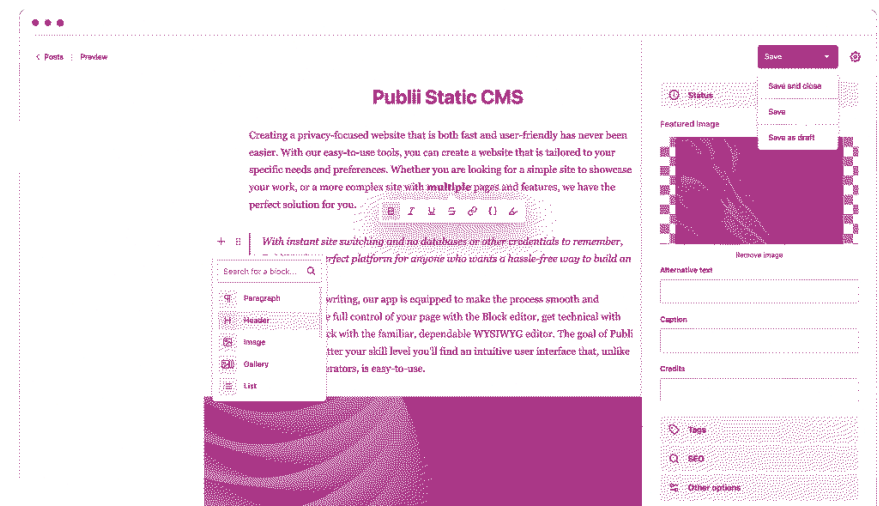
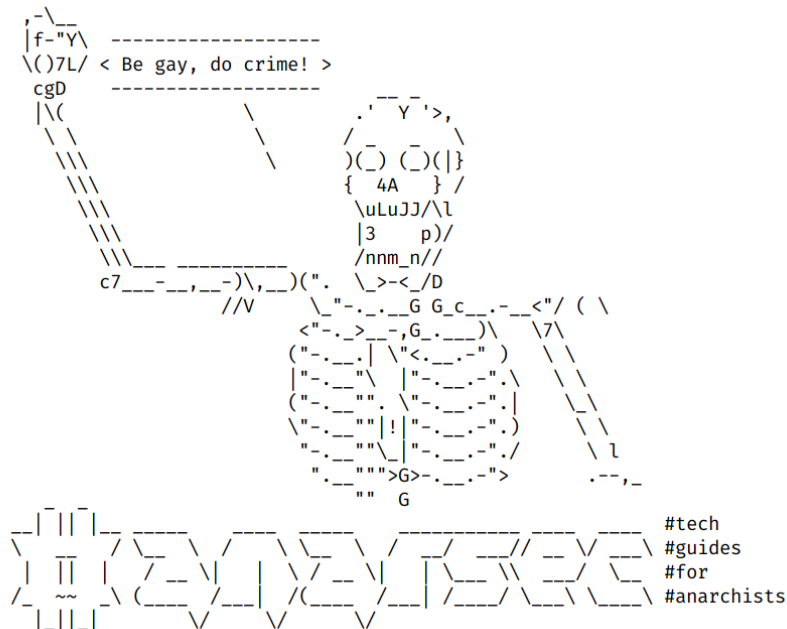


This guide will explain how to create a website with Publii (a CMS, or Content Management System), on Tails (an operating system that leaves no trace of your activity on your computer), and how to publish it with the help of one of several radical hosting providers—the comrades who manage the servers on which your site will be published.

# Create a Static Website with Publii



Series: Defensive

AnarSec is a resource designed to help anarchists navigate the hostile terrain of technology — defensive guides for digital security and anonymity, as well as offensive guides for hacking. All guides are available in booklet format for printing and will be kept up to date.

## Defensive

### *Tails*

- Tails for Anarchists
- Tails Best Practices
- Create a Static Website with Publii

### *Qubes OS*

- Qubes OS for Anarchists

### *Phones*

- Kill the Cop in Your Pocket
- GrapheneOS for Anarchists

### *General*

- Linux Essentials
- Remove Identifying Metadata From Files
- Encrypted Messaging for Anarchists
- Make Your Electronics Tamper-Evident

## Offensive

*Coming soon*

This version of the zine was last edited on 2026-10-16. Visit [anarsec.guide](https://anarsec.guide) to see whether it has been updated since.

The dagger symbol † on a word means that there is a glossary entry for it. Ai ferri corti.

nection from learning what sites you visit, and it prevents the operators of the sites you visit from learning your physical location.

Every website visited through the Tor network passes through 3 relays. Relays are servers hosted by different people and organizations around the world. No single relay ever knows both where the encrypted connection is coming from and where it is going. An excerpt from a leaked top-secret NSA assessment calls Tor “the King of high secure, low latency Internet anonymity” with “no contenders for the throne in waiting”. The Tor network can be accessed through the Tor Browser on any operating system. The Tails<sup>†</sup> operating system forces every program to use the Tor network when accessing the Internet.

For more information, see Tails for Anarchists<sup>44</sup> and Privacy Guides<sup>45</sup>. To understand the limitations of Tor, see the Whonix documentation<sup>46</sup>.

## Contents

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Download Publii .....                                                    | 5  |
| Create your Site .....                                                   | 7  |
| Publish your Site .....                                                  | 9  |
| Server Settings .....                                                    | 11 |
| Maintain a Backup of Your Site Data .....                                | 16 |
| Backup your Tails key .....                                              | 16 |
| Make a remote backup .....                                               | 17 |
| Operational Security for Site Managers .....                             | 17 |
| Appendix: Trusting Publii For Tails .....                                | 17 |
| Appendix: Making your Website Accessible through an .Onion Address ..... | 18 |
| Appendix: Collaborating with Others on the Same Website .....            | 18 |
| Appendix: Adding a Contact Form .....                                    | 18 |
| Appendix: Making a Multilingual Site .....                               | 18 |
| Appendix: Recommended Configuration for Hosting Providers .....          | 19 |
| Appendix: Recommendations .....                                          | 19 |
| Your Phone .....                                                         | 20 |
| Your Computer .....                                                      | 20 |
| Encrypted Messaging .....                                                | 21 |
| Storing Electronic Devices .....                                         | 21 |
| Appendix: Glossary .....                                                 | 21 |
| Operating system (OS) .....                                              | 21 |
| Tor network .....                                                        | 21 |

---

<sup>44</sup>[anarsec.guide/posts/tails/#tor](https://anarsec.guide/posts/tails/#tor)

<sup>45</sup>[privacyguides.org/en/advanced/tor-overview/](https://privacyguides.org/en/advanced/tor-overview/)

<sup>46</sup>[whonix.org/wiki/Warning](https://whonix.org/wiki/Warning)

This guide will explain how to create a website with Publii (a CMS, or Content Management System), on Tails (an operating system<sup>†</sup> that leaves no trace of your activity on your computer), and how to publish it with the help of one of several radical hosting providers<sup>1</sup>—the comrades who manage the servers on which your site will be published.

Publii is an open-source software that runs on your computer and allows building a static website. You write your content and decide how your website looks, and Publii builds the website and publishes it to the server of your choice. In technical terms, Publii is a static CMS. Because the website it builds is *static*, it can't include user-generated content such as comments or forum sections. In contrast to a *dynamic* website like one made with WordPress, a static website can only change when you update it.

Tails is an operating system that leaves no trace of your activity on your computer, and routes all your Internet activity through the Tor anonymity network<sup>†</sup>. The present guide assumes that you already know how to install and use Tails; if you don't, first read our guide Tails for Anarchists<sup>2</sup>.

Compared to using a dynamic CMS (such as the popular Wordpress), using Publii has several benefits for your hosting provider:

- Better security. Dynamic CMS software must run on your provider's servers, and it is known to regularly suffer from critical vulnerabilities that allow individuals (or intelligence agencies) to steal user data and sometimes take control of servers. Just in 2026, several radical hosting providers have been hacked because of vulnerabilities in CMS software (websites from the French network "Réseau Mutu"<sup>3</sup> in June and Noblogs<sup>4</sup> in August). In contrast, Publii runs on your computer and isn't accessible from the Internet, and the hosting provider only has to maintain a web server and a software that lets you up-

---

<sup>1</sup>[riseup.net/en/security/resources/radical-servers](https://riseup.net/en/security/resources/radical-servers)

<sup>2</sup>[anarsec.guide/posts/tails](https://anarsec.guide/posts/tails)

<sup>3</sup>[reseau.mutu.info/Piratage-de-deux-sites-du-reseau-Mutu-011](https://reseau.mutu.info/Piratage-de-deux-sites-du-reseau-Mutu-011)

<sup>4</sup>[keepitfree.ai/technical-updates/noblogs-status-update](https://keepitfree.ai/technical-updates/noblogs-status-update)

but much more securely than a standard Windows computer. See Qubes OS for Anarchists<sup>39</sup>.

See When to Use Tails vs. Qubes OS<sup>40</sup>. We do not offer "harm reduction" advice for Windows or macOS computers, as this is already widespread and gives a false sense of privacy and security.

## Encrypted Messaging

See Encrypted Messaging for Anarchists<sup>41</sup>

## Storing Electronic Devices

See Make Your Electronics Tamper-Evident<sup>42</sup>.

# Appendix: Glossary

## Operating system (OS)

The system software that runs your device before any other software. Some common examples include Windows, macOS, Linux, Android, and iOS. Linux and some versions of Android are the only open-source options on this list.

## Tor network

Tor<sup>43</sup> (short for The Onion Router) is an open and distributed network that helps defend against traffic analysis. Tor protects you by routing your communications through a network of relays run by volunteers around the world: it prevents someone monitoring your Internet con-

---

<sup>40</sup>[anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os](https://anarsec.guide/posts/qubes/#when-to-use-tails-vs-qubes-os)

<sup>41</sup>[anarsec.guide/posts/e2ee/](https://anarsec.guide/posts/e2ee/)

<sup>42</sup>[anarsec.guide/posts/tamper/](https://anarsec.guide/posts/tamper/)

<sup>43</sup>[torproject.org/](https://torproject.org/)

## Your Phone

**Operating system<sup>†</sup>:** **GrapheneOS** is the only reasonably secure choice for cell phones. See GrapheneOS for Anarchists<sup>34</sup>. If you decide to have a phone, treat it like an “encrypted landline” and leave it at home when you are out of the house. See Kill the Cop in Your Pocket<sup>35</sup>.

## Your Computer

**Operating system<sup>†</sup>:** **Tails** is unparalleled for sensitive computer use (writing and sending communiques, moderating a sketchy website, researching for actions, reading articles that may be criminalized, etc.). Tails runs from a USB drive and is designed with the anti-forensic property of leaving no trace of your activity on your computer, as well as forcing all Internet connections through the Tor network<sup>†</sup>. See Tails for Anarchists<sup>36</sup> and Tails Best Practices<sup>37</sup>.

**Operating system<sup>†</sup>:** **Qubes OS** has better security than Tails for many use cases, but has a steeper learning curve and no anti-forensic features. However, it is accessible enough for journalists and other non-technical users. Basic knowledge of using Linux is required — see Linux Essentials<sup>38</sup>. Qubes OS can even run Windows programs such as Adobe InDesign,

load your site (Publii can upload through SFTP<sup>5</sup> or Git<sup>6</sup>), which are typically simpler and more robust software with far fewer vulnerabilities.

- Smaller workload. Because the hosting provider doesn’t have to maintain a complex CMS and worry about its potential vulnerabilities, they have less work to do and are at less risk of burn-out.

Publii also has benefits for you:

- Because it requires less work from the hosting provider, it can be easier to find one. There are more radical hosting providers that offer static website hosting than ones that offer access to a server-side CMS such as Wordpress (especially since the shutdown of radical Italian provider Autistici/Inventati in September 2026, and of their Noblogs platform).
- Because you build the website on your computer, you are fully in control of your site’s data. Even if your hosting provider suddenly disappears, bringing your website back online just requires finding a new provider and updating the server configuration in Publii.

If that sounds interesting to you, let’s dive in and see how this works!

To protect your website against censorship, we highly recommend choosing a hosting provider that is able to make your website accessible through an .onion address<sup>7</sup>.

## Download Publii

Publii is a free and open-source software that can be downloaded from its official website<sup>8</sup>. However, the official version of Publii does not

<sup>34</sup>[anarsec.guide/posts/grapheneos/](https://anarsec.guide/posts/grapheneos/)

<sup>35</sup>[anarsec.guide/posts/nophones/](https://anarsec.guide/posts/nophones/)

<sup>36</sup>[anarsec.guide/posts/tails/](https://anarsec.guide/posts/tails/)

<sup>37</sup>[anarsec.guide/posts/tails-best/](https://anarsec.guide/posts/tails-best/)

<sup>38</sup>[anarsec.guide/posts/linux](https://anarsec.guide/posts/linux)

<sup>39</sup>[anarsec.guide/posts/qubes/](https://anarsec.guide/posts/qubes/)

<sup>5</sup>[en.wikipedia.org/wiki/SSH\\_File\\_Transfer\\_Protocol](https://en.wikipedia.org/wiki/SSH_File_Transfer_Protocol)

<sup>6</sup>[en.wikipedia.org/wiki/Git](https://en.wikipedia.org/wiki/Git)

<sup>7</sup>[anarsec.guide/posts/publii/#appendix-making-your-website-accessible-through-an-onion-address](https://anarsec.guide/posts/publii/#appendix-making-your-website-accessible-through-an-onion-address)

<sup>8</sup>[getpublii.com](https://getpublii.com)

work well with Tails, because it isn't designed for Tails' distinctive security features.

Therefore, we recommend that you download the modified version of Publii made by AnarSec called **Publii For Tails**. It is almost identical to the official version, but has a few small changes to make it more compatible with Tails. The most important change is that your site data is kept in a folder named Publii next to the Publii For Tails application file, instead of being kept in the **Home > Documents** folder where it would disappear when you shut down Tails. You can see a full list of changes here<sup>9</sup>.

To download Publii For Tails:

- Start Tails and unlock your Persistent Storage.
- In **Tor Browser**, download PubliiForTails-0.48.1.zip<sup>10</sup>, and save it to your **Persistent** folder.
- Once the download is finished, open the **Files** app and select **Persistent** in the left panel. Right-click on **PubliiForTails-0.48.1.zip** and select **Extract**.

And that's it! Both the Publii software and your future site data will be available in **Home > Persistent > PubliiForTails**. Proceed to the next section to learn how to launch Publii and create your site.

If you follow the recommendations in our guide Tails Best Practices<sup>11</sup> and store your data on a separate encrypted USB rather than using Persistent Storage, you can follow the instructions above; just save **PubliiForTails-0.48.1.zip** to your separate USB rather than to Persistent Storage.

<sup>9</sup>[0xacab.org/anarsec/publii-for-tails#changes-compared-to-the-original](https://0xacab.org/anarsec/publii-for-tails#changes-compared-to-the-original)

<sup>10</sup>[0xacab.org/anarsec/publii-for-tails#download](https://0xacab.org/anarsec/publii-for-tails#download)

<sup>11</sup>[anarsec.guide/posts/tails-best-practices](https://anarsec.guide/posts/tails-best-practices)

## Appendix: Recommended Configuration for Hosting Providers

*Coming November 2026.*

## Appendix: Recommendations

As anarchists, we must defend ourselves against police and intelligence agencies that conduct targeted digital surveillance<sup>29</sup> for the purposes of incrimination<sup>30</sup> and network mapping<sup>31</sup>. Our goal is to obscure the State's visibility into our lives and projects. Our recommendations are intended for all anarchists, and they are accompanied by guides to put the advice into practice.

We agree with the conclusion of an overview of targeted surveillance measures in France<sup>32</sup>: "So let's be clear about our responsibilities: if we knowingly bring a networked device equipped with a microphone and/or a camera (cell phone, baby monitor, computer, car GPS, networked watch, etc.) close to a conversation in which "private or confidential words are spoken" and must remain so, even if it's switched off, we become a potential state informer.."

You may also be interested in the Threat Library's "Digital Best Practices"<sup>33</sup>.

<sup>29</sup>[notrace.how/threat-library/techniques/targeted-digital-surveillance.html](https://notrace.how/threat-library/techniques/targeted-digital-surveillance.html)

<sup>30</sup>[notrace.how/threat-library/tactics/incrimination.html](https://notrace.how/threat-library/tactics/incrimination.html)

<sup>31</sup>[notrace.how/threat-library/techniques/network-mapping.html](https://notrace.how/threat-library/techniques/network-mapping.html)

<sup>32</sup>[actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/](https://actforfree.noblogs.org/post/2023/07/24/number-of-the-day-89502-preventive-surveillance-measures-france/)

<sup>33</sup>[notrace.how/threat-library/mitigations/digital-best-practices.html](https://notrace.how/threat-library/mitigations/digital-best-practices.html)

## Appendix: Making your Website Accessible through an .Onion Address

*Coming November 2026.*

## Appendix: Collaborating with Others on the Same Website

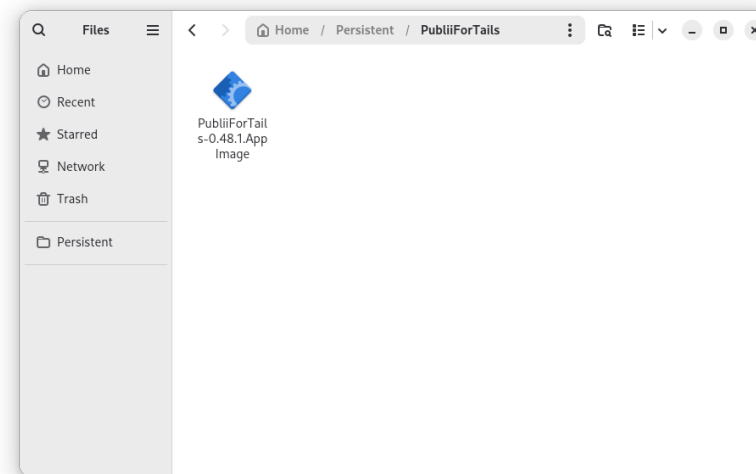
*Coming November 2026.*

## Appendix: Adding a Contact Form

*Coming November 2026.*

## Appendix: Making a Multilingual Site

*Coming November 2026.*



## Create your Site

To launch Publii, in the **Files** app, navigate to **Home > Persistent > PubliiForTails** and double-click on **PubliiForTails-0.48.1.AppImage**.

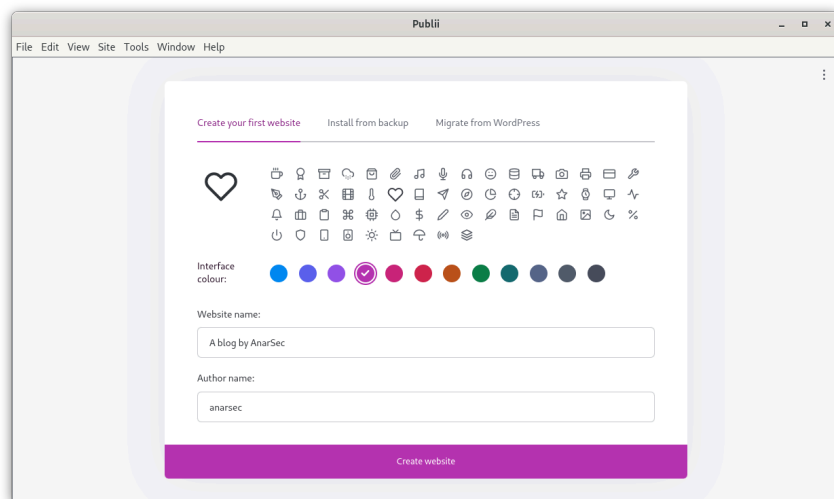
The first time you launch Publii, it will ask that you accept the terms of its open-source license. It will then prompt you to create your first website, either from scratch or by importing a Publii backup or a Wordpress backup. You can find more information on all these options in the “Creating website” section<sup>12</sup> of Publii’s official documentation.

---

<sup>28</sup>[0xacab.org/anarsec/publii-for-tails#build](https://0xacab.org/anarsec/publii-for-tails#build)

---

<sup>12</sup>[getpublii.com/docs/creating-your-website.html](https://getpublii.com/docs/creating-your-website.html)



After creating your website, you will be presented with Publii’s main interface, allowing you to create posts and pages, decide what your website will look like, and configure various settings related to your site’s content. When creating a post or page you will be asked to choose your preferred editor—for most people we recommend the WYSIWYG (“What You See Is What You Get”) editor, but feel free to experiment and choose the one you prefer. “Preview” buttons scattered throughout the interface open local versions of your site’s pages in Tor Browser, allowing you to see what your website will look like once it’s published online.

## Make a remote backup

*Coming November 2026.*

## Operational Security for Site Managers

*Coming November 2026.*

## Appendix: Trusting Publii For Tails

Publii<sup>26</sup> is developed by a small Polish software company called Tidy-Customs. Publii For Tails<sup>27</sup> is a fork (a modified version) of Publii that AnarSec maintains. Both are *open-source*, meaning that their source code is publicly available and can be audited.

There are two ways a malicious backdoor could be inserted in Publii For Tails:

- Insert the backdoor in its source code, or in the source code of one of the pieces of software it depends on. To defend against this, the only solution is to have its source code audited by a software developer or security researcher. We encourage you to do this, if you have the required skills or know someone who does. Publii has many users, so there are already some sets of eyes on the source code.
- Insert the backdoor while building the AppImage file. To defend against this, the Publii For Tails AppImage file is built by AnarSec, instead of relying on the official file. Additionally, if you are comfortable with Linux, you can build the AppImage file yourself using instructions provided by AnarSec<sup>28</sup>.

<sup>26</sup>[getpublii.com](https://getpublii.com)

<sup>27</sup>[0xacab.org/anarsec/publii-for-tails](https://0xacab.org/anarsec/publii-for-tails)

# Maintain a Backup of Your Site Data

When you use Publii For Tails, your site data—all your posts, pages, images, settings, everything that allows Publii to build your website—is kept in a folder named Publii inside the PubliiForTails folder. You are responsible for this data: if you lose it, your hosting provider won't be able to give it back to you! You should therefore maintain a backup of it, in case you lose your Tails key.

We recommend two possible ways to regularly backup your site data: backup your Tails key, or make a remote backup.

## Backup your Tails key

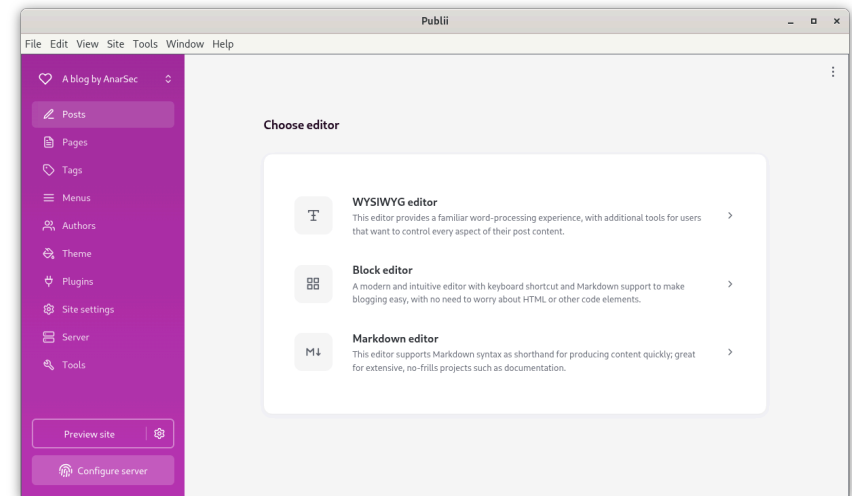
To backup your Tails key:

- Start Tails and unlock your Persistent Storage.
- Open **Tails Cloner (Apps > Tails > Tails Cloner)**
- Check **Clone the current Tails** and **Clone the current Persistent Storage**
- Insert your backup USB key and select it in the list.
- Select **Install** and wait for the process to finish.

We recommend storing your backup Tails key outside your home, so you don't lose both your main Tails key and your backup one in case of a police raid.

If you follow the recommendations in our guide Tails Best Practices<sup>25</sup> and store your data on a separate encrypted USB rather than using Persistent Storage, instead of making a backup of your Tails key, manually copy the PubliiForTails folder to a backup encrypted USB.

<sup>25</sup>[anarsec.guide/posts/tails-best-practices](https://anarsec.guide/posts/tails-best-practices)



Everything should be pretty intuitive, especially if you've managed a Wordpress site before. If you have any questions, the "Content Creation"<sup>13</sup> and "Options and Features"<sup>14</sup> sections of Publii's documentation explain how everything works in detail.

The next time you start Tails and launch Publii, it will prompt you again to create a website. Unless you want to create a new website (you can create as many as you want!) just select **Cancel** and select your site in the list.

## Publish your Site

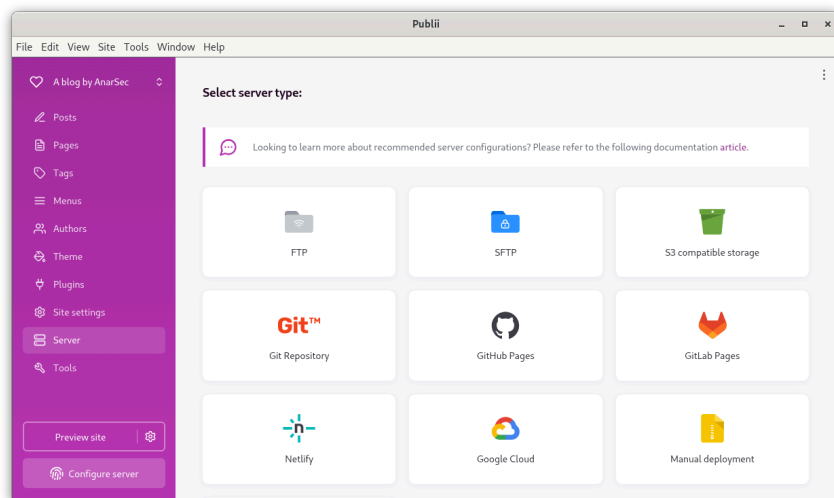
Firstly, you should find a hosting provider—people who will manage the servers on which your site will be published. If you have friends or comrades who could do this, ask them! Otherwise, you can take a look at this list of radical hosting providers<sup>15</sup>—several of them will host

<sup>13</sup>[getpublii.com/docs/frontpage-configuration.html](https://getpublii.com/docs/frontpage-configuration.html)

<sup>14</sup>[getpublii.com/docs/theme-settings.html](https://getpublii.com/docs/theme-settings.html)

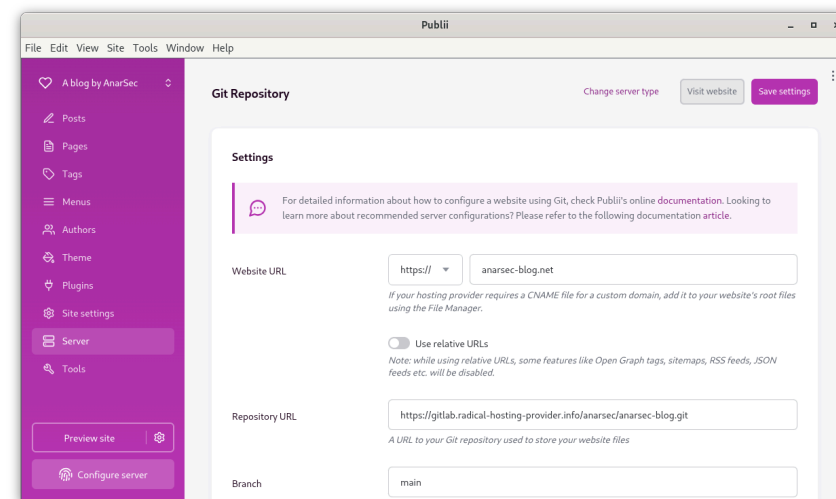
<sup>15</sup>[riseup.net/en/security/resources/radical-servers](https://riseup.net/en/security/resources/radical-servers)

your website if they feel affinity towards your project. Or you could pay a reputable commercial hosting provider that accepts the Monero<sup>16</sup> cryptocurrency, such as 1984<sup>17</sup>. On Tails, you can exchange Monero using Feather<sup>18</sup>.



Publii supports many different ways of publishing your website to your provider's servers, listed in the **Server** tab of its main interface. However, due to Tails' security features, only three of those ways work on Tails: **SFTP**, **Git Repository**, and **Manual deployment**. Most providers will ask you to publish with SFTP, some may ask you to publish with a Git repository. If your provider supports neither SFTP nor Git, you will have to resort to manual deployment. Refer to the appropriate section below depending on what your provider asks you to use.

Some hosting providers may require you to purchase a domain name to publish your website. If you need to purchase a



## Publish with Manual Deployment

In Publii's main interface, select the **Server** tab, then select **Manual deployment** and fill in the fields:

- **Website URL:** The address at which your website will be accessible. If your site will use both a normal address and an .onion address, you should set the normal address here. If your site will only use an .onion address, set the .onion address. If you don't know what address your site will use, you can check **Use relative URLs**.
- **Output type:** Format of the files output by Publii.
- **Output directory:** Folder where Publii will output your website files.

Once you've fill in all the fields, select **Save settings**, then **Sync your website** on the left, and **Prepare website files**. Wait for the process to finish, then upload the files output by Publii to your provider's servers (ask your provider how you should do this).

Whenever you want to update your website in the future, select **Sync your website** and upload the files again.

<sup>16</sup>getmonero.org

<sup>17</sup>1984.hosting

<sup>18</sup>tails.net/doc/advanced\_topics/feather/index.en.html

## Publish with Git Repository

In Publii's main interface, select the **Server** tab, then select **Git Repository** and fill in the fields:

- **Website URL:** The address at which your website will be accessible. If your site will use both a normal address and an .onion address, you should set the normal address here. If your site will only use an .onion address, set the .onion address. If you don't know what address your site will use, you can check **Use relative URLs**.
- **Repository URL:** Address of the Git repository. This can be an .onion address. (Your provider will tell you what to set.)
- **Branch:** Name of the Git branch. (Your provider will tell you what to set.)
- **Username:** Username used for the Git connection. (Your provider will tell you what to set.)
- **Password / Token:** Password or token used for the Git connection. (Your provider will tell you what to set.)
- **Commit author, Commit author email and Commit message:** Enter whatever you want in these fields, taking into account that what you set will probably be visible publicly. The email doesn't have to be a real email address.

Once you've filled in all the fields, select **Save settings**, then **Sync your website** on the left, and **Sync your website** again. Wait for the process to finish: your website is published!

Whenever you want to update your website in the future, select **Sync your website**.

domain name anonymously, we recommend doing so through domain name sellers that accept Monero, such as 1984<sup>19</sup>, OrangeWebsite<sup>20</sup>, Mynymbox<sup>21</sup>, or Njalla<sup>22</sup>, and paying in Monero. Alternatively, you can ask your provider to make your website exclusively available through an .onion address<sup>23</sup>, in which case you don't need a domain name.

## Server Settings

### Publish with SFTP

In Publii's main interface, select the **Server** tab, then select **SFTP** and fill in the fields:

- **Website URL:** The address at which your website will be accessible. If your site will use both a normal address and an .onion address, you should set the normal address here. If your site will only use an .onion address, set the .onion address. If you don't know what address your site will use, you can check **Use relative URLs**.
- **Port:** Network port used for the SFTP connection. (Your provider will tell you what to set.)
- **Server:** Address of the server used for the SFTP connection. This can be an .onion address. (Your provider will tell you what to set.)
- **Username:** Username used for the SFTP connection. (Your provider will tell you what to set.)
- **Remote path:** Server sub-folder where your site will be published. (Your provider will tell you what to set. If in doubt, just leave it blank.)

---

<sup>19</sup>1984.hosting

<sup>20</sup>orangewebsite.com

<sup>21</sup>mynymbox.io

<sup>22</sup>njalla

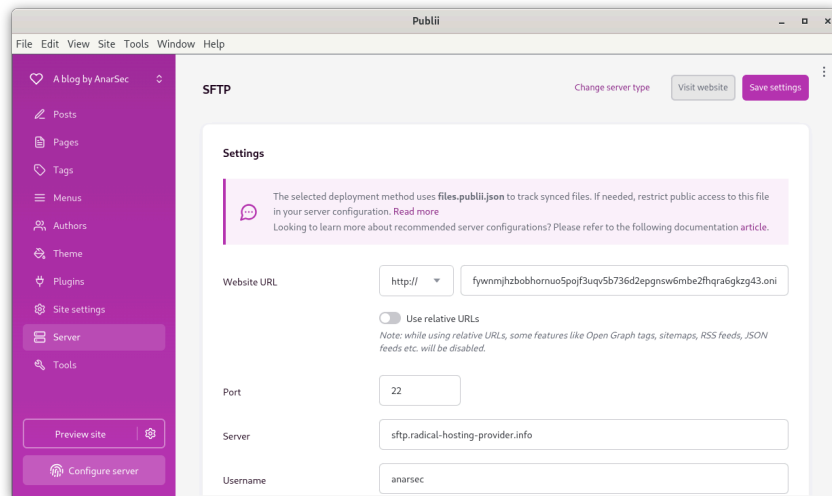
<sup>23</sup>anarsec.guide/posts/publii#appendix-making-your-website-accessible-through-an-onion-address

Configure your **Authentication method** depending on what your provider tells you to use:

- **Password:** If your provider tells you to use a password. (They will tell you what to set.)
- **Key file:** If your provider tells you to use a SSH key. Refer to the next section to learn how to do this.

Once you've filled in all the fields, select **Save settings**, then **Sync your website** on the left, and **Sync your website** again. Wait for the process to finish: your website is published!

Whenever you want to update your website in the future, select **Sync your website**.



### Optional: Create and use a SSH key

A SSH key is a credential that can be used for SFTP connections. It's actually two keys: a *private* key and a *public* key. Both are small files that will be kept in your Persistent Storage. You should never send your private key to anyone, but you will send your public key to your provider. To create a SSH key on Tails:

- Select **Apps > Tails > Persistent Storage** and check **SSH Client**.

- Select **Apps > System Tools > Console**. In the console:
  - Type `ssh-keygen` and press Enter.
  - When it asks you where to save the key, press Enter.
  - When it asks you for a passphrase, either type a passphrase and press Enter to set a passphrase, or just press Enter if you don't want to set a passphrase. Since your Persistent Storage is already encrypted, it's acceptable not to set a passphrase.
  - When it asks you for the same passphrase again, same thing: either type the same passphrase you typed before and press Enter, or just press Enter if you don't want to set a passphrase.

Congratulations, you've created a SSH key! Your key is located in your **Home** folder, in the `.ssh` sub-folder. Your private key is named `id_ed25519` and your public key is named `id_ed25519.pub`. *Tip: If you are in your Home folder and can't see the `.ssh` sub-folder, press `CTRL+H` to make it appear.*

Now:

- Send your public key, `id_ed25519.pub`, to your hosting provider, for example by email.
- Back in Publii, finish configuring the SFTP connection. Under **Your private key** select your private key, `id_ed25519`. Under **Key passphrase**, enter your key passphrase if you've set one, otherwise leave blank.

If you follow the recommendations in our guide [Tails Best Practices<sup>24</sup>](#) and store your data on a separate encrypted USB rather than using Persistent Storage:

- Skip the bullet point instructing to open **Apps > Tails > Persistent Storage**.
- After creating the SSH key, copy both the public and private key to the separate USB.

<sup>24</sup>[anarsec.guide/posts/tails-best-practices/](https://anarsec.guide/posts/tails-best-practices/)