

Connection Dialog

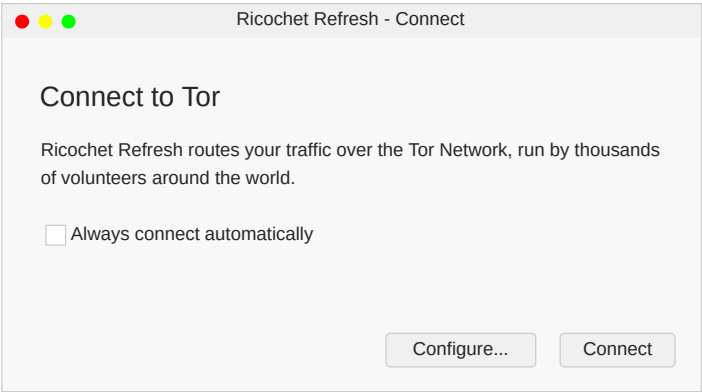
This is the first window that will appear if Ricochet Refresh is managing its own Tor provider (versus using a system-owned Tor or Arti instance). If we are using an external Tor provider, we will go directly to the Main window.

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.

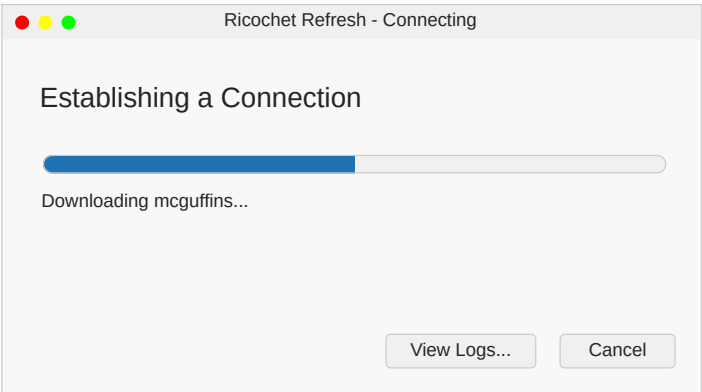
On the other hand, if you say ok one guard per profile, then you run into the problem having a stable guard solves: increased probability of a bad/adversarial guard versus a good guard.

We will try to follow a desktop'ified version of Tor Browser's [about:torconnect](#) page here



Configure opens the Preferences dialog

Connect begins bootstrapping tor



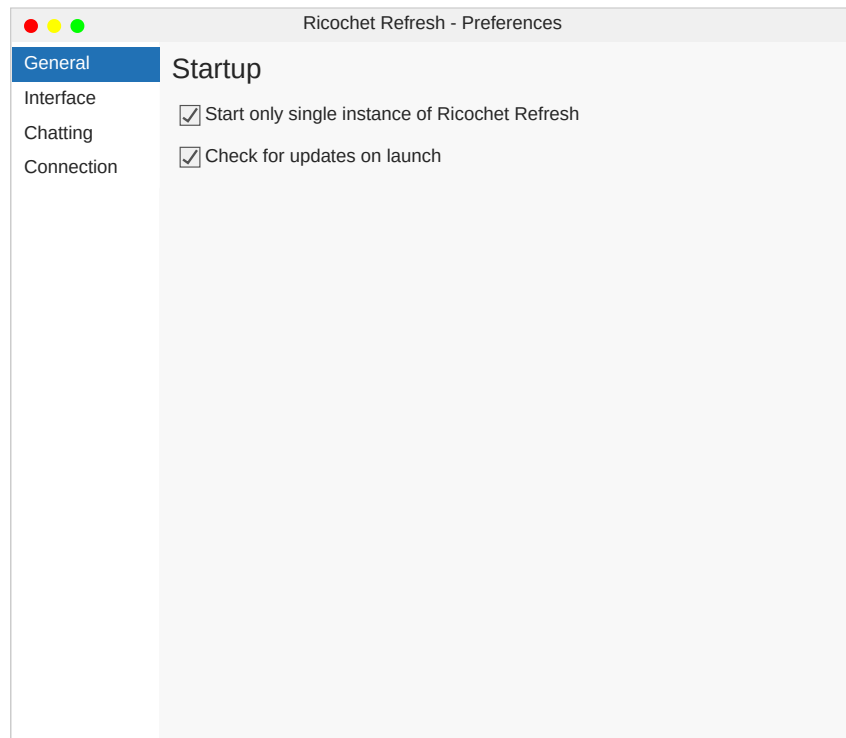
Open the Tor Logs dialog

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?

General

Interface

Chatting

Connection

Language

Select interface language: English (en-US)

Toolbars

Button style: Icon only

Alerts

☒ Show desktop notifications

☒ Blink taskbar icon

☒ Enable audio notifications

Tray Icon

☒ Minimize to system tray

☒ Close to system tray

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

Ricochet Refresh - Preferences

General

Interface

Chatting

Connection

Logging

☒ Enable conversation logging

☒ Display conversation scrollbar

Scrollbar lines:

1000

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

General

Interface

Chatting

Connection

Quickstart

Bridges

Network Settings

Advanced

Quickstart connects Ricochet Refresh to the Tor Network automatically when launched, based on your last used connection settings

☒ Always connect automatically

Bridges help you securely access the Tor Network in places where Tor is blocked. Depending on where you are, one bridge may work better than another

☒ Use Bridges

Add bridges

☒ Chose from one of Ricochet Refresh's built-in bridges

☒ obfs4

Makes your Tor traffic look like random data. May not work in heavily censored regions.

☐ Snowflake

Routes your connection through Snowflake proxies to make it look like you're placing a video call, for example.

☐ meek-azure

Makes it look like you're connected to a Microsoft website, instead of using Tor. May work in heavily censored regions, but is usually very slow.

☐ Enter bridge addresses you already know

Paste your bridge addresses here

Network Settings

☐ I use a proxy to connect to the internet

Proxy Type

SOCKS5

Address

IP address or hostname

Port

Username

Optional

Password

Optional

☐ This computer goes through a firewall that only allows connections to

Allowed Ports

80,443

Advanced

View the Tor logs

View Logs...

Backend

Select which Tor client implementation to use. Changing requires an application restart.

☒ Out-of-Process Tor daemon (default)

☐ System Tor daemon

☐ In-Process Arti

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

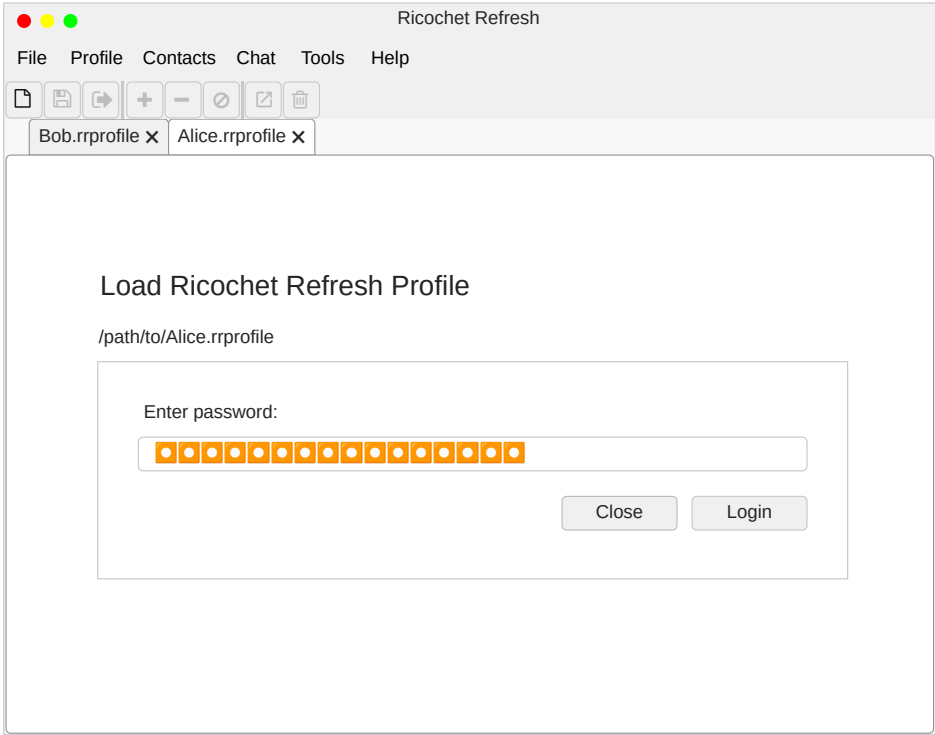
Provide logs from the underlying Tor Provider. This dialog should match layout of Tor Browser's about:preferences#connection Tor Logs dialog. Some Tor Providers will not have logs to display (eg System Tor Daemon)



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.

- TODO: New profile flow
- TODO: Open Profile toolbar button?



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

Menus

File:	Profile:	Contacts:	Chat:	Tools:	Help:	
- New Profile	- Set Visibility >	- Add Contact...	- Export Logs...	- Downloads...	- Manual	- Licenses menu option
- Open Profile...	- Online	- Delete Contact	- Delete Logs...	- Tor logs...	- Licenses...	should open a folder
- Close Profile	- Restricted	- Connect/Disconnect		- Preferences...	---	containing relevant licenses
- Save Profile As...	- Hidden	Contact			- Check for Updates...	- Changelog menu option
---	- Copy Ricochet Id	- Ban/Unban Contact			- Changelog...	opens CHANGELOG.txt in
- Logout	- Edit Profile...				- About	system default text editor
- Logout All Profiles						

- Quit						

Toolbar Icons

[New Profile](#), [Save Profile As](#), [Logout](#) | [Add Contact](#), [Delete Contact](#), [Ban Contact](#), [Connect/Disconnect Contact](#) | [Export Logs](#), [Delete Logs](#)

The screenshot displays the Ricochet Refresher application. The top menu bar includes File, Profile, Contacts, Chat, Tools, and Help. Below the menu is a toolbar with icons for file operations and chat functions. The main window is divided into two panes. The left pane shows a list of contacts, categorized into 'Connected', 'Disconnected', 'Requesting', and 'Banned'. The right pane shows a chat window with a conversation history and a text input field at the bottom. The chat window title is 'Alice.rrprofile'. The chat history shows a conversation between Alice and Cameron. The text input field at the bottom contains the text 'It really is|'. The status bar at the bottom shows 'Online' and a contact icon.

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 Attachment
- 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

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

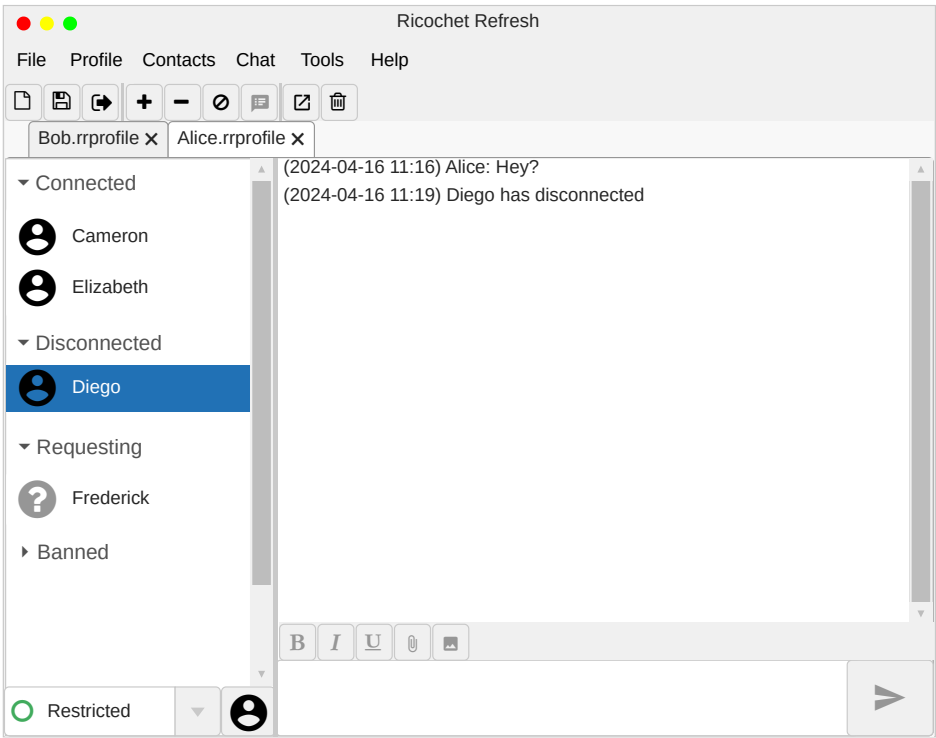
TODO: Downloads dialog

TODO: About dialog

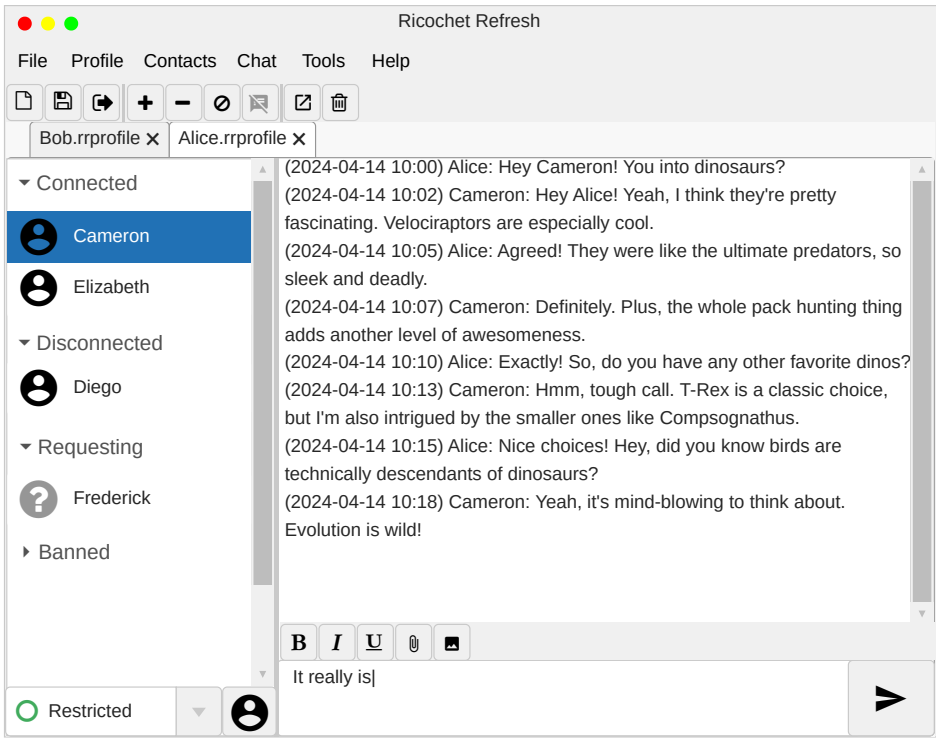
TODO: Edit Profile dialog

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 strangers 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.

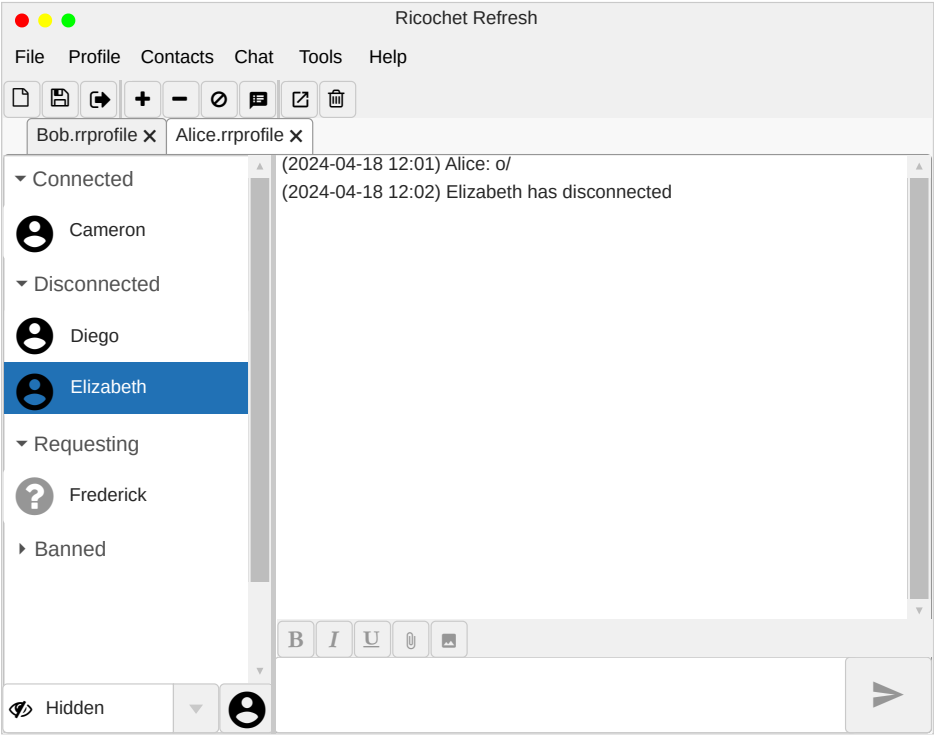


- Chat input widgets are disabled if the user is not connected



Main Window (Hidden)

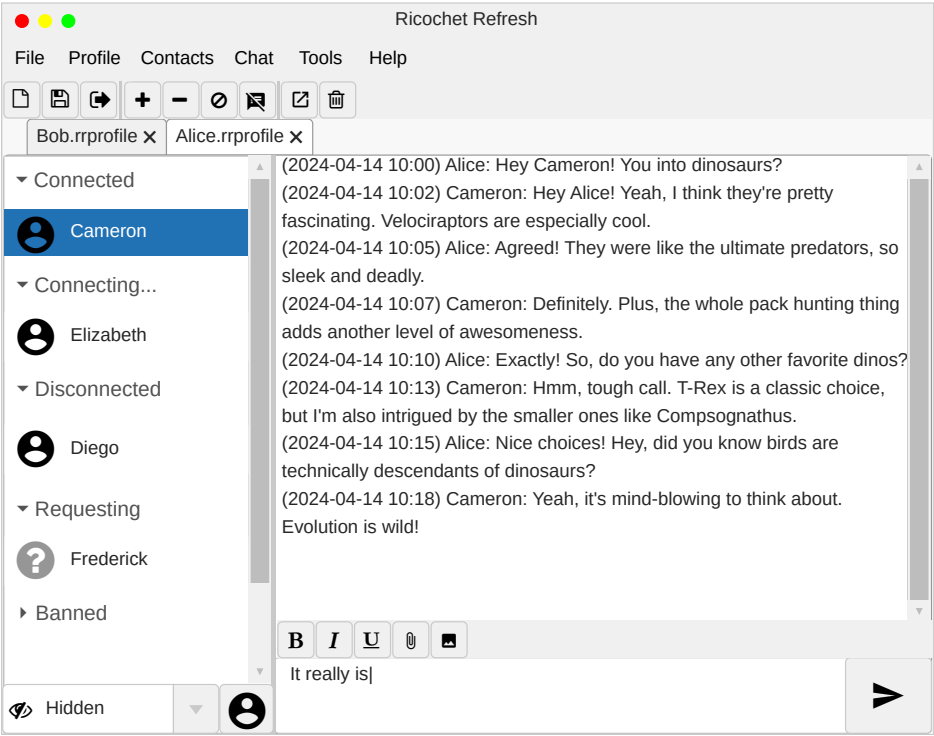
In 'Hidden' mode we do not enable any of our endpoint servers or identity servers, so even contacts do not gain our online/offline metadata. Connections are outgoing only and must be explicitly initiated by the user. This does imply that two users which are both in 'Hidden' mode will not be able to ever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



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

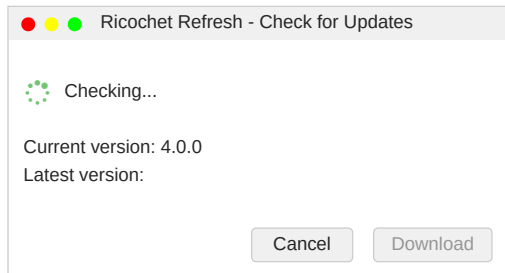
- User must opt-in to connecting to contacts when in Hidden mode using the chat icon in the toolbar or connect action in the contacts menu

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

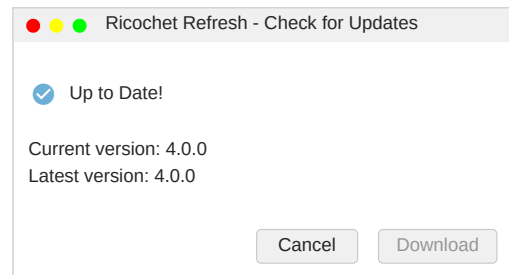


Check for Updates Dialog

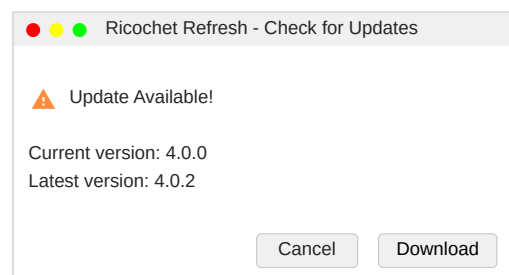
Accessed via the Help > Check for Updates... menu item. This will open a dialog which pings an onion service for update jsons, which will tell this dialog which install media/package to download.



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



- Ricochet Refresh s 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