

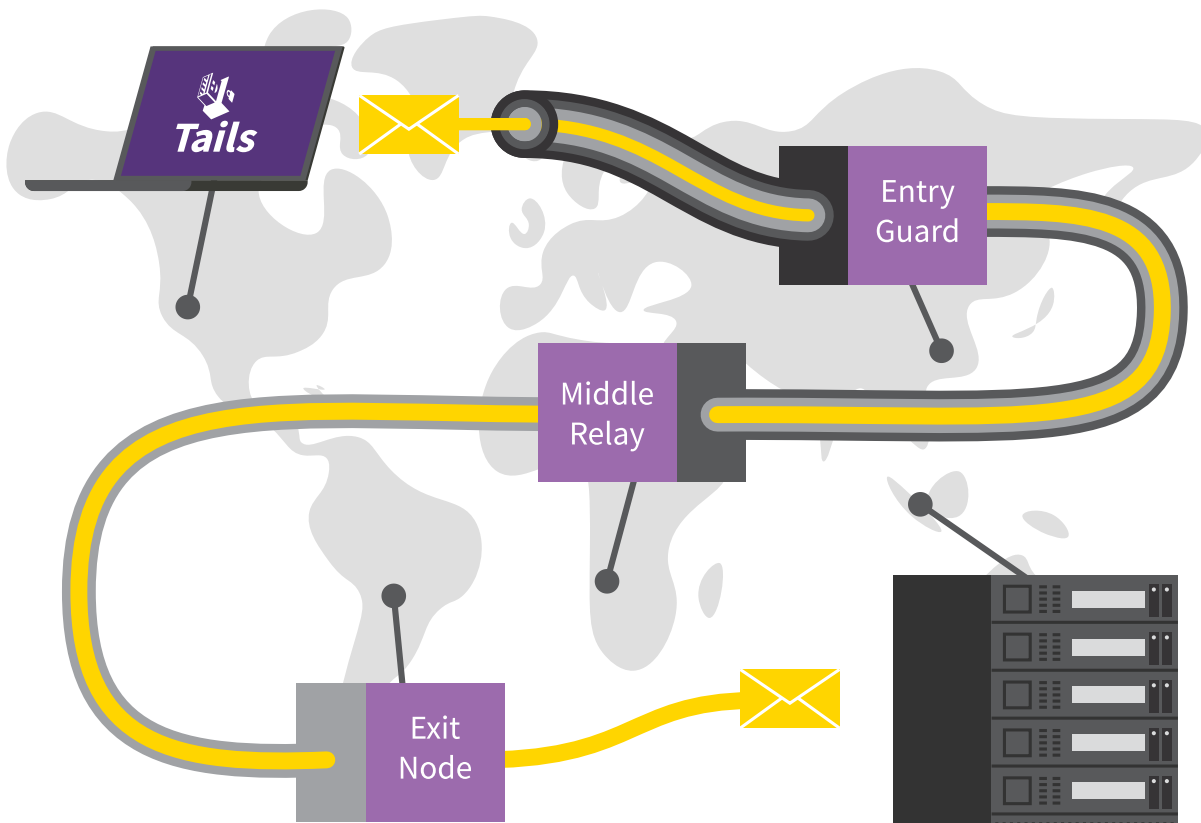
[Donate](#)[Home](#) [How Tails works](#) [Get Tails](#) [Documentation](#) [Support](#) [Contribute](#) [News](#)[doc](#)[anonymous internet](#)[Connecting to the Tor network](#)[English](#) [DE](#) [ES](#) [FR](#) [IT](#) [PT](#) [RU](#)

Connecting to the Tor network

- I. [Tor relays and bridges](#)
- II. [Connecting to Tor automatically](#)
- III. [Hiding to your local network that you are connecting to Tor](#)
- IV. [Viewing the status of Tor](#)
- V. [Troubleshooting connecting to Tor](#)

Everything you do on the Internet from Tails goes through the Tor network.

Tor encrypts and anonymizes your connection by passing it through 3 relays. Tor relays are servers operated by different people and organizations around the world.



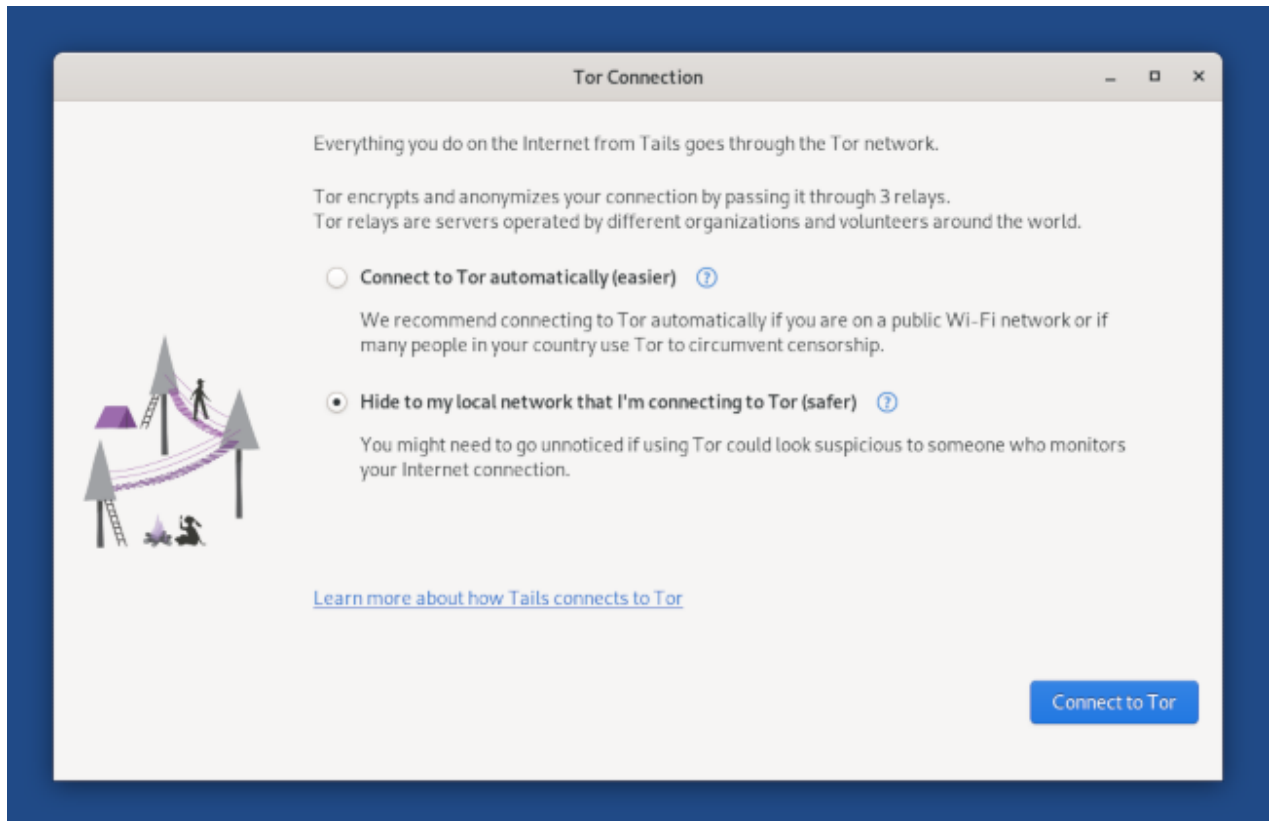
Browser displays the error message `Proxy server refusing connections` until you are connected to Tor.

Because Tor routes your Internet traffic through 3 relays before reaching its destination, the connection is slower than when you are not using Tor.

See our documentation on [why Tor is slow](#).

To connect to the Tor network:

1. [Connect to a local network](#), wired, Wi-Fi, or mobile.
2. The *Tor Connection* assistant appears to help you connect to the Tor network.



3. Choose whether you want to:
 - Connect to Tor automatically
 - Hide to your local network that you are connecting to Tor

The implications of both methods are detailed below.

Tor relays and bridges

- **Public Tor relays**

Most of the time, your local network does not block access to the Tor network and you can use a public relay as your first Tor relay.

Using a public Tor relay as your first Tor relay makes it clear to your local network that you are connecting to Tor, while still keeping your online activity secure and anonymous.

- **Tor bridges**

Tor bridges are secret Tor relays that keep your connection to the Tor network hidden.

Use a bridge as your first Tor relay if connecting to Tor is blocked or if using Tor could look suspicious to someone who monitors your Internet connection.

The technology used by Tor bridges is designed to circumvent censorship where connections to Tor are blocked, for example in some countries with heavy censorship, by some public networks, or by some parental controls.

It does so by camouflaging your connection so it cannot be recognized as a connection to Tor. As a consequence, the same technology can be used to hide that you are using Tor if it could look suspicious to someone who monitors your Internet connection.

Tor bridges are often less reliable and slower than public Tor relays.

Connecting to Tor automatically

We recommend connecting to Tor automatically if you are on a public Wi-Fi network or if many people in your country use Tor to circumvent censorship.

When you choose this option:

1. First, Tails synchronizes the clock of the computer automatically, because a correct time is needed to be able to connect to the Tor network.

Tails learns the current time by connecting to the captive portal detection service of [Fedora](#), which is used by most Linux distributions. This connection does not go through the Tor network and is an exception to our policy of only making Internet connections through the Tor network.

You can learn more about our security assessment of this time synchronization in our [design documentation about non-Tor traffic](#).

If you choose instead to [hide that you are connecting to Tor](#), you might have to fix the computer clock manually.

2. Then, Tails tries different ways of connecting to Tor until it succeeds:

1. Tails tries to connect to Tor directly using **public relays**, without using a bridge.
2. Tails tries to connect to Tor using one of the **default bridges**, already included in Tails, if connecting using public relays fails.
3. If public relays and default bridges don't work, Tails asks you to configure a **custom bridge**, if connecting using the default bridges fails.

Someone monitoring your Internet connection could identify these attempts as coming from a Tails user.

In the future, Tails will also automatically:

- Detect if you have to sign in to the local network using a captive portal ([#5785](#))

Hiding to your local network that you are connecting to Tor

You might need to go unnoticed if using Tor could look suspicious to someone who monitors your Internet connection.

When you choose this option, Tails will only connect to Tor after you configure a Tor bridge. Bridges are secret Tor relays that hide that you are connecting to Tor.

It is impossible to hide to the websites that you visit that you are using Tor, because the [list of exit nodes of the Tor network](#) is public.

Our team is doing its best to help you connect to Tor using the most discrete types of Tor bridges. That is why, when you decide to hide that you are connecting to Tor:

- Default bridges are not available.

You will have to know the address of a custom bridge.

To request a custom bridge, you can either:

1. Request a bridge on <https://bridges.torproject.org/>.

We recommend doing so before starting Tails and ideally from a different local network than the one on which you want to hide that you are using Tor.

2. Send an empty email to bridges@torproject.org from a Gmail or Riseup email address.

For example, you can send the email from your phone and type the bridge in Tails.

Sending the email reveals to Gmail or Riseup that you are trying to connect to Tor but not to someone who monitors your Internet connection.

Even someone who knows your bridge cannot know what you are doing online from Tails.

- You can only use the types of bridges that our team considers discrete enough.

Currently in Tails, only **obfs4 bridges** hide that you are using Tor.

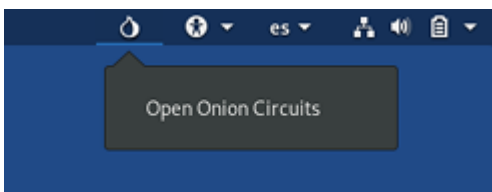
To save the last Tor bridge that connected to Tor successfully, turn on the [Tor Bridge feature of the Persistent Storage](#).



In the future, we will make it easier to use a custom bridge by:

- Allowing you to scan the QR code returned by [#18219](mailto:bridges@torproject.org))
- Allowing you to request a bridge from Tails by solving a CAPTCHA ([#15331](#))

Viewing the status of Tor

The status of Tor appears as an onion icon in the notification area:



-  You are connected to Tor.
-  You are not connected to Tor.

Troubleshooting connecting to Tor

See our documentation on [troubleshooting connecting to Tor](#).

tails

- Home
- How Tails works
- Get Tails
- Documentation
- Support
- Contribute
- News

Support

- FAQs
- Known issues
- Warnings
- Accessibility
- Upgrade

Contribute

- Report an error
- Translate
- Source code
- GitLab
- Roadmap
- Donate

ABOUT US

- Contact
- Mission and values
- Social contract
- Sponsors
- Code of conduct
- License
- Jobs

News

Subscribe to our newsletter:

