

ALWAYS UPDATE TAILS ASAP! If you can't automatically update, you'll need two USB sticks. Follow these instructions:

Windows:

<https://tails.boum.org/install/win/usb/overview/index.en.html>

Mac:

<https://tails.boum.org/install/mac/usb/overview/index.en.html>

Linux:

<https://tails.boum.org/install/linux/usb/overview/index.en.html>

Check out the official tutorials/documentation!

(Online) <https://tails.boum.org/doc/index.en.html>

(Offline from tails) <file:///usr/share/doc/tails/website/doc.en.html>

Getting started!

Persistence: this will create an partition (section) on your Tails USB to store files!

(Online) <https://tails.boum.org/install/clone/index.en.html#create-persistence>

(Offline from Tails) <file:///usr/share/doc/tails/website/install/clone.en.html#create-persistence>

file:///usr/share/doc/tails/website/install/clone.en.html#create-persistence

Search

6/6. Create an encrypted persistent storage (optional)



You can optionally create an *encrypted persistent storage* in the remaining free space on the new Tails USB stick to store any of the following:

- Your personal files and working documents
- Some of your settings
- Your encryption keys

The data in the encrypted persistent storage:

- Remains available across separate working sessions.
- Is encrypted using a passphrase of your choice.



The encrypted persistent storage is not hidden. An attacker in possession of the USB stick can know whether it has an encrypted persistent storage. Take into consideration that you can be forced or tricked to give out its passphrase.



It is possible to open the encrypted persistent storage from other operating systems, but it might break your security. Other operating systems should probably not be trusted to handle sensitive information or leave no trace.

Create the persistent storage

1. Choose **Applications ► Tails ► Configure persistent volume**.
2. Specify a passphrase of your choice in both the **Passphrase** and **Verify Passphrase** text boxes.



We recommend choosing a long passphrase made of five to seven random words. [Learn more.](#)

3. Click on the **Create** button.
4. Wait for the creation to finish.



If you close the assistant before the creation finishes, you might not be able to start Tails from this USB stick anymore.

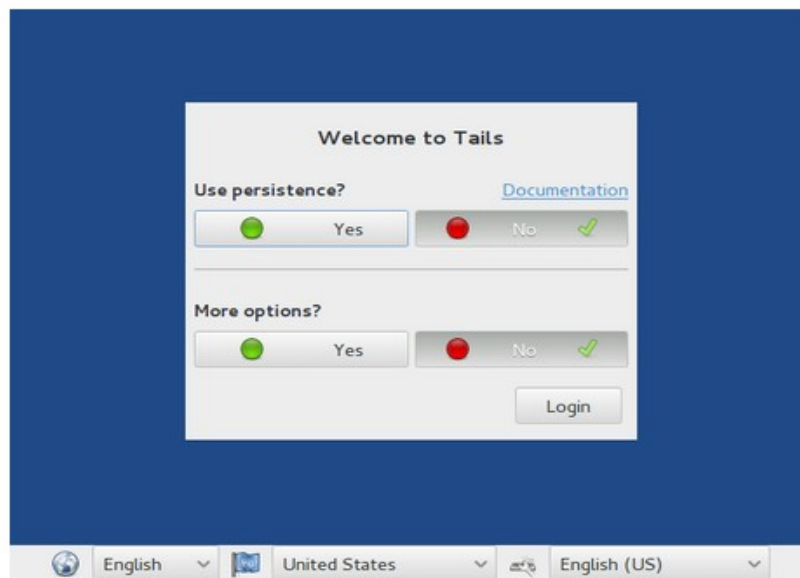
5. The assistant shows a list of the possible persistence features. Each feature corresponds to a set of files or settings to be saved in the encrypted persistent storage.

We recommend you to only activate the **Personal Data** persistence feature for the time being. You can activate more features later on according to your needs.

6. Click **Save**.

Restart and activate the persistent storage

1. Shut down the computer and restart on the new Tails USB stick.
2. In *Tails Greeter*:



- Select your preferred language in the drop-down list on the bottom left of the screen.
 - In the **Use persistence?** section, choose **Yes** to activate the encrypted persistent storage for the current working session.
 - Enter the passphrase of the persistent volume in the **Passphrase** text box.
 - Click **Login**.
3. After 15–30 seconds, the Tails desktop appears.

4. You can now save your personal files and working documents in the **Persistent** folder. To open the **Persistent** folder choose **Places ► Persistent**.



You now have a working Tails, congrats!

FINAL RECOMMENDATIONS



Tails does not protect you from everything! Have a look at our [warnings](#).



If you face any problem, use the **Report an error** launcher on the Tails desktop or visit our [support pages](#).

We hope you enjoy using Tails :)

Tails and Tor Browser:

Connecting to Wi-Fi:

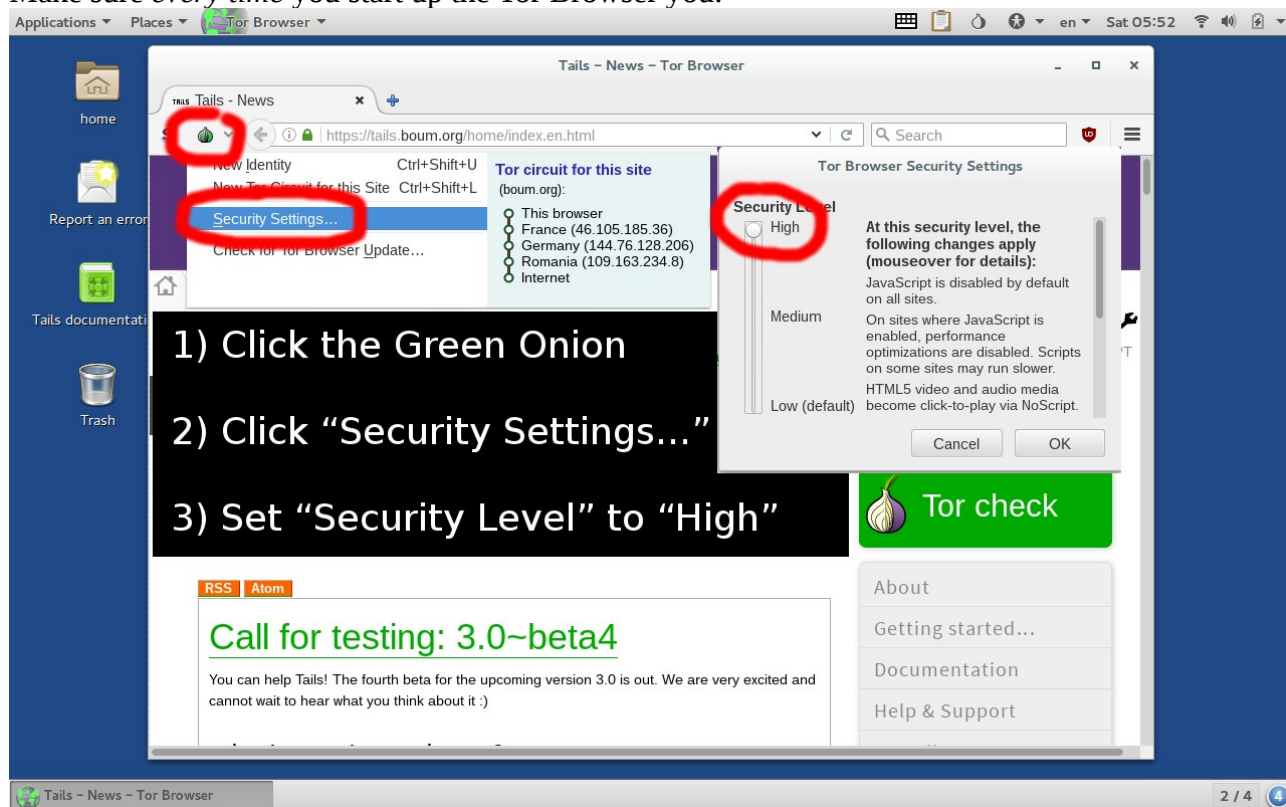
The screenshot shows the Tails desktop with a blue background. On the left, there are icons for 'home', 'Report an error', 'Tails documentation', and 'Trash'. On the right, the system menu is open, showing volume, network, and battery settings. The 'Wi-Fi' section is highlighted, and the 'Select Network' button is circled in red. A red arrow points from the 'Tor is ready' notification at the bottom to the 'Select Network' button. The notification text reads: 'Tor is ready You can now access the Internet.' Below the notification, there is a 'Testing' button.

Connecting to Wi-Fi:

- 1) Click down arrow in upper right of the screen
- 2) Click Wi-Fi
- 3) Click "Select Network" and select your network
- 4) Enter in your network's password
- 5) Wait for "Tor is ready" notification

Security Settings:

Make sure *every time* you start up the Tor Browser you:



Javascript:

If a website is acting differently than you expect (windows aren't popping up, images aren't loading, you aren't able to post something or login, etc.), you'll need to turn on *Javascript* for that website:

- 1) Click the "S" with the red slash through it (upper left by green onion)
- 2) Click "Temporarily allow all this page"
- 3) Refresh page

"Tor hidden services" aka ".onion" websites

source: <http://nzh3fv6jc6jskki3.onion/en/security/network-security/tor#riseups-tor-hidden-services>

facebook.com:	facebookcorewwi.onion (needs <i>javascript</i> on and " <i>Medium</i> " security setting on the Tor Browser security slider)
mail.riseup.net:	zsolxunfmbfuq7wf.onion
pad.riseup.net:	5jp7xtmox6jyoqd5.onion
share.riseup.net:	6zc6sejeho3fwr4.onion
account.riseup.net:	j6uhdvbhz74oefx.onion
we.riseup.net:	7lvd7fa5yfbdqaii.onion ("Crabgrass")
help.riseup.net:	nzh3fv6jc6jskki3.onion

Useful Tails Applications and Info:

Screenshots in tails: Applications>Utilities>Screenshot

Textpad in tails: Applications>Accessories>Gedit

“New Identity” function: In Tor Browser if you need to connect to a website from a *different location*:

- Click the Green Onion
- Click “New Identity”

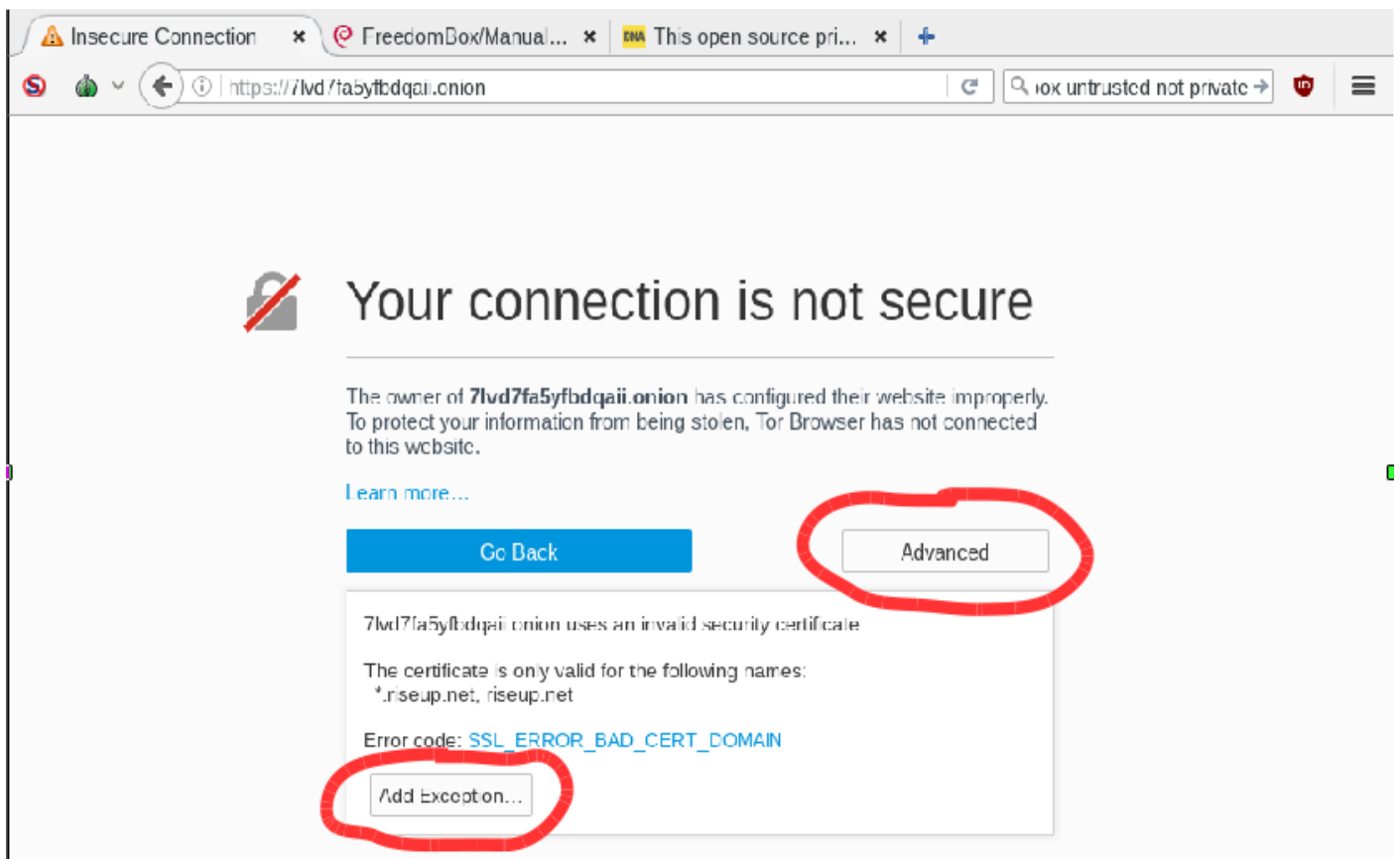
Crabgrass:

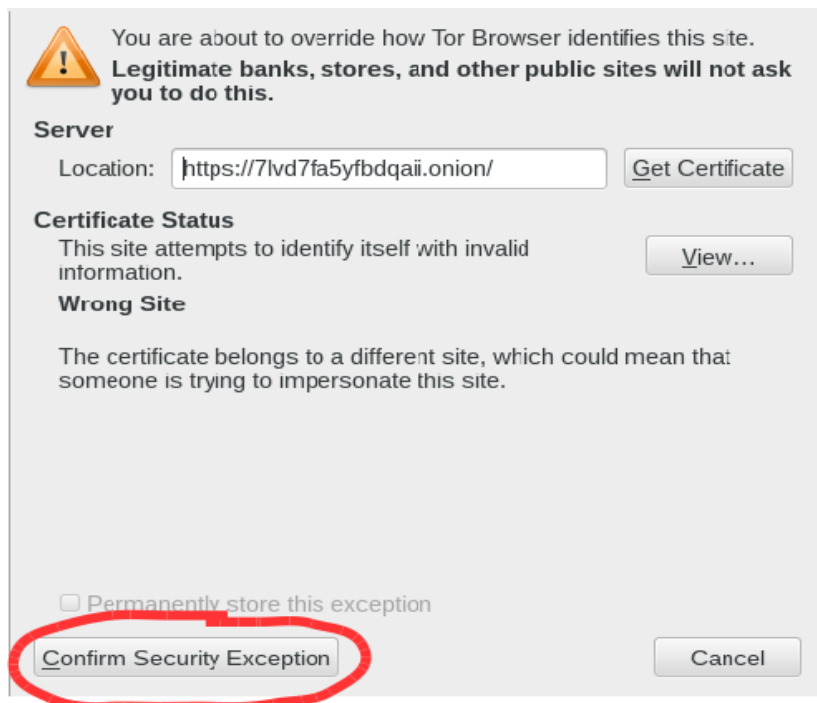
To access Crabgrass aka we.riseup.net:

7lvd7fa5yfbdqaii.onion

(this is what the website URL looks like...note the ".onion" *NOT* ".com"...this type of website is only accessible via Tor Browser)

Every time you access the Crabgrass *hidden service* (.onion address) your browser will warn you that “Your connection is not secure”. Your browser might also use words such as "untrusted", "not private", "privacy error" or "unknown issuer/authority". Telling your browser that you are aware of this might involve pressing buttons such as "I understand the Risks", "proceed to ... (unsafe)" or "Add exception".





Uploading files/pictures to Crabgrass from Tails:

Since Tails is built for security, the Tor Browser only has access to the *Home>Tor Browser* folder (note: **NOT** the *Persistence>Tor Browser* folder)

To upload any file to the Internet, you'll most likely need to *turn Javascript on*. Then copy the file to the *Home>Tor Browser* folder! Then you can upload!

