

Forum:[Hack Forums](#)

Thread: [OffCode - Web based tor chat | Encrypted | Self-hosted | Freemium](#)

OffCode - August 2, 2026, 1:01 pm

Setting up your own self-hosted chat on the Tor network has never been this easy. Guests open your .onion link in Tor Browser — no port forwarding, no cloud account, and no complicated setup. OffCode Tor Chat is designed to make secure Tor Hidden Service hosting simple.

Messages are encrypted in-browser with WebCrypto AES-256-GCM (PBKDF2-v2, 600k iterations) before reaching the server — ChatServer relays and stores ciphertext only. Password rooms use separate KDF domains so the host cannot derive the key; open rooms are public encrypted channels.

Host with Server Manager on Windows, or headless Docker (ChatServer + Tor HS). Password rooms are server-blind E2EE (the host cannot derive the room key). Open rooms still encrypt in the browser, but the key is derived from the room id: intentional public channels. Hidden rooms stay off the public list and use invite links; add a password for private E2EE. Creators get Settings for close joins, slow mode, lock later, and delete room, plus a Profile recovery code (My rooms for hidden). Required message TTL, E2EE attachments, and optional Full Vanguard complete the stack.

Full Vanguard - Guard-Discovery Protection

A standard Tor Hidden Service chooses its entry (guard) nodes randomly on every circuit build. Over time a network-level adversary can watch which relays the server connects to and gradually narrow down the real server IP. This is called a guard-discovery attack and is especially dangerous for long-lived hidden services.

L2 Vanguard

4 pinned middle-layer nodes, rotated ~1-45 days (addon defaults)

L3 Vanguard

8 pinned nodes, rotated ~1-48 hours (addon defaults)

By pinning layers, only a tiny controlled set of relays ever see the hidden service's circuit-building traffic, making large-scale guard-discovery statistically infeasible.

Server manager

Frequently Asked Questions:

Do I host Tor Chat myself?

-Yes. Server Manager on Windows starts ChatServer (wait for health) then a Tor v3 Hidden Service. Optional Full Vanguards hardens long-lived onions. Headless Docker compose (ChatServer + Tor, no host ports) is also supported. There is no OffCode-hosted chat cloud; you control the onion URL and the stack.

Do clients need Tor Browser?

-Yes. Guests open <http://ADDRESS.onion/> in Tor Browser. The chat HTTP stack binds loopback only; Tor publishes the Hidden Service. The UI is Tor Browser-friendly: self-hosted fonts, SRI scripts, and no third-party CDNs.

Is Tor Chat free? Does it need port forwarding?

-Yes, The prebuilt binary release is free (self-hosted, Windows Server Manager or Docker). No port forwarding needed: Tor Hidden Service handles inbound connections via rendezvous; the host only needs outbound Tor access. Works behind NAT, CGNAT, and firewalls.

How does Tor Chat relate to EU Chat Control 1.0?

-Chat Control 1.0 lets major messaging providers voluntarily scan private communications. Tor Chat is a different model: self-hosted on Tor, not a centralized big-tech messenger. You avoid that scanned platform path by hosting your own Hidden Service with browser E2EE. This is architectural privacy, not legal advice.

How does end-to-end encryption work?

Clients encrypt with WebCrypto (PBKDF2-HMAC-SHA256 at 600 000 iterations, then AES-256-GCM) before sending. Locked rooms: join proof and room key use separate v2 KDF domains (torchat-join-v2 / torchat-e2ee-v2) so the server cannot derive the message key; the password never leaves the browser. The server stores a second PBKDF2 hash of the join proof (250 000 iters, iter:salt:hash). Open rooms: still encrypted (pbkdf2-v2), but the key is derived from the room id — anyone who knows the id (including the host) can decrypt. 1:1: ECDH hybrid plus a safety number for out-of-band peer verify.

Price: \$49 | Source-code

The source code is paid, but the application itself is free to use.

[contract=tid]Start Contract[/contract]

Binance - August 3, 2026, 9:26 am

`claude code go brrrrrrrrrrrrrrrrrrrrrrr.`

OffCode - August 3, 2026, 11:58 am

(Aug 3, 2026 09:26 AM)Binance Wrote: [\[CITE\]](#) claude code go brrrrrrrrrrrrrrrrrrrrrr.

I'm using cursor and model: Grok 4.5

Claude is too expensive.

Grok is almost at same level with claude.

(Aug 3, 2026 09:26 AM)Binance Wrote: [\[CITE\]](#) claude code go brrrrrrrrrrrrrrrrrrrrrr.

AI is a great tool, but it doesn't solve every problem. The more programming knowledge and experience you already have, the more powerful AI becomes as a development tool.

OffCode - August 13, 2026, 7:01 am

UPDATE!

Changelog:

-FileSeal: Client wraps a random DEK with the room/hybrid CryptoKey (AES-GCM + AAD), encrypts the file in 256 KiB plaintext chunks, and uploads opaque ciphertext via PUT /api/attachments/{id}/chunks/{n} with HMAC X-Transfer-Token.

-Disable attachments: Creator Room Settings toggle (attachments_disabled in SQLCipher). Members get AttachmentsPolicy on join / toggle; Attach button gated in room-attachments.js. Server enforces a text-only PayloadB64 size cap when disabled (blind relay cannot inspect ciphertext kind).

-Max members: Creator Room Settings toggle (max_members in SQLCipher, 0 = off, else 2–50). Enforced in RoomPresenceService.Join; public "Room is full.", hidden generic "Cannot join room." Existing members stay if the cap is lowered.

-Announcement / read-only: Creator Room Settings toggle (read_only). Only the creator may SendEncrypted / BeginAttachmentUpload; owner tokens are extra hub args (not persisted). Members get a disabled composer (room-readonly.js).

Much more...

OffCode - October 9, 2026, 9:17 am

Update coming soon!

- Room creator can pin messages

- Security improved a lot!

- More settings to server manager

OffCode - October 12, 2026, 7:33 am

Update is available!

Much improvements