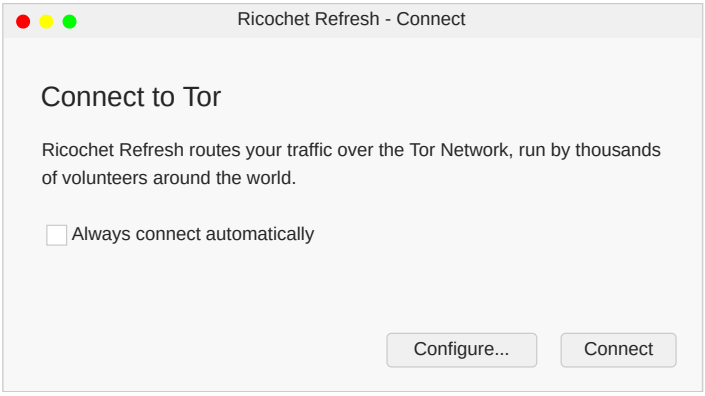
Connection Dialog

This is the first window that will appear if Ricochet Refresh is managing its owned own Tor provider (versus using a system-owned Tor or Arti instance). If we are using an external Tor provider, we will go directly to the Main window.

Potentially multiple profiles using the same guard is probably the least-bad option.

There is a linkability concern here: if an adversary disabled a guard node and multiple Ricochet Refresh users go offline, then they have (probably) identified their guard node, and that the two profiles (may) be the same person. Maybe not terribly useful for a fishing expedition (since if we have more Ricochet Refresh users than there are guard relays, there will necessarily be profiles sharing guards), but more useful as a piece of evidence to add to a larger case, especially if this behaviour is stable across multiple guard rotations.

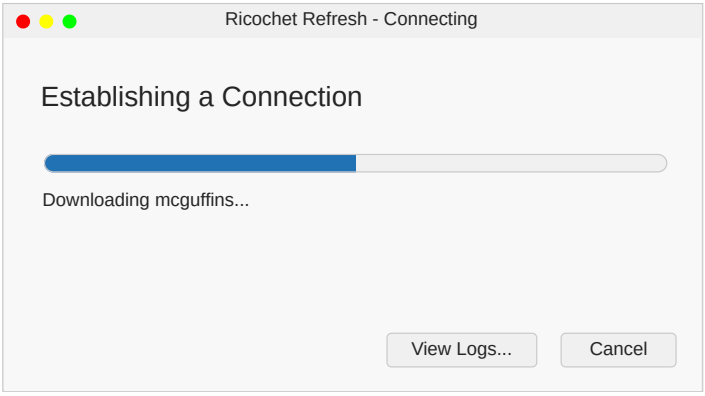
On the other hand, if you say ok one guard per profile, then you run into the problem having a stable guard solves: increased probability of a bad/adversarial guard versus a good guard.



Configure opens the Preferences dialog

Connect begins bootstrapping tor

We will try to follow a desktop'ified version of Tor Browser's about:torconnect page here



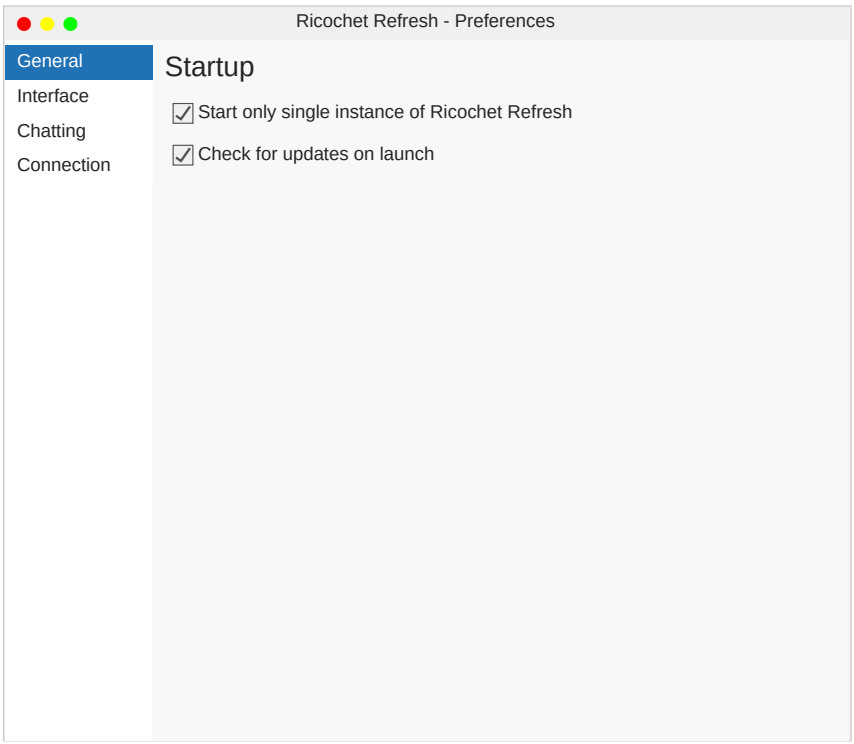
Open the Tor Logs dialog

Cancel current bootstrap attempt

Preferences (General) Dialog

The General section of the Preferences dialog. Should enable configuring general application behaviour that are not specific to the other sections.

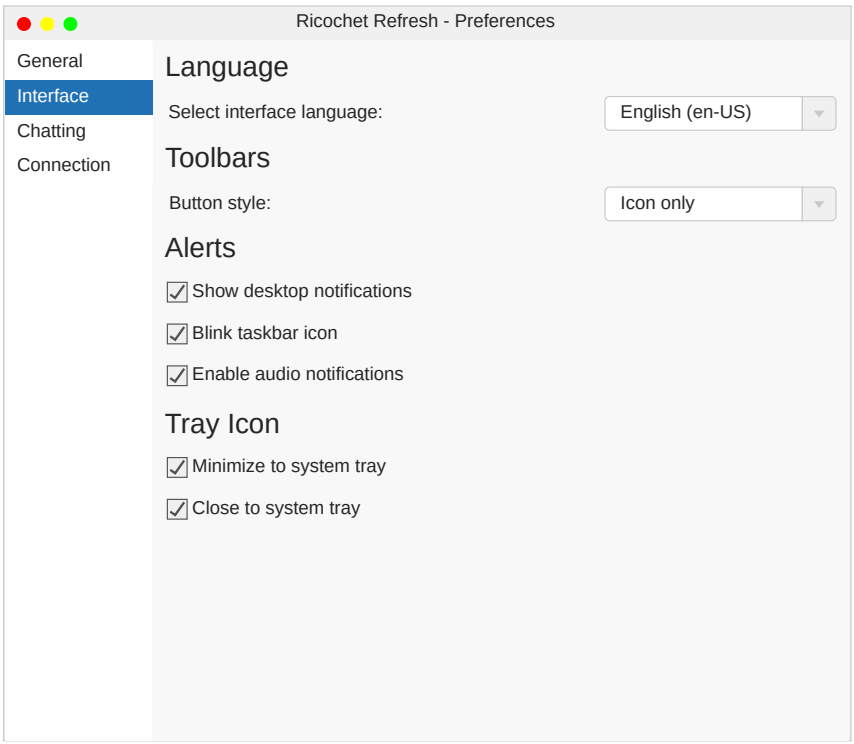
TODO: Ensure these ALL options are safe to store unencrypted, since they are the app-wide settings and so won't be stored in a profile



Preferences (Interface) Dialog

The Interface section provides users with UI customisation options

TODO: Enabled/Disabled icons in the Main taskbar?



Languages sorted by language code

- Icon only
- Text only
- Text beside icon

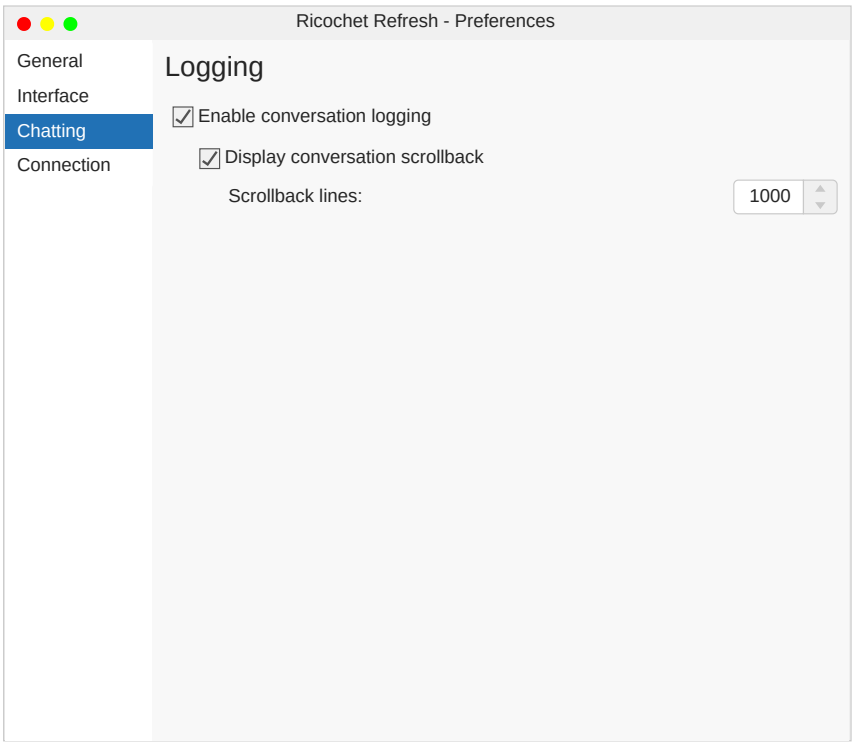
NOTE: probably platform-specific

Preferences (Chatting) Dialog

The Chatting section provides users with conversation-related options.

TODO: Chat formatting/density

TODO: Timestamp formatting/localisation



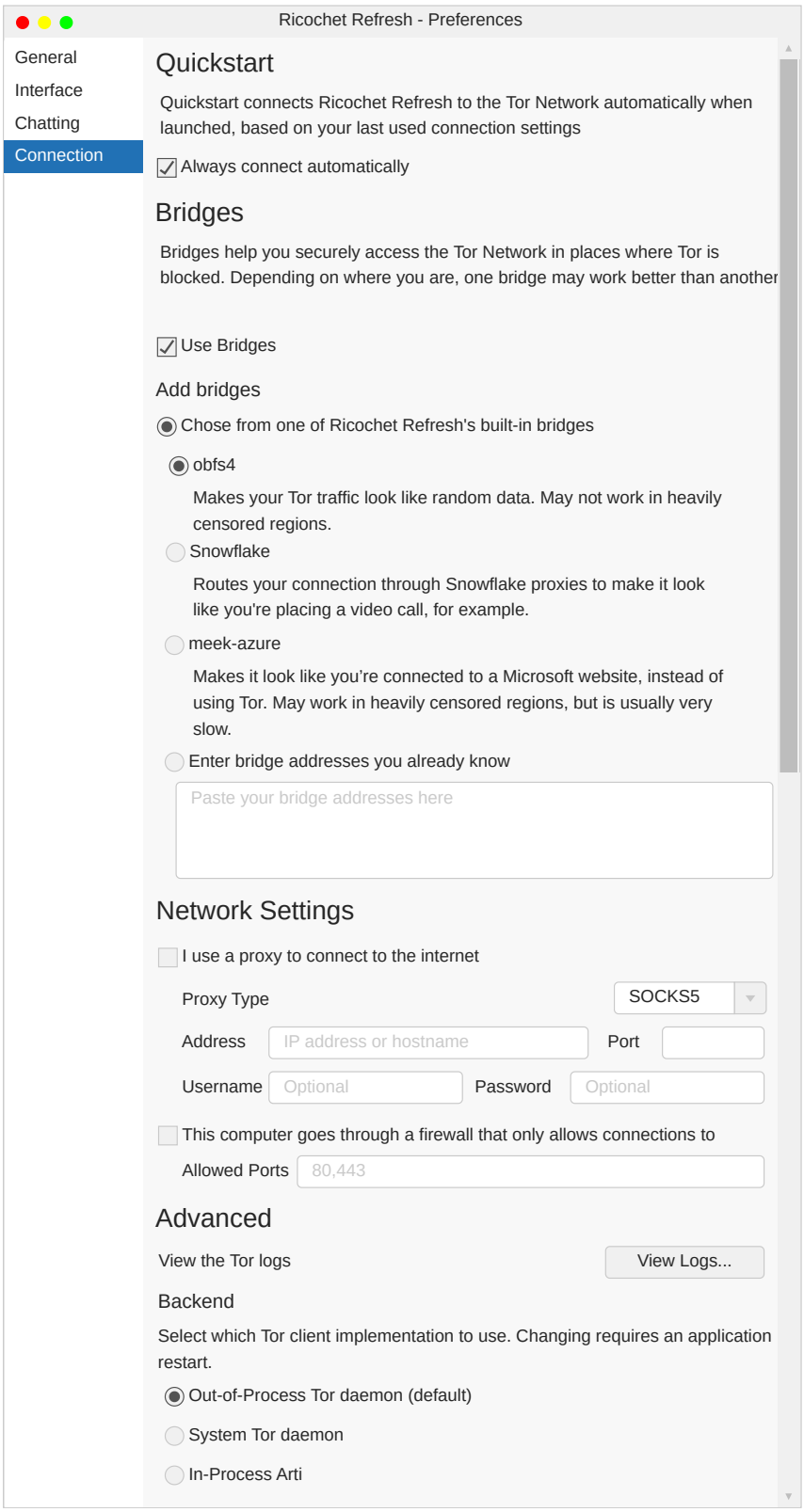
Logs are stored in the encrypted profile file

Timestamps should be stored in un-localised format

Preferences (Connection) Dialog

The Connection section provides users with Tor Provider related options. This page may vary a lot depending on which Tor Provider is selected. For instance, a System Tor Daemon Tor Provider (eg on Tails) would have this section almost entirely empty. For now let's have this mostly mirror about:preferences#connection in Tor Browser.

TODO: Bridge Card support



Add bridges region collapses if Use bridges is not ticked

TODO: Maybe Backend should be the *first* configurable item in the list?

Tor Logs Dialog

Provide logs from the underlying Tor Provider. This dialog should match layout of Tor Browser's about:preferences#connection Tor Logs dialog. Some Tor Providers will not have logs to display (eg System Tor Daemon)

Main Window

Users reach this window after bootstrapping via the Connection dialog, or directly if the Tor Provider does not require explicit bootstrapping (eg System Tor Daemon). A password is required to decrypt a Ricochet Refresh profile. Obviously we draw a lot of inspiration here from KeyPassXC and friends.

Menus

File:
- New Profile
- Open Profile...
- Close Profile
- Save Profile As...

- Logout
- Logout All Profiles

- Quit

Profile:
- Set Visibility >
  - Online
  - Restricted
  - Hidden
- Copy Ricochet Id
- Edit Profile...

Contacts:
- Add Contact...
- Delete Contact
- Connect/Disconnect Contact
- Ban/Unban Contact

Chat:
- Export Logs...
- Delete Logs...

Tools:
- Downloads...
- Tor logs...
- Preferences...

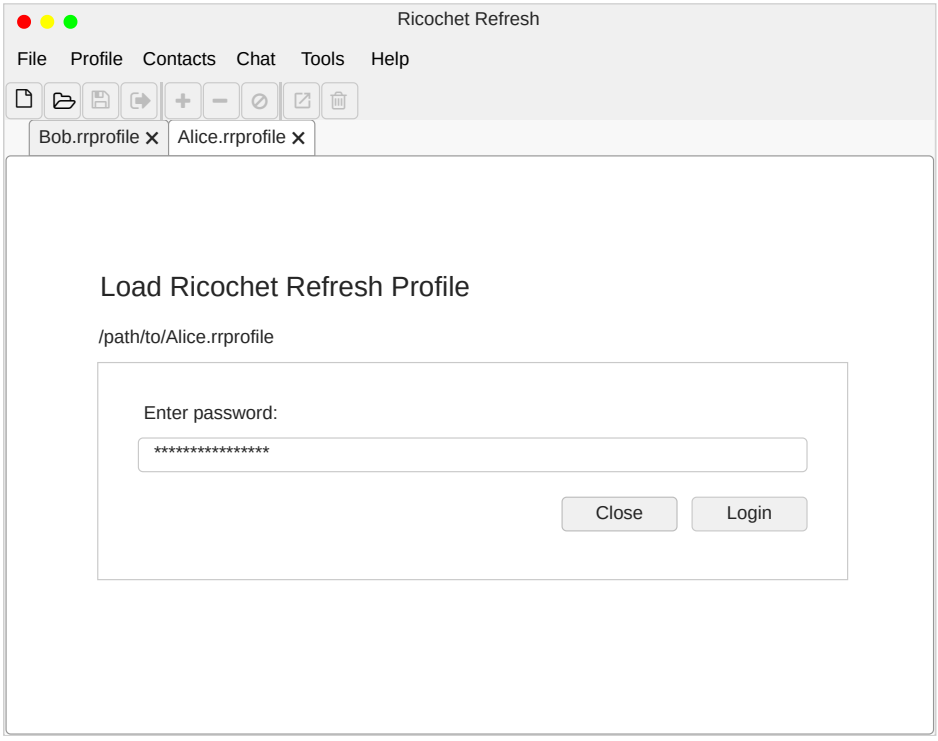
Help:
- Manual
- Licenses...

- Check for Updates...
- Changelog...
- About

- Licenses menu option should open a folder containing relevant licenses
- Changelog menu option opens CHANGELOG.txt in system default text editor

Toolbar Icons

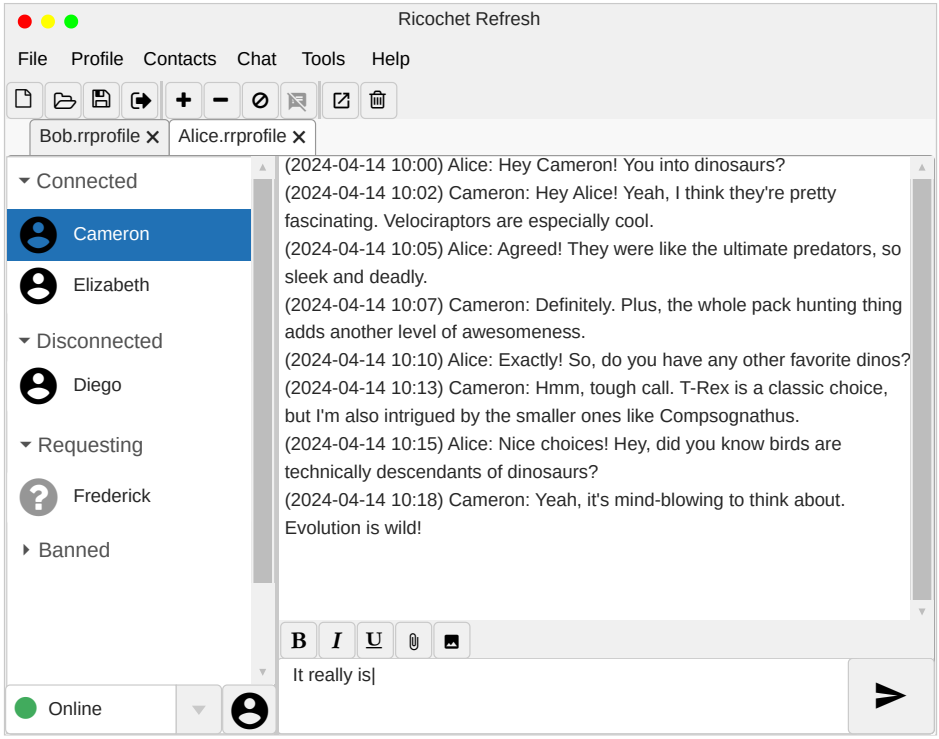
New Profile, Open Profie, Save Profile As, Logout | Add Contact, Delete Contact, Ban Contact, Connect/Disconnect Contact | Export Logs, Delete Logs



Users will always 'login' into the 'offline' state, they will opt-in to less private visibility states

Main Window (Online)

Profile tab when the user is logged in. In 'Online' mode identity and endpoint servers are enabled, anyone can cyberstalk the user if they know the user's Identity Server Service ID



- Hide a conversation by clicking on a user entry again to unselect

- Per-contact context menu will have all the per-contact commands from the Contacts menu

User groups:

- Connected: users which have connected to our, or which we have connected to their endpoint server

- Connecting: users which we are explicitly attempting to connect to (Hidden mode only)

- Disconnected: no active connection; 'offline' to us

- Requesting: in-progress outoing friend requests

- Banned: no endpoint server, actively blocking attempts when accessing our identity server

Visibility Modes:

- Online: identity and endpoint servers are enabled

- Restricted: endpoint servers are enabled

- Hidden: no endpoints enabled, but outgoing connections can occur

- Offline: no endpoints enabled, no outgoing connections either

NOTE: Online should really communicate 'most risk', users can be cyberstalked if they always stay in Online mode

Profile button:

Open an Edit Profile dialog where user can:

- get Ricochet id
- set display name
- set profile image
- set profile info
- w/e else metadata users opt into

Minor text formatting:
- Bold
- Italic
- Underline
Add Atachment
Inline-image

NOTE:

- Attachments are sent as-is, but are not rendered/previewed by the application.
- Inline-images will be somehow re-encoded to hopefully avoid malformed image decoder bugs/exploits

- URLS will never open a browser, only open a context menu with the option to copy the URL to clipboard

- exported conversations should be standardised to avoid leaking user's locale re timestamps, any potential formatting options, etc

- user status (connect/disconnect) messages will appear in chat

TODO: Chat Thumbnail and Image UI; images should have be optionally spoiler'd and have text descriptions

TODO: Chat Attachment UI

TODO: Incoming Friend Request flow

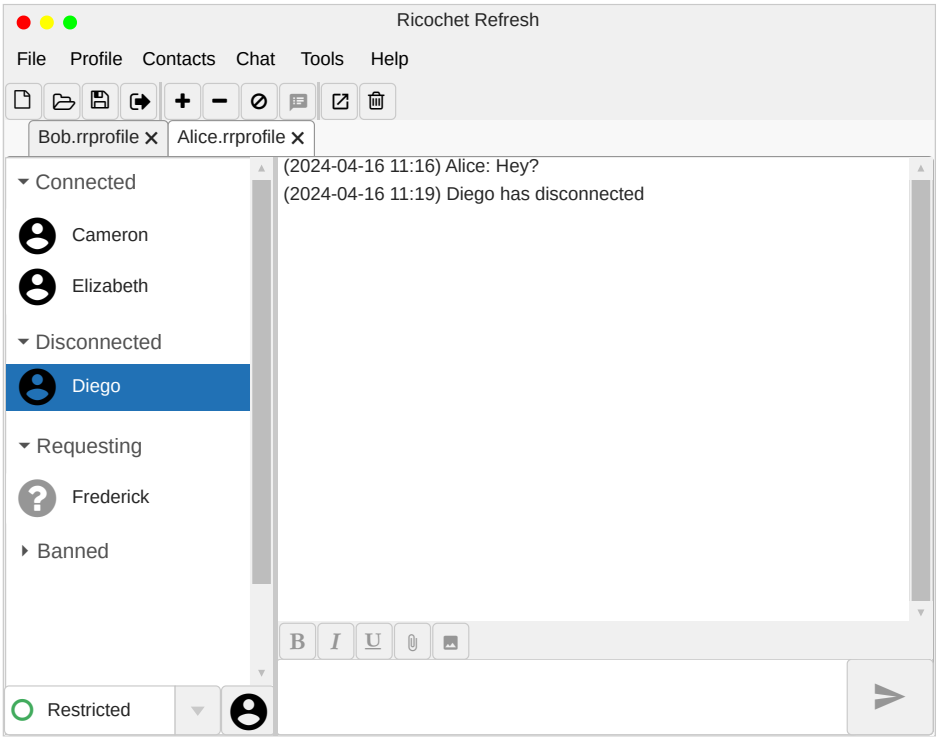
TODO: Downloads dialog

TODO: About dialog

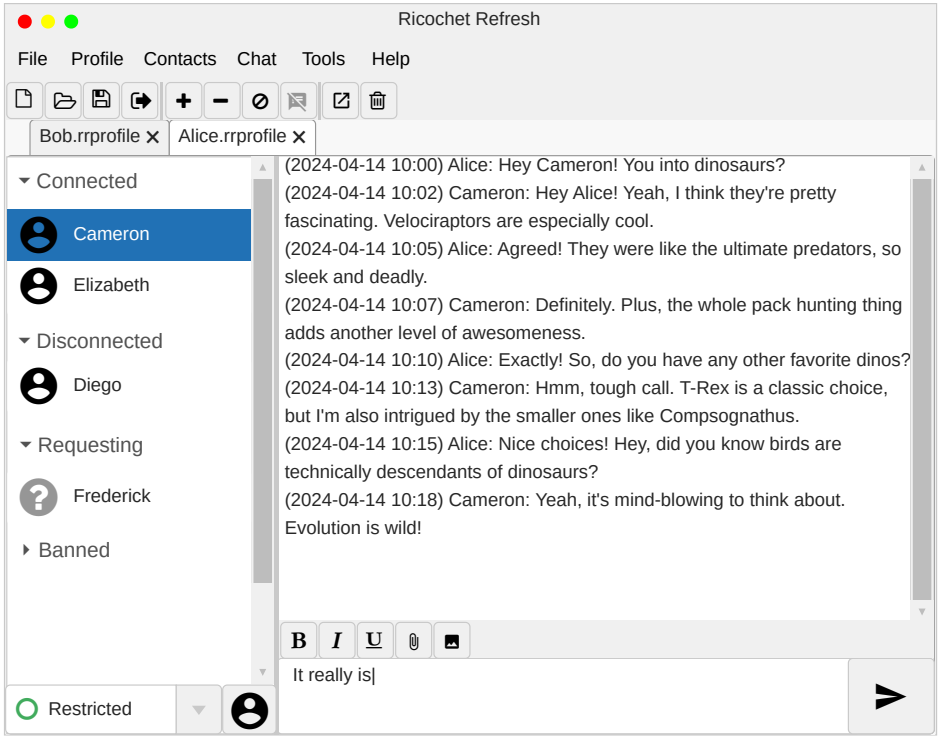
TODO: Edit Profile dialog

Main Window (Restricted)

In 'Restricted' mode (identity server disabled, endpoint servers enabled) only confirmed/allowed contacts may contact us. New contacts will not be able to access the public identity server to get through the gosling handshake to get their own endpoint server. This way stranges will not be able to cyber-stalk a user based off of their (potentially) public identity server. The UX should be identical to Online mode, except the user will never receive new friend requests.

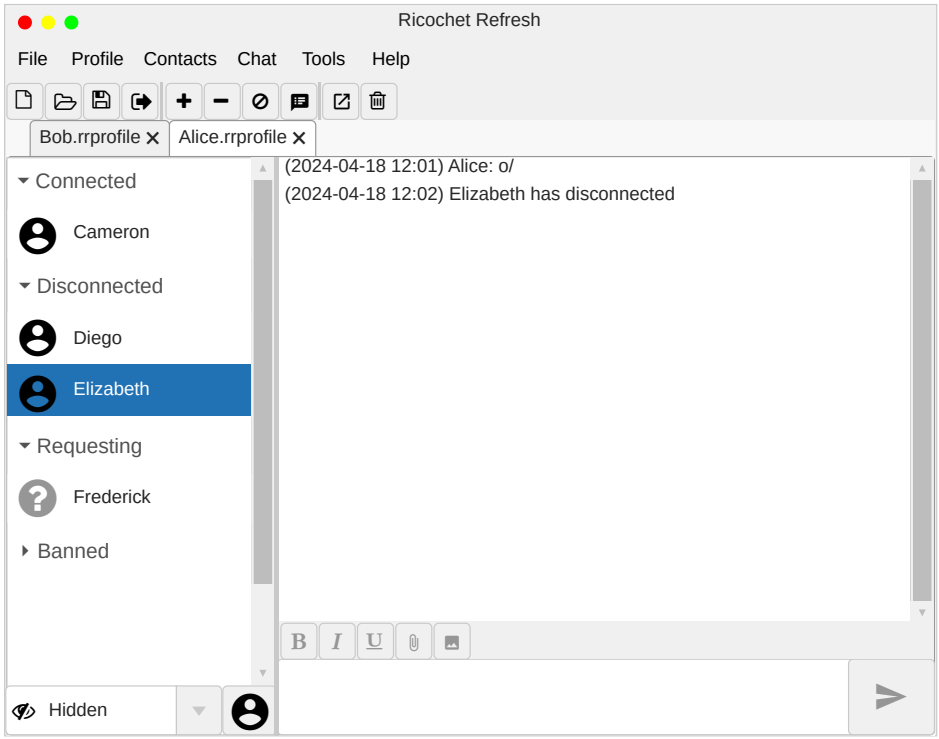


- Chat input widgets are disabled if the user is not connected



Main Window (Hidden)

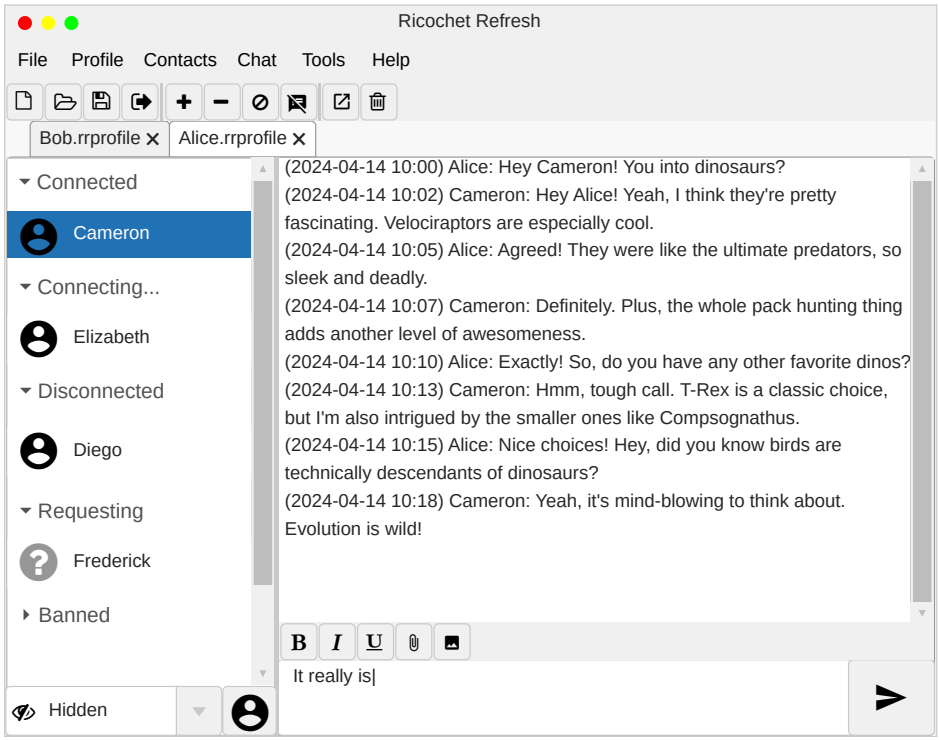
In 'Hidden' mode we do not enable any of our endpoint servers or identity servers, so even contacts do not gain our online/offline metadata. Connections are outgoing only and must be explicitly initiated by the user. This does imply that two users which are both in 'Hidden' mode will not be able to ever connect to each other!



- Chat input widgets are disabled if the user is not connected

- User must opt-in to connecting to contacts when in Hidden mode using the chat icon in the toolbar or connect action in the contacts menu

- Contact goes into Connecting... group when connect is initiated
- Once a user reaches Connected, then chat can happen



New Profile Dialog

Accessed via New Profile button or New Profile... option in File menu. Walks the user through creating a new Ricochet Refresh profile

TODO: We could make the allowed visibility options configurable here, IE maybe I want a profile which *never* runs an onion service (ie is alwasy in Hidden mode)

TODO: We *could* allow legacy contacts to connect to our identity service. Would require re-implementing a subset of the Ricochet Refresh 3.0 protocol

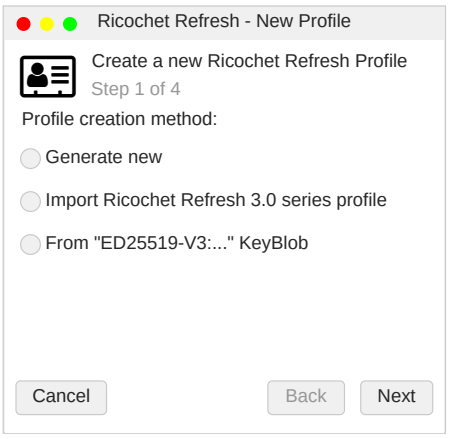
Start

Minimum Requirements:

- Display Name
- Profile info:
  - icon
  - pronouns
  - status
  - text description
- Save Path

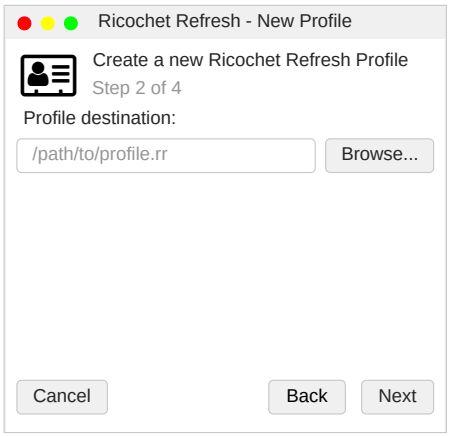
Other:

- Encryption Options?
  - key generation
  - see KeePassXC db options for instance

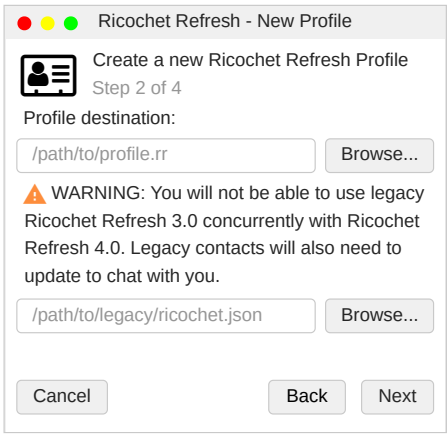


- Generate New: Create a new Ed25519 private key for identity service
- Import: open a user's legacy Ricochet-Refresh ricochet.json profile, import users and add them to the Requesting... set
- From KeyBlob: allow user to just import their private key

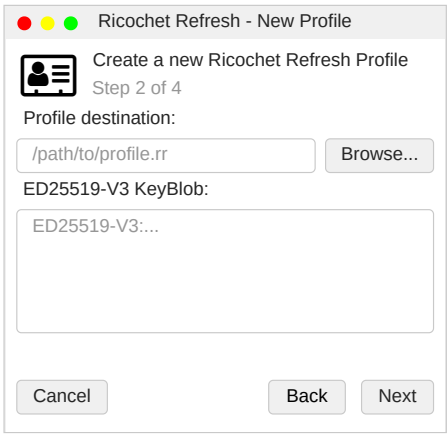
Generate New



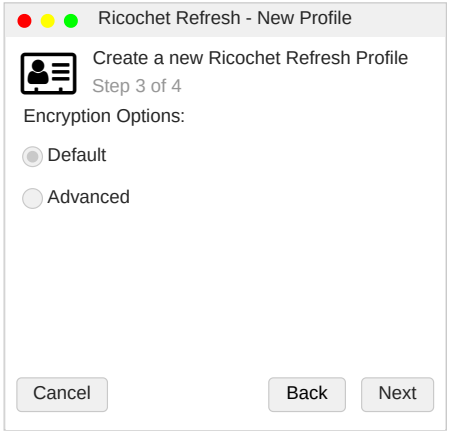
Import Legacy



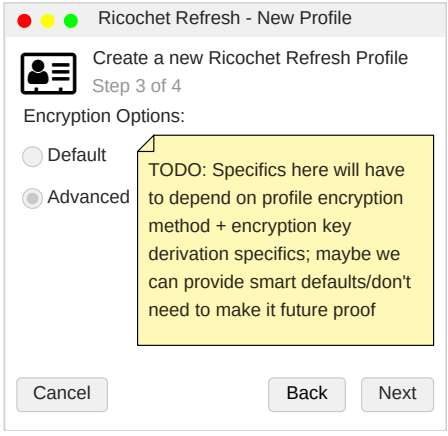
From KeyBlob



Encryption Options (Default)

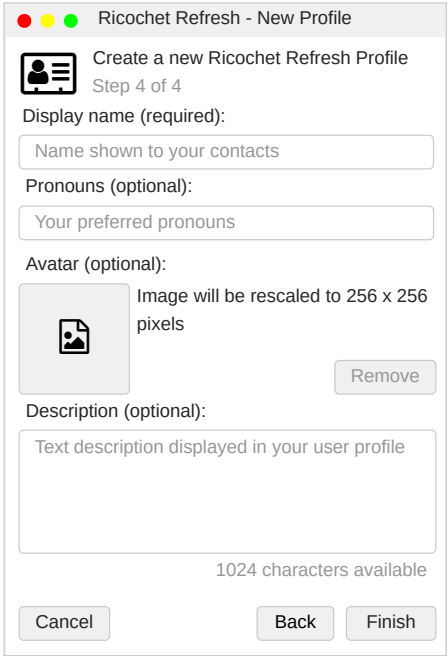


Encryption Options (Advanced)



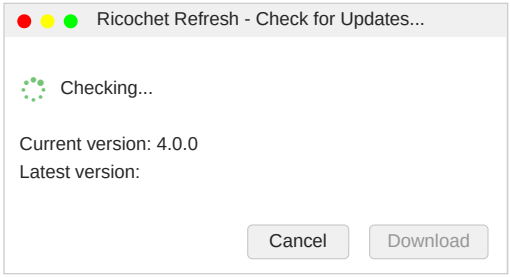
See KeePassXC new profile flow for examples of things we should potentially provide knobs for; presumably going to use some variant of Argon2 for encryption key derivation, who knows what for encryption (this will also depend on the profile file format which requires some technical investigation work)

Profile Details

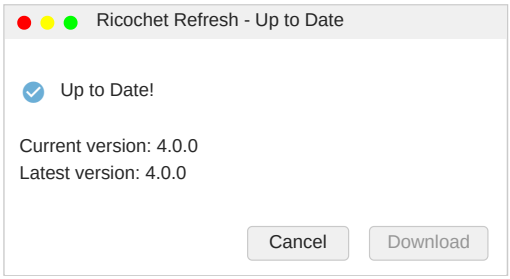


Updates Dialog

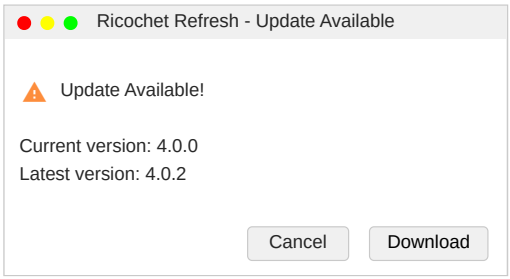
Accessed via the Help > Check for Updates... menu item. This will open a dialog which pings an onion service for update jsons, which will tell this dialog which install media/package to download.



- Check happens over Tor to Onion Service endpoint
- Will need some to maintain some update jsons



- Ricochet Refresh is up to date so we good



- Download the correct package based on the current insalled version (eg a deb, appimage, dmg, windows installer, etc

- Download button will open Downloads dialog