



OFFICIAL GUIDE

AnonChat

Private messaging with no company in the middle,
over the Anyone network.

Version 1.0.3

October 2026

Open source · AGPL-3.0

CONTENTS

In this guide

01	What AnonChat is	2
02	Why an alternative to centralized messengers	3
03	How it works	4
04	Circuits: seeing the path your messages take	6
05	Security features	10
06	Getting started and everyday use	12
07	What AnonChat can't do	19
08	Frequently asked questions	20

AnonChat is a private messenger for your computer in which no company sits in the middle: your own copy of the app is your server, and it is reachable only through the Anyone network.

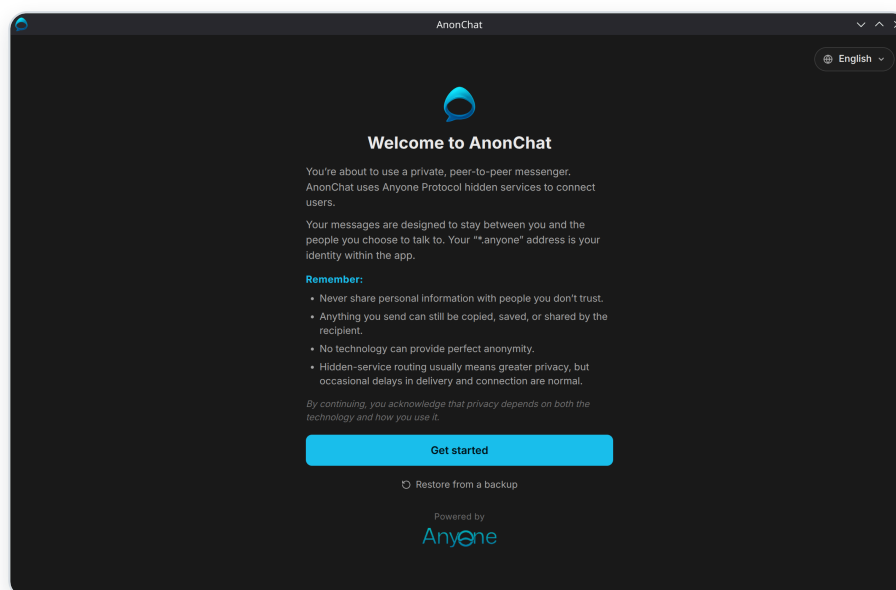
What AnonChat is

You install AnonChat on Windows or Linux (a macOS version is on its way). On first start it creates an address for you, a long string ending in `.anyone`. That address is your identity: no phone number, no email, no account, no sign-up.

You share your address with the people you want to talk to, and they share theirs. Messages, photos, voice messages, files and voice calls then travel directly between your two computers, end-to-end encrypted, through the Anyone network. Nobody else stores them, reads them or knows who talks to whom.

What you get in one app

- One-to-one chats and groups of up to 10 people
- Voice calls, encrypted from end to end
- Photos, videos, voice messages and files up to 5 MB
- Disappearing messages, replies, reactions and emoji search
- Message requests, so strangers can't land straight in your chats
- Encrypted backups, to move your identity to another computer and keep your address
- A live view of the network circuits your messages take, on a 3D globe
- 10 languages: English, Spanish, French, Italian, German, Portuguese, Chinese, Japanese, Polish and Hindi



Welcome screen. The first thing you see: what AnonChat is and a few honest reminders about what no app can do for you. The language menu is at the top right, and **Restore from a backup** is for moving from another computer.

Why an alternative to centralized messengers

Most messengers, even encrypted ones, run through one company's servers. Those servers may not read your messages, but they still see a great deal around them.

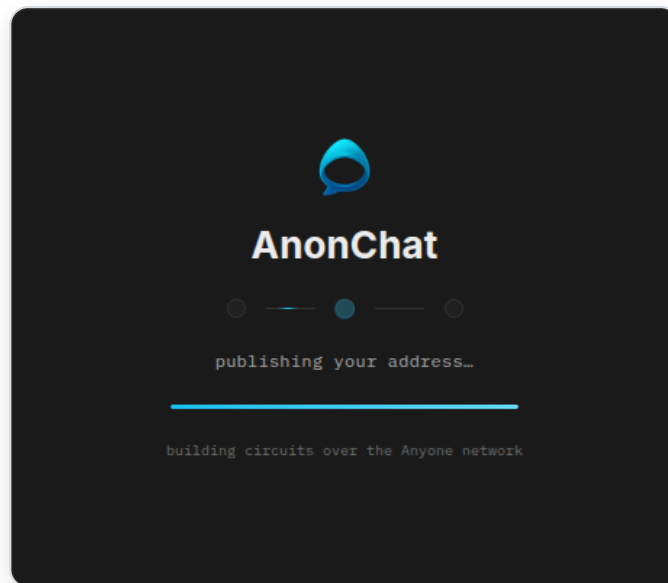
	Centralized messenger	AnonChat
How you sign up	Phone number or email, an account	Nothing: the app creates an address
Where messages pass	The company's servers	Directly between your computers, over the Anyone network
Who sees who talks to whom, and when	The company, and anyone who can make it hand that over	No central party: there is no server to ask
Your IP address	Known to the company's servers	Hidden from everyone, your contacts included
If the company shuts down or blocks your country	The service stops	Nothing depends on a company; the network is run by independent relays
Can you check the code?	Usually not	Yes: open source under the AGPL-3.0 licence

The point is not only that nobody can read your messages. It is that nobody is in a position to collect the record of your conversations in the first place.

How it works

Every AnonChat is a small server of its own: a hidden service on the Anyone network, reachable at your `.anyone` address and nowhere else.

Your address. On first start, AnonChat creates your encryption keys and starts a hidden service on your computer. Your `.anyone` address is derived from that key, so only your computer can answer at it. The start screen shows "publishing your address" while the network learns how to reach you.



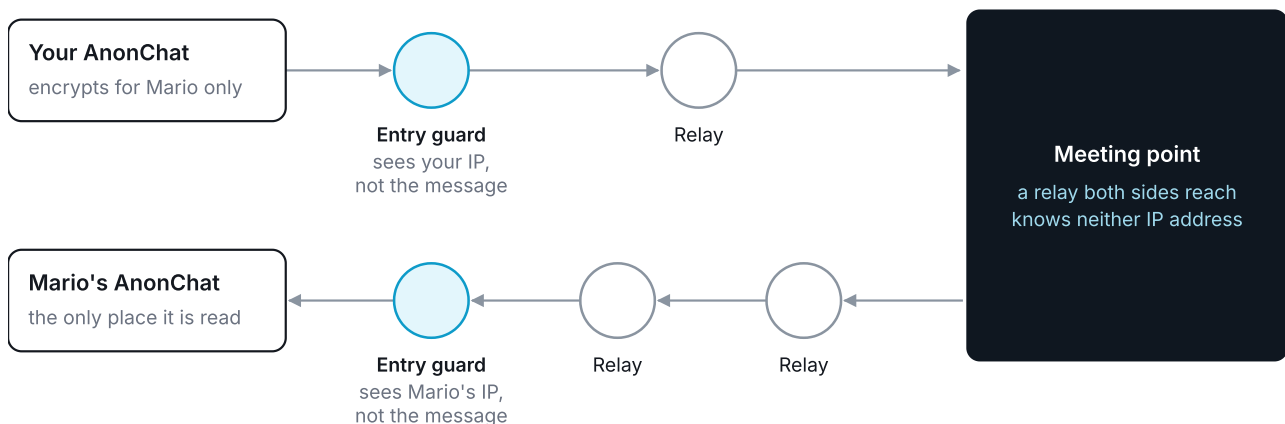
Starting up. AnonChat connects to the Anyone network, builds its circuits and publishes your address.

The Anyone network. Anyone is a network of independent relays run by operators around the world, who are rewarded for the capacity they provide. No single company runs it. Traffic is wrapped in layers of encryption and passed from relay to relay; each relay knows only the one before it and the one after it. No relay ever sees both who sent something and where it is going.

Hidden services. Neither side of a chat reveals where it is. Your app builds a path of relays towards a meeting point, your contact's app builds its own path to the same point, and the message crosses both. Your contact never learns your IP address, and you never learn theirs.

Five relays and a meeting point: neither side learns where the other is

Built separately: your path (top), and Mario's (bottom), one relay longer because his address is the one reached.



Each entry guard knows one person's IP address but never sees the message; every other relay sees only encrypted traffic passing between two neighbours.

Sending a message

1. Your app encrypts the message for your contact alone.
2. It sends the encrypted message through the Anyone network to your contact's address.
3. Your contact's AnonChat receives it, stores it encrypted, and their app decrypts it.
4. Their app confirms delivery: you see ✓, and ✓✓ once it is read if they turned read receipts on.

When your contact is offline. There is no server to hold messages for them, so your app holds them. It shows 🕒 and tries again every 15 seconds until the message is delivered or the waiting time you chose runs out: 1 hour, 12 hours or 24 hours (the default), set per chat. When your contact comes back online, their app tells yours, and everything waiting for them goes out at once; the same happens when they write to you. If messages to one contact still wait while they can write to you, choose **Test connection** in that chat's ⋮ menu (section 04), or **Rebuild network path**. Both apps need to be running for a message to cross.

Online or offline. A green or red dot on each contact shows whether their app can be reached. AnonChat checks quietly every few minutes, and a message from them counts as proof they are online. Section 04 explains every light.

Waiting for the network. After the app starts, it holds back sending, the online checks and the "back online" notices until the network is fully connected and has a current list of relays, normally well under a minute. A lookup of someone's address that fails is remembered by the network for about 15 minutes, so a try made too early could keep a contact out of reach long after they are there. Messages written meanwhile wait in the queue, and when the network is ready AnonChat clears that memory once and sends them.

Circuits: seeing the path your messages take

A circuit is the chain of relays your traffic passes through, and AnonChat lets you see each one: which relays, in which countries, carrying what.

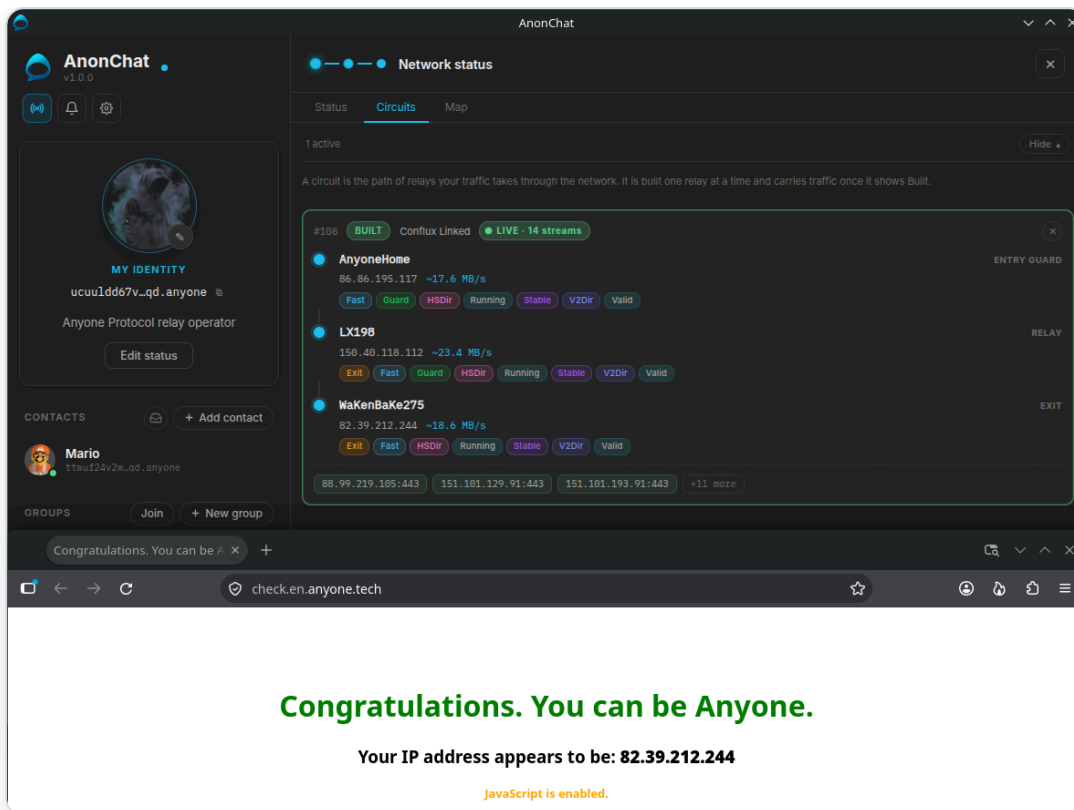
A circuit is built one relay at a time and normally has three. Each relay has a role, shown in English in every language as the network names it:

Role	What it does
Entry guard	The first relay. The only one that sees your IP address, and it never sees what you send or to whom. AnonChat keeps the same few guards for months, which makes you harder to trace.
Relay	A middle relay. It sees only the relays on either side.
Exit	The last relay, used only for traffic that leaves the network, such as a website opened through the SOCKS5 proxy. Messages to your contacts never use an exit.

Open the network panel with the antenna button at the top left. It has three tabs.

Status. Your address, how long the app has been connected, the connection progress, and two checks on your hidden service: **Service** (is it published, with how many introduction points others reach you through) and **Findable** (can your own address really be found through the network). The log underneath shows what the network is doing; when messages to someone are waiting, lines marked [AnonChat] say why (the address shortened), and when they got through.

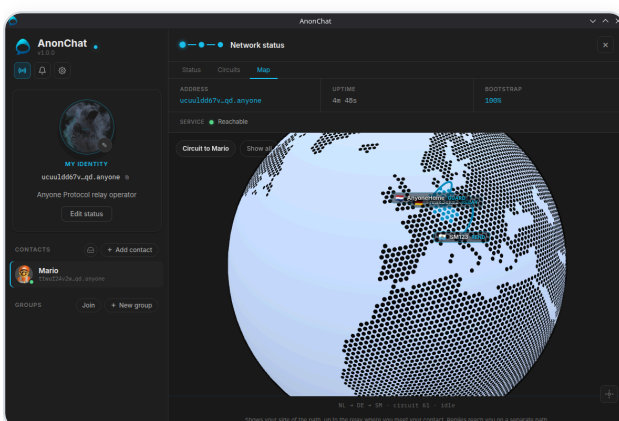
Circuits. Every circuit in use right now. For each relay you see its nickname, IP address, bandwidth and the flags the network gives it (Guard, Exit, Fast, Stable and others). A circuit marked LIVE is carrying traffic at that moment. Close one with ✕, or press **Request new circuit** for a fresh one. A call you make is marked **Voice call**.



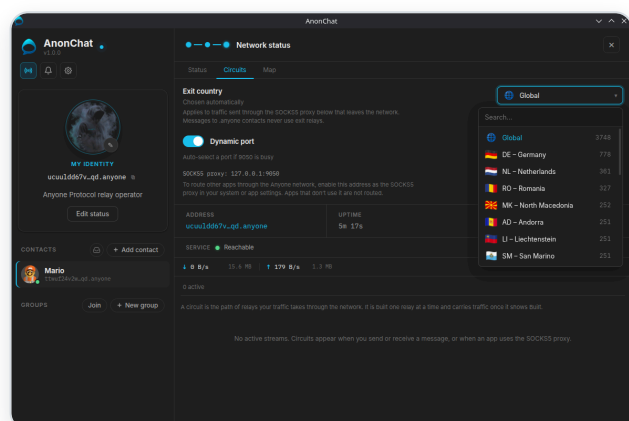
A live circuit, and a browser using the proxy. Top: a live circuit, entry guard to exit. Below it, a browser set to use AnonChat's SOCKS5 proxy: the check page sees the exit relay's address (82.39.212.244, the exit WaKenBaKe275), never the user's.

Map. A 3D globe with the circuit drawn on it, relay by relay. **SOCKS** shows the circuit used for traffic leaving the network. **Hidden** shows the circuit that carries your messages to a contact: your side of the path, up to the relay where you meet them. Their replies come back on a separate path. Open a chat and use its circuit button to jump straight to that contact's circuit.

Exit country and the SOCKS5 proxy. AnonChat also gives your computer a SOCKS5 proxy, 127.0.0.1:9050 by default. Set a browser or another app to use it, and that app's traffic goes through the Anyone network too. In the Circuits tab you can choose the country that traffic leaves from, with the number of exit relays in each. **Global** lets the network choose. If port 9050 is busy, **Dynamic port** picks the next free one and shows the address to use.



The circuit to a contact. Through the Netherlands, Germany and San Marino. The caption under the globe reads the same path in country codes.



Choosing an exit country. The number beside each country is how many exit relays it has.

The status lights

Five small lights tell you, at a glance, whether the network, your contacts and your own address are in order. Hover over one for its text.

Light	What it tells you
1 · Name light next to the app name, top left	<ul style="list-style-type: none">● Cyan, pulsing: the network is ready (light 3), your address is reachable (light 4) and a lookup of it finds it (light 5). People can reach you.● Amber: something is not confirmed. The network is still starting, your address is not reachable yet, or the lookup of your own address just failed, and AnonChat is repairing it. Hover over the light to see which. "Not checked yet" or "could not check" do not turn it amber.● Red: the window has lost its link to the app itself. If it stays red, close AnonChat and start it again. <p>Cyan says people can reach you. It does not say that a given contact is online: that is light 2.</p>
2 · Contact dot on each contact's picture	<ul style="list-style-type: none">● Green: their app answered the last check, or they wrote to you recently.● Red: two checks in a row, half a minute apart, got no answer. They may be off or asleep, or their address may not be findable yet. It is not proof: use Test connection. <p>No dot: nothing is known yet, for a new contact or just after the app starts.</p> <p>The app checks every few minutes, and only once the network is ready.</p>
3 · Connection progress three linked dots in the network panel's title	<p>One lit: starting, under 60%. Two lit: from 60%, loading the network's information. Three lit: 100%, fully connected. The percentage is in the Status tab.</p>
4 · Service Status tab	<ul style="list-style-type: none">● Reachable, with introduction points: your address is published and the network's meeting doors for it are open (usually 3 to 6).● Amber: not published yet, still being set up, published with no introduction points, or no address yet. Normal for the first minute after a start; if it lasts several minutes, restart the app. <p>This is what the app's own network program reports about itself. It does not prove that others can find you: that is light 5.</p>
5 · Findable Status tab, beside Service	<ul style="list-style-type: none">● Yes: the app looked up its own address through the network, the way a contact would, and found it. It looks again every 10 minutes.● No, looking again: that lookup failed. The app clears the network's memory of failed lookups, looks again, then sends your address details to the network again (at most every 10 minutes), and keeps looking every 3 minutes. It usually recovers within a few minutes, and the log says when: <i>your address can be found again</i>.● Grey: not checked yet, checking now, or the check could not run, for instance while the network is down.

While Findable says No, contacts who try your address at that moment may be told it was not found. They try again, and nothing is lost: their messages wait in their app until yours can be found.

Test connection

When messages to one contact stay at ⏳, open that chat's ⋮ menu and choose **Test connection**. It looks for the cause, one step at a time, and ends with one sentence on what to do. It takes up to about 45 seconds.

- **Your address:** published, with introduction points, and (once checked) findable.
- **Contact's address:** found on the network, or not.
- **Reaching the contact's app:** a small request to their app, answered or not.
- **Clocks:** your computer's clock against theirs. Addresses are published under a daily period worked out from the time, so clocks that differ by minutes can't find each other. Fix the clock on the computer that is wrong.
- **Messages waiting for the contact:** how many are queued.

A step is marked ✓ (fine), × (failed) or – (not measured, for instance the clocks when the contact's app didn't answer). If the test succeeds, messages that were waiting are sent at once. If it doesn't, the sentence at the bottom says which side to look at: wait for your own address to become findable, check that the contact's computer is on and AnonChat is running, correct a wrong clock, or choose **Rebuild network path** in the same menu.

Security features

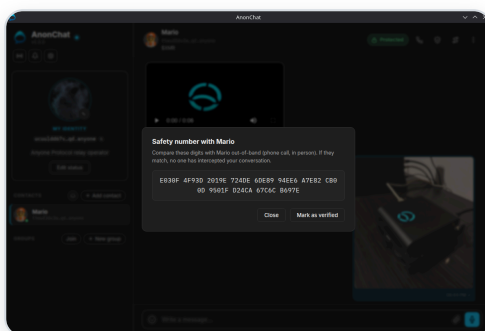
AnonChat protects you in three layers: the network hides where you are, encryption hides what you say, and your computer keeps everything locked.

Protection	What it does for you
End-to-end encryption	Every message, photo, file and call is encrypted on your computer and decrypted only on your contact's. It uses the Double Ratchet with an X3DH handshake (P-256, AES-256-GCM): each message has its own key, so a key stolen later can't open earlier messages. A chat shows Protected in its header.
Weekly key refresh	The key a new contact uses to start a chat with you is replaced every week, and old ones are deleted after 60 days (never put in a backup). Contacts pick up the new one by themselves, after checking it is signed by the identity key they saved when they added you. So even a first message stays protected if a key is stolen later.
Pinned identity keys	When you add someone, AnonChat fetches their key from their own address and keeps it. A message that claims to be from them but uses another key is refused, so nobody can slip in as your contact.
Safety numbers	Two people can compare a short number, in person or by phone. If it matches on both screens, nobody is in the middle. Then press Mark as verified .
Message stamps	Each pair of contacts shares a secret only they know, and every message between them carries a stamp made with it. A stranger can't pose as one of your contacts to get past your limits.
Message requests	Someone who isn't your contact lands in Requests, not in your chats. They can send text only until you accept, and each request is marked <i>Not verified yet</i> until Accept checks the address on it. You can delete, block, or turn requests off completely.
Flood protection	Each stranger, and strangers together, get only a small allowance. During a flood, senders who aren't contacts must solve a small computing puzzle first. The check comes first, so the answer never reveals who your contacts are, and every request has a time limit, so a slow contact can't hold up the rest.
Stops instead of leaking	If the Anyone network program stops, or port 9050 is taken by another program, AnonChat stops and says why, instead of sending through whatever is on that port.

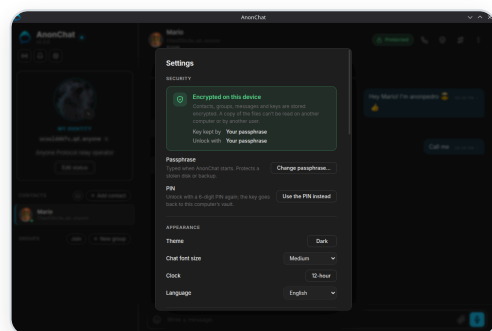
Encrypted on your computer	Contacts, messages, keys and media are stored encrypted. The key is kept by your system's vault (Windows, GNOME Keyring or KWallet) and opened with a 6-digit PIN, or protected by a passphrase you type at each start. The one exception is the private key of your address: the Anyone network program reads it from its own file, which only your user account can open.
Locked to the network	The app can't connect to anything outside the Anyone network. The window may only talk to the app on your own computer, names are looked up inside the network, and voice calls use no WebRTC and no direct connection.
Padding	Your link to the network always carries dummy traffic, so someone watching your connection can't easily tell when you send or receive.
Calls that hide when you speak	Call audio is sent in fixed-size pieces at a steady rate, even while you are silent or muted, so the traffic doesn't reveal when you talk.
Nothing on by default that tells on you	Read receipts are off unless you turn them on. Updates are checked only when you ask, and through the Anyone network.
Encrypted backups	A backup holds your address and keys, sealed with a passphrase of its own (at least 12 characters). AnonChat asks for your PIN or passphrase before it makes one, and the file is readable only by your user account.
Erase everything	One button in Settings deletes your identity, contacts, messages and groups from the computer.

PIN or passphrase?

With a PIN, your system's vault holds the key and the 6-digit PIN unlocks the app; it protects against someone opening the app on your computer. With a passphrase (at least 12 characters), the key never touches the vault; it also protects a stolen disk or a backup. Neither can be recovered if you forget it: there is no company to reset it. AnonChat asks which you want on first start, and you can switch later in Settings.



Safety number. Read it to your contact over a channel you trust; if theirs is the same, mark the chat as verified.



Settings → Security. Your messages, contacts and keys on this computer are encrypted, here with a passphrase. You can change the passphrase or switch to a PIN at any time.

Getting started and everyday use

From install to your first message takes a few minutes, most of it the app connecting to the network.

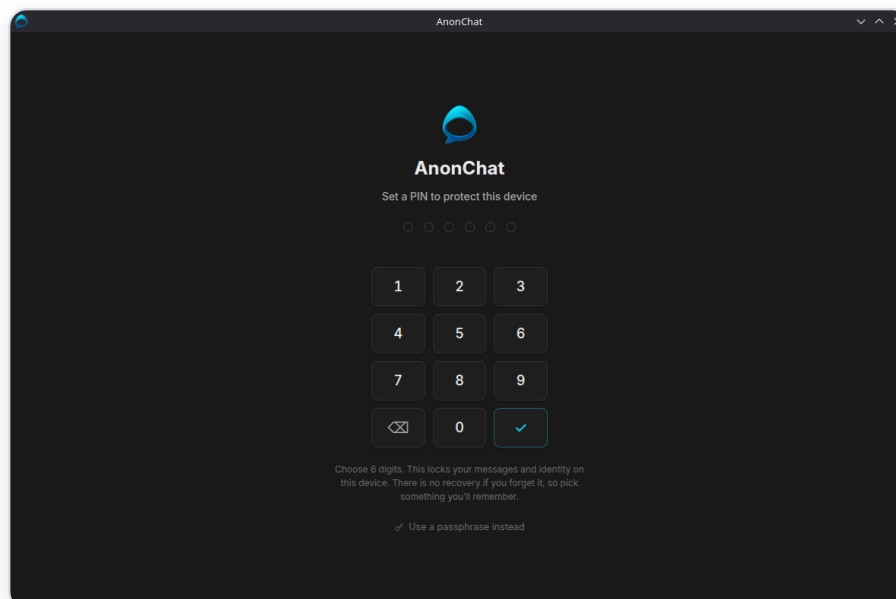
1. Install and start

AnonChat comes as an installer for Windows and as Linux packages for Ubuntu and Debian (.deb), Arch (.pacman) and Fedora and openSUSE (.rpm); a macOS version is on its way. Everything it needs, including the Anyone network client, is inside: there is nothing else to install and no account to create.

If Windows blocks the installer

AnonChat isn't signed yet. **"Windows protected your PC"**: More info → Run anyway. **"Smart App Control blocked an app"**: Windows Security → App & browser control → Smart App Control → Off, then run the installer again. This applies to all programs and may not be reversible without resetting Windows.

On first start, pick your language with the menu at the top right if you need to, read the welcome screen and press **Get started**. (Moving from another computer? Press **Restore from a backup** instead: see step 7.) Then choose how to lock the app: a 6-digit PIN, or **Use a passphrase instead** (see *PIN or passphrase?* in section 05). Write it down somewhere safe; nobody can recover it for you.



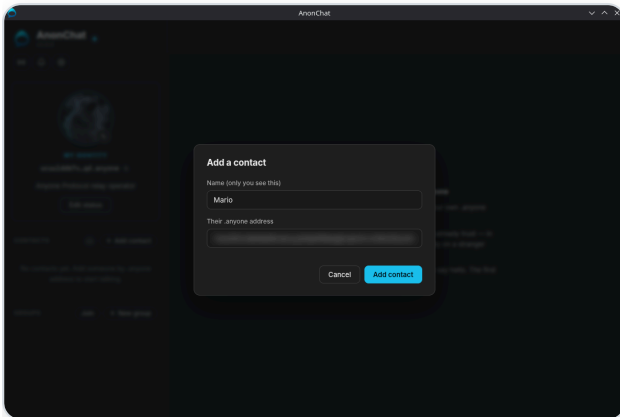
Choosing a PIN. The link at the bottom switches to a passphrase.

The first connection to the network usually takes under a minute. When it is done, your address appears top left, under **My identity**, with a button to copy it.

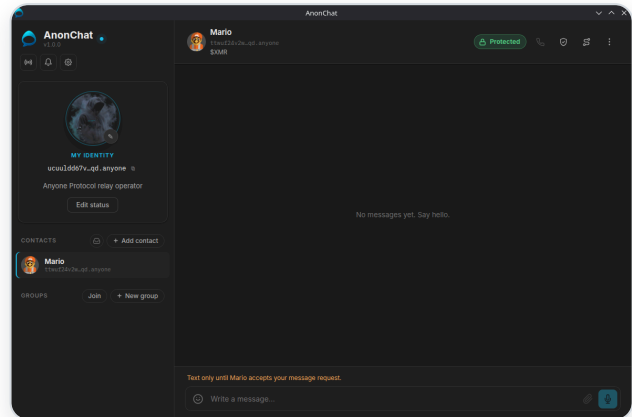
2. Add a contact

AnonChat has no directory and no search: you can only reach someone whose address you have. Swap addresses through a channel you already trust, in person or in another secure app, and never trust an address a stranger sends you.

Press **+ Add contact**, type a name for them (only you see it), and paste their address. Ask them to add you the same way.



Adding a contact. The name is your own label for the contact; nobody else sees it.



A new chat. Text only until Mario accepts the message request.

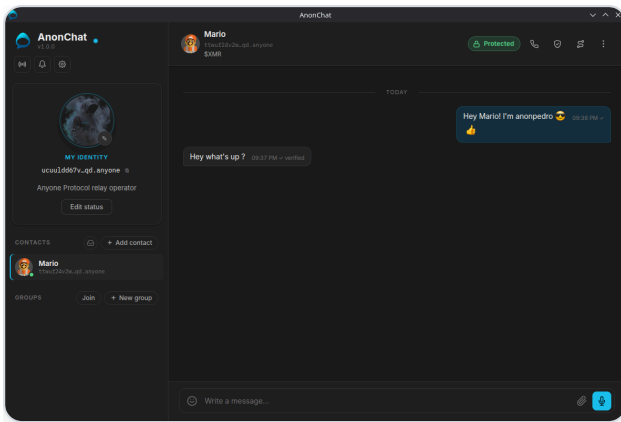
Your first message to someone new arrives on their side as a message request. Until they accept it, you can send text only.

If you remove a contact, anything they write afterwards arrives as a message request instead of in a chat, and their app limits them to text until you accept them again, so they learn that you removed them. To stop hearing from someone altogether, block them.

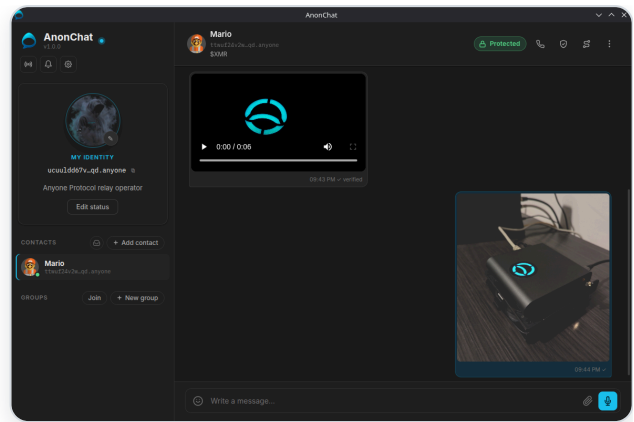
3. Chat

Once accepted, a chat works the way you expect, and the **Protected** badge confirms it is end-to-end encrypted.

- **Media:** photos, videos, files up to 5 MB, and voice messages up to one minute. Drag a file into the chat or use the paperclip. Photos, videos and audio are cleaned of location, camera and time first, and large photos are shrunk to fit; if a file cannot be cleaned it is not sent.
- **Replies and reactions:** hover over a message to reply to it or add a reaction.
- **Emoji:** the picker has a search box (English names), and a message of just a few emoji is shown large.
- **Disappearing messages:** set a chat's messages to vanish after 30 seconds, 5 minutes, 1 hour, 1 day or 1 week.
- **Your profile:** a picture and a short status line your contacts can see; the members of your groups see your picture too. There is no display name: each person sees the name they gave you.



A conversation. ✓ means delivered; "verified" on incoming messages means they came from the key pinned for that contact.

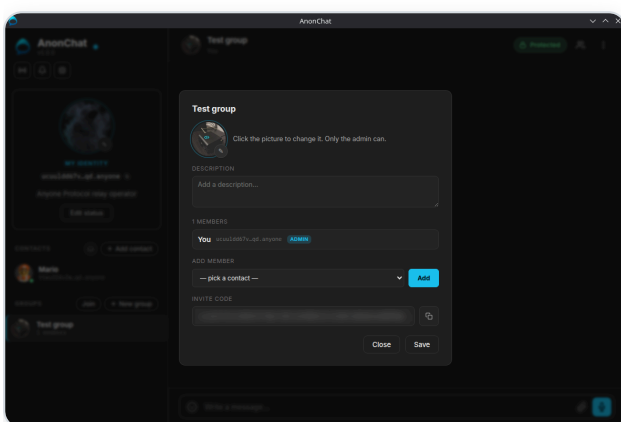


Media in a chat. Videos and photos play and display right in the chat.

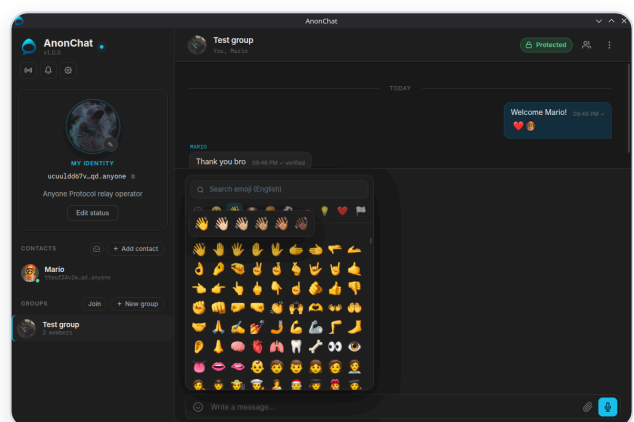
4. Groups

Groups hold up to 10 people, you included. Press **+ New group**, give it a name, an optional description and picture, and pick members from your contacts. The person who creates a group is its admin.

- Only the admin adds members, and only from their own contacts.
- Anyone else can join with the group's **invite code**, which the admin shares.
- Members who aren't each other's contacts can still talk in the group, with the same encryption and key pinning.
- A group keeps working while its admin is offline; only joining and changes to the group wait for them.
- Your message shows at once (⌚ while it reaches everyone). When someone leaves, the admin's app sends everyone the new member list.
- When the admin leaves, the group is closed for everyone.



Group settings. Picture, description, members, and the invite code (blurred here).

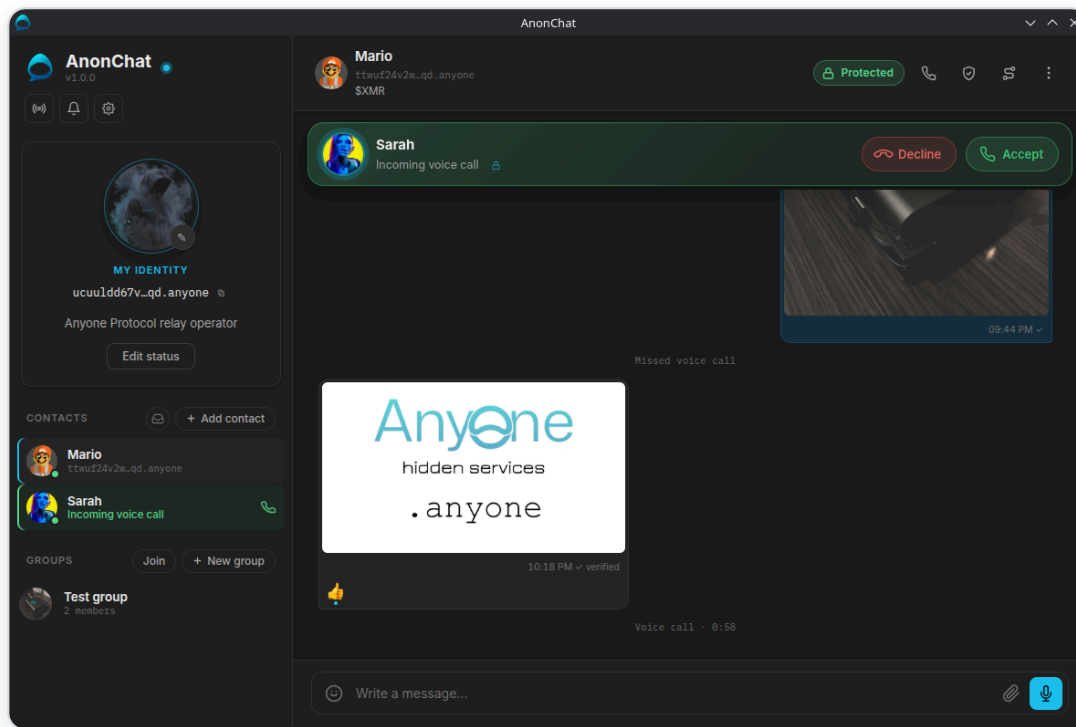


A group chat. The emoji picker has a search box at the top.

5. Voice calls

Press the phone button in a chat's header. Only contacts can call each other, and a switch in Settings refuses all incoming calls.

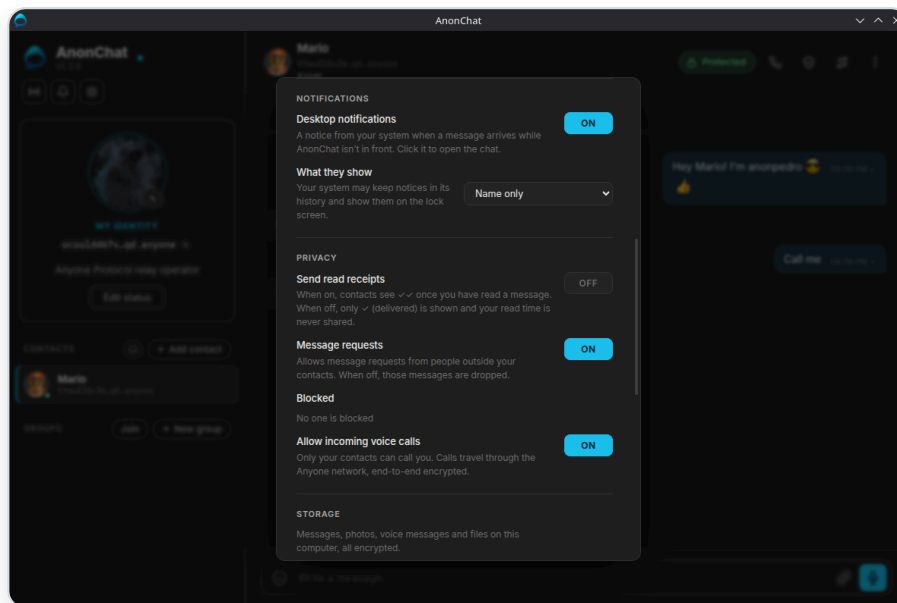
A call crosses five relays and a meeting point, so expect about 2 to 3 seconds of delay, like a satellite call: a little audio is kept in reserve so the network's pauses don't cut it. Headphones give the cleanest sound. When someone calls, their card in the contact list pulses green and a bar with **Accept** and **Decline** appears. If AnonChat is minimised, your system shows a notification for the call and the taskbar button asks for your attention until the call is answered or ends.



An incoming call. Sarah's card glows green in the list, and the call bar offers Accept or Decline.

6. Notifications and settings

New messages play a sound (the bell at the top turns it off), mark the chat unread, and show a count in the window title and on the app icon. When AnonChat isn't in front, your system can also show a notification. You choose what it shows: the name only (the default), the name and the message, or nothing but "New message". Message requests always say only "New message request".



Settings → Notifications and Privacy. Your system may keep notifications in its history, which is why the message text is off by default.

Settings also has the theme, chat font size, clock format and language, storage use (with a button to clear old media), **Backup**, a manual update check, and **Erase everything**.

7. Back up and move to another computer

A backup lets you keep your address when you change computers. It is one encrypted file holding your address and its keys, your identity keys (so contacts keep trusting you), your contacts, groups, blocked list and settings. Messages, photos and files are not in it: they stay on the computer that received them. Other people's profile pictures aren't either; they come back when those people next write.

1. **Make the backup.** Settings → Backup → **Create backup**. Confirm with your PIN or passphrase, then choose a passphrase for the file itself, at least 12 characters. AnonChat saves the file in your Downloads folder.
2. **Restore it on the new computer.** Install AnonChat and, on the welcome screen, press **Restore from a backup**. Choose the file, type its passphrase, then choose a PIN or passphrase for this computer. AnonChat restarts with your address, sets up a new secure session with each contact automatically, and gets the current member list from each group's admin.
3. **Erase the old computer.** Use your identity on one computer only: if two computers run the same address, they compete for it and messages go missing. Use **Erase everything** on the old one.

Create a backup

- ✓ Your address v5c5t2kqwr...qd.anyone and its keys
- ✓ Your identity keys, so contacts keep trusting you
- ✓ Contacts, groups, blocked list and settings
- ✗ Messages, photos and files stay on this computer

Protect the file with a passphrase of its own:

..... Show

Strong

..... Show

Anyone with this file and its passphrase can be you. Keep it offline, and never share it.

☒ I understand a forgotten backup passphrase can't be recovered

Cancel Save backup

Creating a backup. What goes in the file, and a passphrase only for it.

Restore from a backup

anonchat-backup-2026-10-15.anonchat

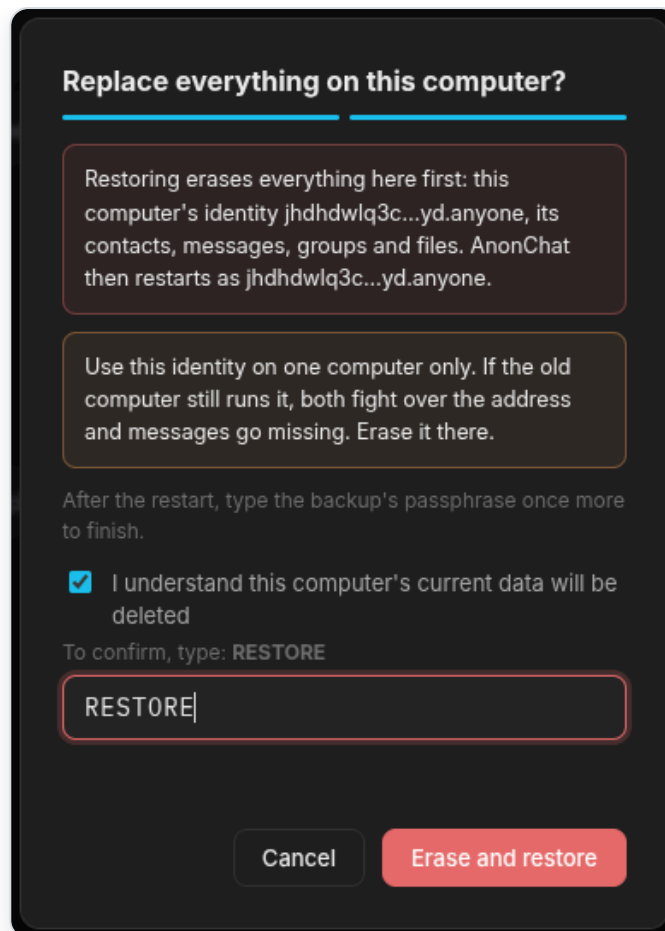
Backup passphrase Show

✓ Backup opened: v5c5t2kqwr...qd.anyone
Contacts: 2 · Groups: 0 · Made on 10/15/2026
Next, choose a PIN or passphrase for this computer.

Cancel Continue

Restoring on a new computer. The backup opened: its address, how many contacts and groups, and the date.

To restore on a computer that already has an identity, use Settings → Backup → **Restore....** Everything on that computer is erased first, so AnonChat asks you to type **RESTORE** to confirm. It then restarts and asks for the backup's passphrase once more to finish.



Restoring over an existing identity. AnonChat says what will be erased before anything happens.

Keep the backup safe

Anyone with the file and its passphrase can be you. Keep it offline, on a USB stick or another place only you control, and don't send it to anyone. A forgotten backup passphrase can't be recovered.

What AnonChat can't do

No tool makes you invisible, and it is better to know the limits before you rely on one.

- **It has not had a human security audit.** It uses well-established cryptography and the code is open for anyone to review. Independent reviews by an AI model have checked it, but no outside firm has formally audited it yet.
- **Only photos, videos and audio are cleaned.** AnonChat removes the location, camera model and time from photos, videos and audio before sending, and gives them a neutral name. Files you send as plain files (PDF, documents) go exactly as they are, so clean those yourself first. A file AnonChat cannot clean is not sent.
- **Your computer is the weak point.** Malware on your machine, or someone using it while it is unlocked, can see what you see. Lock the app and keep your system up to date.
- **What you send can be kept.** Your contact can copy, screenshot or forward anything you send them. Disappearing messages vanish from both apps, not from someone's memory or camera.
- **Both apps must be running.** With no server to hold messages, a message waits on your computer for up to 24 hours. If your contact stays offline longer, it is marked undelivered and you send it again later.
- **Messages take a few extra hops.** Each message passes through several relays, which adds a little latency that you rarely notice. The first message after a contact comes back online can take a few seconds while the network finds them, and calls carry a delay of about 2 to 3 seconds.
- **One computer at a time.** An identity runs on one computer, with no sync between devices and no phone app yet. A backup moves it to another computer (section 06, step 7). Without a backup, losing the computer or forgetting your PIN or passphrase means the identity is gone and your contacts need your new address.
- **Using the network is visible.** Your internet provider can see that you connect to the Anyone network, though not to whom or what you send.
- **Links open outside AnonChat.** A link in a message opens in your usual browser, after a warning. Unless that browser uses AnonChat's SOCKS5 proxy, the site sees your IP address.
- **The SOCKS5 proxy is not a privacy browser.** It hides your IP address from websites, but the exit relay can see traffic that isn't encrypted (plain http), and a normal browser can still be recognised by its fingerprint.

Frequently asked questions

Do I need a phone number, an email or an account?

No. Installing the app creates your address, and that is all.

Can the people who make AnonChat read my messages, or switch it off?

No. There is no AnonChat server: messages go from your computer to your contact's, encrypted with keys that never leave those two computers.

Can someone find out where I am from my address?

No. A `.anyone` address doesn't reveal your IP address or location, to your contacts or to anyone else. Anyone who has your address can send you a message request, so share it only with people you want to hear from. You can also turn requests off.

Do I need tokens or cryptocurrency to use it?

No. Relay operators earn the rewards; AnonChat only uses the network. Nothing to buy or hold.

Can I use the same identity on two computers?

Not at the same time, but you can move it. Make a backup in Settings → Backup, restore it on the new computer, then erase the old one. Your contacts keep writing to the same address.

Why did my message show ⌚?

Your contact's app wasn't reachable at that moment. Your app keeps trying, and the message goes out as soon as they are back, within the waiting time you set for that chat. If it stays that way while the contact seems to be online, open the chat's `⋮` menu and choose **Test connection**.

My contact shows green, but my messages wait. Why?

The green dot also lights when they write to you, which proves their messages reach you, not that yours reach them. **Test connection** checks the way from you to them and says what to do.

Findable says "No — looking again". Is something wrong?

Your address is published but the app's own lookup of it failed, often after a short network hiccup. The app repairs it by itself and usually turns it back to Yes within a few minutes. If it stays on No for over 10 minutes, restart AnonChat and check your computer's clock.

AnonChat closed and said the Anyone network program stopped, or that port 9050 is in use. What now?

It stops on purpose, so that nothing is sent through another program. Start AnonChat again. If it says the port is in use, close the other program that uses 9050 (often another Anyone or Tor program), or turn on **Dynamic port** in the Circuits tab so AnonChat picks a free one.

Will I get a warning when a contact's key refreshes every week?

No. The weekly refresh is automatic and signed by the identity key your contact had when you added them. A warning appears only if someone's identity key itself changes.

I forgot my PIN or passphrase. Can it be reset?

No. Only you ever had it, so nobody can reset it. If you made a backup, erase everything and restore it: you keep your address, and you need the backup's own passphrase. Without one, you start again with a new address.

Does a backup include my messages?

No. It holds your address, keys, contacts, groups, blocked list and settings. Messages, photos and files stay on the computer that received them.

What is the SOCKS5 proxy for?

It lets other apps, such as a browser, send their traffic through the Anyone network too. AnonChat doesn't need it for messaging.

Is it open source?

Yes, under the GNU Affero General Public License v3.0 or later (AGPL-3.0). Anyone can read, check and build the code.

AnonChat 1.0.3 · Official guide · October 2026. AnonChat is open-source software licensed under the GNU AGPL-3.0. It uses the Anyone network; Anyone is operated by independent relay operators and is not run by AnonChat.