功的信息显示为绿色向上的箭头。

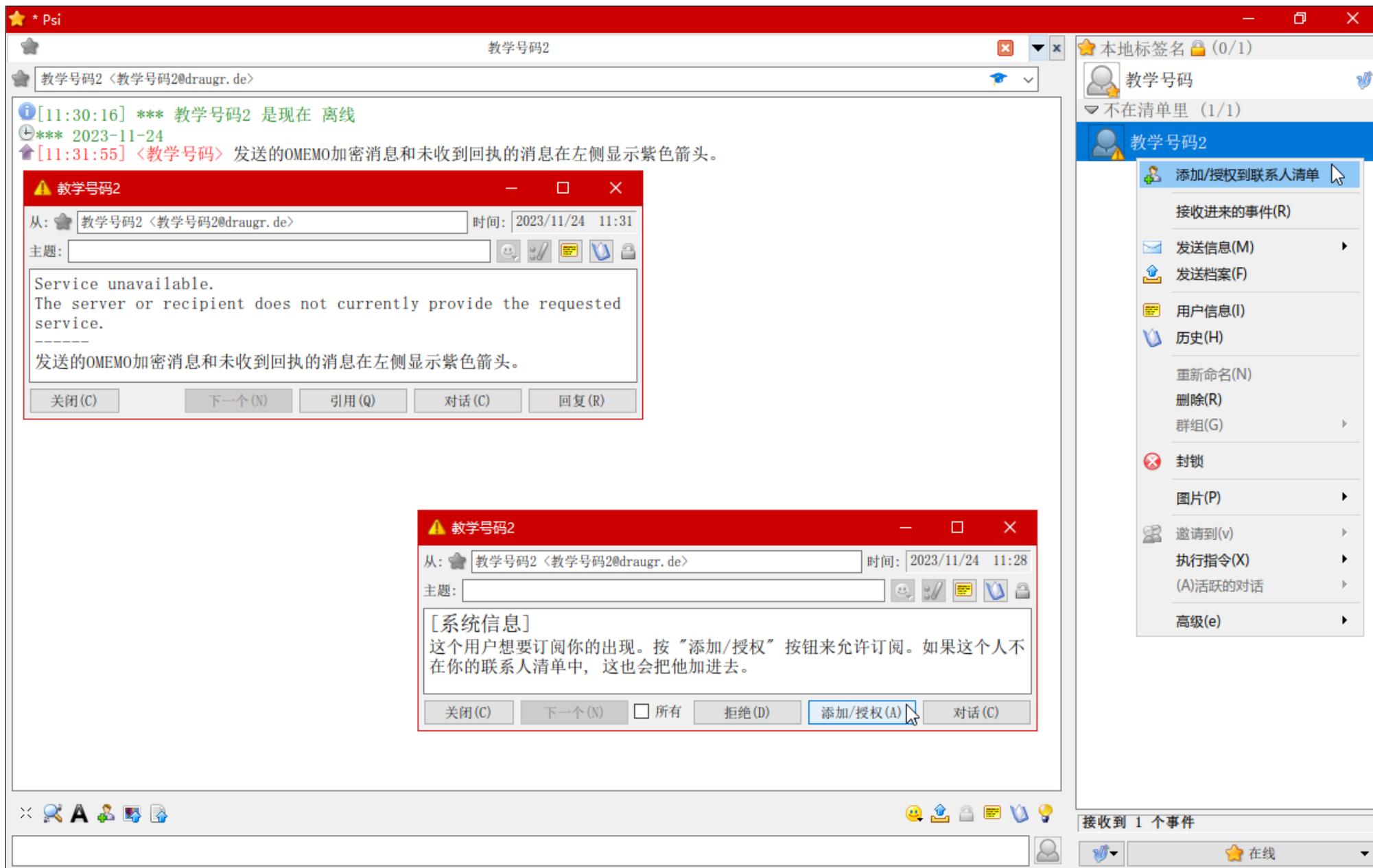
通过拖动边框可以调整三个区域的宽度。输入框也可以隐藏。

如果你要使用“Ctrl+C”来复制文字，最好在快捷键设置里将已经被占用的这个快捷键设置项删除。

普通私信



如果要给非联系人发送一条信息，就点击选单里的“新建空白信息”。发送消息之后便可以双击出现的新对话项打开会话窗口。



这是普通私信的界面，也是室内私信通道的界面。当你第一次打开这个界面时，它也许会崩溃，重新打开Psi就好了。

你需要自己查看联系地址或对话项显示名称来判断这是室内私信还是普通私信。你也可以和联系人的仅仅某一个登录点联系。

添加和删除联系人，以及调整分享在线状态，都在对联系人的快捷选单里。如果对方不是你的联系人，那么对话界面左下角还会有添加对方为联系人的按钮。

工具栏右侧的按钮除了表情按钮外：在线传输文件（操作不那么方便）、切换加密方式、用户虚拟身份信息卡、历史消息、“？”。

主窗口的下方会显示“事件”（通知），例如当有人向你请求分享在线状态时，以及消息发送失败时，就会出现它，点击以决定后面的操作。

如果要显示或隐藏离线的联系人，请点击底部的通用选单按钮，到“视图群组”子选单操作。

Psi (+) 不支持音视频通话。

高级屏蔽名单

The screenshot displays the Psi chat client interface with three main windows:

- 教学号码@draugr.de: 隐私清单 (Privacy List Settings):**
 - 设置 (Settings):
 - 启用清单 (当前会话): blocked
 - 默认清单 (所有会话): blocked
 - 清单编辑器 (List Editor):
 - 清单: blocked
 - Buttons: 新清单, 重命名名单, 删除清单
 - 规则 (Rules):
 - 如果 JID 是 '教学号码@draugr.de' 那么 允许 全部
 - 如果 JID 是 'conference.draugr.de' 那么 允许 全部
 - 如果 JID 是 'proxy.draugr.de' 那么 允许 全部
 - 如果 JID 是 'pubsub.draugr.de' 那么 允许 全部
 - 如果 JID 是 'upload.draugr.de' 那么 允许 全部
 - 如果订阅是 'none' 那么 拒绝 信息
 - Buttons: 添加, 删除, 上, 下, 编辑..., 应用
 - Close button
- 查找服务 (Search Service):**
 - 地址 (A): draugr.de | 节点 (N):
 - 浏览 (B) button
 - Table:

名称	JID	节点
draugr.de	draugr.de	
> 聊天室	conference.draugr.de	
> SOCKS5 字节流	proxy.draugr.de	
> 发布-订阅	pubsub.draugr.de	
> HTTP文件上传	upload.draugr.de	
 - 由JID的筛选: []
 - 自动浏览目标:
 - 自动取得项目资料:
 - Buttons: PSI, 关闭 (C)
- 编辑隐私规则 (Edit Privacy Rule):**
 - 如果: 订阅 | 无
 - 然后: 拒绝
 - 信息
 - 查询
 - 即将离任的存在
 - 传入的存在
 - Buttons: 确定, 取消

On the right, the main chat window shows a menu with '隐私名单' (Privacy List) selected. The status bar at the bottom right shows '在线' (Online).

只要这个界面是可以互动的，而不是蒙灰的，就说明你所使用的用户服务器支持XEP-0016功能。请确保和服务器的连接状况稳定。

虽然一个筛选类别是“JID”，但实际上可以干填写服务器地址。

“默认清单（所有会话）”的意思是应用于所有登录点的通用高级屏蔽名单，由服务器记录启用了哪一条。“启用清单（目前会话）”的意思是只用于Psi这个登录点的当前这一次登录的高级屏蔽名单，服务器和Psi都不长久记录具体某个登录点用哪一条。Psi会用服务器提供的默认名称的高级屏蔽名单来作为Psi自己这个登录点每次登录时使用的，所以，经常使用Psi且设置了多张高级屏蔽名单的用户应该将服务器安排的默认名称的高级屏蔽名单作为自己默认使用的高级屏蔽名单，以避免在Psi端每次登录时重新设置当前登录点使用的高级屏蔽名单为其它的。

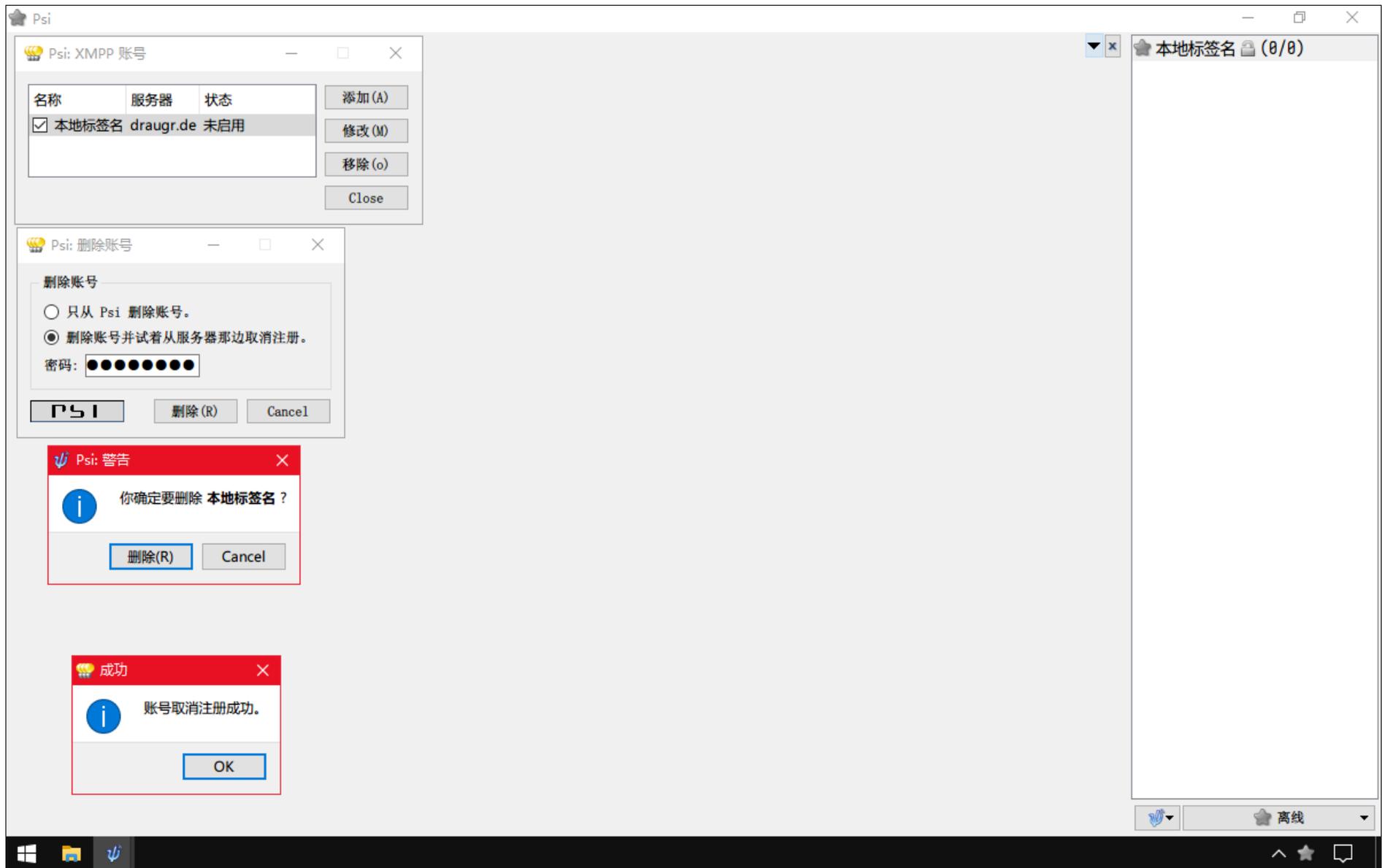
当你编辑完毕后，记得点击“应用”以向服务器发送修改请求来保存它。

“订阅”太术语化，意思是“在线状态共享情况”。

四个过滤项都不选时，提交后自动改为全选。

Psi在单个账号管理窗口的“隐私”标签页里会显示你的黑名单，如果你的高级屏蔽名单里有手动添加的黑名单不支持的项目，那么它就会提醒“你正在使用高级设置，这个清单可能会不准确”。但在XMPP标准中黑名单是基于高级屏蔽名单的，如果特别的服务器软件支持黑名单但却不支持高级屏蔽名单，那么Psi会在这个界面显示“你的服务器不支持封锁”，这是错误的反馈信息。

注销

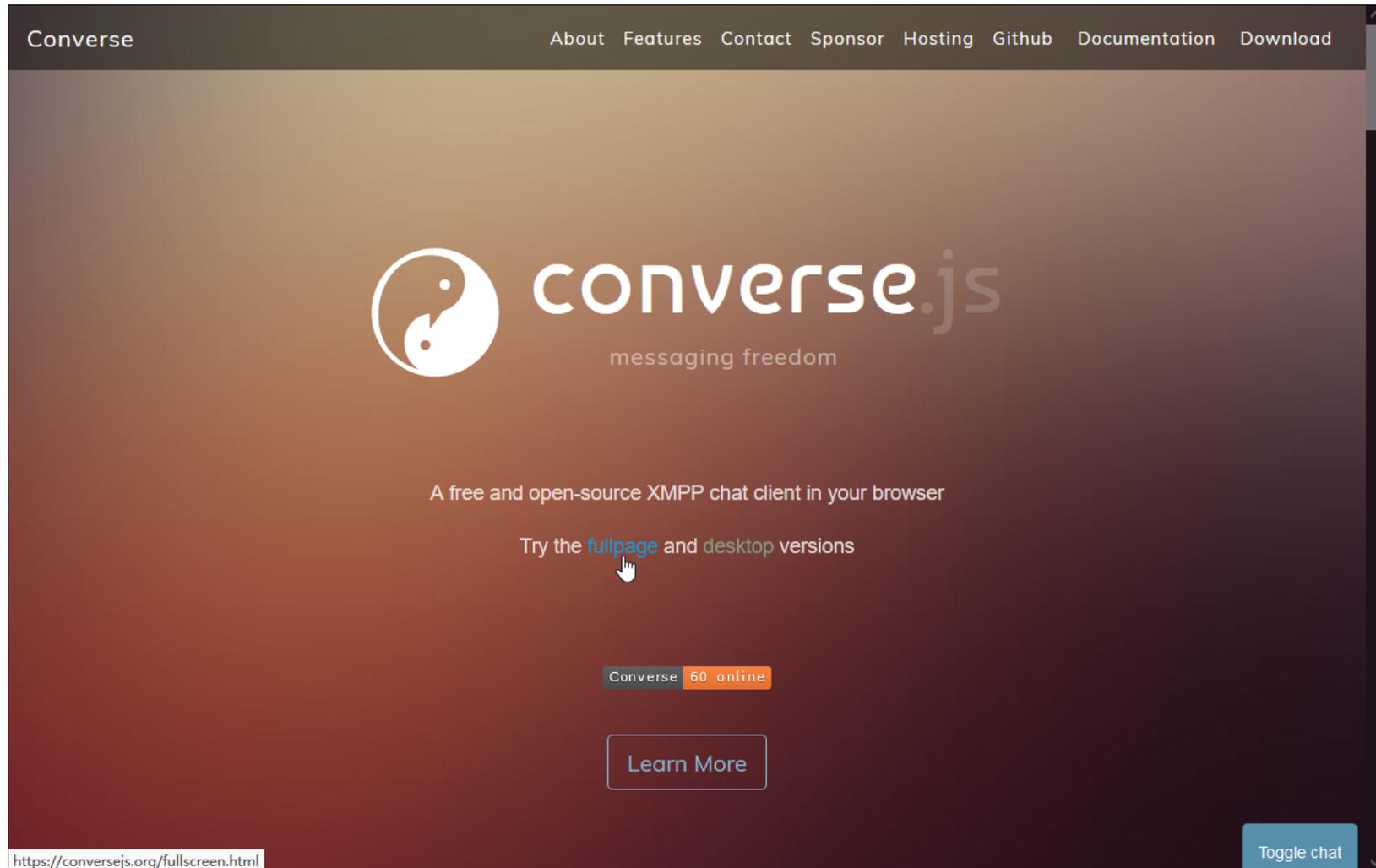


要注销你的号码，在XMPP身份管理窗口里选择要注销的号码并点击“移除”。选择“删除账号并试着从服务器那边取消注册”，输入你的登录密码。确定“删除”。无论服务器有什么奇怪的反应，只要之后你无法再用密码登录你的号码了，那么就是注销成功了。

Converse的介绍

也可以叫它“converse.js”。它是一个网页端XMPP用户端软件。访问它时，网页浏览器会获取这个软件，并在本地运行。所以你的XMPP相关网络数据保存在你的网页浏览器软件里，而不是一个第三方服务器上。

除了这个官方网站 (<https://conversejs.org/>) 以外，一些公共服务器的网站上也提供这个组件。



点击右下角的按钮就可以开始。但，这是用来同时阅读网页上的其它内容的折叠模式，它的功能很少。请不要使用此模式，而要使用全屏模式（“<https://conversejs.org/fullscreen.html>”），点击“fullpage”按钮即可跳转到全屏模式。



作为辅助，它可以帮助你：

- 它可以完整地展示服务器的注册表单，当你的用户端软件不支持这么做，因此不能注册时，它可以帮助你。
- 它可以获取会议室的设置表单，不过是服务器的首要语言。
- 它对人员的管理等级和参与等级的调整有完备的支持。

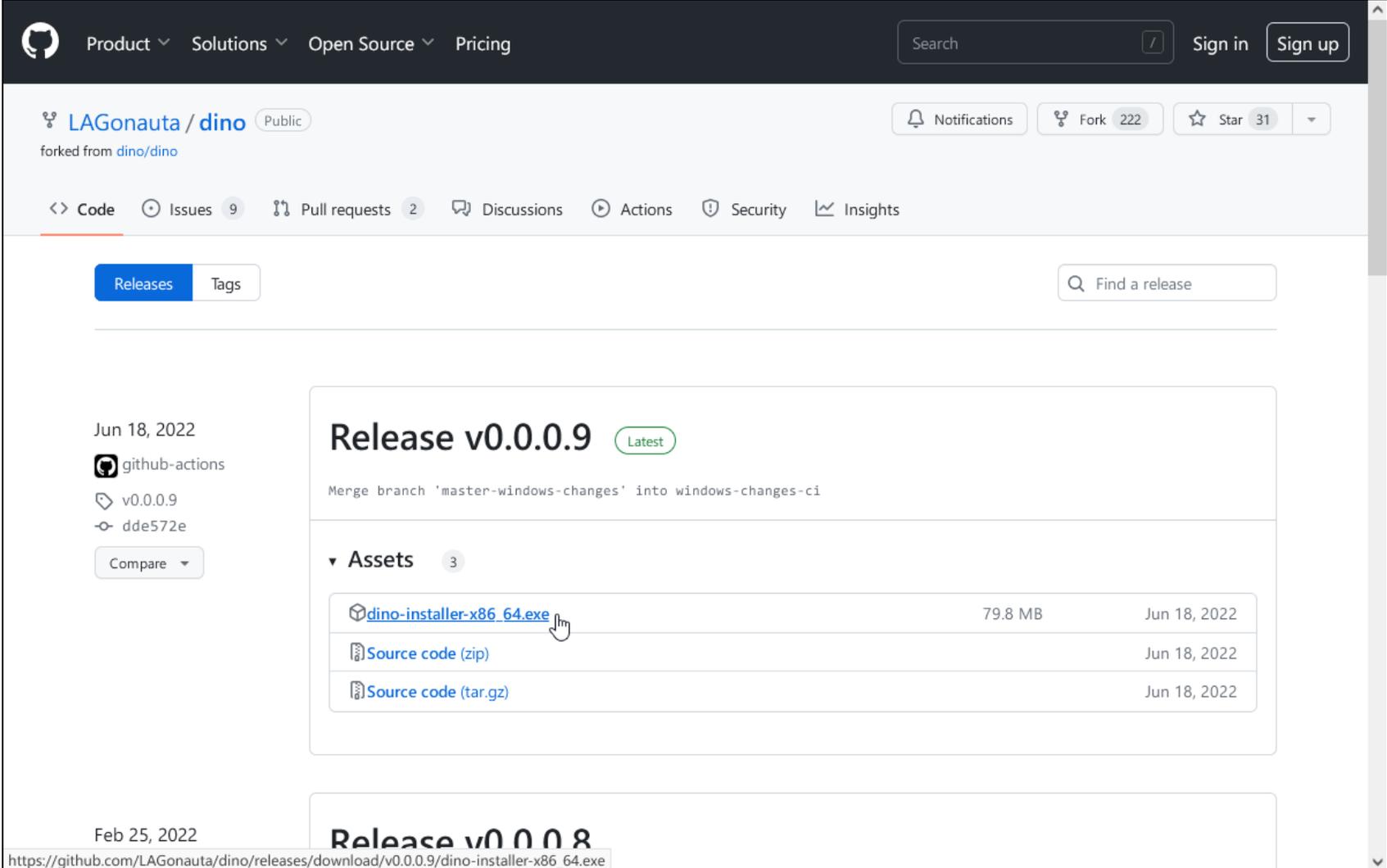
如果你在一台别人也会用的电脑上使用，那么就应该取消勾选“**This is a trusted device**”。取消后，当你关闭Converse时，你使用XMPP的相关数据不会保留在网页浏览器里；同时无法使用OMEMO加密。

当你登录的时候，它会需要长一点的时间来下载功能组件、获取用户们的虚拟肖像。它在加载时也会占用较多的运行内存。

Dino的介绍、下载、安装

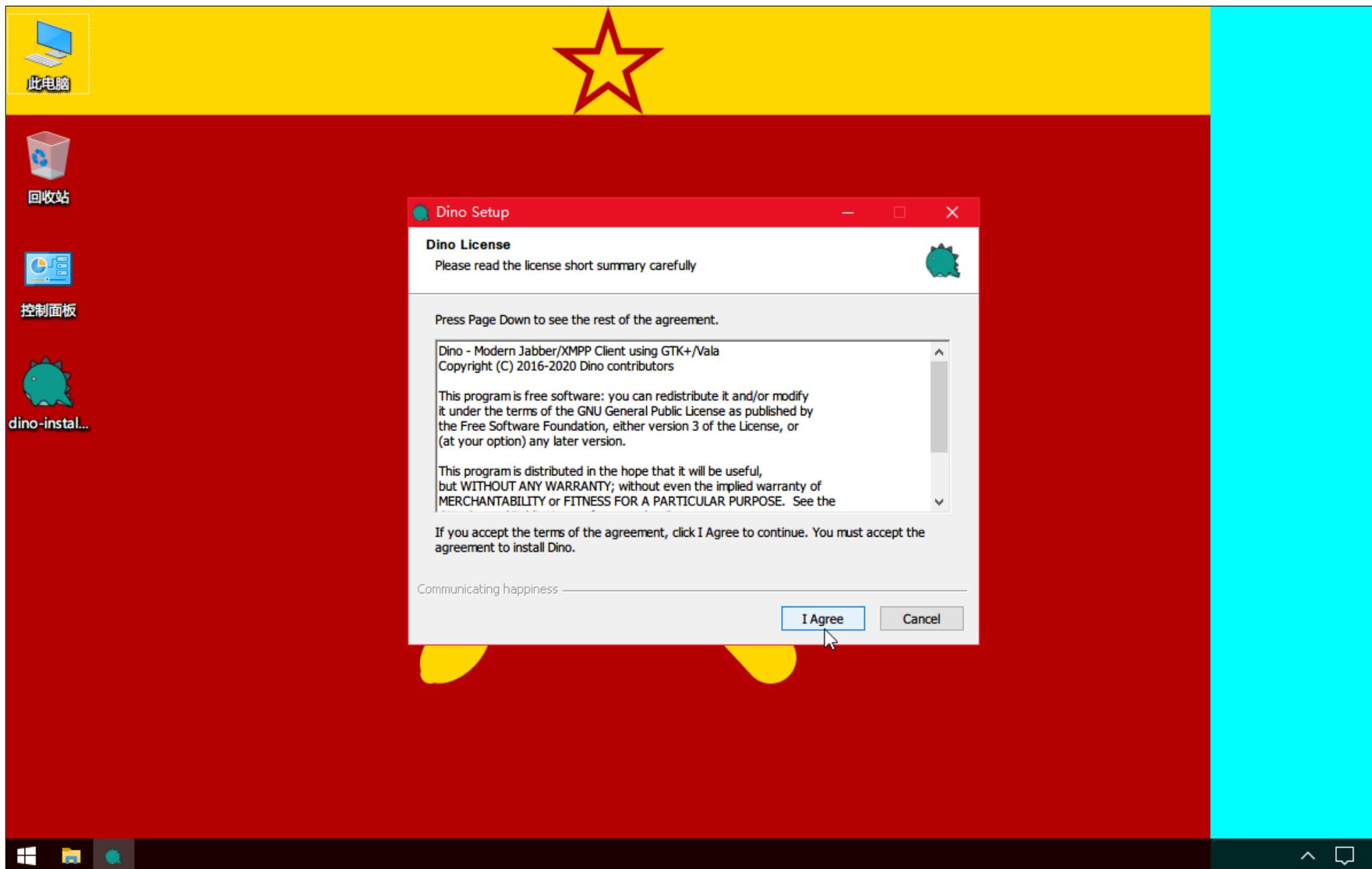
Dino有可用于Microsoft Windows 10 ×64上的非官方移植版本。可用作Gajim的临时替代品。特点是对支持音视频通话有良好支持。在对会议室人员的管理方面，它不支持等级管理，只能授予或撤销公开发言权。

使用网页浏览器访问此网址：[“https://github.com/LAGonauta/dino/releases”](https://github.com/LAGonauta/dino/releases)。

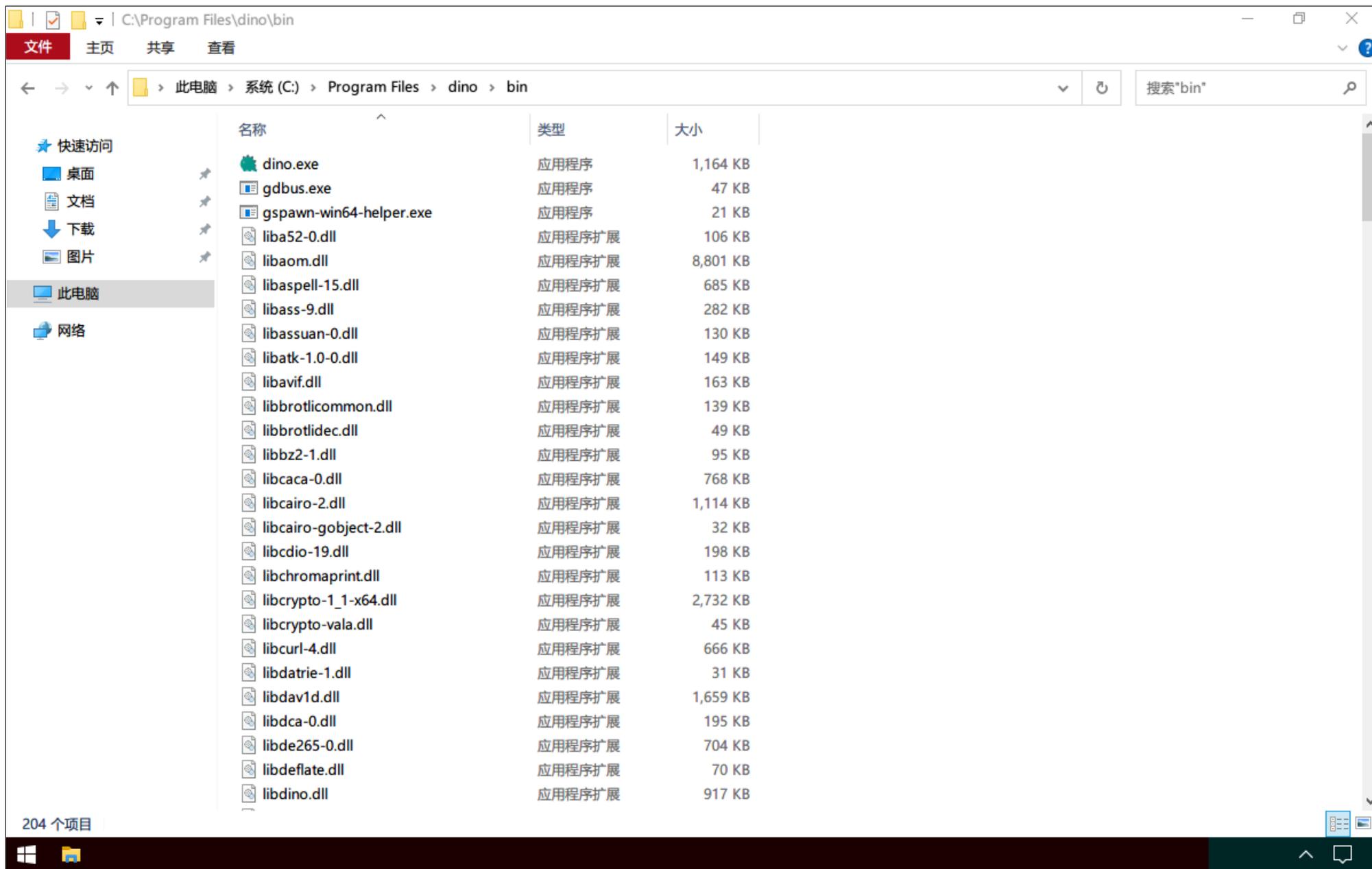


The screenshot shows the GitHub repository page for LAGonauta/dino. The page is in the 'Releases' tab, displaying the latest release, v0.0.0.9, dated Jun 18, 2022. The release is marked as 'Latest' and includes a commit message: 'Merge branch 'master-windows-changes' into windows-changes-ci'. Under the 'Assets' section, there are three items: 'dino-installer-x86_64.exe' (79.8 MB, Jun 18, 2022), 'Source code (zip)', and 'Source code (tar.gz)'. A mouse cursor is pointing at the 'dino-installer-x86_64.exe' link. The URL at the bottom of the page is https://github.com/LAGonauta/dino/releases/download/v0.0.0.9/dino-installer-x86_64.exe.

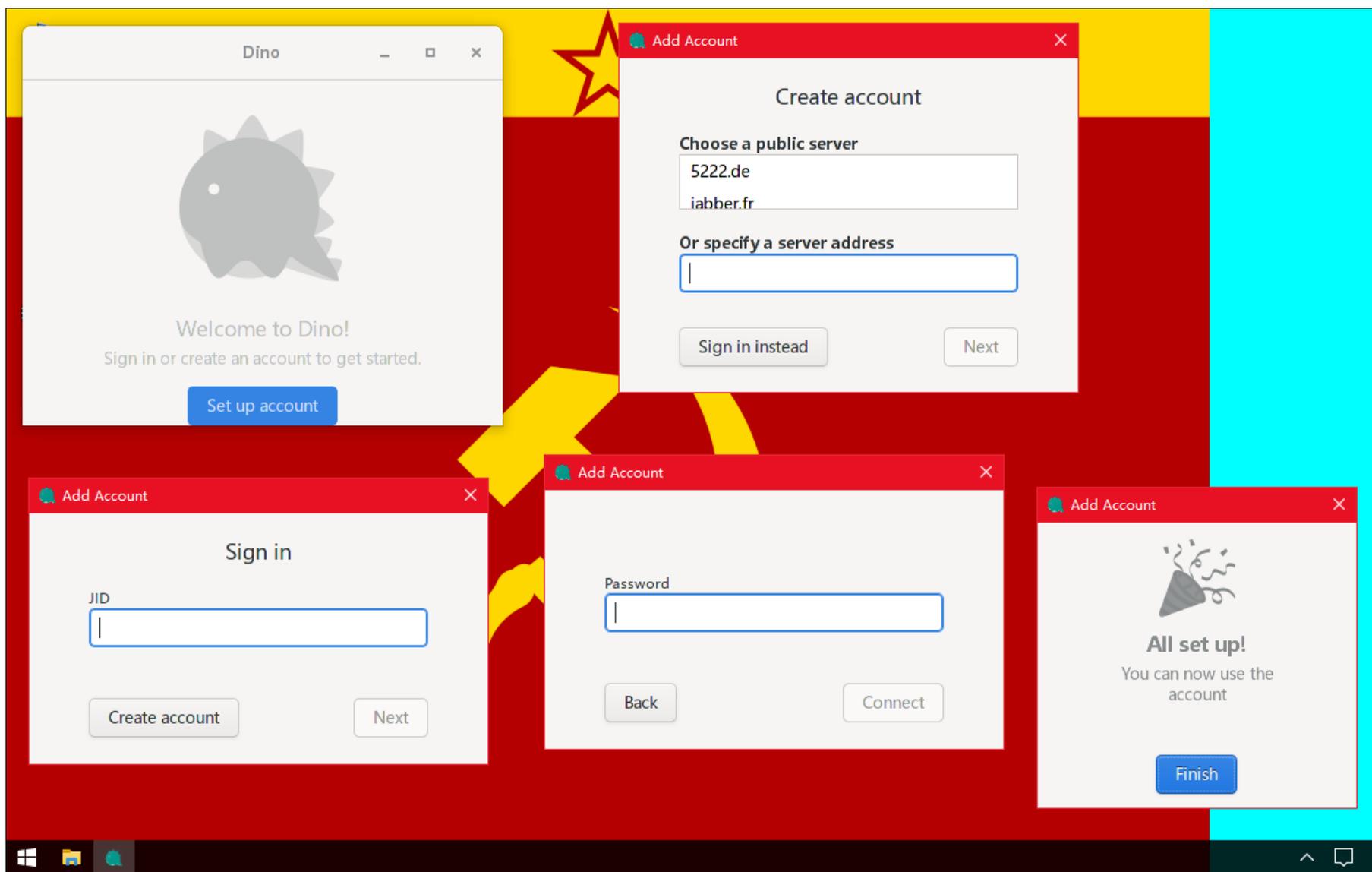
点击“dino-installer-x86_64.exe”下载Dino的安装包。



双击打开安装包。点击“I Agree”会立刻开始安装，无法选择安装位置。安装完毕后点击“Finish”。

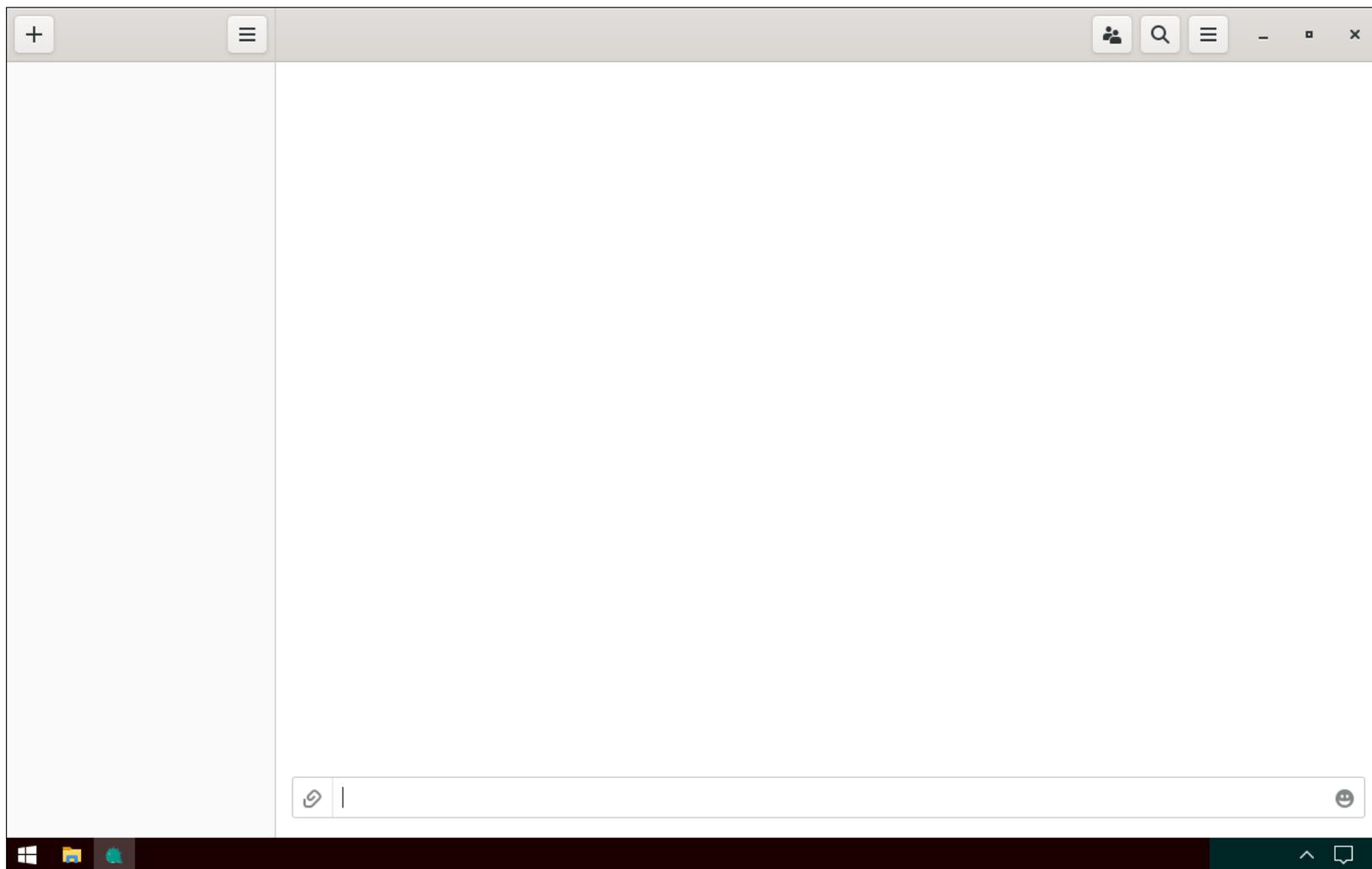


安装位置如图所示。双击dino.exe来启动。



从左上的窗口开始，点击按钮登录一个XMPP身份。在下方的两个窗口中依次输入你的XMPP地址，密码，到右下角的对话框即为登录成功。

如果你要注册一个XMPP身份号码，那么点击左下窗口的“Create account”按钮，到右上角的窗口输入你要注册的服务器地址。之后，它并不能展示验证码，你需要复制给你的图片链接到网页浏览器里访问获取验证码图片，再输入验证码。



空白界面如图。

左栏是你所有的对话选项。左上角的加号“+”按钮用来从通讯录和地址簿中添加一个对话选项。更多选项按钮用来调整XMPP身份设置和客户端软件设置。

右栏是对话界面。上方标题栏从左到右的三个按钮依次是：会议室人员、搜索消息、会议室信息和设置。下方从左到右分别是：发送文件、消息输入框、添加表情。

关闭窗口即为关闭此软件。

附录：TLS加密

TLS加密是用户端和服务器之间的加密通信，使得只有用户端和服务器可以解读消息，网络通道里的窃听者无法解读。

和其它所有加密一样，它可以确保传输的数据是无误的，不被篡改的。

TLS常见于访问网页时的HTTPS连接，只要在访问HTTP链接时添加“s”使链接开头成为“https://”即可。也用于其它地方，例如XMPP。

每个使用TLS加密的站点都有TLS加密证书，由公认的证书签发机构颁布。

TLS已经成为互联网的标准功能配置，最新的版本是1.3。如果一个网站不支持TLS 1.2或1.3，那么它的评分就会大打折扣；如果一个网站不支持HTTPS，那么它就太差劲了。

TLS是由服务器负责配置的。配置完毕时，服务器可以拒绝用户使用不加密的连接，也可以通过TLS协商拒绝使用低版本的TLS连接（主要为了阻止受到了TLS降级攻击的用户访问）。

为了避免被试错破解进而被窃听通信，服务器的TLS证书每隔一些个月就要换新的。TLS证书有明确的有效期及起止时间，如果因为过期而出现了警告，那么只要不是自己系统的时间错误地超前，就意味着服务器缺乏维护：

- 这项服务可能要被管理员们抛弃了，或者只是把它放在一边长期置之不理。
- 这也意味着和服务器的加密连接不够安全，如果有在进行试错破解的攻击者，那么加密通信可能已经被破解并窃听了。
- 证书过期时访问软件们会给出警告。
- 有的用户喜欢这种情况，因为这常常意味着服务器管理员不会在意，进而不会发现有人肆意执行别人可能不喜欢的操作。

如果错误信息是“证书签发者未知”，那么TLS加密的安全与否无法判断；服务器管理员是否活跃也无法判断。

TLS证书也可以自己生成并应用，不过这基本只用于测试，或者不太在意的个人网站、小众网站、没什么重要功能的网站。自己签发的TLS证书基本不会受到访问软件们的信任，需要手动设为信任才可以访问。

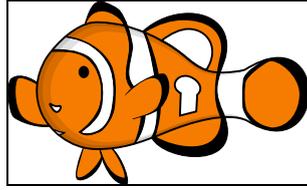
如果自己系统的时间错误地过早，那么很多网站都将无法正常访问，且网页浏览器不一定会给出正确的提醒。

操作系统会自己存储一些证书用来访问网站，如果多年没有更新，那么使用这些证书的网页浏览器就会无法正常访问许多HTTPS网站，就需要安装新的证书。有的网页浏览器自带证书用，所以不同的网页浏览器在访问同一HTTPS网站时可能有不同的结果。

当TLS加密出现问题时，用户将处于被动局面。以下是解决办法参考：

- 用户可以忽视警告继续使用HTTPS连接。
- 访问不加密的HTTP版本，如果服务器允许而且用户愿意的话。
- 等待或提醒服务器管理员解决。
- 访问其它的内容一模一样的备份站点，如果有的话。

附录：OMEMO加密



OMEMO的徽标

实际上，没有任何一种加密方式适合新手使用。在使用OMEMO时遇到障碍时，可以先使用无主动加密的消息交流，请记住你和服务器还有一层TLS加密，使得只有服务器、发信方、收信方可以解读消息，网络通道里的窃听者无法解读。

功能

- 多端到多端加密。
- 支持群聊。
- 支持向离线端发送。
- 支持文件加密。
- 抵御中间人互联网攻击（次要）。

操作性

它非常方便使用，不需要多少手动配置，几乎就只是一个按钮或开关的事情。

但新手在群聊里使用OMEMO加密总是容易遇到问题，会议室的房主和管家都是新手时则更严重。

属性

端到端：OMEMO的发信端和收信端指的是登录点（登录端），而非XMPP身份，每一个虚拟用户都可以有多个登录端，每个登录端各自都有本地的密钥获取情况和设置。

登录点：每一个支持并启用了OMEMO的登录点都会有一个自己的，和其它登录点不同的OMEMO身份标识，也叫“OMEMO指纹”，为8乘8共64位的十六进制数。只是一串号码，无法根据它直接查到具体的时间、设备型号、软件名称。（但可以解读一条加密消息就可以看到这条加密消息的来源指纹，用户以此可以辅助判断消息来源于对方的哪个登录设备和哪个用户端软件。）通常，一个用户有多少指纹，就意味着有多少个在使用的支持OMEMO的登录点。OMEMO指纹实际上是根据属于对应登录点的OMEMO密钥生成的，用户端软件们用指纹代表对应登录点的密钥。

保密：每一条加密消息在发送时都有明确且固定的目标收信端，非目标收信端（服务器及其管理员、在加密消息发送之后才成为会议室成员的人）无法解读消息。如果有一条消息在某个登录点无法解读，那么这条消息在此登录点就是永远无法解读的。不需要记密码。每一条加密消息都有不同的加密密钥，两条内容相同的消息，加密的结果也会不相同，所以无法解读加密消息的人也无法判断是否发送了两条相同的消息。

获取密钥：在发送加密消息前，加密程序必须拥有收信用户的密钥。如果没有，就需要联系收信用户所属的用户服务器来获取密钥（不需要有联系人关系）。如果已经有了收信端的密钥，那么用户端软件的加密程序就可能直接发送加密消息；也可能再去检查一下看看目标收信用户们有没有新的密钥（新的登录点），以避免收信用户的新登录点无法解读自己发送的加密消息。如果你发现自己的新登录点无法解读某个发信端发送的加密消息（自己的新登录点没有被那个发信端发现），那么主动发送一条加密消息，以后就可以解读对方以后发送的加密消息了（如果还是不行，可能是那个发信端禁用了自己的密钥）。

预留密钥：服务器为每一个登录点存储一些预留密钥，当OMEMO发现一个新登录点给自己发送第一条加密消息，并且成功被自己接收时，自己的每一个登录点便会消耗一个预留密钥。预留密钥耗尽后，其它用户便不能在新登录点为你发送第一条加密消息。为了自己的预留密钥不被耗尽：

- 当你加入一个加密交流的群聊后，如果是第一次加入这个群聊，那么你的加密程序就会有 很多新用户要认识，请一定要主动发送一条加密消息和大家打招呼，不要干看戏。
- 不要长期在线却不使用OMEMO加密。如果你的OMEMO加密程序经常遇到以前没见过的别人的新登录点，那么你的预留密钥的消耗速度就会较快，请记得使用OMEMO来发送加密消息补全预留密钥。
- 排查会议室里的内鬼。内鬼可以不断地重置自己的OMEMO密钥再发送一条加密消息来浪费别人的预留密钥。不过这种攻击非常罕见而且收效低，一般不用对此怀疑。

群聊条件：锁门+小桌是正常使用OMEMO的前提条件。有些客户端软件在获取了收信端的密钥后就会无视这一条件地允许发送加密消息，通常这种设计弊大于利。需要锁门的原因很简单：如果是敞门的，那么就是任何人都能加入的，敞门本身的目的也就是把消息给所有人看，这种情形下的消息保密没有意义。小桌则是因为OMEMO需要有收信方的XMPP用户地址才能保证获取密钥，通过室内私信地址则不一定可行。

不要复制：一个XMPP身份的一个登录点的密钥可以转移到不同的设备和不同的登录点，但（和普通登录点标识类似），不能让两个相同的密钥同时在线。备份文件恢复只能用于迁移数据到另一个位置，而不能用于完全复制登录点并同时在线使用。

信任机制：一个登录点可以对其它登录点设为“不信任”并禁用，被禁用的登录点就不再被视为目标收信端，且从其发来的加密消息会被打上“不信任”的标记。通常，这只有在这种情况下才使用——一个虚拟用户由多个人一起使用，你不想自己的加密消息被对面所有人解读。

强谨慎：XMPP虚拟用户是有登录密码保护的，因此不会被轻易盗用。而OMEMO则细化到了对每一个登录点进行验证，当发现别人有了一个新登录点时，不着急启用新密钥，用户可以先加密联系对方的旧登录点，确认对方确实添加了一个新登录点，而不是别人盗用了它的XMPP身份，再启用对方的新OMEMO密钥。但这很麻烦，毕竟从验证人细化到了验证每一个登录点，大多数用户都不会这么做。客户端软件的OMEMO加密程序通常有“盲目信任”（“blind trust”）（对普通用户而言最好叫“直接信任”或者叫“自动信任”）的设计，一般用户都应该启用它；否则，当遇到一个新的指纹时，都要用户手动确认这个指纹是自己信任的（也就是手动启用它），之后自己发送出去的加密消息才能被对方解读，这会很麻烦。有直接信任设计的客户端软件有的会用两个图标来区分一条加密消息的来源指纹有没有经过用户手动确定信任。

加密负担：OMEMO程序的工作负担和加密消息的目标收信端数量成正比。不过这基本是不用担心的，因为设计良好的客户端软件发现自己XMPP身份的某个登录点很久没活动时，会自动请求服务器删除它，并在此端禁用它，以减小加解密程序的负担（静谧天数，以及连续有多少条加密消息不来自此登录端，是客户端软件可用的两种判断因素）。被服务器删除指纹的登录端在线时会立刻向服务器请求再次添加它的指纹，不用担心某个登录点因为只挂机从来不主动发送加密消息而被彻底废弃。总体而言，它的加密工作负担并不大。

手动删除：用户可以手动请求服务器删除自己的某个离线登录点的密钥。之后对应的离线登录点在下次上线前将无法解读在此期间自己收到的来自其它用户新登录点的加密消息，和此期间来自自己的所有登录点的加密消息。

“不支持”的提醒：如果你的设备收到了OMEMO加密的消息，但是你的客户端软件完全不支持OMEMO，那么可能会有备用的无加密的消息来提醒你说“此用户为你发送了一条OMEMO加密的消息，但你的客户端软件不支持。”。

加密文件：OMEMO加密的文件的下载链接开头为“aesgcm://”，将此链接复制发给别人是无法下载的。

无法发送加密消息的情形归纳

此处说的是无法开始发送的情形，而不是传递失败的情形。也就是试图发送加密消息时的获取密钥步骤出现问题。在群聊中，如果有一个收信方出现此问题，有的用户端软件会忽视它，有的用户端软件会停止进行发送加密消息。常见情况如下：

- 收信方服务器不支持OMEMO。
- 收信方从来没有用过支持并启用了OMEMO的用户端软件，因此一个指纹也没有。
- 双方服务器无法正常相互通信（可能性有：一方服务器掉线、存在互联网连接障碍、服务器的服务策略拒绝和对方服务器连接、服务器地址输入错误因而找不到，等等），因此无法获取密钥。
- 添加的联系地址错误（可能性有：用户从来不存在、已经注销了，等等）。
- 收信方的预留密钥耗尽。此时应该叫那个收信方主动发送一条加密消息。如果此XMPP身份被弃用了，就应该在会议室成员列表里删除它。也可以考虑在联系人列表里也删除它。能把预留密钥耗尽的，一般是只在场看戏而且很久不参与交流的。

无法解读加密消息的情形归纳

- 收信方的用户端软件不支持或未启用OMEMO。
- 收信方的服务器不支持OMEMO（此时收信方仅在群聊里才可能收到加密消息）。
- 收信端离线时服务器删除了其密钥。
- 收信端的密钥被发信端禁用：
 - 发信端没有启用自动信任且没有手动启用收信方的密钥。
 - 发信端手动禁用了收信方的密钥。新手乱操作可能会导致这种情况。
- 收信方用新登录点（必然无法解读历史加密消息）：
 - 安装一个新的用户端软件并在没有预留用户数据的情况下登录。或，用户端软件清除本地存储的用户数据后重新登录。这会生成新的不同密钥。
 - 重置自己登录端的密钥+清除本地存储的历史消息+重新获取历史消息。（除了和OMEMO无关的通用登录端标识一样之外，这基本相当于上一条了。）
 - 发信方在发送加密消息时尚未发现收信方有新的密钥。
- 在群聊里可见的情况：
 - 加密消息本来就不是给你发送的，只是你收到了而已。也就是说，刚加入群聊的时候无法解读历史加密消息。
 - 一个新人加入群聊，在第一次获取大家的密钥时，有个服务器掉线了，只好先获取其它人的密钥并发送加密消息。在那个服务器上线之前，新人在此期间发送的加密消息都无法被那个掉线服务器的用户们解读。

在群聊里避免OMEMO加密出现麻烦

如果要使用加密还要避免出现加密问题的话，基本上要确保群聊人数规模不太大。这从很多方面来讲都是必要的：

- 人数越多，越是可能有更多不同的服务器参与通信，其中越是可能有两个不同的服务器无法正常相互通信。
- 人数越多，越是可能有的成员主动注销自己的身份或因长期离线而被服务器注销。
- 人数越多，加密的计算负担就越大。
- 人数越多，里面的消息就越无法算得上是秘密。
- 毕竟要公开所有成员的XMPP地址。如果有的成员想尽量避免让更多人得知自己的XMPP

地址的话，这就会是个问题。人数越多，确保成员们两两相互信任的难度就越高，信任的门槛就越高，越是要求成员们有严格的组织性和纪律性。

- 有的用户端软件在群聊里要求成功获取所有成员的密钥后才允许发送加密消息（以确保所有收信用户都能解读）。

所以情况难缠时有必要让人员们用不主动加密的消息来交流：

- 放弃群聊加密条件。锁门和小桌修改其一，结果自然是锁门+大桌。不过，有些用户端软件在获取了成员的密钥后，就忽视会议室设置，即使会议室设置改到已经不应该再用加密时，还是会允许使用加密（只要会议室是大桌的，那么新加入的登录点就不可能获取密钥了）；因此，在如此修改会议室设置后，如果仍有成员顽固地使用加密消息，导致许多人无法解读消息，那么这就是一种历史遗留问题，也是群聊人员的组织性问题。
- 号召所有成员使用不主动加密的消息来交流。如果一切顺利，而没有执意用加密消息的成员，那么交流就能一切顺畅。小桌的设置状态可以留着，也可以更改。

如果你的人组织性更强，那么就可以组织全员使用不多的公共服务器来进行群聊加密交流，并把多余的虚拟用户吊销成员资格——这样可以减小因不同服务器的相互连接情况而产生障碍的可能性，尤其是当在以后想接纳新人时。不过这舍弃了XMPP群聊里可以容纳很多来自不同服务器的用户的特点。还要确保每个人都学会了使用代理网络连接，以防将来可能无法直接连接服务器。如果组织性不强，那么就不要再指望加密在群聊里一切顺利了。人越多，同时会议室人员越涣散，OMEMO就越不如不用。

如果你的计划明确就是要往会议室里招揽到很多人，那么，你从一开始，就该好好地考虑自己组织众人的能力（也就是说，别人会不会按你说的去做）。如果确定组织能力不足，那么从一开始就不要用锁门+小桌，以避免群聊加密的问题，以及避免出现可能的基于此的历史遗留问题。

抵御中间人互联网攻击

只有在你非要用不该信任的服务器或无TLS加密的连接时，你才需要考虑这一点；否则，这一节的剩余内容可以跳过了。

确认没有中间人互联网攻击的方法是：确认联系人在它的登录端看到的它自己的指纹和你在你的登录端看到的联系人的指纹是相同的，且没有多余的指纹。

当你使用用户端软件生成并分享你的XMPP链接时，可能会带有额外的关于OMEMO的信息，形式如“xmpp:XMPP用户地址?omemo-sid-登录端标识=你在此登录端的OMEMO指纹”。这些信息就是用来验证的。用户端软件也可能有在本地记录验证关系的功能——别人点击此链接后就可以在它的登录端上记下“这是我确信无疑的联系端。”；你对自己的其它登录端也可以这么做。这段用来验证的文字也能够以二维码的形式存在。

有的用户端软件会在用户对联系人进行了验证操作后，对这个联系人取消自动信任新密钥。

自己有多少正在使用的支持并启用了OMEMO的登录端，自己最清楚。有两个在线登录点用相同的密钥和指纹则会让加密交流出现明显异常。另外，你要确保不会有人敢拿信任或个人名誉作赌注来故意演戏欺骗你说“我们的交流中存在中间人互联网攻击”。如果声称出现异常的人实际没什么用，也没有什么名誉，那么你也就不应该有任何理由跟着它的空赌注下自己的赌注。

附录：第三方会议室搜索引擎

XMPP标准规定露天会议室能通过访问其所属的服务器来查找到。一切跨服务器的搜索引擎都属于第三方。本附录要介绍的搜索引擎正是如此。

此搜索引擎也被集成在了Conversations里和Gajim里。

打开你的网页浏览器，访问此地址：“<https://search.jabber.network/>”。

你可以通过输入文字来搜索会议室。至少要输入三个字符才有效。会议室的地址、描述、名字属于检索范围。

并不是会议室设置了“露天”后就能被搜索到，除了要等待搜索引擎收录以外，还要符合此搜索引擎提出的条件：砖屋+露天+门神守卫+敞门，会议室所属的服务器没有被滥用，等。

小众公共服务器的露天会议室也不会被收录。

当XMPP普及后，你可以试试用这个搜索引擎来搜索各政治行政区的地方会议室。

将会议室用于政治活动的话，就不要期望第三方搜索引擎能保证收录你的会议室地址了，不要过于依赖第三方搜索引擎。第三方搜索引擎的主人会有自己的收录主意（而删除含有自己不喜欢的内容的会议室地址），也可能会顺从网站或自己所属国家的法律而拒绝收录一些内容的会议室信息。

附录：反馈错误信息实例

“Remote domain is not an IDN hostname”：可能是你在一个正确的用户地址后面添加了“?……”的后缀。

“No available resource found”：你在给纯服务器地址发送消息？如果要联系服务器管理员，你更应该找到服务器管理员的联系地址，而不应该直接给服务器地址发消息。

“service unavailable”：收信的服务器存在，但是对应的用户身份不存在（未注册或者是已注销），或者收信方的黑名单或白名单没有允许和你通信。（如果确信存在，请试试和对方相互添加联系人并共享在线状态。）

“Connection failed: timeout”：收信的服务器地址存在，但它不是个XMPP服务器，无法作出正确的回应。

“DNS lookup failed: non-existing domain”：收信的服务器地址不存在。

“Connection failed: connection refused.”：添加的联系地址里的服务器地址是错误的。或者收信服务器配置不正确。

“Bad value of attribute 'to' in tag <message/> qualified by namespace 'jabber:client'”：联系地址里面有个不该有的空格。

“Messages from strangers are rejected”：收信服务器拒收非联系人消息。这是由收信服务器决定的，用户无法改变此设置。这种情况下要联系对方的话，需要对方将你添加为联系人，同时请求并获取你的在线状态共享。这一特性可能不拒收和自己同一服务器地址或同一服务方的非联系人的消息。

“Stream closed by peer: Your server's certificate is invalid, expired, or not trusted by 【服务器地址】 (not-authorized)”：收信的服务器地址存在，但你的使用的服务器的TLS证书有问题，不被收信服务器信任。

“Connection failed: connection closed”：收信服务器有问题。

“Your active privacy list has denied the routing of this stanza.”：你使用了高级屏蔽名单功能，你目前启用的名单没有允许和这个地址通信。

“Access denied by service policy”：你用的服务器的服务策略拒绝和对方通信。有的公共服务器曾经被发垃圾信息的滥用过，因此一些其它公共服务器的服务策略拒绝与它通信，会显示此反馈信息。至于被滥用的服务器清理滥用的XMPP身份并恢复后，其它服务器有没有解除屏蔽它，就是其它服务器的事情了。

“Your contact offline message queue is full. The message has been discarded.”：对方有太多离线消息还没接收，服务器拒绝为它再存储更多离线消息了。常见于较久没上线的用户。对方较可能是个经常有很多人联系的名人，或者是遭到了垃圾信息攻击。

“User session not found.”：很可能你的用户端软件没有自动识别对话类型，同时你把一个用户地址误当成会议室地址来添加了。请关闭对话框，在个人地图里删除这个错误的地址（可能还需要删除历史消息），并重新添加此用户。

“Recipient not in room”：目标收信人已经离开了或者更改了占座名（也就是更改了室内收信地址）。

附录：周边技术问题

周边技术问题不被保证在此说明书里被详细论述。如果论述太多，那么这本说明书就太臃肿了。这些周边技术问题也可能在以后被挪到我们网站的其它地方或其它册子里。

上网环境阻碍问题

关于硬件方面，应该使用普通的、专一的、不为帝国服务的光调制解调器、路由器、终端上网设备。在和中国的互联网运营商相关的路由器上发现过限制互联网访问的现象（包括限制连接速度和阻碍访问，这是用户无法调整的）。

测试和判断你的上网环境是否受阻碍的办法：

- 简单且必要的前提：
 - 使用同一互联网运营商的网络。
 - 如果国内地区的政治政策有不同的话，那么还要在同一行政地区测试。
 - 使用国际通用的网页浏览器。不要使用专门为一个或几个的国家或行政区或语言服务的，或者对这些要素有差别对待的网页浏览器。例如，应该使用Chromium和国际版的Firefox（不要中国版的Firefox），以及它们的具有国际性的衍生品。
 - 挑一些国外的小众网站测试。除了测试是否能访问以外，下载速度也要考虑测试（不低于1MiB/s为宜）。
- 试试移动网络。如果使用移动网络可以访问到路由器网络访问不到的一些网址，那么结论是：你使用的路由器和光调制解调器中至少有一者没有忠心为你服务。（要排查路由器是否有鬼的话，就要拆除路由器而只连接光调制解调器。）
- 在相同接入光纤、相同光调制解调器、相同路由器的前提下，如果不同的设备的访问效果不同，那么结论是访问受阻的设备中有程序在阻碍访问。

要排查自己的操作系统内是否有鬼的话，更换操作系统是一个好办法，不过这是不懂技术的人干不来的事情。对搭载Microsoft Windows的设备而言，使用Windows PE来测试互联网访问；对搭载衍生Android的设备而言，就要更换原生Android系统来测试。

你的操作系统所选用的DNS服务器也可能影响访问结果。

如果你能顺利使用代理网络连接，而且这么做有效，能够借此通过该条目所述问题的障碍的话，那么也是一种办法。

帝国衍生Android系统阻碍安装软件的问题

能随意安装离线软件包，能安装所谓的“民间自制的”、资本主义公司不乐意让你安装的软件包，是Android系统的优势。如果你的手机系统阻止安装一些软件，那么它肯定不是原生Android系统，而是资本主义设计的衍生品。你不该使用这个手机或这个系统。

如果你执意要使用这种鬼东西的话：对应品牌手机的高级用户可能会有办法解决这种问题，考虑向它们寻求帮助。

钓鱼诈骗问题

钓鱼网站伪装成XMPP的登录页面，以诱骗用户输入自己的XMPP用户地址和密码。瞄一眼网页端登录页面的网址，看看是否是可信的。如果要使用网页端用户端软件，请去网页用户端软件的官方网站，或者提供这个组件的可信的公共服务器官方网站。

敌人做一个假的用户端软件，诱骗你输入你的用户XMPP地址和密码，这种情况是不是可能的呢？这是可能的。用户应当从可信的网站下载用户端软件。

XMPP并不代理HTTP连接，否则它就成了一个代理网络连接工具而不是即时通讯服务了。也就是说，敌人给你发送一个专门用来获取你的IP地址的HTTP链接，这种做法仍然有效。如果

不想自己的IP地址暴露，就请使用代理网络连接；或者在你的用户端软件上禁用自动预览链接和自动下载文件（这样只能手动访问想下载的文件和网页链接）。

用户端软件软件自动下载文件时下载到计算机病毒并不会导致系统中毒，因为计算机病毒是要系统执行运行命令才能生效的。危险的情况只有自己手贱运行病毒，或者系统内本来就有正在运行的病毒接应新病毒。

消息定时撤回（或者“远程阅后即焚”）功能

只有专有的用户端软件才能保证做到这一点。即使是有这种功能的通讯平台，也没人保证收信方不会手动记录收到的信息。记住，你的信息是送给别人的，不是借给别人的。

公开日志功能

公开日志功能注定是无法成为稳定的国际标准来广泛实现并普及的。因为人们很容易要求各种各样的花哨的，甚至截然不同的，也就是说，难以成为稳定标准的功能。公开日志功能可比即时通讯要有更加复杂的，更加众口难调的设计，不如让人们自己去做这件事。而且，公开日志往往被视为一种长期存储服务，这不仅大大占用公共服务器的存储空间，也很难保证长期的用户体验。请不要指望XMPP能普及这种功能。

Markdown格式化文本

一些用户端软件们会使用一种手动格式化文本的规则来显示文本，叫作“Markdown”，来方便人们用文字表达。例如加粗、删除线、斜体、引用。常用的格式是引用：

- 不添加文字用于表示某条消息已经被发过了。
- 自己再添加些文字用于表示自己对某条消息进行回复。
- 可以手动编辑Markdown显示格式，将场外的文字复制到编辑框里，这表示你引用除了室内人员的其它人的言辞笔记。

这偶尔会带来负面效果，可能出现的问题是：

- 它没有严格的标准化，这在不同软件的设计和相互配合上可能出现的问题。
- 它本身算是用户端软件扩展的功能，而非基础功能。有些用户端软件不支持Markdown，就会原般地显示修饰符号且没有格式化显示文本。
- 有时你并不想用Markdown格式来表达，但确实用到了那些修饰标记。例如当你想用“><”来表达双眼紧闭的表情时，因为它用“>”字符开头作为修饰标记来对后面的内容套用“引用”格式来显示，它会显示为引用“<”字符，你只能用其它方式例如“(><)”来表达。
- 汉文用户在源自西文的Markdown教程里可能找不到只有汉文才会遇到的问题（例如删除线标记“~”得在前面加个空格才有效）。

字符显示问题

emoji表情本身是字符，它显示什么样子，决定于你的系统或应用软件用来显示文字的字体文件是什么。不同的字体会有不同的设计样子，加上许多emoji字符在标准上并没有准确的描述。所以有时这会给不同人以不同的感觉，甚至造成严重的歧义。例如，有的把“🔫”这个字符设计成水枪，有的设计成火枪；例如，有的把“🙄”这个字符表情设计成望向一边，像是在疑惑和思考，而有的设计成面向读者，像是在对读者表达质疑。

即使是自然语言文字，在使用花里胡哨的，歪七扭八的字体文件显示时，也会给人明显不同的感觉，其截图会让许多人感到厌恶，不愿阅读。

模仿字符问题

XMPP身份号码和会议室门牌号码都不支持大写英文字母。但如果你看到了有人用了“大写英文字母”而且运作正常，那么此字符就不是大写英文字母，而是其它字母语言的和英文字母模

样相同的字母。例如俄文字母第一个的大写是“А”，而不是“A”；它们的显示模样很可能是相同的（决定于你用来显示它们的字体有没有区别对待它们的设计），但是在计算机用的国际通用文字编码（Unicode）里却不同；本质上，它们是不同的，你搜索“A”无法找到“А”。同样的道理，使用所属语言不同但和英文的字母模样相同的字母可以起到混淆和伪装的效果。用户端软件可能有突出显示容易混淆的字符的设计。小心字形相似的，容易混淆的字符。它们的显示差别有多大，决定于你使用的显示字体的设计如何。试试分辨英语键盘上本就存在的这些不同字符：“1”、“l”、“I”、“|”；“0”、“O”、“o”。如果再加上其它语言文字，那么就更复杂，例如“6”、“6”；“v”、“v”。有的用户喜欢在XMPP身份号码和会议室门牌号码里使用一些容易混淆的字符；甚至有的服务器地址的非一级域名也试图这么用，不过它基本只支持小写英文字母和阿拉伯数字。

有的字符是用来组合成一体的。例如“ó”，占了一个位置，但你（在部分软件上）却可能需要按两次回删键才能完全删除（第一次按回删键只删除锐音符而保留“o”）——这实际上是两个字符。这种组合字符能让文字串的长度显得短但数据量却大，这也是为什么有的垃圾信息长度看起来短但却很耗处理性能，这种组合用的字符是不占宽度的。

Exif信息问题

见我们网站上对应的技术文章。

软件的版本号

有些软件的版本号是按照月份日期来制订的，例如“23.10”的意思是“2023年10月发布的正式版本”。这很直观。

有些软件的版本号用数字“1”左右的小数作版本号，通常这意味着它们期望版本号“1”为功能完整的正式版。但实际上，版本号小于“1”并不意味着功能差；版本号大于“1”也并不意味着存在的程序差错少，也不意味着开发和更新会停止。

软件版本号存在小数点时并不一定是指数学中的小数。例如“2.12”读作“二点一二”，版本号“2.2”实际上是早于“2.12”的版本。

软件版本号可能会有一些英文标识：Alpha（早期测试版）、Beta（中期测试版）、RC（Release Candidate，正式发布前的候选版本）。这些都不是正式版的意思，旨在告诉用户出现程序差错的可能性的太小。

消息转发器滋生的问题

消息转发器被用来跨平台地将一个通讯平台的消息转发到另一个或好几个不同的通讯平台的联系点。相互起效时，这可以实现不同平台的用户一起交流，作为消息互转器；或者仅仅单向起效，作为消息输出器，不会让会议室内的交流直接受室外因素干扰。

我们并不建议使用消息互转器。因为这会带来非常多的问题：

- 如果一起交流的人们组织性很强，那么这些问题的严重性就会稍小一点。不过话又说回来：如果人员们组织性很强，就像一个组织的或者就是一个组织的，那么也就不会分散到不同的交流平台（再用消息互转器）了。分散到不同的交流平台，本身就是组织性差的表现；使用消息互转器，则是一些人试图无视立场差异和目的差异来增多参与人数以活跃交流氛围，抱团取暖（作贬义）罢了。
- 每多串入一个不同的通讯平台，那么群聊的负责人就要多学习使用一个通讯平台，还要多学习管理一个不同平台的群聊。这是一个严重的原生问题。
- 不同平台一起交流的人们很可能会相互询问：别的联系平台“怎么样？”、“有什么功能？”、“安全吗？”、“怎么用？”等等，导致这个拼合群聊成为一个技术交流群，干扰本来的交流话题和交流目的，堵塞本来的交流进程。

- 不同地区的人们思想有的很进步，有的尚腐朽，而共产主义是全世界都必须做的事情。因此无可置疑：革命进程中的地域歧视是无法避免的，即使是革命派也无法避讳地域歧视，而且地域歧视也是革命派不该避讳的。通讯平台也是——不同的人们使用不同的通讯平台各有不同的目的。当提出“哪一个通讯平台最适合为社会主义革命服务？”、“为什么金星革命委员会不推荐其它通讯平台？”诸如此类的问题时，争执就不可避免地开始了。人们用各自喜欢的不同交流平台的的目的性越强，那么争执就越严重，同时可以从这个所谓的“技术问题”（或者被称为“兴趣爱好问题”）中看出政治思想和政治路线的严重差异。
- 消息转发器的形式和功能往往很简陋，就像自己用的交流平台缺失了很多重要的功能。例如，它常被用作进一步增强隐匿性的工具，这并不利于双方融洽交流、相互结识、共事——过于沉溺于隐匿，想要逃离社会，摆脱社会责任的人们要的正是这个。骂一句就走人了，讲完一句道理就不再回信答疑了。乌合之众，作鸟兽散。
- 管理问题。这既是一个技术问题（不同平台的设计不同、功能不同、操作指令不同，消息互转器有兼容性问题）；还是一个组织性问题。来自不同通讯平台的人们基本是属于不同组织的，严重时甚至毫无组织性。谁来当这个拼合群聊的统领呢？消息互转器又由谁负责呢？如果没有总的群聊管理员，那么这种议会制的小政治形式又如何保证各不同平台的群聊的管理人员能尽职且目标一致，默契配合呢？一旦有人在某个交流平台倒垃圾信息，那么所有串联的交流平台一起遭殃。
- 遗留问题。不同组织的人们一旦发现政治路线冲突，那么合作就会破裂。要么撤除消息互转器，把以前认识的不同通讯平台的人抛弃掉，置之不理；要么为了保持拼合群聊的存在而妥协求同存异，失去革命性。

敞门会议室人员们即使不喜欢有人安置消息转发器，也无法阻止有人不通知地安置一个仅旁听的消息输出器。面对此情景时请记住：

- （再说一次，）敞门会议室里的消息是全世界人都能看的，包括战友，包括敌人。
- 会议室的人们应该知道敞门会议室有被安置消息输出器的可能性。（这算好事，在场列表不会太长，节省了会议室座位，减轻了群聊服务器压力。）
- 如果期望有敌人过来试图参与交流，那么就应该刺激它们。单一类型刺激的效果强弱为：让它们的错误信仰破碎崩塌 > 让它们感到威胁 > 发布它们反对的主张 > 辱骂它们。

附录：周边疑问

不是所有的周边疑问都会在这里得到解答，不然这本说明书就太臃肿了。

会遇到什么样的人？

如果是问“有哪些种类的人？”，那么回答是“根本上决定于这个世界上有什么样的人（例如说外语的）（当然，它们还得用上XMPP）”。因为XMPP是开放给所有人用的。会有卑躬屈膝苟活的现实主义者，会有想改变世界的理想主义者。会有革命派，会有反动派。会有立场模糊的“中立”派，会有泥潭派。也会有倒垃圾的。

如果是问不同种类的人的占比，那么以下种类的人在XMPP宣传普及的初期总是占比较多的：

- 开源软件爱好者。非革命派的开源软件爱好者们对社会主义初学者们以及为政治活动而使用XMPP的初学者们有极强的误导性。
- 对政治感兴趣的人。这既包括只喜欢高谈阔论和唱戏的人们，也包括要真刀真枪地杀敌的人们。作为一个不受敌人的政治审查，不容易失联的交流平台，自然而然如此。
- 缺乏胆识的懦夫。许多人称不上是革命派，它们来到这个平台只是为了试图逃避帝国的追查，而缺乏和帝国对着干的准备。它们不为自己传播的言论负责，谣言很容易在它们中间传播开来并把它们吓得落荒而逃。
- 说大白话，不忌讳的人。相对受言论审查的互联网而言：这里说大白话的自然占比更多，你能见到很多在被政府控制的互联网平台上人们发布不出的言论。同时，造谣和传谣的成本与惩罚也更低；但最终是帝国的政府媒体造谣传谣厉害，还是XMPP平台的人们造谣传谣厉害，这是不确定的。
- 无头苍蝇。包括“口头革命派”、包括喜欢叫苦不迭的人们、包括自称“中立”同时却鬼话连篇的人们、包括只想看戏的人们。
- 男性。在资本主义社会里，男性和女性学习电子软件的兴趣和能力差别很明显。

至于你最初会遇到的人，这决定于你主动去找了哪些人，或者是谁把你带到XMPP平台的。

犯罪问题和法律问题

XMPP只是个工具，它本身没有也无法有任何犯罪的意愿，连“罪”的概念都没有。一些人试图通过消灭被人用于犯罪的工具来消灭犯罪，而我们负责消灭这种“非我也，兵也”态度的人。你不能因为糖品可作为炸弹的化学工业原料就把糖品禁止掉，你只能消灭让这个世界产生革命斗争的必要性的敌人。

“遵守法律（和道德）”基本是公共服务器管理员们的套话。要知道，法律这种东西之所以叫“法律”并出现和存在，就是因为有人不同意它。承认了法律的存在，本身就是承认了有不同意见的人存在。

一些XMPP公共服务器会告诉用户们“遵守法律”，少数服务器还可能让你走个敷衍的法律流程，但这都是套话了。鬼才知道某个用户有什么国籍、现在在哪个地区、管得着它的法律有哪些、这些法律是否相互冲突、它到底愿不愿意遵守等等。

“暗网”

“暗网”只是个抽象的技术概念，意味着（人们自愿的）匿名、私密、安全；它并不是和干违反道德之事绑定在一起的。如果将干坏事和暗网的概念绑定起来，那么帝国里任何一种流行的通讯工具，都算是“暗网”。通过它们诈骗、贩毒、嫖娼的，不算少。

就像敌人们会扭曲暗网的概念一样。敌人们当然也会恶毒地斥责XMPP和其它用来通讯的平台。

如果有一张“明网”，人人都公布自己的政治身份信息，并为自己的发表的言论负责；那么可以有效地激化社会矛盾，加速革命进程。但是只有动用政治力量才能做到这一点，保皇党不会这么做，革命党在夺得占领区并建立根据地之前也是无法做到的。

国家主义者问题

国家主义者们必然会嫌这种通信方式对政权造成威胁并大肆宣传它的敌对性和危险性。鼓励它们来参观一下，考验考验它们的政治立场是否坚定。

附录：供新手尝试的服务器地址列表

记住：不要（依赖XMPP可以换服务器用的特点而）把XMPP当做通过互联网封锁的工具！
身处有互联网封锁的国家的用户要么学会使用代理网络连接，要么改变政府。

有可能允许直接注册的服务器

redlibre.es
chat.sum7.eu
yourdata.forsale
libretank.org
jabjab.de
projectsegfau.lt
magicbroccoli.de
draugr.de
thesecure.biz
marxist.club
lsd-25.ru
01337.io
macaw.me
trashserver.net
conversations.im
chatterboxtown.us
creep.im
07f.de

只能在网页端注册的服务器

anoxinon.me
elaon.de
jabber.tcpreset.net
jabbx.de
jix.im
suchat.org
0n11ne.at
hookipa.net
jabber.systemausfall.org