Previous Page (https://blog.nowhere.moe/opsec/index.html)

XMRONLY - 30 / 11 / 2024

Easy Private Chats - SimpleX

Introduction

Online communication is one of the most ubiquitous activities on all of the internet. From newsletters, corporate emails and even down to instant messaging with friends, its spread cannot be denied. With such wide reach, it would seem very important to protect these communication channels, yet this is almost an after-thought for most mainstream messengers. Platforms with millions of users market their services with the latest buzz words yet close-source their protocols leaving users with a "trust me bro". With so many options to choose from how can we best decide which app to use? In this article we'll compare a few options (Telegram, Signal and SimpleX) to see how their technical details stack up and determine which is best for easy private chats.

Overview of Telegram, Signal and SimpleX

Telegram is a very popular messaging app that boasts close to 1 billion (https://www.statista.com/

statistics/258749/most-popular-global-mobile-messenger-apps/) active users worldwide. With support for massive chatrooms, Telegram is almost more akin to social media than to a traditional messaging app. Many companies offer news, updates, and support through their official Telegram channels making it a very convenient place for users to stay up to date with various interests. Due to its strong stance on free speech, Telegram built a reputation for not cooperating with law enforcement investigations. However, after the arrest of CEO Pavel Durov in part relating to Telegram's refusal hand over user data in lawful orders, Telegram changed their privacy policy (https://files.catbox.moe/988lhl.png) to say they may share user phone numbers and IP addresses and indeed have done so (https://www.404media.co/telegram-confirms-it-gave-u-s-user-data-to-the-cops/). Telegram supports E2EE but this is not enabled by default, which is probably its most significant drawback.

Signal is a champion for user freedom and its state-of-the-art security is the foundation upon which other chat applications are built. Signal is very intuitive to use, supporting all of the usual text/image/voice/video/etc features that users expect. Unlike Telegram, Signal is E2EE by default and the only information it knows about users are their phone number and time of registration. Numerous court orders (https://signal.org/bigbrother/) have solidified how Signal has nothing else to hand over to law enforcement. The phone number requirement for SMS verification, while concretely a drawback if not acquired anonymously (https://blog.nowhere.moe/opsec/anonsms/index.html), is an intentional decision for Signal's target audience (normies) as everyday users can be notified if other stored contacts join Signal.

SimpleX is a relative newcomer on the scene and has a unique angle in that there are no user identifies of any kind. As such, users can create unlimited profiles (and even hidden profiles to improve plausible deniability) and connect with others anonymously. Unlike Signal, SimpleX supports native onion routing as well as the ability to self-host servers. Because of its default E2EE, servers are not able to see message contents and self-hosted servers can be shared with others, contributing to decentralization and thus making SimpleX more resilient. SimpleX's founder, in an interview (https://www.wired.com/story/neo-nazis-flee-telegram-encrypted-app-simplex/), implied that SimpleX sees no information about its users but since it is new, it remains to be seen how they would respond to actual court orders. SimpleX has received some criticism for its reliance on Venture Capital to establish itself while it works to develop a business model.

A comparison from privacyspreadsheet.com (https://privacyspreadsheet.com/messaging-apps) has a breakdown of all the technical details.

		Telegram	Signal	Simplex
2	Recommended for private communication?	No	Yes	Yes
3	End to end encrypted by default	No	Yes	Yes
4	End to end encryption is available	Yes	Yes	Yes
5	Voice/video calls are end to end encrypted	Sometimes	Yes	Yes
6	Utilizes Perfect Forward Secrecy	No	Yes	Yes
7	Data is encrypted in transit	Yes	Yes	Yes
8	Data is encrypted at rest (server side)	Sometimes	Yes	Yes
9	Data is encrypted at rest (client side)	No	Yes	Yes
10	Decentralized network	No	No	Yes
11	Dependant on DNS	Yes	Yes	No
12	Requires global identity	Yes	Yes	No
13	Email required for signup	No	No	No
14	Phone required for signup	Yes	Yes	No
15	Billing details required for signup	No	No	No
16	App and Server are fully open source	No	No	Yes
17	You can verify contacts out of band	No	Yes	Yes
18	You can self-host the platform	No	Yes	Yes
19	Third-party clients are allowed	Yes	Sometimes	Yes
20	Client provides a portable database	No	Android Only	Yes
21	Client functions over overlay networks	Sometimes	Sometimes	Yes
22	There has been a third party code audit	No	Yes	Yes
23	Users must exchange phone numbers	No	Yes	No
24	Provider can scan for illegal content	Yes	No	No
25	Provider trains AI with user data	No	No	No
26	Provider uses user data for marketing	No	No	No
27	Provider can shut down a community	Yes	No	No
28	Provider is funded by authoritarian regimes	Russia	USA	No
29	Provider actively feeds data to law enforcen	No	No	No
30	Provider complies with preservation reques	No	No	No
31	Client scans users photo/video library	No	No	No
32	Client removes image metadata	No	Yes	Yes
33	Linked to external account	No	No	No
34	Client logs users location	No	No	No
35	Client logs running processes	No	No	No
36	Can be hosted on an airgapped network	No	No	Yes
37	Deleted messages are removed immediatel	Yes	Yes	Yes
38	Recieved messages are removed from serv	No	Yes	Yes
39				
40	What can the apps hand to police?			
41	IP address	Yes	No	No
42	Real name	Yes	No	No
43	Username	Yes	N/A	N/A
44	Phone number	Yes	Yes	N/A
45	Email address	Sometimes	No	N/A
46	Message contents	Sometimes	No	No
47	Crypto wallets	Yes	No	N/A
48	Profile pictures	Yes	No	No
49	Account creation date	Yes	Yes	No
50	Account last active timestamp	Yes	Yes	No
51	Billing details	No	No	N/A
52	Groups that you manage	Yes	No	No
53	Groups that you are a member of	No	No	No
54	Channels / broadcast rooms you are a mem	Yes	N/A	No
55	People you talk to	No	No	No
56	People you've blocked	No	No	No
57	People who have blocked you	No	No	No
58				
59	What can an adversary find on their own?			
60	IP address	No	No	No
61	Real name	No	No	No
62	Username	Yes	N/A	No
63	Phone number	Sometimes	Yes	No
64	Email address	No	No	No
65	Message contents	No	No	No
66	Crypto wallets	No	N/A	N/A
67	Profile pictures	Sometimes	No	No
68	Account creation date	No	No	No

69	Account last active timestamp	Sometimes	No	No
70	Billing details	No	No	No
71	Groups that you are a member of	No	No	No
72	Channels / broadcast rooms you are a mem	Sometimes	No	No
73	People you talk to	No	No	No
74	People you've blocked	No	No	No
75	People who have blocked you	No	No	No

When selecting a messaging app, certain OPSEC criteria (https://blog.nowhere.moe/opsec/anonsimplex/index.html) should be considered.

Privacy:

1. The application is free and open source (FOSS).
2. The application is end-to-end-encrypted by default (E2EE).
3. The application allows self-hosting our own servers (Decentralization).

Anonymity:

1. The application supports Tor servers out of the box (Onion Routing).
2. The application requires no sign-up information (Emails, Usernames, Phone Numbers).
3. The application allows joining chatrooms without revealing our identity (Incognito Mode).

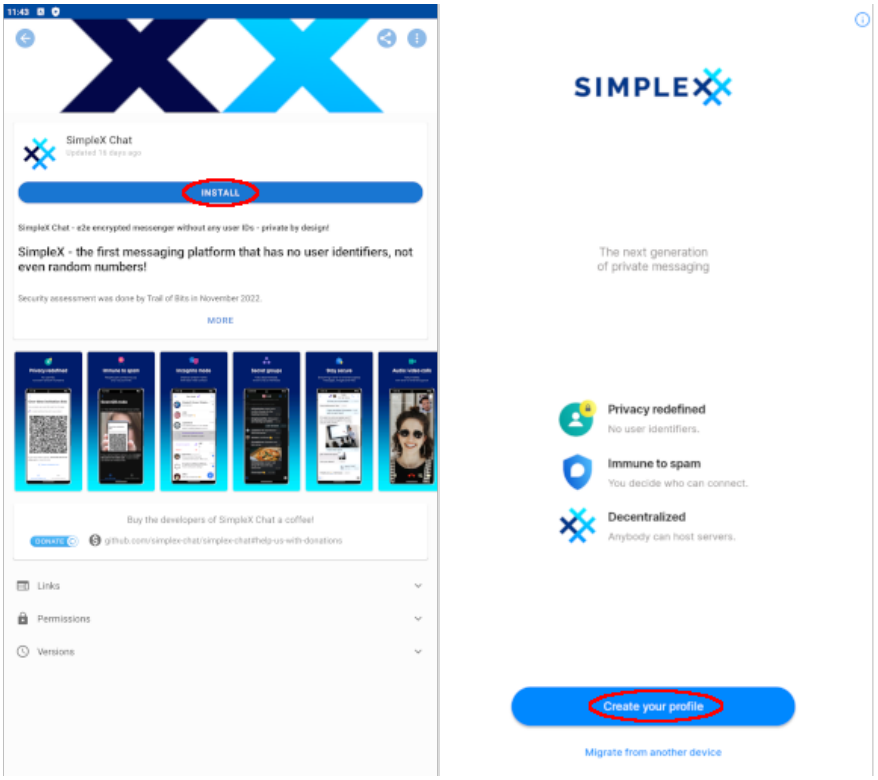
Deniability:

1. The application allows disappearing messages (Plausible Deniability).
2. The application allows creation/deletion of multiple profiles (Plausible Deniability).
3. The application allows hidden profiles (Plausible Deniability).

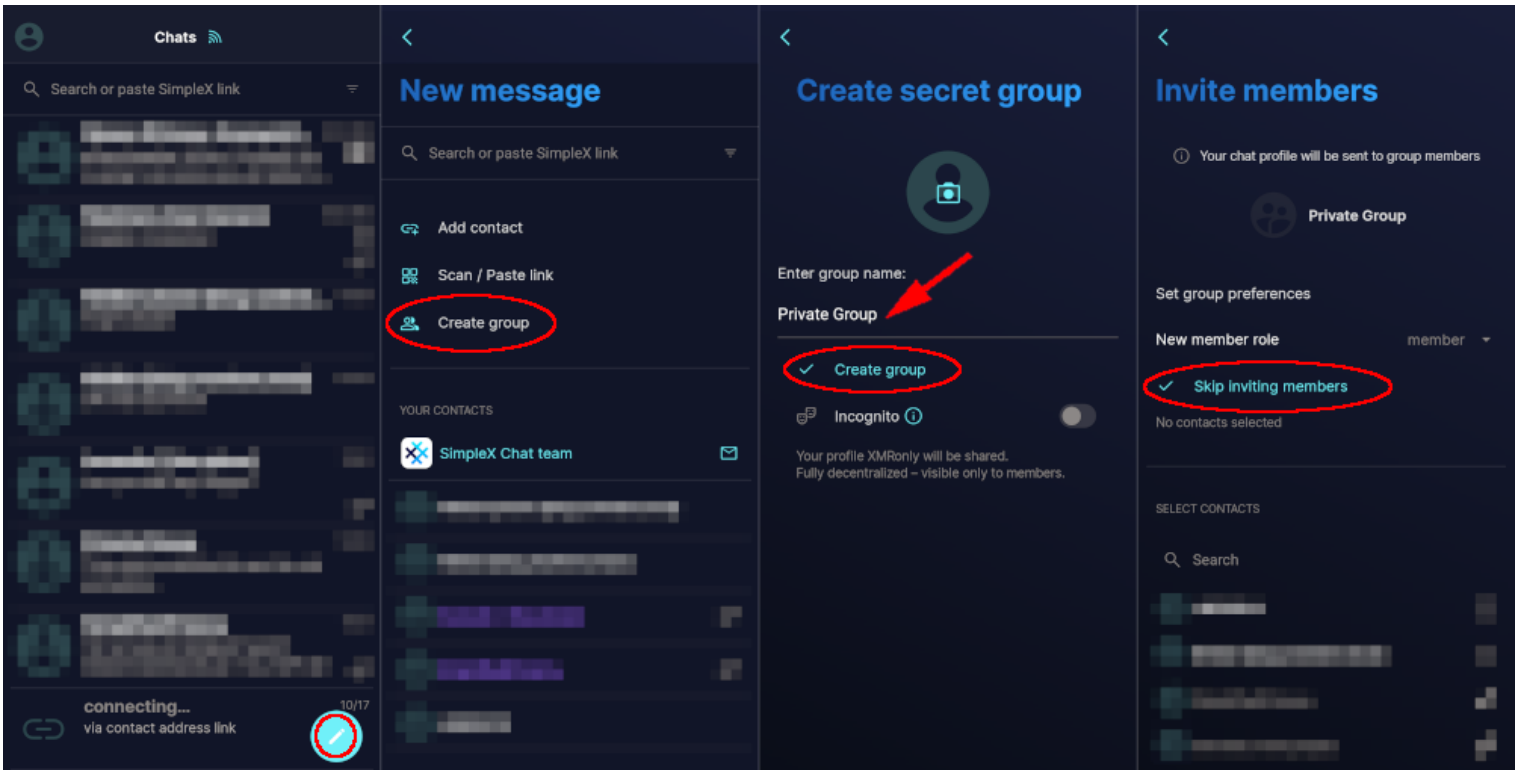
From the above comparison, we can see that only SimpleX meets all of the criteria. While we only focus on Privacy in this article, it doesn't hurt to have the other benefits of Anonymity and Plausible Deniability.

Using SimpleX

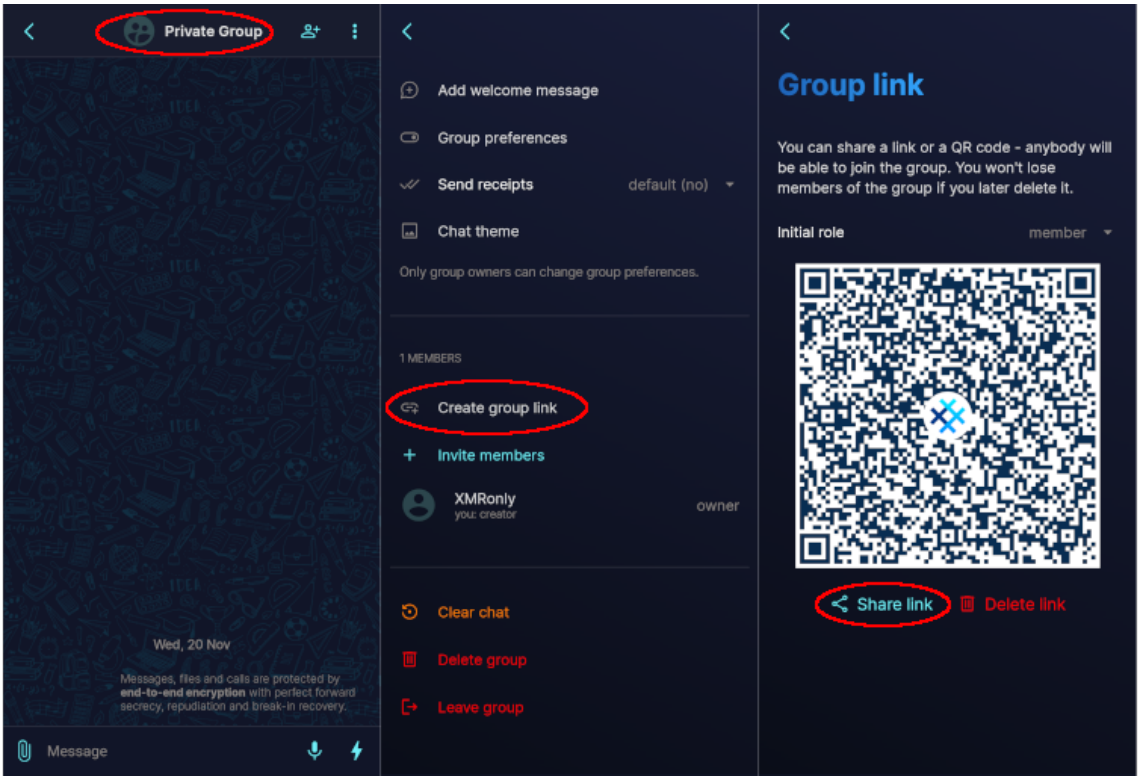
To start using SimpleX, we will start by installing it from F-Droid (https://f-droid.org/packages/chat.simplex.app/). Search for the app and then click Install. Navigate through the setup process, choose a username and click Create your profile.



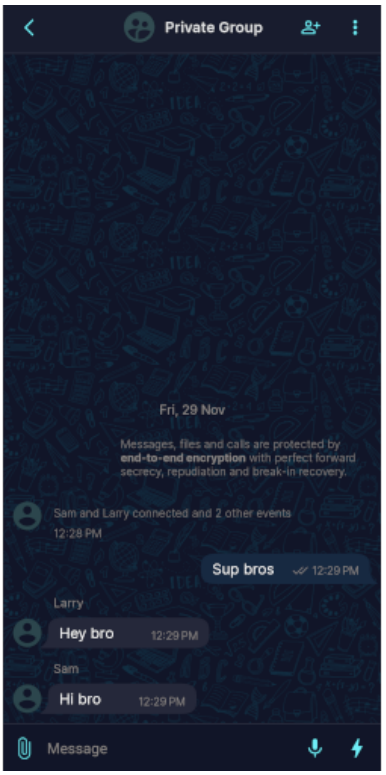
With your profile complete, it's time to create a private group chat. Click on the pencil icon at the bottom of the screen and select Create group. Give your group a name and click Create group. Finally, skip inviting members for now.



Click on the group name to see some options. Click on Create group link. Finally, share the group link with your friends out-of-band.



Once your friends connect, you can start messaging.



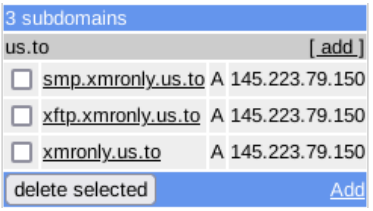
Out of the box, SimpleX works perfectly fine. However, more advanced users may wish to tweak a few settings or self-host their own servers.

Self-Hosting SimpleX Servers

Requirements

1. A VPS running Debian 12 (or Ubuntu 22.04)
2. A domain name (or subdomain)

To start, we will need a domain name. A subdomain such as a free one obtained from **https://freedns.afraid.org** will also work. Create A record entries for smp.yourdomain.tld and xftp.yourdomain.tld and point them at the IP address of your VPS.



We will SSH into our VPS and set up our environment.

```
~ ❯ torsocks ssh root@145.223.79.150
The authenticity of host '145.223.79.150 (145.223.79.150)' can't be established.
ED25519 key fingerprint is SHA256:AGZHyLpidaSu+ZE3cLFZ3KWxQq3Mx9rDH+HLVNF/okc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '145.223.79.150' (ED25519) to the list of known hosts.
root@145.223.79.150's password:
Linux srv636770 6.1.0-26-cloud-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.112-1 (2024-09-30) x
86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 20 21:05:02 2024 from 185.220.101.103
root@srv636770:~#
```

Once connected, we will follow the official instructions (https://docs.docker.com/engine/install/debian/) to install Docker. Run:

```
# Add Docker's official GPG key:
apt update
apt install -y ca-certificates curl gnupg openssl vim
install -m 0755 -d /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/debian/gpg | gpg --dearmor -o /etc/apt/keyring
s/docker.gpg
chmod a+r /etc/apt/keyrings/docker.gpg

# Add the repository to Apt sources:
echo \
"deb [arch="$(dpkg --print-architecture)" signed-by=/etc/apt/keyrings/docker.gpg] https://d
ownload.docker.com/linux/debian \
"$(. /etc/os-release && echo "$VERSION_CODENAME")" stable" | \
tee /etc/apt/sources.list.d/docker.list > /dev/null
apt update
```

With the Docker apt repositories out of the way, install the Docker packages:

```
apt install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-pl
ugin
```

OPTIONAL: You can test everything is working up to this point by a deploying a test container to see some output. Run:

```
docker run hello-world
```

We will now set up a docker-compose.yml file with all the build instructions:

```
vim docker-compose.yml
```

Copy/paste the following and change the **ADDR** fields to your domain.
HINT: It's **p** to paste in vim, then **ESC :wq** to write changes and quit the file.

```
networks:
  simplex:
```

```
services:
  simplex-smp-server:
    image: simplexchat/smp-server:v6.0.6
    container_name: simplex-smp
    restart: unless-stopped
    ports:
      - "5223:5223"
    volumes:
      - ./simplex/smp/config:/etc/opt/simplex:Z
      - ./simplex/smp/logs:/var/opt/simplex:Z
    environment:
      - ADDR=smp.xmronly.us.to
#     - PASS=${SIMPLEX_PASSWORD} #for non public servers
    networks:
      - simplex
    security_opt:
      - no-new-privileges:true
    cap_drop:
      - ALL

  simplex-xftp-server:
    image: simplexchat/xftp-server:v6.1.3
    container_name: simplex-xftp
    ports:
      - "443:443"
    restart: unless-stopped
    volumes:
      - ./simplex/xftp/config:/etc/opt/simplex-xftp:Z
      - ./simplex/xftp/logs:/var/opt/simplex-xftp:Z
      - ./simplex/xftp/files:/srv/xftp:X
    environment:
      - ADDR=xftp.xmronly.us.to
      - QUOTA=10gb #change to set your own quota
    networks:
      - simplex
    security_opt:
      - no-new-privileges:true
    cap_drop:
      - ALL
```

A note about versioning: at the time of writing, there was an open issue (https://github.com/simplex-chat/simplexmq/issues/1373) with the "latest" (v6.1.3) tag and HTTPS credentials for the SMP server. The most recent working version for the SMP server (v6.0.6) was definitively tagged here and the "latest" version for XFTP server (v6.1.3) was also definitively tagged to ensure working builds with the presented instructions. For reference, the "latest" version used in the HackLiberty (https://forum.hackliberty.org/t/simplex-server-docker-installation-guide-smp-xftp/140) documentation for June 1st, 2024 is v5.8.0-beta.6 which is now several security fixes behind.

Everything is now ready to be deployed. Run:

```
docker compose up -d
```

Run the following command to see the SMP and XFTP server addresses:

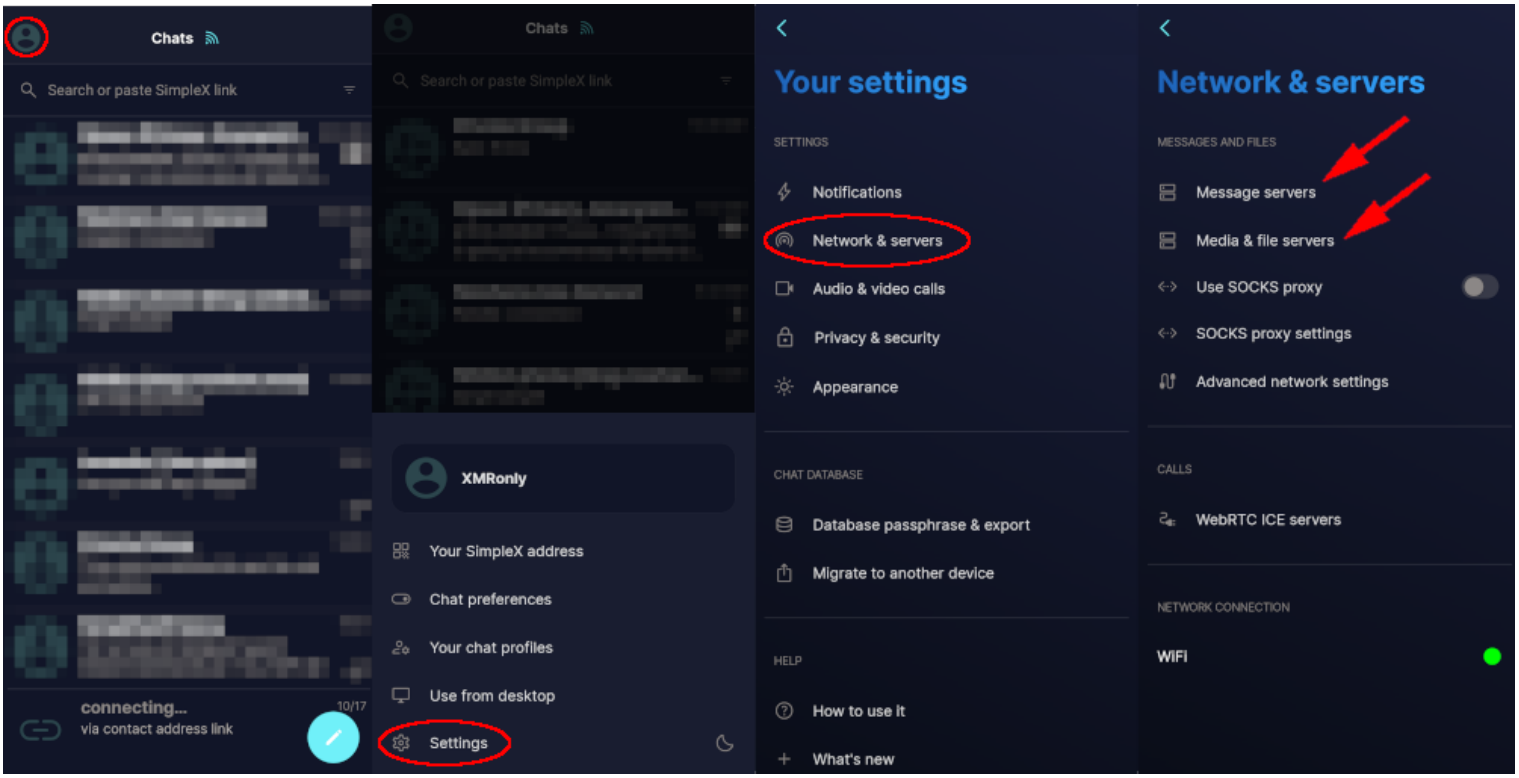
```
echo "smp://$(<simplex/smp/config/fingerprint)@$(awk -F '=' '/ADDR=/ {print $2}' docker-com
pose.yml | head -1)" && \
echo "xftp://$(<simplex/xftp/config/fingerprint)@$(awk -F '=' '/ADDR=/ {print $2}' docker-c
ompose.yml | tail -1)"
```

You should see output similar to this and just like that your self-hosted SimpleX servers are now ready!

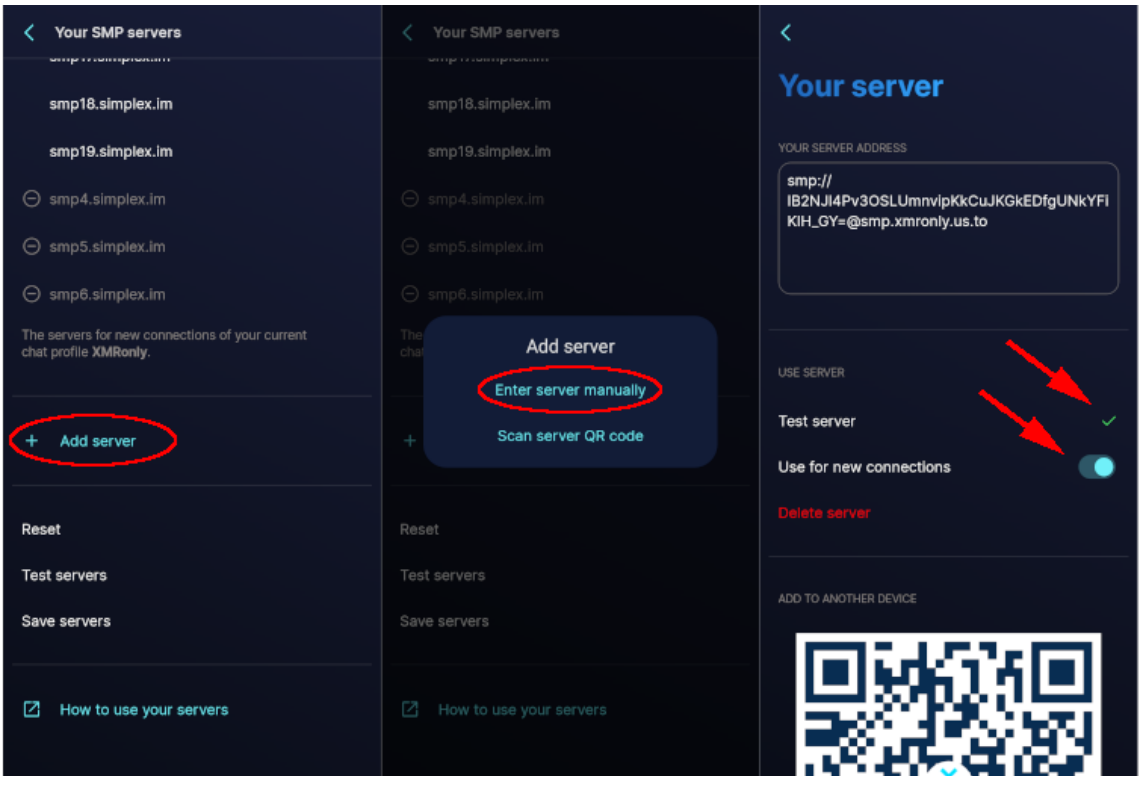
```
smp://IB2NJl4Pv3OSLUmnvipKkCuJKGkEDfgUNkYFiKIH_GY=@smp.xmronly.us.to
xftp://t_H_I_h5Iz7X-ChxA3nJeyw0s_2PJIFkfSK7Ng6UulU=@xftp.xmronly.us.to
```

Adding Your Self-Hosted SimpleX Servers

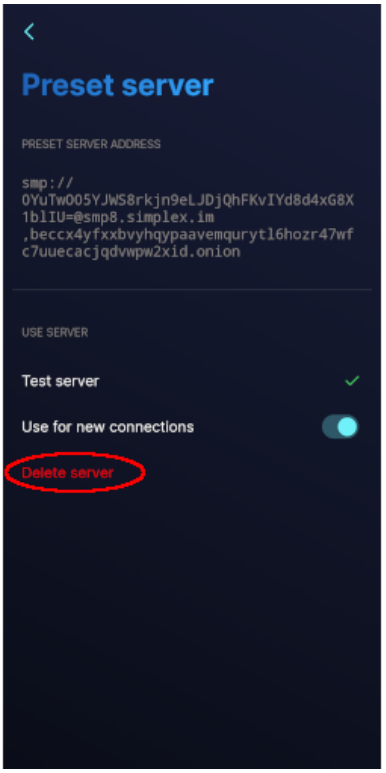
To add the newly created self-hosted SimpleX servers to your client, click on your profile on the top left, followed by Settings. Click on Network & servers. We will modify both the Message servers (SMP) and the Media & file servers (XFTP).



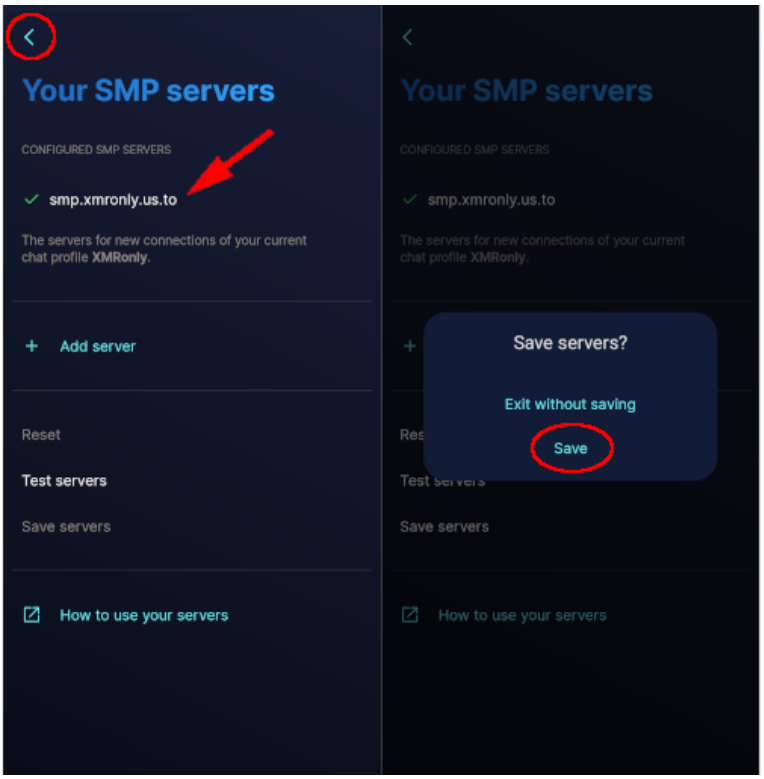
Click on **Message servers** and scroll down to Add server. Select Enter server manually. Paste in your SMP server address from above, click Test server and receive a green check mark. Finally, tick Use for new connections.



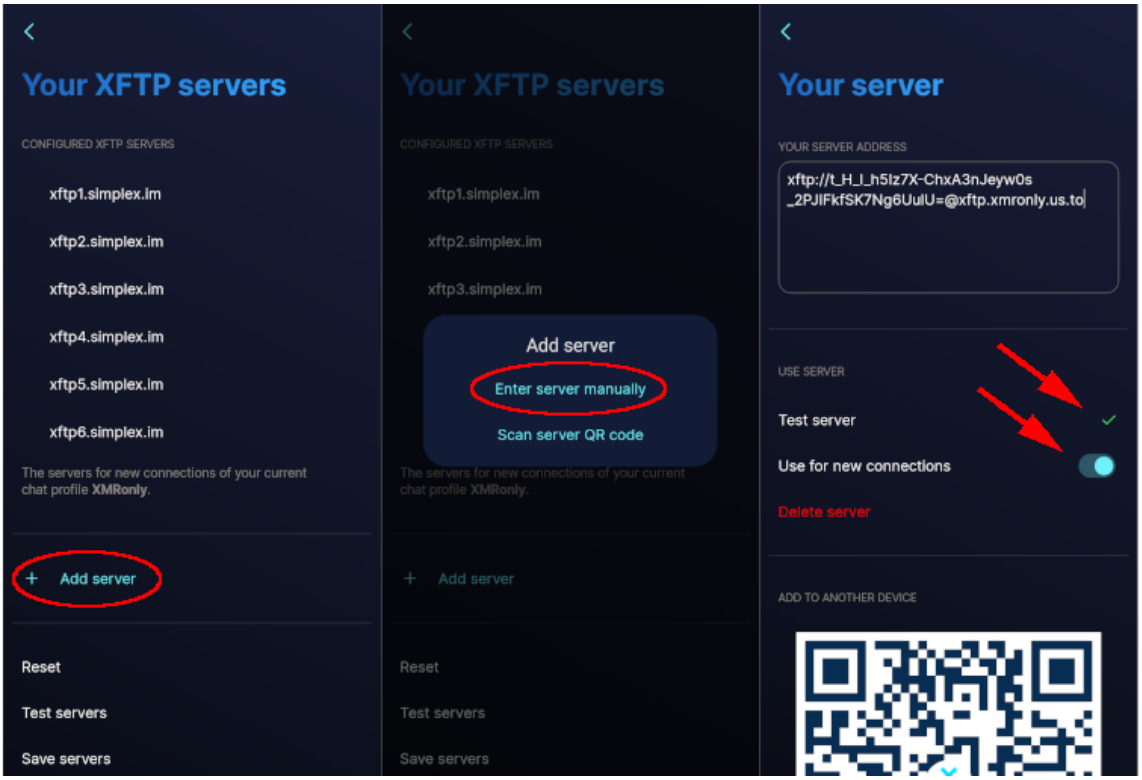
With our self-hosted SMP server set, it's time to remove the default SimpleX servers. Click on each of the presets, then click Delete server.



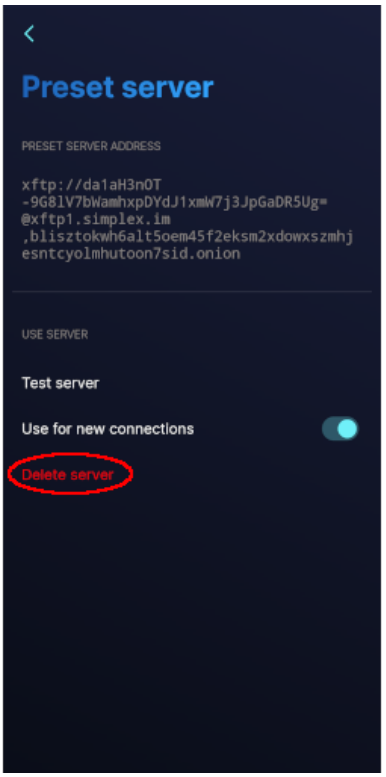
With only our self-hosted SMP server remaining, click the back arrow, then save changes.



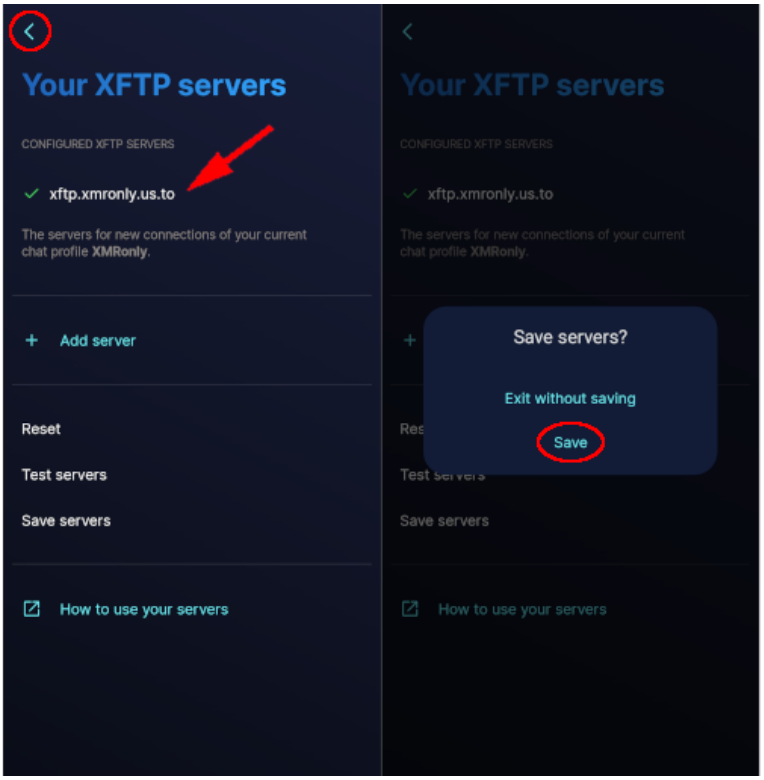
We will now repeat the process for **Media & file servers**. Scroll down to Add server. Select Enter server manually. Paste in your XFTP server address from above, click Test server and receive a green check mark. Finally, tick Use for new connections.



With our self-hosted XFTP server set, it's time to remove the default SimpleX servers. Click on each of the presets, then click Delete server.



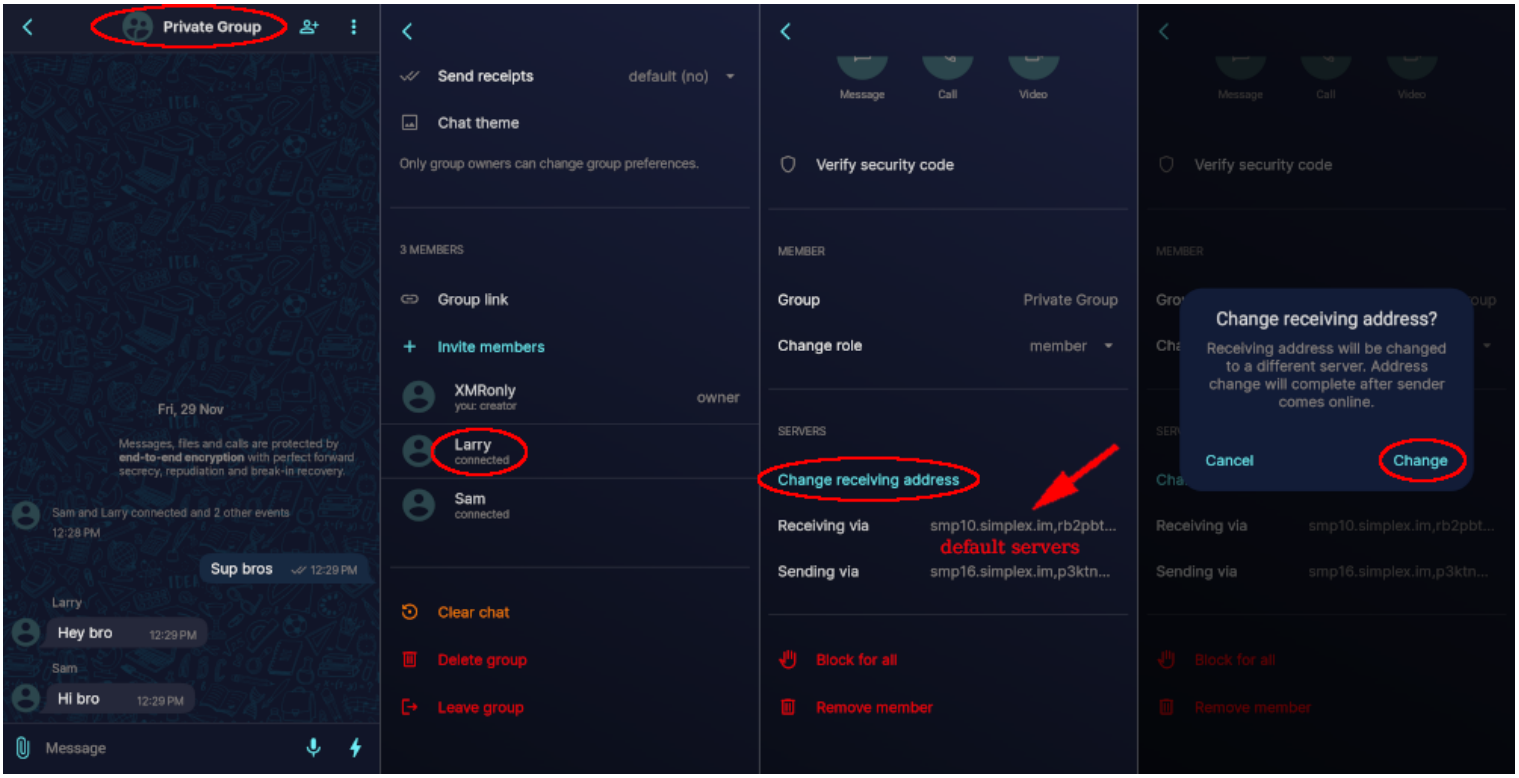
With only our self-hosted XFTP server remaining, click the back arrow, then save changes.



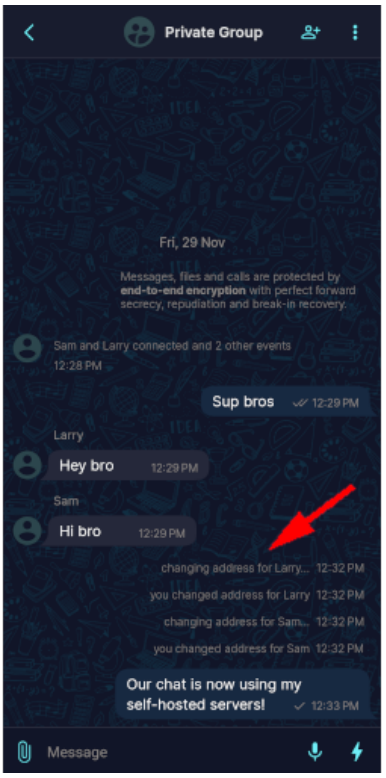
It is possible to self-host onion servers as well, but since this article is focusing on privacy and not anonymity, that part of the setup has been omitted.

Using Your Self-Hosted SimpleX Servers

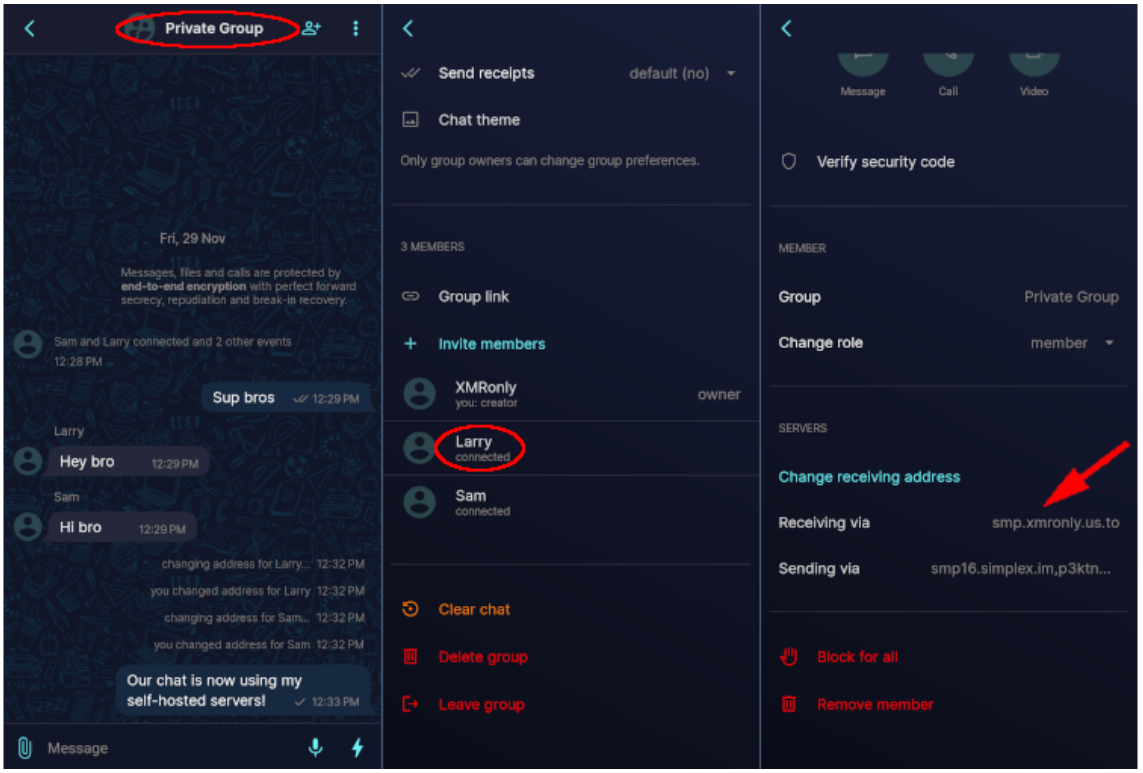
All new connections will automatically use your self-hosted SimpleX servers, but what about already existing connections that were made using the default Simplex servers? It turns out existing connections do not automatically update, so we will need to manually change them. Click on the group name and scroll down to the members section. Click on a group member and scroll down to servers. We can see that Larry is using the default SimpleX servers. Click on Change receiving address and confirm the change.



Repeat the process for Sam and you have now configured the group chat to use your self-hosted servers!



You can confirm this by clicking on the group chat name and clicking on any of the members.



Conclusion

In this article we saw how SimpleX compares to a few other popular instant messengers and some of its unique advantages. We saw how to easily install and start using it, and going the extra mile, how to self-host and use your own servers. With that knowledge in hand, you can easily make all your chats private!

Nihilism

Until there is Nothing left.

My Links

RSS Feed (http://blog.nowhere.moe/rss/feed.xml)

SimpleX Chat (https://simplex.chat/contact#/?v=2-7&smp=smp%3A%2F%2FL5jrGV2L_Bb20Oj0aE4Gn-m5AHet9XdpYDotiqpcpGc%3D%40nowhere.moe%2FH4g7zPbitSLV5tDQ51Yz-R6RgOkMEeCc%23%2F%3Fv%3D1-3%26dh%3DMCowBQYDK2VuAyEAkts5T5AMxHGrZCCg12aeKxWcpXaxbB_XqjrXmcFYlDQ%253D&data=%7B%22type%22%3A%22group%22%2C%22groupLinkId%22%3A%22c3Y-iDaoDCFm6RhptSDOaw%3D%3D%22%7D)

About nihilist

Donate XMR:

8AUYjhQeG3D5aodJDtqG499N5jXXM71gYKD8LgSsFB9BUV1o7muLv3DXHoydRTK4SZaaUBq4EAUqpZHLrX2VZLH71Jrd9k8

Donate XMR to the author:

8AHNGepbz9844kfCqR4aVTCSyJvEKZhtxdyz6Qn8yhP2gLj5u541BqwXR7VTwYwMqbGc8ZGNj3RWMNQuboxnb1X4HobhSv3

Contact: nihilist@contact.nowhere.moe (PGP (https://nowhere.moe/nihilist.pubkey))