build GitHub downloads GitHub release Join on Reddit Follow on Mastodon

| 30/03/2023 | EN, FR, CZ |

SimpleX - the first messaging platform that has no user identifiers of any kind - 100% private by design!

Welcome to SimpleX Chat!

1. Install the app.
2. ↔ Connect to the team, join user groups and follow our updates.
3. Make a private connection with a friend.
4. Help translating SimpleX Chat.
5. ⚡ Contribute and help us with donations.

Learn more about SimpleX Chat.

Install the app

iOS app Android app F-Droid iOS TestFlight APK

- 📷 Protects your messages and metadata - who you talk to and when.
- Double ratchet end-to-end encryption, with additional encryption layer.
- Mobile apps for Android (Google Play, APK) and iOS.
- TestFlight preview for iOS with the new features 1-2 weeks earlier - **limited to 10,000 users**!
- 🖥 Available as a terminal (console) app / CLI on Linux, MacOS, Windows.

Connect to the team

You can connect to the team via the app using "chat with the developers button" available when you have no conversations in the profile, "Send questions and ideas" in the app settings or via our SimpleX address. Please connect to:

- to ask any questions
- to suggest any improvements
- to share anything relevant

We are replying the questions manually, so it is not instant – it can take up to 24 hours.

If you are interested in helping us to integrate open-source language models, and in joining our team, please get in touch.

Join user groups

You can join the groups created by other users via the new directory service. We are not responsible for the content shared in these groups.

Please note: The groups below are created for the users to be able to ask questions, make suggestions and ask questions about SimpleX Chat only.

You also can:

- criticize the app, and make comparisons with other messengers.
- share new messengers you think could be interesting for privacy, as long as you don't spam.
- share some privacy related publications, infrequently.
- having preliminary approved with the admin in direct message, share the link to a group you created, but only once. Once the group has more than 10 members it can be submitted to SimpleX Directory Service where the new users will be able to discover it.

You must:

- be polite to other users
- avoid spam (too frequent messages, even if they are relevant)
- avoid any personal attacks or hostility.
- avoid sharing any content that is not relevant to the above (that includes, but is not limited to, discussing politics or any aspects of society other than privacy, security, technology and communications, sharing any content that may be found offensive by other users, etc.).

Messages not following these rules will be deleted, the right to send messages may be revoked, and the access to the new members to the group may be temporarily restricted, to prevent re-joining under a different name - our imperfect group moderation does not have a better solution at the moment.

You can join an English-speaking users group if you want to ask any questions: #SimpleX-Group-4

There is also a group #simplex-devs for developers who build on SimpleX platform:

- chat bots and automations
- integrations with other apps
- social apps and services
- etc.

There are groups in other languages, that we have the apps interface translated into. These groups are for testing, and asking questions to other SimpleX Chat users:

#SimpleX-DE (German-speaking), #SimpleX-ES (Spanish-speaking), #SimpleX-FR (French-speaking), #SimpleX-RU (Russian-speaking), #SimpleX-IT (Italian-speaking).

You can join either by opening these links in the app or by opening them in a desktop browser and scanning the QR code.

Follow our updates

We publish our updates and releases via:

- Reddit, Twitter, Lemmy, Mastodon and Nostr.
- SimpleX Chat team profile.
- blog and RSS feed.
- mailing list, very rarely.

Make a private connection

You need to share a link with your friend or scan a QR code from their phone, in person or during a video call, to make a connection and start messaging.

The channel through which you share the link does not have to be secure - it is enough that you can confirm who sent you the message and that your SimpleX connection is established.

Make a private connection Conversation Video call

After you connect, you can verify connection security code.

User guide (NEW)

Read about the app features and settings in the new User guide.

Help translating SimpleX Chat

Thanks to our users and Weblate, SimpleX Chat apps, website and documents are translated to many other languages.

Join our translators to help SimpleX grow!

locale	language	contributor	**Android** and **iOS**	**website**	Github docs	
en	English		✓	✓	✓	✓
ar	العربية	jermanuts	android app -	website		
bg	Български		android app ios app			
cs	Čeština	zen0bit	android app ios app	website	✓	
de	Deutsch	mlanp	android app ios app	website		
es	Español	Mateyhv	android app ios app	website		
fi	Suomi			website		

locale	language	contributor	Android and iOS	website	Github docs
			android app ios app		
fr	Français	ishi_sama	android app ios app	website	✓
he	עִבְרִית		android app -		
it	Italiano	unbranched	android app ios app	website	
ja	日本語		android app ios app	website	
nl	Nederlands	mika-nl	android app ios app	website	
pl	Polski	BxOxSxS	android app ios app		
pt-BR	Português		android app -	website	
ru	Русский		android app ios app		
th	ภาษาไทย	titapa-punpun	android app ios app		
uk	Українська		android app ios app	website	
zh-CHS	简体中文	sith-on-mars	android app ios app		
		Float-hu		website	

Languages in progress: Arabic, Japanese, Korean, Portuguese and others. We will be adding more languages as some of the already added are completed – please suggest new languages, review the translation guide and get in touch with us!

Contribute

We would love to have you join the development! You can help us with:

- share the color theme you use in Android app!
- writing a tutorial or recipes about hosting servers, chat bot automations, etc.
- contributing to SimpleX Chat knowledge-base.
- developing features - please connect to us via chat so we can help you get started.

Help us with donations

Huge thank you to everybody who donated to SimpleX Chat!

We are prioritizing users privacy and security - it would be impossible without your support.

Our pledge to our users is that SimpleX protocols are and will remain open, and in public domain, - so anybody can build the future implementations of the clients and the servers. We are building SimpleX platform based on the same principles as email and web, but much more private and secure.

Your donations help us raise more funds – any amount, even the price of the cup of coffee, would make a big difference for us.

It is possible to donate via:

- GitHub - it is commission-free for us.
- OpenCollective - it charges a commission, and also accepts donations in crypto-currencies.
- Monero: 8568eeVjaJ1RQ65ZUn9PRQ8ENtqeX9VVhcCYYhnVLxhV4JtBqw42so2VEUDQZNk
- Bitcoin: 1bpefFkzuRoMY3ZuBbZNZxycbg7NYPYTG
- BCH: 1bpefFkzuRoMY3ZuBbZNZxycbg7NYPYTG
- USDT:
  - BNB Smart Chain: 0x83fd788f7241a2be61780ea9dc72d2151e6843e2
  - Tron: TNnTrKLBmdy2Wn3cAQR98dAVvWhLskQGfW
- Ethereum: 0x83fd788f7241a2be61780ea9dc72d2151e6843e2
- Solana: 43tWFWDczgAcn4Rzwkpqg2mqwnQETSiTwznmCgA2tf1L

Thank you,

Evgeny

SimpleX Chat founder

Contents

Why privacy matters

Everyone should care about privacy and security of their communications - innocuous conversations can put you in danger even if there is nothing to hide.

One of the most shocking stories is the experience of Mohamedou Ould Salahi that he wrote about in his memoir and that is shown in The Mauritanian movie. He was put into Guantanamo camp, without trial, and was tortured there for 15 years after a phone call to his relative in Afghanistan, under suspicion of being involved in 9/11 attacks, even though he lived in Germany for the 10 years prior to the attacks.

It is not enough to use an end-to-end encrypted messenger, we all should use the messengers that protect the privacy of our personal networks - who we are connected with.

SimpleX approach to privacy and security

Complete privacy of your identity, profile, contacts and metadata

Unlike any other existing messaging platform, SimpleX has no identifiers assigned to the users - not even random numbers. This protects the privacy of who are you communicating with, hiding it from SimpleX platform servers and from any observers. Read more.

The best protection against spam and abuse

As you have no identifier on SimpleX platform, you cannot be contacted unless you share a one-time invitation link or an optional temporary user address. Read more.

Complete ownership, control and security of your data

SimpleX stores all user data on client devices, the messages are only held temporarily on SimpleX relay servers until they are received. Read more.

Users own SimpleX network

You can use SimpleX with your own servers and still communicate with people using the servers that are pre-configured in the apps or any other SimpleX servers. Read more.

Frequently asked questions

1. How SimpleX can deliver messages without any user identifiers? See v2 release announcement explaining how SimpleX works.

2. Why should I not just use Signal? Signal is a centralized platform that uses phone numbers to identify its users and their contacts. It means that while the content of your messages on Signal is protected with robust end-to-end encryption, there is a large amount of meta-data visible to Signal - who you talk with and when.

3. How is it different from Matrix, Session, Ricochet, Cwtch, etc., that also don't require user identities? Although these platforms do not require a real identity, they do rely on anonymous user identities to deliver messages – it can be, for example, an identity key or a random number. Using a persistent user identity, even anonymous, creates a risk that user's connection graph becomes known to the observers and/or service providers, and it can lead to de-anonymizing some users. If the same user profile is used to connect to two different people via any messenger other than SimpleX, these two people can confirm if they are connected to the same person - they would use the same user identifier in the messages. With SimpleX there is no meta-data in common between your conversations with different contacts - the quality that no other messaging platform has.

News and updates

Recent and important updates:

Sep 25, 2023. SimpleX Chat v5.3 released: desktop app, local file encryption, improved groups and directory service.

Jul 22, 2023. SimpleX Chat: v5.2 released with message delivery receipts.

May 23, 2023. SimpleX Chat: v5.1 released with message reactions and self-destruct passcode.

Apr 22, 2023. SimpleX Chat: vision and funding, v5.0 released with videos and files up to 1gb.

Mar 1, 2023. SimpleX File Transfer Protocol – send large files efficiently, privately and securely, soon to be integrated into SimpleX Chat apps..

Nov 8, 2022. Security audit by Trail of Bits, the new website and v4.2 released.

Sep 28, 2022. v4.0: encrypted local chat database and many other changes.

All updates

:zap: Quick installation of a terminal app

```
sh curl -o- https://raw.githubusercontent.com/simplex-chat/simplex-chat/stable/install.sh | bash
```

Once the chat client is installed, simply run `simplex-chat` from your terminal.

simplex-chat

Read more about installing and using the terminal app.

SimpleX Platform design

SimpleX is a client-server network with a unique network topology that uses redundant, disposable message relay nodes to asynchronously pass messages via unidirectional (simplex) message queues, providing recipient and sender anonymity.

Unlike P2P networks, all messages are passed through one or several server nodes, that do not even need to have persistence. In fact, the current SMP server implementation uses in-memory message storage, persisting only the queue records. SimpleX provides better metadata protection than P2P designs, as no global participant identifiers are used to deliver messages, and avoids the problems of P2P networks.

Unlike federated networks, the server nodes **do not have records of the users**, **do not communicate with each other** and **do not store messages** after they are delivered to the recipients. There is no way to discover the full list of servers participating in SimpleX network. This design avoids the problem of metadata visibility that all federated networks have and better protects from the network-wide attacks.

Only the client devices have information about users, their contacts and groups.

See SimpleX whitepaper for more information on platform objectives and technical design.

See SimpleX Chat Protocol for the format of messages sent between chat clients over SimpleX Messaging Protocol.

Privacy and security: technical details and limitations

SimpleX Chat is a work in progress – we are releasing improvements as they are ready. You have to decide if the current state is good enough for your usage scenario.

We compiled a glossary of terms used to describe communication systems to help understand some terms below and to help compare advantages and disadvantages of various communication systems.

What is already implemented:

1. Instead of user profile identifiers used by all other platforms, even the most private ones, SimpleX uses pairwise per-queue identifiers (2 addresses for each unidirectional message queue, with an optional 3rd address for push notifications on iOS, 2 queues in each connection

between the users). It makes observing the network graph on the application level more difficult, as for `n` users there can be up to `n * (n-1)` message queues.

2. End-to-end encryption in each message queue using NaCl cryptobox. This is added to allow redundancy in the future (passing each message via several servers), to avoid having the same ciphertext in different queues (that would only be visible to the attacker if TLS is compromised). The encryption keys used for this encryption are not rotated, instead we are planning to rotate the queues. Curve25519 keys are used for key negotiation.
3. Double ratchet end-to-end encryption in each conversation between two users (or group members). This is the same algorithm that is used in Signal and many other messaging apps; it provides OTR messaging with forward secrecy (each message is encrypted by its own ephemeral key) and break-in recovery (the keys are frequently re-negotiated as part of the message exchange). Two pairs of Curve448 keys are used for the initial key agreement, initiating party passes these keys via the connection link, accepting side - in the header of the confirmation message.
4. Additional layer of encryption using NaCL cryptobox for the messages delivered from the server to the recipient. This layer avoids having any ciphertext in common between sent and received traffic of the server inside TLS (and there are no identifiers in common as well).
5. Several levels of content padding to frustrate message size attacks.
6. All message metadata, including the time when the message was received by the server (rounded to a second) is sent to the recipients inside an encrypted envelope, so even if TLS is compromised it cannot be observed.
7. Only TLS 1.2/1.3 are allowed for client-server connections, limited to cryptographic algorithms: CHACHA20POLY1305_SHA256, Ed25519/Ed448, Curve25519/Curve448.
8. To protect against replay attacks SimpleX servers require tlsunique channel binding as session ID in each client command signed with per-queue ephemeral key.
9. To protect your IP address all SimpleX Chat clients support accessing messaging servers via Tor - see v3.1 release announcement for more details.
10. Local database encryption with passphrase - your contacts, groups and all sent and received messages are stored encrypted. If you used SimpleX Chat before v4.0 you need to enable the encryption via the app settings.
11. Transport isolation - different TCP connections and Tor circuits are used for traffic of different user profiles, optionally - for different contacts and group member connections.
12. Manual messaging queue rotations to move conversation to another SMP relay.
13. Sending end-to-end encrypted files using XFTP protocol.
14. Local files encryption, except videos (to be added later).

We plan to add:

1. Senders' SMP relays and recipients' XFTP relays to reduce traffic and conceal IP addresses from the relays chosen, and potentially controlled, by another party.
2. Post-quantum resistant key exchange in double ratchet protocol.
3. Automatic message queue rotation and redundancy. Currently the queues created between two users are used until the queue is manually changed by the user or contact is deleted. We are planning to add automatic queue rotation to make these identifiers temporary and rotate based on some schedule TBC (e.g., every X messages, or every X hours/days).
4. Message "mixing" - adding latency to message delivery, to protect against traffic correlation by message time.
5. Reproducible builds – this is the limitation of the development stack, but we will be investing into solving this problem. Users can still build all applications and services from the source code.

For developers

You can:

- use SimpleX Chat library to integrate chat functionality into your mobile apps.
- create chat bots and services in Haskell - see simple and more advanced chat bot example.
- create chat bots and services in any language running SimpleX Chat terminal CLI as a local WebSocket server. See TypeScript SimpleX Chat client and JavaScript chat bot example.
- run simplex-chat terminal CLI to execute individual chat commands, e.g. to send messages as part of shell script execution.

If you are considering developing with SimpleX platform please get in touch for any advice and support.

Please also join #simplex-devs group to ask any questions and share your success stories.

Roadmap

- ✅ Easy to deploy SimpleX server with in-memory message storage, without any dependencies.
- ✅ Terminal (console) client with groups and files support.
- ✅ One-click SimpleX server deployment on Linode.
- ✅ End-to-end encryption using double-ratchet protocol with additional encryption layer.
- ✅ Mobile apps v1 for Android and iOS.
- ✅ Private instant notifications for Android using background service.
- ✅ Haskell chat bot templates.
- ✅ v2.0 - supporting images and files in mobile apps.
- ✅ Manual chat history deletion.

- ✅ End-to-end encrypted WebRTC audio and video calls via the mobile apps.
- ✅ Privacy preserving instant notifications for iOS using Apple Push Notification service.
- ✅ Chat database export and import.
- ✅ Chat groups in mobile apps.
- ✅ Connecting to messaging servers via Tor.
- ✅ Dual server addresses to access messaging servers as v3 hidden services.
- ✅ Chat server and TypeScript client SDK to develop chat interfaces, integrations and chat bots (ready for announcement).
- ✅ Incognito mode to share a new random name with each contact.
- ✅ Chat database encryption.
- ✅ Automatic chat history deletion.
- ✅ Links to join groups and improve groups stability.
- ✅ Voice messages (with recipient opt-out per contact).
- ✅ Basic authentication for SMP servers (to authorize creating new queues).
- ✅ View deleted messages, full message deletion by sender (with recipient opt-in per contact).
- ✅ Block screenshots and view in recent apps.
- ✅ Advanced server configuration.
- ✅ Disappearing messages (with recipient opt-in per-contact).
- ✅ "Live" messages.
- ✅ Contact verification via a separate out-of-band channel.
- ✅ Multiple user profiles in the same chat database.
- ✅ Optionally avoid re-using the same TCP session for multiple connections.
- ✅ Preserve message drafts.
- ✅ File server to optimize for efficient and private sending of large files.
- ✅ Improved audio & video calls.
- ✅ Support older Android OS and 32-bit CPUs.
- ✅ Hidden chat profiles.
- ✅ Sending and receiving large files via XFTP protocol.
- ✅ Video messages.
- ✅ App access passcode.
- ✅ Improved Android app UI design.
- ✅ Optional alternative access password.
- ✅ Message reactions
- ✅ Message editing history
- ✅ Reduced battery and traffic usage in large groups.
- ✅ Message delivery confirmation (with sender opt-out per contact).
- ✅ Desktop client.
- ✅ Encryption of local files stored in the app.
- 🏗 Using mobile profiles from the desktop app.
- Message delivery relay for senders (to conceal IP address from the recipients' servers and to reduce the traffic).
- Post-quantum resistant key exchange in double ratchet protocol.
- Large groups, communities and public channels.
- Privacy & security slider - a simple way to set all settings at once.
- Improve sending videos (including encryption of locally stored videos).
- Improve experience for the new users.

- SMP queue redundancy and rotation (manual is supported).
- Include optional message into connection request sent via contact address.
- Improved navigation and search in the conversation (expand and scroll to quoted message, scroll to search results, etc.).
- Feeds/broadcasts.
- Ephemeral/disappearing/OTR conversations with the existing contacts.
- Privately share your location.
- Web widgets for custom interactivity in the chats.
- Programmable chat automations / rules (automatic replies/forward/deletion/sending, reminders, etc.).
- Privacy-preserving identity server for optional DNS-based contact/group addresses to simplify connection and discovery, but not used to deliver messages:
    - keep all your contacts and groups even if you lose the domain.
    - the server doesn't have information about your contacts and groups.
- High capacity multi-node SMP relays.

Disclaimers

SimpleX protocols and security model was reviewed, and had many breaking changes and improvements in v1.0.0.

The security audit was performed in October 2022 by Trail of Bits, and most fixes were released in v4.2.0 – see the announcement.

SimpleX Chat is still a relatively early stage platform (the mobile apps were released in March 2022), so you may discover some bugs and missing features. We would really appreciate if you let us know anything that needs to be fixed or improved.

The default servers configured in the app are provided on the best effort basis. We are currently not guaranteeing any SLAs, although historically our servers had over 99.9% uptime each.

We have never provided or have been requested access to our servers or any information from our servers by any third parties. If we are ever requested to provide such access or information, we will be following due legal process.

We do not log IP addresses of the users and we do not perform any traffic correlation on our servers. If transport level security is critical you must use Tor or some other similar network to access messaging servers. We will be improving the client applications to reduce the opportunities for traffic correlation.

Please read more in Terms & privacy policy.

Security contact

To report a security vulnerability, please send us email to chat@simplex.chat. We will coordinate the fix and disclosure. Please do NOT report security vulnerabilities via GitHub issues.

Please treat any findings of possible traffic correlation attacks allowing to correlate two different conversations to the same user, other than covered in the threat model, as security vulnerabilities, and follow this disclosure process.

License

AGPL v3

iOS app   Android app   F-Droid   iOS TestFlight   APK