SecureDrop Documentation

Release stable

SecureDrop Team and Contributors

Jan 16, 2026

OVERVIEW

SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources.

This documentation is intended for sources, journalists, and administrators. If you would like to contribute to SecureDrop, please see our developer documentation.

Note

This documentation is also available as a Tor Onion Service at http://dftlffjdogaragaxkc6jqxpo77s7rrngimyoq7uuq3clowhmttblcoyd.onion/en/stable/.

CHAPTER

ONE

GET STARTED

I want to learn more about how SecureDrop works.

I have information I want to share, and would like to learn how to do so safely.

I am looking to set up a SecureDrop installation.

I have a SecureDrop installation and am interested in next steps.

I am a journalist and would like information about how to best use this system.

1.1 What Is SecureDrop?

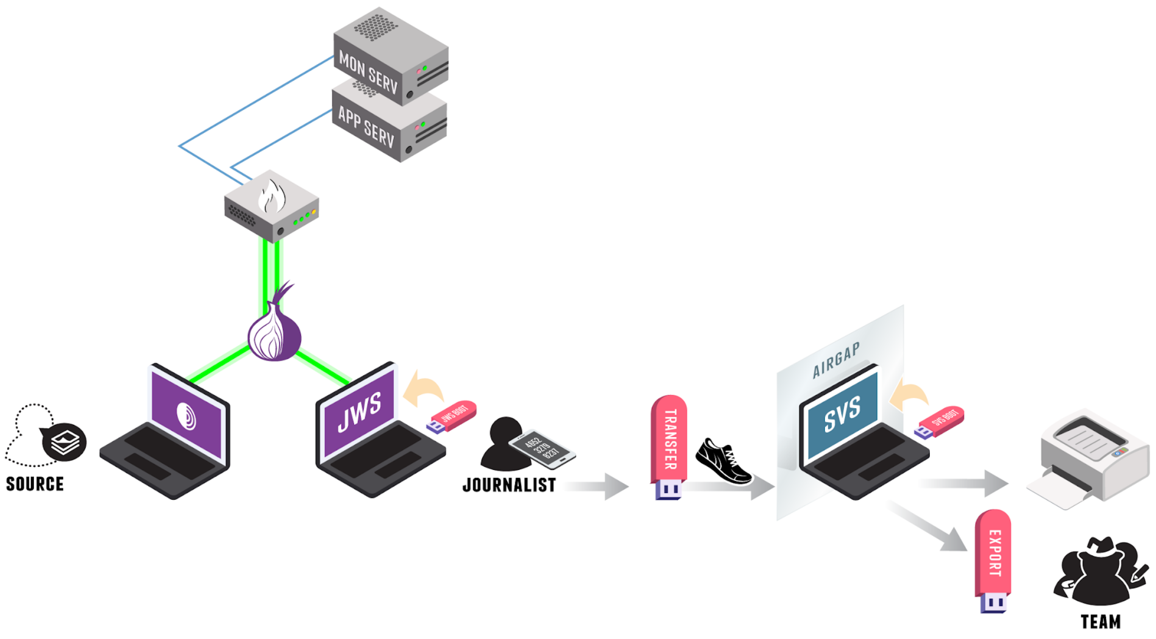
SecureDrop is an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources.

1.1.1 Purpose

In many of the recent leak prosecutions in the United States, sources have been investigated because authorities are able to retrieve both metadata and content of communications from third parties like email and phone providers in secret. SecureDrop attempts to completely eliminate third parties from the equation so that news organizations can challenge any legal orders before handing over any data.

SecureDrop also substantially limits the metadata trail that may exist from journalist-source communications in the first place. In addition, it attempts to provide a safer environment for those communications than regular corporate news networks, which may be compromised.

1.1.2 How It Works



Sources and journalists connect to SecureDrop using the Tor network (represented in the diagram above by the onion symbol). The SecureDrop software is running on premises on dedicated infrastructure (two physical servers and a firewall).

The following steps describe how a SecureDrop submission is submitted, received and reviewed:

1. A source (bottom left in the diagram) uploads a submission to the news organization using Tor Browser.
2. A journalist connects to SecureDrop using their *Journalist Workstation* (booted from a USB drive) and physically transfers files to the air-gapped Secure Viewing Station, a machine that is never connected on the Internet.
3. On the *Secure Viewing Station*, the journalist can view the document, process it (e.g., to remove metadata or potential malware), print it, or export it to a dedicated device.

See also

Check out *What makes SecureDrop Unique* to read more about SecureDrop's approach to keeping sources safe.

1.1.3 User Roles

There are three main user roles that interact with a SecureDrop instance:

Sources

A source submits documents and messages by using Tor Browser (or Tails) to access the *Source Interface*: a public onion service. Submissions are encrypted in place on the *Application Server* as they are uploaded.

Journalists

Journalists working in the newsroom use two machines to interact with SecureDrop. First, they use a *Journalist Workstation* running Tails to connect to the *Journalist Interface*, an authenticated onion service. Journalists download GPG-encrypted submissions and copy them to a *Transfer Device* (a thumb drive or DVD). Those submissions are then connected to the airgapped *Secure Viewing Station* (*SVS*) which holds the key to decrypt them. Journalists can then use the *SVS* to read, print, and otherwise prepare documents for publication. Apart from those deliberately published, decrypted documents are never accessed on an Internet-connected computer.

Note

The terms in italics are terms of art specific to SecureDrop. The *Glossary* provides more-precise definitions of these and other terms. SecureDrop is designed against a comprehensive *Threat Model*, and has a specific notion of the *roles* that are involved in its operation.

Admins

The SecureDrop servers are managed by a systems admin; for larger newsrooms, there may be a team of systems admins. The admin uses a dedicated *Admin Workstation* running Tails, connects to the *Application* and *Monitor Servers* over authenticated onion services, and manages them using Ansible.

1.1.4 Project History

The web application, which was originally called DeadDrop, was developed by Aaron Swartz in 2012 before his tragic death. The hardening guide and security environment was architected by James Dolan. Investigative journalist Kevin Poulsen originally managed the project. The New Yorker launched the first implementation and branded their version StrongBox in May 2013.

In October 2013, Freedom of the Press Foundation took over management and development of the open source project and re-named it SecureDrop. In the project's early years at FPF, development was driven by James Dolan and Garrett Robinson. Today, SecureDrop is maintained by a small full-time development team at FPF and a growing volunteer community.

1.1.5 Technology

SecureDrop does not seek to re-invent the wheel. Instead it combines several well-respected tools into an application that is easier to use for sources and enforces the use of many security best practices by news organizations.

Among the tools used in and around the SecureDrop application are: Tor, GnuPG encryption, Apache, OSSEC, grsecurity, Ubuntu Server, the Tails operating system, and an air-gap to minimize exfiltration risks.

1.1.6 Privacy

The SecureDrop application does not record your IP address, information about your browser, computer, or operating system. Furthermore, the SecureDrop pages do not embed third-party content or deliver persistent cookies to your browser. The server will only store the date and time of the newest message sent from each source. Once you send a new message, the time and date of your previous message is automatically deleted.

Journalists are also encouraged to regularly delete all information from the SecureDrop server and store anything they would like saved in offline storage to minimize risk. More detailed information can be found in our *sample privacy policy*, which we encourage news organizations using SecureDrop to adopt from when creating their own. Make sure to also follow our *best practices for creating the SecureDrop landing page* so that it logs as little information as possible as well.

1.1.7 Security

While we can't guarantee 100% security (no organization or product can), the goal of SecureDrop is to create a significantly more secure environment for sources to share information than exists through normal digital channels. Of course, there are always risks. That said, each release of SecureDrop with major architectural changes goes through a security audit by a reputable third party security firm.

1.1.8 Audits

Before major code changes are shipped, our policy is to have SecureDrop audited by a professional, third-party security firm. Five audits of SecureDrop have been completed so far:

1. The first audit of SecureDrop, conducted in the Spring of 2013, was conducted by a group of University of Washington researchers and Bruce Schneier, and can be found here.
2. After significant changes to the system, the second audit of SecureDrop was conducted by Cure53 at the end of 2013 and can be read here.
3. In the summer of 2014 iSEC Partners completed the third audit of SecureDrop. Their report can be read here and you can also read about how we resolved the issues they found.
4. The fourth audit was conducted in summer 2015, also by iSEC Partners, and can be found in full here.
5. The most recent audit was independently undertaken by Leviathan Security on behalf of Sofwerx in late 2018, and can be found in full here.

In addition to these audits, we also have a bug bounty program hosted by Bugcrowd.

1.1.9 Cost

SecureDrop is a free and open source application that costs nothing to install. However, the application does require hardware that news organizations must purchase, including two servers, several USB sticks, an air-gapped computer, and a firewall.

We have created a *recommended hardware guide;* following these recommendations wherever possible will minimize incompatibility risks. We are aiming to offer a set of recommendations that work for organizations at different scales.

It is critical that the hardware is owned by the media organization and stored on its premises in a secure space.

The total cost of the hardware we recommend is $2,200 to $2,400, though it can be done for less if you are willing to sacrifice size and speed on the servers or are able to use recycled machines sourced from within your organization.

As part of priority support agreements and on a pro-bono basis for smaller news organizations, Freedom of the Press Foundation will visit your offices, help set up SecureDrop and train journalists to use it. (For pro-bono support, we request that our travel costs are covered.)

1.1.10 Environment Overview

Server Infrastructure

At SecureDrop's heart is a pair of servers: the *Application ("App") Server*, which runs the core SecureDrop software, and the *Monitor ("Mon") Server*, which keeps track of the *Application Server* and sends out alerts if there's a problem. These two servers run on dedicated hardware connected to a dedicated firewall appliance. They are typically located physically inside the newsroom, and must be physically located on-site within your organization's premises.

- ***Application Server***:

  An Ubuntu server running two segmented Tor hidden services. The source connects to the *Source Interface*, a public-facing Tor Onion Service, to send messages and documents to the journalist. The journalist connects to the *Journalist Interface*, an authenticated Tor Onion Service, to download encrypted documents and respond to sources.

- ***Monitor Server***:

  An Ubuntu server that monitors the *Application Server* with OSSEC and sends email alerts.

The servers connect to the network via a dedicated hardware firewall.

Application Environment

The SecureDrop application environment consists of at least two computers, in addition to the servers described above:

- ***Secure Viewing Station***:

  A physically-secured and air-gapped laptop running the Tails operating system from a USB stick, that journalists use to decrypt and view submitted documents.

In addition to the *Secure Viewing Station* computers, each journalist will also need a computer to connect to SecureDrop:

- ***Journalist Workstation:***

  The computer used by the journalist to connect to the *Journalist Interface* to download encrypted documents that they will transfer to the *Secure Viewing Station*. The *Journalist Workstation* is also used to respond to sources via the *Journalist Interface*.

Depending on your organization's threat model, the *Journalist Workstation* can either be the journalist's every-day laptop or a dedicated computer. In either case, it is recommended that journalists always use the Tails operating system on their *Journalist Workstation* when connecting to the *Journalist Interface*.

SecureDrop administrators will also require a computer to connect to SecureDrop and perform administrative tasks. This computer is referred to as the *Admin Workstation*, and must be capable of running the Tails operating system. The *Admin Workstation* may also be used as a *Journalist Workstation* if necessary.

1.1.11 Operation

Planning & Preparation

Setting up SecureDrop is a multi-step process. Before getting started, you should make sure that you're prepared to operate and maintain it. You'll need a systems admin who's familiar with Linux, the GNU utilities, and the Bash shell. You'll need the *hardware* on which SecureDrop runs — this will normally cost $2000-$3000. The journalists in your organization will need to be trained in the operation of SecureDrop, and you'll need to publish and promote your new SecureDrop instance afterwards — using your existing websites, mailing lists, and social media.

It is recommended that you have all of this planned out before you get started. If you need help, contact the Freedom of the Press Foundation who will be glad to help walk you through the process and make sure that you're ready to proceed.

Technical Setup

Once you are familiar with the architecture and have all the hardware, *setting up SecureDrop* will take at least a day's work for your admin. We recommend that you set aside at least a week to *complete and test* your setup.

Provisioning & Training

Once SecureDrop is installed, journalists will need to be provided with accounts, two-factor credentials, workstations, and so on — and then *trained* to use these tools safely and reliably. You will probably also need to train additional backup admins so that you can be sure that your SecureDrop setup keeps running even when your main admin is on holiday.

Introducing staff to SecureDrop takes half a day. Training a group to use SecureDrop proficiently takes at least a day — and a single trainer can only work with so many people at once. You will probably need to run several training sessions to instruct an entire newsroom. Depending on staff availability, training and provisioning may take a week or more. If you have multiple offices, training will need to happen at each location. Again, the Freedom of the Press Foundation are happy to help you plan and train your team.

Going Public

Once you have a SecureDrop instance and your team knows how to use it, you should test it thoroughly and then tell the world. The Freedom of the Press Foundation are happy to help you check that your SecureDrop setup is up-to-code and properly grounded. After that you'll want to check out the *best practices* for your SecureDrop *Landing Page* and our guide to *promoting your SecureDrop instance*.

1.1.12 Sharing Access

With Other Journalists In Your Organization

While SecureDrop supports having multiple journalist accounts for the document interface, all accounts will access the same inbox. To avoid confusion, we recommend news organizations assign 1-3 journalists to regularly check SecureDrop and make sure that they all are in contact as to who is responsible for responding to each source.

We are considering alternative workflows for future SecureDrop releases; please visit our development roadmap for up-to-date information.

With Other Organizations

Currently you cannot use SecureDrop with multiple organizations for security reasons. One of the benefits of SecureDrop is that it completely eliminates third parties from your communication channel. The media organization owns and operates the server that both the source and journalist connect to.

Any legal request or order has to be served on the media organization operating the SecureDrop server, giving them a chance to challenge it before handing over any data. If a third party operated a SecureDrop server which multiple organizations used, a legal order could be served on the operator without the media organizations knowing.

1.2 What Makes SecureDrop Unique?

SecureDrop attempts to solve or mitigate several problems journalists and sources have faced in recent legal investigations, attacks from state actors, and other threats to the confidentiality of communications.

1.2.1 No Third Parties that Can Secretly be Subpoenaed

For decades, there were very few leak prosecutions in the United States in large part because the government would have to subpoena reporters to testify against a source to get a conviction. That proved incredibly difficult, if not impossible, when reporters regularly refused to testify and threatened to go to jail rather than betray a source.

More recently, there have been a record number of leak prosecutions largely because the government has learned they don't need reporters to testify against their sources anymore. Instead, they can just secretly subpoena third-party services like Google or AT&T or Verizon or Facebook and get a treasure trove of digital information on reporters and sources' communications. For example, the Associated Press had twenty of their phone lines subpoenaed without their knowledge in order to identify a source. The government also got a warrant for Fox News reporter James Rosen's Gmail account without him knowing. In both cases, their alleged sources were prosecuted, even though journalists never directly divulged their sources.

SecureDrop completely eliminates third parties from the equation and puts the power to challenge such cases back in the hands of reporters. The journalist and source communicate exclusively through one server that the news organization owns and sits on their property, so any legal order for information must go directly to the news organization rather than Google or AT&T. The news organization again has the power to contest the order or refuse to comply if they so wish.

1.2.2 Limits the Metadata Trail as Much as Possible

In many leak cases, the metadata of a journalist's communications—where you're located, who you're talking to, when you're talking to them, and how often—can lead to trouble just as much as the actual content of your conversations.

Even if a government serves a court order directly to a news organization to compel the disclosure of information, SecureDrop logs much less information than email providers or phone companies do.

The source can only log into SecureDrop through Tor Browser, which masks the source's IP address to begin with, so there is no indication who the source is (unless they disclose it) and where they are sending information from. The Tor IP address, the computer, and the browser type that the source is using is not logged either.

For each source, only the time and date of each submission is logged on the server. When a source sends a new message, the time and date of the last message is overwritten. This means that there won't be a trail of metadata showing exactly when the source and journalist were talking.

In addition, sources cannot create a custom username that could reveal information about them. Instead, SecureDrop automatically generates two random codenames, one to show to the source and another to the journalists using the system.

1.2.3 Encrypted and Air-Gapped

Communications through SecureDrop are both encrypted in transit, so messages cannot be easily intercepted and read while they are traversing the Internet and are also encrypted on the server so if any attacker manages to break into the server, they would not be able to read past messages.

In addition, the decryption key for SecureDrop submissions sits on an air-gapped computer (not connected to the Internet). This air-gapped computer is the only place SecureDrop submissions are decrypted and read so that they are much harder for an attacker to access.

1.2.4 Protects Against Hackers

A 2014 study showed that 21 of the top 25 news organization had, at one time or another, been targeted by state sponsored hackers.

Because of this threat, SecureDrop completely segments its traffic from a news organization's normal network. Submissions are accessed and downloaded using the Tails operating system, which boots off of a USB, does not touch your computer's hard drive, and routes all its Internet traffic through Tor.

Submissions are decrypted on an air-gapped computer also using Tails. This mitigates against the risk that an attacker could send malware through SecureDrop in an attempt to infect the news organization's normal network as well.

The SecureDrop servers also undergo significant system hardening in order to make it as difficult as possible for hackers to break in. By doing so, SecureDrop protects sources against networks that are already compromised, as well as a news organization's normal network from attacks that could potentially come through SecureDrop.

1.2.5 Free and Open Source Software

100% of SecureDrop's code is free and open source. Not only does this mean anyone can install SecureDrop themselves, but the code is available online for security experts to test for vulnerabilities.

SecureDrop has gone through four audits by third-party penetration testing firms and will continue to go through audits when major changes are made to the code base in the future. We always publish these audits publicly so everyone can be assured that SecureDrop is as safe to use as possible.

1.3 Glossary

A number of terms used in this guide, and in the *SecureDrop workflow diagram <what_is_securedrop>*, are specific to SecureDrop. The list below attempts to enumerate and define these terms.

1.3.1 Admin Workstation

The *Admin Workstation* is a machine that the system admin can use to connect to the *Application Server* and the *Monitor Server* using Tor and SSH. The admin will also need to have an Android or iOS device with the FreeOTP app installed.

1.3.2 Application Server

The *Application Server* runs the SecureDrop application. This server hosts both the website that sources access (the *Source Interface*) and the website that journalists access (the *Journalist Interface*). Both are published through an *onion service* because sources, journalists, and admins may only connect to this server using Tor.

1.3.3 Export Device

The *Export Device* is the physical media (e.g., designated USB drive) used to transfer decrypted documents from the *Secure Viewing Station* to a journalist's everyday workstation, or to another computer for additional processing.

Please see the detailed security recommendations for the choice, configuration and use of your *Export Device* in the *journalist guide* and in the *setup guide*.

1.3.4 Journalist

The *Journalist* uses SecureDrop to communicate with and download documents submitted by the *Source*. Journalists do this by using the *Journalist Workstation* to connect to the *Journalist Interface* through Tor.

The *Journalist* also uses a *Transfer Device* to move documents to the *Secure Viewing Station*. If a *Journalist* chooses to release any of these documents, they can be prepared for publication on the *Secure Viewing Station* before being transferred to an Internet-connected computer.

Instructions for using SecureDrop as a *Journalist* are available in our *Journalist Guide*.

1.3.5 Journalist Alert Public Key

The *Journalist Alert Public Key* is used for encrypting the *daily alert* that notifies journalists via encrypted email about whether or not there has been submission activity in the past 24 hours. The journalist uses an associated private key to decrypt the alerts.

1.3.6 Journalist Interface

The *Journalist Interface* is the website that journalists access to download new documents and communicate with sources. This site is hosted on the *Application Server* and can only be accessed over Tor. In previous releases, this was called the *Document Interface*, but we have renamed it to avoid ambiguity.

Instructions for using the *Journalist Interface* are available in our *Journalist Guide*.

1.3.7 Journalist Workstation

The *Journalist Workstation* is a machine that is online and used together with the Tails operating system on the *online* USB stick. This machine will be used to connect to the *Journalist Interface*, download documents, and move them to the *Secure Viewing Station* using the *Transfer Device*.

Instructions for using the *Journalist Workstation* are available in our *Journalist Guide*.

1.3.8 Landing Page

The *Landing Page* is the public-facing webpage for a SecureDrop instance. This page is hosted as a standard (i.e. non-Tor) webpage on the news organization's site. It provides first instructions for potential sources and includes the instance's *Source Interface* address.

1.3.9 Monitor Server

The *Monitor Server* keeps track of the *Application Server* and sends out an email alert if something seems wrong. Only system admins connect to this server, and they may only do so using Tor.

1.3.10 Onion Service

Tor onion services provide anonymous inbound connections to websites and other servers exclusively over the Tor network. For example, SecureDrop uses onion services for the *Journalist Interface* and *Source Interface* websites, as well as for administrative access to the servers in SSH-over-Tor mode.

Onion services can be accessed by clicking a link or pasting the onion service address into Tor Browser. For example, `sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion` is the onion service address for the SecureDrop website.

Read more about onion services in Tor's glossary.

Onion Service versions

Distinguishing between different generations of onion services is easy: v3 addresses are longer (56 characters) than v2 addresses (16 characters).

The third generation of onion services (v3) provides stronger cryptographic algorithms than v2 onion services, and includes redesigned protocols that guard against service information leaks on the Tor network.

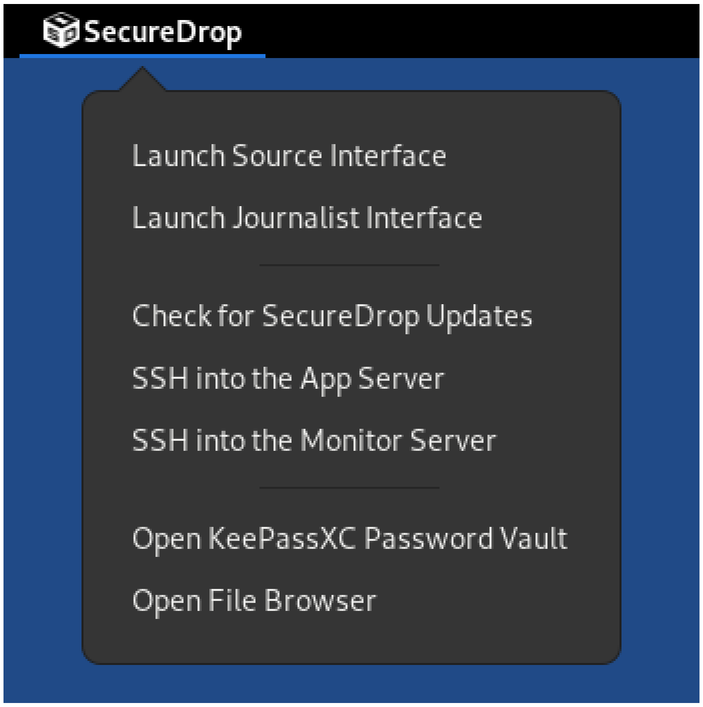
Only v3 onion services are supported by SecureDrop.

1.3.11 OSSEC Alert Public Key

The *OSSEC Alert Public Key* is the GPG key that OSSEC will encrypt alerts to. The associated private key is used by the admin to access encrypted OSSEC alerts from the *Monitor Server*. Instructions for setting up OSSEC alerts can be found in the *OSSEC Guide*.

1.3.12 SecureDrop Menu

The *SecureDrop Menu* is a dedicated menu available in both the *Admin Workstation* and the *Journalist Workstation*. It is located on the top bar, and is available once a Tor connection has been established.


SecureDrop
Launch Source Interface
Launch Journalist Interface
Check for SecureDrop Updates
SSH into the App Server
SSH into the Monitor Server
Open KeePassXC Password Vault
Open File Browser

It provides access to the *Source Interface* and *Journalist Interface*, allows you to check for updates to SecureDrop, and gives you quick access to a file browser and KeePassXC vault.

On an *Admin Workstation*, it also allows quick SSH access to connect to the *Application Server* and *Monitor Server*.

1.3.13 Secure Viewing Station

The *Secure Viewing Station* (or *SVS* for short) is the computer you use to decrypt and view documents and messages submitted to your SecureDrop. This computer is permanently kept offline. It is “air-gapped”, meaning that there is a gap between it and any computer connected to the Internet.

You will boot the *SVS* from a designated USB stick running the Tails operating system. Once you have created it, you should never attach this USB stick to any Internet-connected device.

During the installation, the *SVS* is used to generate the *Submission Key* for encrypting and decrypting documents and messages submitted to SecureDrop. In addition, we recommend importing the public keys of individual journalists to the *SVS*, so you can securely encrypt files to their keys before exporting them.

Since this machine will never touch the Internet or run an operating system other than Tails on a USB, it does not need a hard drive or network device. We recommend physically removing the drive and any networking cards (wireless, Bluetooth, etc.) from this machine.

1.3.14 Source

The *Source* is the person who submits documents to SecureDrop and may use SecureDrop to communicate with a *Journalist*. A *Source* will always access SecureDrop through the *Source Interface* and must do so using Tor.

Instructions for using SecureDrop as a *Source* are available in our *Source Guide*.

1.3.15 Source Interface

The *Source Interface* is the website that sources will access to submit documents and communicate with journalists. This site is hosted on the *Application Server* and can only be accessed through Tor.

Instructions for using the *Source Interface* are available in our *Source Guide*.

1.3.16 Submission Key

The *Submission Key* is the GPG keypair used to encrypt and decrypt documents and messages sent to your SecureDrop. Because the public key and private key must be treated very differently, we sometimes refer to them explicitly as the *Submission Public Key* and the *Submission Private Key*.

The *Submission Public Key* is uploaded to your SecureDrop servers as part of the installation process. Once your SecureDrop is online, anyone will be able to download it.

The *Submission Private Key* should never be accessible to a computer with Internet connectivity. Instead, it should remain on the *Secure Viewing Station* and on offline backup storage.

1.3.17 Transfer Device

The *Transfer Device* is the physical media (e.g., designated USB drive) used to transfer encrypted documents from the *Journalist Workstation* to the *Secure Viewing Station*, where they can be decrypted.

Please see the detailed security recommendations for the choice, configuration and use of your *Transfer Device* in the *journalist guide* and in the *setup guide*.

1.3.18 Two-Factor Authentication

There are several places in the SecureDrop architecture where two-factor authentication is used to protect access to sensitive information or systems. These instances use the standard TOTP and/or HOTP algorithms, and so a variety of devices can be used to generate 6-digit two-factor authentication codes. We recommend using one of:

- FreeOTP for Android or for iOS installed
- A YubiKey

Tip

We recommend using FreeOTP (available for Android and for iOS) to generate two-factor codes because it is Free Software. However, if it does not work for you for any reason, alternatives exist:

- Google Authenticator for Android and iOS (proprietary)
- authenticator for the desktop (Free Software)

1.4 Threat Model

This document outlines the threat model for SecureDrop 0.3 and is inspired by a document Adam Langley wrote for Pond. The threat model is defined in terms of what each possible adversary can achieve. This document is always a work in progress. If you have questions or comments, please open an issue on GitHub or send an email to securedrop@freedom.press.

The threat model for the SecureDrop Workstation based on Qubes OS is summarized in a separate document.

1.4.1 Actors

The SecureDrop ecosystem comprises a host of actors, organized by the following high-level categories: *Users*, *Adversaries*, and *Systems*.

Users

The following table of the users who interact with the SecureDrop web application. Note that the airgapped SVS with the GPG *Submission Key* is required to decrypt submissions or messages.

User Type	Trust Level
Source	• Submit a document or message
Recurring source	• Submit another document or message • Read replies
Journalist	• Download *all* GPG-encrypted documents from *all* sources • Download *all* GPG-encrypted messages from *all* sources • Reply to *all* sources
Admin	• Download *all* GPG-encrypted documents from *all* sources • Download *all* GPG-encrypted messages from *all* sources • Reply to *all* sources • Change the SecureDrop instance logo • SSH and root privileges on *app* and *mon* servers

Adversaries

We consider the following classes of attackers for the design and assessment of SecureDrop:

Adversary	Capabilities
Nation State / Law Enforcement / Global Adversary	• Large scale, full-packet network capture • Active network attacks • Advanced attacks on infrastructure • Hardware and software implants for persistence • Cryptanalysis • Exploitation of unknown vulnerabilities
Large Corporation	• Limited network capture • Some targeted attacks on infrastructure • Use of known vulnerabilities • Mostly limited to software-based attacks
Internet Service Provider	• Full network capture • Mostly limited to network-based attacks
User Error	• Source, Journalist, Administrator or Developer error
Dedicated Individual	• Use of known vulnerabilities • Mostly limited to software-based attacks

Systems

For more information about the various systems involved in a SecureDrop deployment, please visit the *hardware section*.

System	Description
Hardware Firewall	• Dedicated Hardware Firewall • pfSense-based • 3 Interfaces: *app*, *mon* and *admin*
Application Server	• SecureDrop Source Interface • SecureDrop Journalist Interface • SSH Server • Ossec Client
Monitor Server	• Ossec Server • SSH Server
Journalist/Admin Workstation	• Internet-connected laptop • Tails USB with persistence volume
Secure Viewing Station (SVS)	• Airgapped and stripped-down laptop • Tails USB with persistence volume

1.4.2 Assumptions

The following assumptions are accepted in the threat model of every SecureDrop project:

Assumptions About the Source

- The source acts reasonably and in good faith, e.g. if the source were to give their credentials or private key material to the attacker that would be unreasonable.
- The source would like to remain anonymous, even against a forensic attacker.
- The source obtains an authentic copy of Tails and Tor Browser.
- The source follows our *guidelines* for using SecureDrop.
- The source is accessing an authentic SecureDrop site.

Assumptions About the Admin and the Journalist

- The admin and the journalist act reasonably and in good faith, e.g. if either of them were to give their credentials or private key material to the attacker that would be unreasonable.
- The admin and the journalist obtain authentic copies of Tails.
- The journalist follows our *guidelines* for using SecureDrop and working with submitted documents.

Assumptions About the Person Installing SecureDrop

- This person (usually the admin) acts reasonably and in good faith, e.g. if they were to give the attacker system-level access that would be unreasonable.
- The person obtains an authentic copy of SecureDrop and its dependencies.
- The person follows our guidelines for *deploying the system*, setting up the *landing page* for the organization, and for *installing SecureDrop*.

Assumptions About the Source's Computer

- The computer correctly executes Tails or Tor Browser.
- The computer is not compromised by malware.

Assumptions About the *Admin Workstation* and the *Journalist Workstation*

- The computer correctly executes Tails.
- The computer and the Tails device are not compromised by malware.
- The two-factor authentication device used with the workstation are not compromised by malware.

Assumptions About the *Secure Viewing Station*

- The computer is airgapped.
- The computer correctly executes Tails.
- The computer and the Tails device are not compromised by malware.

Assumptions About the SecureDrop Hardware

- The servers correctly execute Ubuntu, SecureDrop and its dependencies.
- The servers, network firewall, and physical media are not compromised by malware.

Assumptions About the Organization Hosting SecureDrop

- The organization wants to preserve the anonymity of its sources.
- The organization acts in the interest of allowing sources to submit documents, regardless of the contents of these documents.
- The users of the system, and those with physical access to the servers, can be trusted to uphold the previous assumptions unless the entire organization has been compromised.
- The organization is prepared to push back on any and all requests to compromise the integrity of the system and its users, including requests to deanonymize sources, block document submissions, or hand over encrypted or decrypted submissions.

Assumptions About the World

- The security assumptions of RSA (4096-bit GPG and SSH keys) are valid.
- The security assumptions of scrypt with randomly-generated salts are valid.
- The security/anonymity assumptions of Tor and the onion service protocol are valid.
- The security assumptions of the Tails operating system are valid.
- The security assumptions of SecureDrop dependencies, specifically Ubuntu, the Linux kernel, application packages, application dependencies are valid.

Other Assumptions or Factors

- The level of press freedom may vary in both geography and time.
- The number of daily Tor users in a country can greatly vary.

1.4.3 Assets

Asset Type	Asset
Assets relating to SecureDrop users	• Login details • Encryption key(s) • SSH details
Assets relating to the publicly accessed system	• Access to documents via server • Access to documents via Journalist Interface • Access to admin privileges via Journalist Interface • Access to user alerts, support tickets
Assets relating to the underlying system	• SecureDrop code manipulation • Dependency code manipulation

1.4.4 Implications of SecureDrop Area Compromise

What a Compromise of the *Application Server* Can Surrender

- The server sees the plaintext codename, used as the login identifier, of every source.
- The server sees all HTTP requests made by the source, the admin, and the journalist.
- The server sees the plaintext submissions of every source.
- The server sees the plaintext communication between journalists and their sources.
- The server stores the onion service private key for the source interface.
- The server stores the onion service private key and authentication token for the Journalist interface.
- The server stores and (optional) TLS private key and certificate (if HTTPS is enabled on the source interface)
- The server stores hashes of codenames, created with scrypt and randomly-generated salts.
- The server stores journalist password hashes, created with script and randomly-generated salts, as well as TOTP seeds.
- The server stores only encrypted submissions and communication on disk.
- The server stores a GPG key for each source, with the source's codename as the passphrase.
- The server may store plaintext submissions in memory for at most 24 hours.
- The server stores sanitized Tor logs, created using the SafeLogging option, for the *Source Interface*, the *Journalist Interface*, and SSH.
- The server stores both access and error logs for the Journalist Interface.
- The server stores connection history and audit logs for the admin.
- The server can connect to the *Monitor Server* using an SSH key and a passphrase.

What a Compromise of the *Monitor Server* Can Surrender

- The server stores the plaintext alerts on disk, data may also reside in RAM.
- The server stores the *OSSEC Alert Public Key* the OSSEC alerts are encrypted to.
- The server stores plaintext credentials for the SMTP relay used to send OSSEC alerts.
- The server stores the email address the encrypted OSSEC alerts are sent to.
- The server stores sanitized Tor logs, created using the SafeLogging option, for SSH.

- The server stores connection history and audit logs for the admin.
- The server stores OSSEC and Procmail logs on disk.
- The server can connect to the *Application Server* using an SSH key and a passphrase.

What a Compromise of the Workstations Can Surrender

- The *Admin Workstation* requires Tails with a persistent volume, which stores information such as GPG and SSH keys, as well as a *database with passphrases* for the *Application Server*, the *Monitor Server*, and the GPG key the *Monitor Server* will encrypt OSSEC alerts to.
- The *Journalist Workstation* requires Tails with a persistent volume, which stores information such as the onion service value required to connect to the *Journalist Interface*, as well as a *database with passphrases* for the *Journalist Interface*.
- The *Secure Viewing Station* requires Tails with a persistent volume, which stores information such as the SecureDrop application's GPG key, as well as a *database with the passphrase* for that key.

What a Compromise of the Source's Property Can Surrender

- Use of Tor Browser will leave traces that can be discovered through a forensic analysis of the source's property following either a compromise or physical seizure. Unless the compromise or seizure happens while the source is submitting documents to SecureDrop, the traces will not include information about sites visited or actions performed in the browser.
- Use of Tails with a persistent volume will leave traces on the device the operating system was installed on. Unless the compromise or seizure happens while the source is submitting documents to SecureDrop, or using the persistent volume, the traces will not include information about sites visited or actions performed in the browser or on the system.
- SecureDrop 0.3 encourages sources to protect their codenames by memorizing them. If a source cannot memorize the codename right away, we recommend writing it down and keeping it in a safe place at first, and gradually working to memorize it over time. Once the source has memorized it, they should destroy the written copy. If the source does write down the codename, a compromise or physical seizure of the source's property may result in the attacker obtaining the source's codename.
- An attacker with access to the **source's codename** can:
  - Show that the source has visited the SecureDrop site, but not necessarily submitted anything.
  - Upload new documents or submit messages.
  - Communicate with the journalist as that source.
  - See any replies from journalists that the source has not yet deleted.

What a Physical Seizure of the Source's Property Can Surrender

- Document use of Tor or Tails, but not necessarily research into SecureDrop
- Prevent the source from submitting documents by taking the device the documents are stored on.
- If the property is seized while powered on, the attacker can also analyze any plaintext information that resides in RAM.
- Tamper with the hardware.
- A physical seizure of, and access to, the source's codename will allow the attacker to access the Source Interface as that source.
- A physical seizure of the admin's property will allow the attacker to:

  - Prevent the admin from working on SecureDrop for some period of time.
  - Access any stored, decrypted documents taken off the Secure Viewing Station.
  - If the property is seized while powered on, the attacker can also analyze any plaintext information that resides in RAM.
- A physical seizure of, and access to, the admin's Tails persistent volume, password database, and two-factor authentication device will allow the attacker to access both servers and the *Journalist Interface*.

What Compromise of the Admin's Property Can Surrender

- To access the *Journalist Interface*, the *Application Server*, or the *Monitor Server*, the attacker needs to obtain the admin's login credentials and the admin's two-factor authentication device. Unless the attacker has physical access to the servers, the attacker will also need to obtain the onion service values for the Interface and the servers. This information is stored in a password-protected database in a persistent volume on the admin's Tails device. The volume is protected by a passphrase. If the admin's two-factor authentication device is a mobile phone, this will also be protected by a passphrase.
- An attacker with access to the **admin's computer** can:
  - Access any stored, decrypted documents taken off the Secure Viewing Station.
- An attacker with access to the **persistent volume** on the admin's Tails device can:
  - Add, modify, and delete files on the volume.
  - Access the onion service values used by the Interfaces and the servers.
  - Access SSH keys and passphrases for the *Application Server* and the *Monitor Server*.
  - Access the GPG key and passphrase for the encrypted OSSEC email alerts.
  - Access the credentials for the account the encrypt alerts are sent to.
  - Access the admin's personal GPG public key, if stored there.
- An attacker with admin access to the *Journalist Interface* can:
  - Add, modify, and delete journalist users.
  - Change the codenames associated with sources within the Interface.
  - Download, but not decrypt, submissions.
  - Communicate with sources.
  - Delete one or more submissions.
  - Delete one or more sources, which destroys all communication with that source and prevents the source from ever logging back in with that codename.
- An attacker with admin access to the *Application Server* can:
  - Add, modify, and delete software, configurations, and other files.
  - See all HTTP requests made by the source, the admin, and the journalist.
  - See the plaintext codename of a source as they are logging in.
  - See the plaintext communication between a source and a journalist as it happens.
  - See the stored list of hashed codenames.
  - Access the GPG public key used to encrypt communications between a journalist and a source.
  - Download stored, encrypted submissions and replies from the journalists.

  - Decrypt replies from the journalists if the source's codename, and thus the passphrase, is known.
  - Analyze any plaintext information that resides in RAM, which may include plaintext of submissions made within the past 24 hours.
  - Review logs stored on the system.
  - Access the *Monitor Server*.
- An attacker with admin access to the *Monitor Server* can:
  - Add, modify, and delete software, configurations, and other files.
  - Change the SMTP relay, email address, and GPG key used for OSSEC alerts.
  - Analyze any plaintext information that resides in RAM.
  - Review logs stored on the system.
  - Trigger arbitrary commands to be executed by the OSSEC agent user, which, assuming the attacker is able to escalate privileges, may affect the *Application Server*.

What a Physical Seizure of the Admin's Property Can Achieve

- Tamper with the hardware.
- Prevent the admin from working on SecureDrop for some period of time.
- Access any stored, decrypted documents taken off the Secure Viewing Station.
- If the property is seized while powered on, the attacker can also analyze any plaintext information that resides in RAM.
- A physical seizure of, and access to, the admin's Tails persistent volume, password database, and two-factor authentication device will allow the attacker to access both servers and the *Journalist Interface*.

What a Compromise of the Journalist's Property Can Achieve

- To access the *Journalist Interface*, the attacker needs to obtain the journalist's login credentials and the journalist's two-factor authentication device or seed. Unless the attacker has physical access to the server, the attacker will also need to obtain the onion service value for the Interface. This information is stored in a password-protected database in a persistent volume on the journalist's Tails device. The volume is protected by a passphrase. If the journalist's two-factor authentication device is a mobile phone, this will also be protected by a passphrase.
- An attacker with access to the **journalist's computer** can:
  - Access any stored, decrypted documents taken off the Secure Viewing Station.
- An attacker with access to the **persistent volume** on the journalist's Tails device can:
  - Add, modify, and delete files on the volume.
  - Access the onion service values used by the *Journalist Interface*.
  - Access SSH keys and passphrases for the *Application Server* and the *Monitor Server*.
- An attacker with journalist access to the *Journalist Interface* can:
  - Change the codenames associated with sources within the interface.
  - Download, but not decrypt, submissions.
  - Delete one or more submissions.
  - Communicate with sources.
  - If the journalist has admin privileges on SecureDrop, they can create new journalist accounts.

What a Physical Seizure of the Journalist's Property Can Achieve

- Tamper with the hardware.
- Prevent the journalist from working on SecureDrop for some period of time.
- Access any stored, decrypted documents taken off the Secure Viewing Station.
- If the property is seized while powered on, the attacker can also analyze any plaintext information that resides in RAM.
- A physical seizure of, and access to, the journalist's Tails persistent volume, password database, and two-factor authentication device will allow the attacker to access the *Journalist Interface*.

What a Compromise of the *Application Server* Can Achieve

- If the *Application Server* is compromised, the system user the attacker has control over defines what kind of information the attacker will be able to view and what kind of actions the attacker can perform.
- An attacker with access to the **debian-tor** user can:
  - View, modify, and delete all files owned by this user. This includes sanitized Tor logs, created using the SafeLogging option, for SSH, the *Source Interface* and the *Journalist Interface*.
  - View, modify, and delete the Tor configuration file, root is required to reload the config.
- An attacker with access to the **ossec** user can:
  - Add, view, modify, and delete the log files, and in doing so send inaccurate information to the *Monitor Server* and the admin.
- An attacker with access to the **www-data** user can:
  - View, modify, and delete all files owned by this user. This includes all files in use by the SecureDrop application, such as text, code, the database containing encrypted submissions and communications. The attacker needs root access to reload configuration files.
  - View, modify, and delete both access and error logs for the *Journalist Interface*.
  - View any HTTP requests made by the source, the admin, and the journalist in that moment. This includes seeing plaintext codenames, submissions, and communications.
  - Add and delete communications between a journalist and a source by writing to the database.
- An attacker with access to the **root** user can:
  - Do anything the **www-data** user can do in terms of the SecureDrop application, this user is in full control of the server and can view, modify, and delete anything at will. This user is not able to decrypt submissions or communications, unless the attacker has access to the encryption key required to do so.

What a Physical Seizure of the *Application Server* Can Achieve

- If the *Application Server* is seized, the attacker will be able to view any and all unencrypted files on the server. An attacker will be able to modify any and all files on the server. This includes all files in use by the SecureDrop Application. If the server is seized while it is powered on, the attacker can also analyze any plaintext information that resides in RAM. The attacker can also tamper with the hardware.

What a Compromise of the *Monitor Server* Can Achieve

- If the *Monitor Server* is compromised, the system user the attacker has control over defines what kind of information the attacker will be able to view and what kind of actions the attacker can perform.
- An attacker with access to the **debian-tor** user can:

  - View, modify, and delete all files owned by this user. This includes sanitized Tor logs, created using the SafeLogging option, for SSH.
  - View, modify, and delete the Tor configuration file, root is required to reload the config.
- An attacker with access to the **ossec** user can:
  - View all ossec logs and alerts on disk.
  - Modify the ossec configuration.
  - Send (or suppress) emails to administrators and journalists.
- An attacker with access to the **root** user can:
  - Do anything the **ossec** user can do in terms of the SecureDrop application, this user is in full control of the server and can view, modify, and delete anything at will. This user is not able to decrypt encrypted email alerts, unless the attacker has access to the encryption key required to do so.

What a Physical Seizure of the *Monitor Server* Can Achieve

- If the *Monitor Server* is seized, the attacker will be able to view any and all unencrypted files on the server. This includes all files in use by OSSEC. If the server is seized while it is powered on, the attacker can also analyze any plaintext information that resides in RAM. The attacker can also tamper with the hardware.
- If the *Monitor Server* is no longer online or tampered with, this will have an effect on the quantity and accuracy of notifications sent to admins or journalists.

What a Compromise of the *Secure Viewing Station* Can Achieve

- The *Secure Viewing Station* is only useful to an attacker while powered on and with the Tails persistent volume mounted. The attacker may learn more if the *Transfer Device* or the *Export Device* are in use at the time of compromise or seizure. A physical seizure of this machine, its Tails device, the *Transfer Device* or the *Export Device* will also achieve nothing, assuming that the Tails and VeraCrypt implementations of full-disk encryption work as expected.
- A compromise of the *Secure Viewing Station* allows the attacker to:
  - Run commands as the **amnesia** user.
  - View, modify, and delete files owned by the **amnesia** user. This includes the *Submission Private Key* used to encrypt and decrypt submitted documents.
  - View, modify, and delete submissions in encrypted form
  - View, modify, and delete decrypted submissions, if they are stored in decrypted form on the *Secure Viewing Station*, or if the *Export Device* is in use.
  - Export the *Submission Private Key* key (unless there is a passphrase set).

What a Physical Seizure of the *Secure Viewing Station* Can Achieve

- The *Secure Viewing Station* is only useful to an attacker while powered on and with the Tails persistent volume mounted. The attacker may learn more if the *Transfer Device* or the *Export Device* are in use at the time of compromise or seizure. A physical seizure of this machine, its Tails device, the *Transfer Device* or the *Export Device* will also achieve nothing, assuming that the Tails and VeraCrypt implementations of full-disk encryption work as expected.
- A physical seizure of the *Secure Viewing Station*, while on and with the persistent volume decrypted and mounted, allows the attacker to:
  - Tamper with the hardware.

  - Run commands as the **amnesia** user.
  - View, modify, and delete the *Submission Private Key* used to encrypt and decrypt submitted documents.
  - View, modify, and delete decrypted submissions, if they are stored in decrypted form on the *Secure Viewing Station*, or if the *Export Device* is in use.

What a Local Network Attacker Can Achieve Against the Source, Admin, or Journalist:

- A local network can observe when they are using Tor.
- A local network can block Tor and prevent them from accessing SecureDrop.
- A local network may be able to deduce use of SecureDrop by looking at request sizes, plaintext uploads and encrypted downloads, although research suggests this is very difficult.

What a Global Adversary Can Achieve Against the Source, Admin, or Journalist:

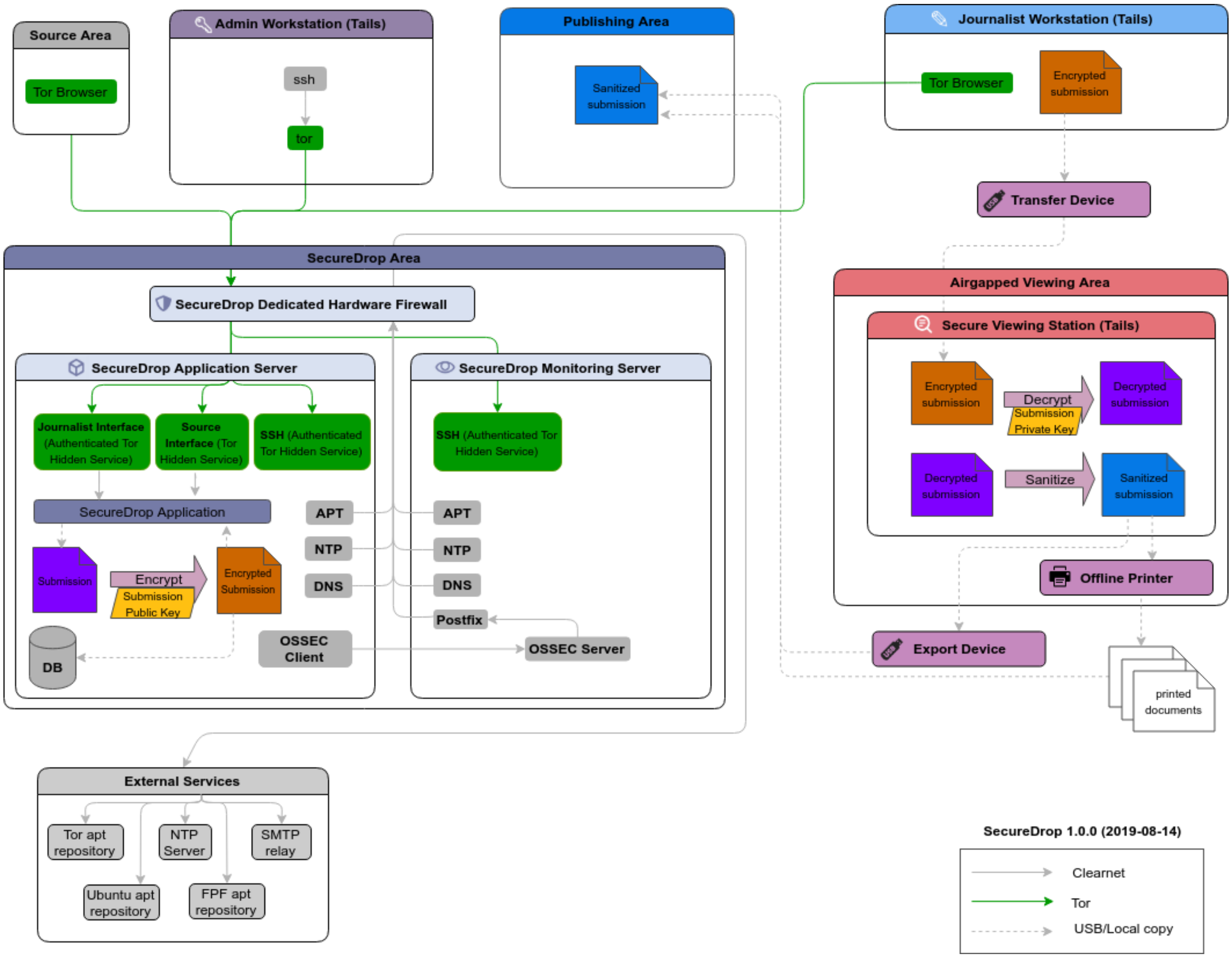
- A global adversary capable of observing all Internet traffic may have more luck than the local network attacker in deducing use of SecureDrop by looking at request sizes, plaintext uploads and encrypted downloads.
- A global adversary may be able to link a source to a specific SecureDrop server.
- A global adversary may be able to link a source to a specific journalist.
- A global adversary may be able to correlate data points during a leak investigation, including looking at who has read up on SecureDrop and who has used Tor.
- A global adversary may be able to forge an SSL certificate and use it to spoof an organization's HTTPS *Landing Page*, thereby tricking the source into visiting a fake SecureDrop site.

What a Random Person on the Internet Can Achieve

- A random person can attempt to DoS the SecureDrop server and overwhelm the journalists by generating a high number of codenames and uploading many large documents.
- A random person can submit empty, forged, or inaccurate documents.
- A random person can submit malicious documents, e.g. malware that will attempt to compromise the *Secure Viewing Station*.
- A random person can attempt to get sensitive information from a SecureDrop user's browser session, such as the source's codename.
- A random person can attempt to compromise the SecureDrop server by attacking the exposed attack surface, including the kernel network stack, Tor, Apache, the SecureDrop web interfaces, Python, OpenSSH, and the TLS implementation.

1.5 Data Flow Diagram

The following diagram captures all data flows to and from a SecureDrop deployment.



1.6 Attacks and Countermeasures on the SecureDrop Environment

SecureDrop is a complex ecosystem comprised of various pieces of hardware, a diverse codebase, multiple user roles, and varied software dependencies. As such, an adversary can compromise any one of these components through a variety of attacks, as detailed below. We've categorized attacks and countermeasures by SecureDrop architecture area for clarity.

There are certain attacks that cannot be mitigated by any of the technical or operational countermeasures built into SecureDrop. Attacks of a political nature — for example, if a source, journalist, or organization is threatened with legal action — are context-dependent, and determined by an ever-shifting climate around press freedoms. While these attack vectors are out of the scope of this document, they should be factored in to any organization's threat model with regional and political specificity.

1.6.1 Application Code — SecureDrop Repository/Release

Attacks to the Application Code — SecureDrop Repository/Release

- Malicious code introduced in SecureDrop repository
- Malicious code introduced in SecureDrop release
- Failure to encrypt submissions as they are written to disk

Countermeasures on the Application Code — SecureDrop Repository/Release

- Code (git tags) and releases (packages uploaded to apt) are signed with the airgapped signing key
- Protection is placed on *main* and *develop* branch on GitHub
- For SecureDrop Developers, two-factor authentication is mandated on GitHub
- Community trust is built through 3 trusted code owners and code reviews

1.6.2 Application Code — *Source Interface* and *Journalist Interface*

Attacks to the Application Code — *Source Interface* and *Journalist Interface*

- Configuration vulnerability in *Source* or *Journalist Interface*
- Lack of segmentation between *Source* and *Journalist Interface*
- Session management vulnerability in *Source* or *Journalist Interface*
- Malicious input vulnerability in *Source* or *Journalist Interface*
- Configuration vulnerability in *Source* or *Journalist Interface*
- Authentication vulnerability in *Source* or *Journalist Interface*
- Access control vulnerability in *Source* or *Journalist Interface*
- Data protection vulnerability in *Source* or *Journalist Interface*
- Communications vulnerability in *Source* or *Journalist Interface*
- Error handling and logging vulnerability in *Source* or *Journalist Interface*
- HTTP security configuration vulnerability in *Source* or *Journalist Interface*
- File and resource vulnerability in *Source* or *Journalist Interface*
- Business logic vulnerability in *Source* or *Journalist Interface*
- Web services vulnerability in *Source* or *Journalist Interface*

Countermeasures on both *Source* and *Journalist Interfaces*

- *Interfaces* run on an end-to-end encrypted Tor Onion Service
- Sensitive source and submission data is sent through HTTP POST
- All source submissions are encrypted with GPG at rest using the airgapped *Submission Key*
- *Interface* sessions are invalidated after a user logs out or inactivity over 120 minutes
- Session control on *Interface* includes CSRF token in Flask Framework
- All *Interface* session data (except language and locale selection) is discarded at logout, and fully deleted upon exiting Tor Browser
- A number of mitigations are in place as protection against malicious input vulnerabilities on the Source and Journalist Interfaces:
  - X-XSS-PROTECTION is enabled
  - Content-Security-Policy is set to “default-src ‘none’; script-src ‘self’; style-src ‘self’; img-src ‘self’; font-src ‘self’;”
  - SQLAlchemy is used as ORM for all database queries
  - Application does not execute uploaded submission data

- A number of mitigations are in place as protection against the risk of an HTTP misconfiguration on the *Source* and *Journalist Interfaces*:
  - Cache control header is set to “no store;”
  - HTTP headers do not expose version information of system components
  - X-Content-Type is set to “nosniff;”
  - Content-Security-Policy is set to “default-src ‘none’; script-src ‘self’; style-src ‘self’; img-src ‘self’; font-src ‘self’;”
  - X-XSS-Protection is set to “1”

Countermeasures unique to *Source Interface*

- TLS on *Source Interface* is opt-in with an EV cert
- Only HTTP GET, POST and HEAD methods are allowed
- A number of mitigations are in place as protection against access control vulnerabilities on the *Source Interface*:
  - Source codenames are long and automatically generated
  - Hashed codenames are stored in a database hashed with a unique salt
  - Source codename reset functionality is not available
  - Source login does not display information about prior submissions
  - Source login requires 7-word codename to check *Source Interface* for replies

Countermeasures unique to *Journalist Interface*

- *Journalist Interface* is located behind an authenticated Onion Service and only privileged users have required authorization token
- Only HTTP GET, POST, HEAD and DELETE methods are allowed
- A number of mitigations are in place as protection against access control vulnerabilities on the *Journalist Interface*:
  - Apache autoindex module is disabled
  - Journalist/Admin passphrases are long and automatically generated
  - Passphrases are stored in a database hashed with a unique salt
  - Account generation/revocation/reset is restricted to Admin role
  - Two-factor authentication is required (via a TOTP app, or an HOTP device like a YubiKey)

1.6.3 *Application Server* and *Monitor Server*

Attacks on the *Application Server* and *Monitor Server*

- *Application* or *Monitor Server* configuration error
- *Source* or *Journalist Interface* is framed
- *Application* or *Monitor Server* is compromised
- Attacker exploits postfix
- Known vulnerabilities in the Linux kernel or packages used by app/mon servers

Countermeasures on Both *Application* and *Monitor Servers*

- Grsecurity/PaX linux patches prevent the exploitation of certain memory-corruption attacks
- AppArmor profiles further reduce process capabilities through Mandatory Access Control
- All SecureDrop infrastructure is provisioned via infrastructure-as-code (Ansible scripts)
- A cron job ensures that automatic nightly security updates are applied for OS packages
- *Journalist Interface* uses ATHS cookie
- *Monitor Server* should only expose SSH via Tor Onion Service. All other traffic should be blocked by firewall

Countermeasures Unique to *Application Server*

- SecureDrop *Source* and *Journalist Interfaces* uses X-Frame-Options: DENY header
- Browser Same Origin Policy should prevent the SecureDrop page from trivial modifications, but more complex attacks are mitigated via the X-Frame-Options: DENY HTTP header

Countermeasures Unique to *Monitor Server*

- OSSEC is used for intrusion detection/file integrity monitoring, and are sent to Admins via end-to-end encrypted email

1.6.4 SecureDrop Dependencies — Python, Tor, Linux Kernel, apt, Tails, Ubuntu, or Hardware Firewall Vulnerabilities

Attacks on SecureDrop Dependencies

- Known vulnerabilities in Python or libraries used by SecureDrop
- Known vulnerabilities in Tor (incl. Onion Service cryptography, authentication)
- Malicious apt package installed at install-time or during updates
- Known weakness in Onion Service cryptography
- GitHub is compromised
- Firewall is not up-to-date
- Tails ISO malicious
- Ubuntu ISO malicious
- Tor apt repo compromised
- Ubuntu apt repo compromised
- Tor Browser exploit
- Vulnerabilities/Compromise of Hardware Firewall

Countermeasures Against Vulnerabilities in Python or Libraries

- FPF performs vulnerability management for all Python packages used by SecureDrop
- CI will run safety check to ensure dependencies do not have a CVE associated with the version

Countermeasures Against Vulnerabilities in Tor

- A cron job ensures that automatic nightly security updates are applied for OS packages, including Tor
- Grsecurity/PaX linux patches prevent the exploitation of certain memory-corruption attacks
- AppArmor profiles further reduce process capabilities through Mandatory Access Control
- Onion service authentication is used as a complementary authentication and only used for defense-in-depth/attack surface reduction

Countermeasures Against Malicious apt Installs

- apt does GPG signature verification of all packages as long as it's not explicitly disabled

Countermeasures Against Malicious Tails or Ubuntu ISOs

- SecureDrop Admin Guide instructs Users/Admins to validate checksum/signatures of downloaded images

Countermeasures Against Vulnerabilities in the Hardware Firewall

- SecureDrop Admin Guide informs administrators to update the hardware firewall and provides a very restrictive policy for accessing the administrative interface (blocked on app and mon ports of the firewall).
- Alert emails are sent out to admins when there are critical pfSense vulnerabilities.
- *Application* and *Monitor Servers* use IPTables as host-based firewall for defense-in-depth
- All application traffic is over Tor onion services (end-to-end encrypted) and all software packages are signed. Only DNS and NTP are transmitted over HTTP (unauthenticated and in cleartext)

1.6.5 Network Infrastructure — FPF Infrastructure or Organization Corporate Network

Attacks on Network Infrastructure

- Landing Page source control is compromised
- Landing Page host is compromised
- Landing Page is framed or unavailable
- Landing Page DNS leaks from SecureDrop/leaks-related subdomain
- Communications vulnerability in *Source* or *Journalist Interface*
- DNS requests to news organization's subdomain for SecureDrop Landing Page, Freedom.press, torproject.org Tor activity, SD submissions may be correlated
- SecureDrop.org is compromised
- User web traffic to SecureDrop Landing Page uses CDN and may be logged
- Tor network exploit
- apt server man-in-the-middle used to serve old or malicious packages
- SecureDrop apt servers are compromised, or apt server man-in-the middle attack injects malicious packages
- News Organization network is compromised
- OSSEC and/or Journalist alert SMTP account credentials compromised
- OSSEC and/or Journalist alert private key compromised
- SMTP relay compromised

- Admin's network is monitored

Countermeasures in FPF Infrastructure

- Builds are independently validated by multiple developers
- Release files containing hashes (MD5, SHA1, SHA256, SHA512) of package file and package hashes are signed with an airgapped GPG key
- Developer key list is published and GPG-signed with the directory key
- SecureDrop updates are packaged in a .deb file and served through FPF's apt repo
- Source code is validated/verified before packaging and signing the .deb

Countermeasures in News Organization Corporate Network

- SecureDrop environment should be strictly segregated from corporate environment
- Most SecureDrop application traffic goes over Tor and as such is encrypted end-to-end
- Alert emails to Journalists and Admins are GPG-encrypted (but not signed) to provide confidentiality
- OSSEC alerts are scrubbed for sensitive contents (application data, server IPs)
- Documented deployment best practices provide instructions to strengthen Landing Page security and privacy

1.6.6 User Behavior and Hardware — SecureDrop Hardware Tampering or Failure in Operational Security

Attacks on User Behavior or Hardware

- Journalist corporate workstation seized/tampered/compromised
- Transfer device seized/stolen/lost
- Admin workstation backup stick is compromised
- Admin two-factor authentication device is lost or compromised
- Admin SSH Key is compromised
- SecureDrop installer misconfigures server/firewall hardware
- Source uses tor2web or employer/corporate device
- Source shares that they are using SecureDrop/leaking documents
- Journalist/Admin gets phished from a submission or otherwise breaks the SVS airgap with malware

Countermeasures in User Behavior Recommendations

- Source Guide gives instructructions on best practices for the entire submission workflow
- Source interface banner suggests that user disables JS (high security settings in Tor Browser)
- Journalist Guide informs users of malware risks, the importance of strict compartmentalization of SecureDrop-related activities
- SecureDrop Deployment Guide gives best practices for proper administration of the SecureDrop system, and its public-facing properties like the Landing Page
- Admin Guide gives instructions for long-term maintenance of the technical properties of the SecureDrop system, as well as operations to support Journalists
- All Admin tasks are completed over Tor/Tor authenticated onion services after installation

- Any Journalist/Admin password/2FA credentials resets can only be done by an Admin with password-protected SSH capability or authenticated Onion Service credentials.
- Persistent storage on the Admin Workstation is protected with LUKS/dm-crypt encryption

1.7 Getting Support

Whether you are interested in learning more about SecureDrop, looking for help with an installation, or needing assistance with an existing SecureDrop instance, there are several support options available to you.

Freedom of the Press Foundation offers direct *support via Signal*.

If you are unable to use Signal, you can always contact us by e-mail at securedrop@freedom.press (PGP encrypted).

Additionally, there is also some level of *Community Support*.

Note

If your installation is up and running, we recommend that you submit your SecureDrop to the SecureDrop directory. This also serves as a first introduction to the SecureDrop team.

While we will provide technical assistance within reason and at our discretion, we encourage you to consider a paid support agreement to receive priority support, staff training, or installation help. Visit the Priority Support and Training pages on the SecureDrop website for more information.

1.7.1 Support via Signal

Because of the sensitive nature of SecureDrop-related communications, we prefer providing support via the encrypted platform Signal.

Once we have connected with you on Signal, you will receive notifications regarding SecureDrop releases and security advisories, and you will be able to contact us with detailed requests for technical support.

Initial onboarding

Please start by submitting a request through the SecureDrop Contact Form.

Please provide an email address so we can reply back to you. We'll review your request and decide how to respond. If we decide to offer you support, we will send you instructions for onboarding you into a Signal group for your organization.

Using Signal

Signal must first be installed on an Android or iOS device and a phone number is required to create an account. A multi-platform desktop application is available which can sync messages and contacts with the mobile application. We recommend using the official Signal website for links and detailed instructions to install Signal on your devices.

Freedom of the Press Foundation has several guides to using Signal:

- Signal for beginners
- Locking down Signal
- Understanding every one of Signal's identifiers

1.7.2 Community Based Support

You can connect directly with the SecureDrop development team and the larger SecureDrop community using the SecureDrop Gitter channel.

Warning

Remember that the Gitter channel is public. **Do not post any sensitive information through public channels.**

1.8 SecureDrop On-Site Training Schedule

1.8.1 Who is This For?

While SecureDrop is open source and available for anyone to install and set up, Freedom of the Press Foundation provides paid support contracts to assist with the initial setup of the system, as well as training and ongoing technical support.

We generally recommend that news organizations set aside two days for the setup and training process. The first day is primarily the installation with the administrators and the second day is the training for those journalists who will regularly check SecureDrop.

Often, the entire process takes less time than two days but sometimes there are unique network or hardware issues that come up and delay completion.

If you are considering a paid contract for your organization, the following will provide you with an idea of the typical on-site installation and training timeline.

1.8.2 Day 1: Install

Installing SecureDrop

Installation may be started by admins ahead of schedule to save on-site time.

Time: 6+ hours

Participants: SecureDrop Admins

Format: For assisted installs, in-person or hybrid-remote (FPF remote, admins in-person)

- Follow *Installing SecureDrop*

1.8.3 Day 2: Admin and Digital Security Training

Admin Training

Time: 4+ hours

Participants: SecureDrop Admins

Format: In-person or hybrid-remote (FPF remote, admins in-person)

- Check access to previously created Tails USB
- Updating Tails
- Setup KeePassXC manager (one for *Secure Viewing Station*, one for *Admin Workstation*)
- Setting up SSH aliases for the *Admin Workstation* if needed
- Go over common OSSEC alerts for security updates and daily reports

- Adding/removing SecureDrop users
- Backups
- Disk space monitoring
- Changing passphrases (for FDE, persistent volumes, 2FA, KeePassXC managers…)
- Enabling logging for troubleshooting
- Sending logs to FPF support team
- Preparing *Journalist Workstation* drives
- Updating SecureDrop
  - Unattended upgrades
  - Upgrades that require admin intervention
- Distribute important info:
  - https://docs.securedrop.org
  - *Admin Best Practice Guide*
  - *Hardware for SecureDrop*
  - *Deployment Overview* guidelines

Digital Security 101

Time: 2 hours

Participants: Journalists to be onboarded to SecureDrop, admins, OSSEC alert recipients and anyone else interested

Format: In-person or remote

- Risk assessment and threat modeling
- Account security fundamentals
  - Passphrases and Password Managers
  - Two-factor authentication (2FA)
- Phishing prevention
- Web browser security
- IP address privacy, VPNs and Tor
- Secure communication tools for colleagues and sources
- Q & A

1.8.4 Day 3: Journalist Training and Onboarding

Journalist Training, Part 1

Time: 2.5 hours

Participants: Journalists to be onboarded to SecureDrop, admins, OSSEC alert recipients and anyone else interested

Format: In-person or remote

- Introduction to Tails and its features
- Importance of the *Landing Page* security

- Demo of source submission process
- Demo of journalist's processes for checking the *Journalist Interface*
- Demo of journalist's processes for replies
- Demo working with submissions on the *Secure Viewing Station*
- Secure-deleting and difference between wipe and erase free space on Tails, and when to use each
- Discuss scrubbing submitted documents prior to publication
  - Using MAT (Metadata Anonymisation Toolkit)
  - Converting files to more benign formats
  - What to do for unsupported formats
- Options for distributing with other news organizations
- Show example of an OSSEC alert, briefly cover what it does
- Overview of *onion names*
- Physical security of servers and *Secure Viewing Station*
- How to securely publicize the organization's *Source Interface* Tor URL
- Distribute important info:
  - https://securedrop.org
  - *Source Best Practice Guide*
  - *Journalist Best Practice Guide*
- Link to security audits
- Q & A

Journalist Training, Part 2

Time: 1+ hours, depending on the number of journalists being onboarded

Participants: Journalists to be onboarded to SecureDrop, admins

Format: In-person or hybrid-remote (FPF remote, journalists and admins in-person)

- Check access to previously created Tails USB drives
- Create SecureDrop accounts for individual journalists
- Setup KeePassXC for *Journalist Workstation* drive
- Disaster recovery for 2FA and password manager
- Updating Tails
- If needed, process for distributing the *Submission Private Key* to a remote journalist's air-gapped *Secure Viewing Station*
- Do complete journalist process walk through once, and repeat for each individual journalist being onboarded

1.9 Passphrase Best Practices

All SecureDrop users—Sources, Journalists, and Admins—are required to memorize at least one passphrase. This document describes best practices for passphrase management in the context of SecureDrop.

1.9.1 General Best Practices

1. **Do** memorize your passphrase.
2. If necessary, **do** write your passphrase down temporarily while you memorize it.

   Caution

   Do store your written passphrase in a safe place, such as a safe at home or on a piece of paper in your wallet. **Do** destroy the paper as soon as you feel comfortable that you have the passphrase memorized. **Do not** store your passphrase on any digital device, such as your computer or mobile phone.

3. **Do** review your passphrase regularly. It's easy to forget a long or complex passphrase if you only use it infrequently.

   Tip

   We recommend reviewing your passphrase (e.g. by ensuring that you can log in to your SecureDrop account) on at least a monthly basis.

4. **Do not** use your passphrase anywhere else.

   If you use your SecureDrop passphrase on another system, a compromise of that system could theoretically be used to compromise SecureDrop. You should avoid reusing passphrases in general, but it is especially important to avoid doing so in the context of SecureDrop.

1.9.2 For Sources

Your passphrase is associated with your pseudonymous account and all of your activity on the SecureDrop server. In order to preserve your anonymity, you should avoid creating physical or digital associations between yourself and your passphrase as much as possible.

1.9.3 For Journalists/Admins

While Sources only have one passphrase that they are required to manage, Journalists and Admins unfortunately have to manage a veritable menagerie of credentials.

We have tried to minimize the number of credentials that Journalists and admins actually have to *remember* by automating the storage and entry of credentials on the Tails workstations wherever possible. For example, a dedicated SecureDrop Menu is provided on each Tails workstation to make it easy to access the onion services without having to look up their `.onion` addresses every time.

Ideally, each admin would only have to:

1. Keep track of their Admin Workstation Tails USB.
2. Remember the passphrase to unlock the persistent storage on that Tails USB.

And each Journalist would only have to:

1. Keep track of their Journalist Workstation Tails USB.

2. Keep track of their Secure Viewing Station Tails USB (and the associated Secure Viewing Station computer).
3. Remember the passphrases to unlock the persistent storage on both of these Tails USBs.

Memorizing further passphrases beyond the ones listed above is counterproductive: an attacker with access to any of those environments would be able to pivot to anything they wish to access, and increasing the burden of keeping track of additional credentials is unpleasant for journalists and admins and increases the risk that they will either forget their credentials, compromising the availability of the system, or compensate for the difficulty by using weak or reused credentials, potentially compromising the security of the system.

There is a detailed list of the credentials that must be managed by each end user role in *Passphrases*. We recommended using the KeePassXC password manager included in Tails to store your credentials and minimize the passphrases that you need to memorize to just the passphrases for the persistent storage on your Tails USBs.

For the *Transfer Device* and the *Export Device*, which are used to copy files to and from the air-gapped *Secure Viewing Station*, we recommend using encrypted USB drives with passphrases stored in the journalist's own password manager (preferably one which is accessible on their smartphone). This ensures that the journalist will have quick access to these passphrases when they need them.

If your organization is not using a password manager already, please see the Freedom of the Press Foundation guide to choosing one.

1.10 SecureDrop for Sources

Note

This guide provides an introduction to using SecureDrop as a source. It is not exhaustive, it does not address ethical or legal dimensions of whistleblowing, and it does not speak to other methods for confidentially communicating with journalists. Please proceed at your own risk. For additional background, also see the Freedom of the Press Foundation guide, How to Share Sensitive Leaks With the Press.

Warning

Freedom of the Press Foundation has no access to any other organization's SecureDrop instance, and cannot assist directly in your communications with them. If you plan to use SecureDrop to maintain your anonymity, you should not discuss your own use of it with others via unsafe methods, including email to Freedom of the Press Foundation.

1.10.1 What is SecureDrop?

SecureDrop is a tool that news organizations and NGOs use that enables secure and anonymous communication between whistleblowers and journalists. No personal information is collected; information submitted to SecureDrop is encrypted, and SecureDrop is not a "cloud" service. If you don't have sensitive information to send to a news organization, it may be okay to use a traditional methods such as phone or email when reaching out.

SecureDrop can accept both messages and individual file uploads (up to 500MB). If you have multiple files to submit, you may do that. As a source, you can also return to receive follow-up correspondence with an organization, or to send additional information. Dozens of news organizations — from *ProPublica* to *The New York Times* — use SecureDrop to accept tips securely and anonymously.

To truly protect your anonymity, it is important for you to take some extra precautions in advance. This resource will describe things you can do to help protect your anonymity when using SecureDrop. Note that your Internet Service Provider, or ISP (e.g., Comcast/Xfinity, Cox, Wave, etc), may already have a record of your visit to this website, docs.securedrop.org.

Before you begin…

- DO NOT access SecureDrop on your employer's network.
- DO NOT access SecureDrop using your employer's hardware.
- DO NOT access SecureDrop on your home internet network.
- **DO** carefully read the remaining instructions, that will carefully step-through the reasons why we advise the above, and provide guidance to minimize risk when using SecureDrop.

1.11 Before You Submit

1.11.1 What NOT to Do

- DO NOT access SecureDrop on your employer's network.
- DO NOT access SecureDrop using your employer's hardware.
- DO NOT access SecureDrop on your home internet network.

1.11.2 Suggested Devices for Using SecureDrop

When sensitive disclosures such as government improprieties are involved, we suggest you buy a new computer and at least one new USB flash drive. You should only use cash to make those purchases.

Many time-saving features of computers and phones can easily compromise your anonymity: bookmarks, recommendations, synchronization features, shortcuts to frequently opened files, etc. Those reasons and more are why using a dedicated computer for whistleblowing activities can be safer.

To build an even stronger buffer for yourself, we recommend booting the computer into the Tails operating system (typically from a USB stick). Tails is specifically designed to run on your computer without leaving traces of your activity. This may take some additional technical steps, but it is safer and fairly simple to get started. Even if you choose to use a dedicated computer for SecureDrop that will never be used for anything else, Tails will help to avoid leaving traces of your activity on the computer's hard disk, in your ISP's logs, or on cloud services.

1.11.3 Choose the Right Location

Find a busy cafe you don't regularly go to and sit at a place with your back to a wall to avoid cameras capturing information on your screen or keystrokes. Be sure to also make any purchases while there (WiFi, tea, snacks) or on your way to the cafe (bus, train, gas) with cash.

1.11.4 Use Tor Browser

Each SecureDrop may **only** be reached through the Tor Browser. SecureDrop pages are only available as onion services—encrypted web pages that end in ".onion," and only the Tor browser is able to open these pages.

Tor is an anonymizing network that makes it difficult for anybody observing the network to associate a user's identity (e.g., the computer's IP address) with their activity. Tor Browser can be downloaded from the Tor Project's website. Tor Browser is a modified version of the Firefox web browser that also includes features protect your security and anonymity. If there is a chance that visiting the Tor Project's website to download Tor Browser might raise suspicion, you have a couple of alternatives:

- If your mail provider is less likely to be monitored, you can send a mail to gettor@torproject.org with the text "linux", "windows" or "osx" in the body (for your preferred operating system) and a bot will answer with instructions.
- You can request to receive the Tor Browser bundle via the @GetTor_bot on Telegram.

While using Tor Browser on your personal computer helps hide your activity on the network, it will leave traces of its own installation on your local machine. Most operating systems keep logs, for example, any time an application is used. The sensitivity of the information you share and the capabilities of those who may not want you to share that information, should be considered when making these decisions.

Important

Tor protects your anonymity, but third parties who can monitor your network traffic can detect *that you are using Tor*. They may even be able to do so long after your browser session, using network activity logs. This is why we recommend using Tor Browser from a cafe you do not visit regularly.

1.11.5 Choose Who to Submit To

We recommend conducting all research related to your submission in Tor Browser. If you are unsure whether you are using Tor, you can visit the address https://check.torproject.org.

All organizations operating SecureDrop have a *landing page* that provides their own organization-specific recommendations for using SecureDrop. We encourage you to consider an organization's *landing page* before submitting to them.

Note

Each SecureDrop instance is operated and administered independently by the organization you are submitting to. Only the journalists associated with that organization can see your submissions.

Most organizations make their SecureDrop prominently accessible from their main website's homepage (for news organizations, typically under sections called "Tips" or "Contact us"). You can also find an incomplete list of organizations accepting submissions through SecureDrop in the SecureDrop Directory maintained by Freedom of the Press Foundation.

Using Tor Browser, find the ".onion" address for the SecureDrop for the organization that you wish to submit to.

Tip

If the organization does have an entry in the SecureDrop Directory, we recommend comparing the address of the entry with the one on the organization's own SecureDrop landing page.

If the two addresses don't match, please do not submit to this organization yet. Instead, please contact us through the SecureDrop website, using Tor Browser. For additional security, you can use our .onion service address in Tor:

```
sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion/report-an-error
```

We will update the directory entry if the information in it is incorrect.

Once you have located the ".onion" address, copy it into the address bar in Tor Browser to visit the organization's SecureDrop.

1.12 How To Submit

Note

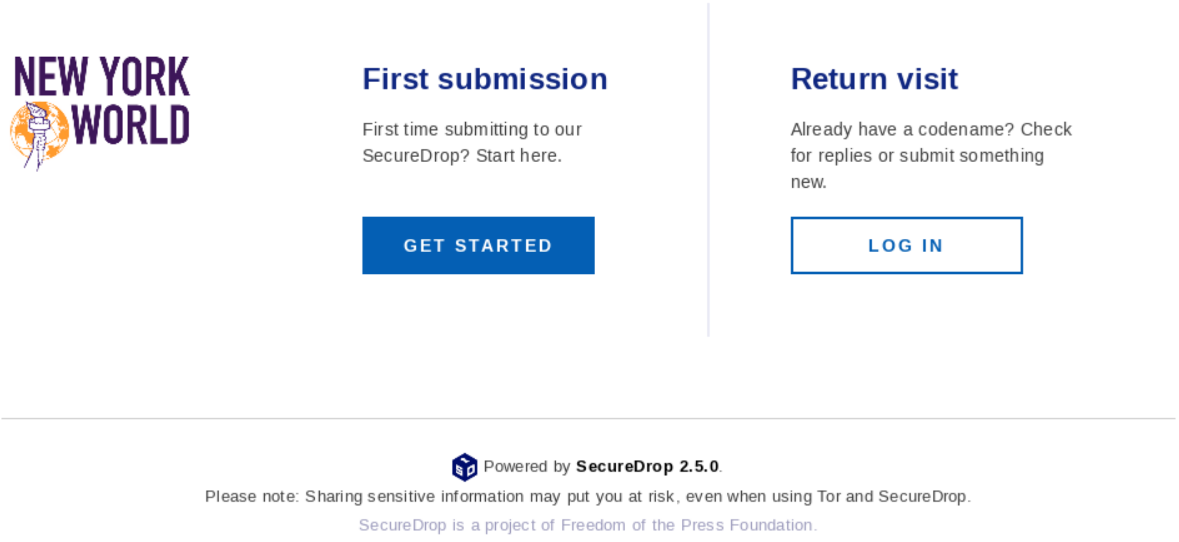
This guide provides an introduction to using SecureDrop as a source. It is not exhaustive, it does not address ethical or legal dimensions of whistleblowing, and it does not speak to other methods for confidentially communicating with journalists. Please proceed at your own risk. For additional background, also see the Freedom of the Press Foundation guide, How to Share Sensitive Leaks With the Press.

Warning

Freedom of the Press Foundation has no access to any other organization's SecureDrop instance, and cannot assist directly in your communications with them. If you plan to use SecureDrop to maintain your anonymity, you should not discuss your own use of it with others via unsafe methods, including email to Freedom of the Press Foundation.

1.12.1 Making Your First Submission

Open Tor Browser and navigate to the .onion address for the SecureDrop you wish to make a submission to. The page will invite you to get started with your first submission or to log in. It should have a logo specific to the organization you are submitting to.



First submission

First time submitting to our SecureDrop? Start here.

GET STARTED

Return visit

Already have a codename? Check for replies or submit something new.

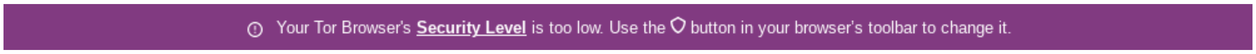
LOG IN

Powered by **SecureDrop 2.5.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

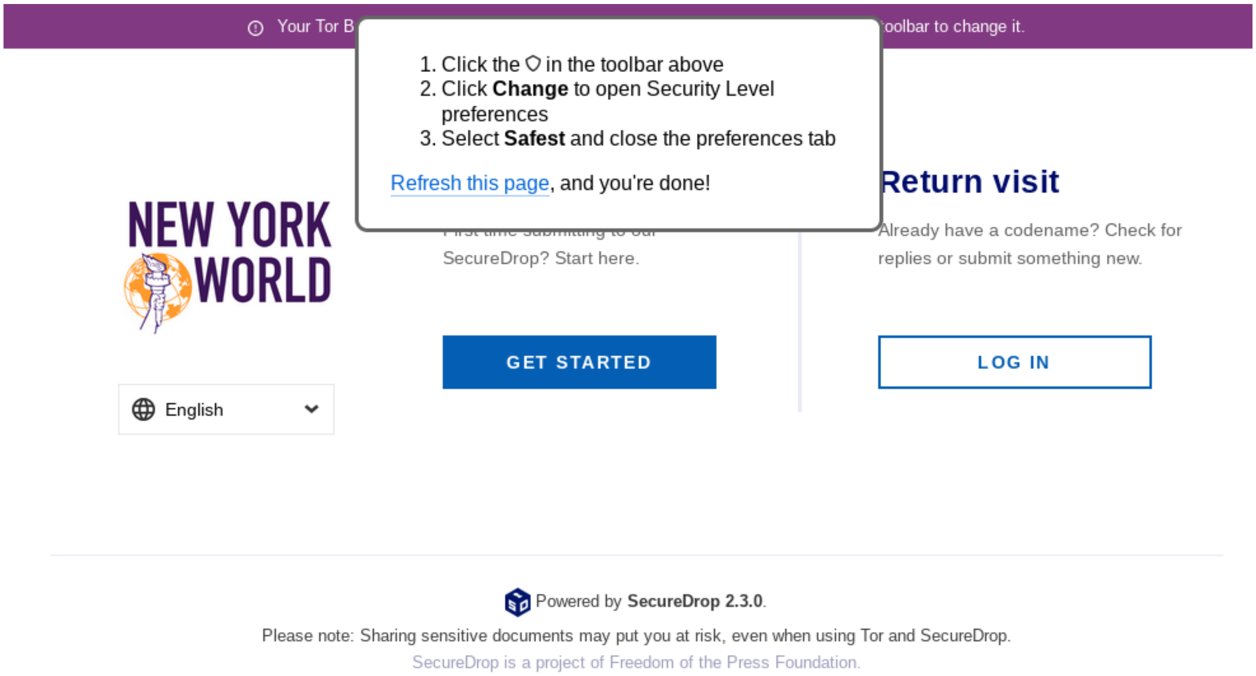
SecureDrop is a project of Freedom of the Press Foundation.

If this is the first time you're using Tor Browser, it's likely that you have JavaScript enabled and that the Tor Browser's security level is set to "Low". In this case, there will be a purple warning banner at the top of the page that encourages you to disable JavaScript and change the security level to "Safest".



ⓘ Your Tor Browser's **Security Level** is too low. Use the ♡ button in your browser's toolbar to change it.

Click the **Security Level** link in the warning banner, and a message bubble will pop up explaining how to increase the security level to **Safest**.



Your Tor B… …oolbar to change it.

1. Click the ⛉ in the toolbar above
2. Click **Change** to open Security Level preferences
3. Select **Safest** and close the preferences tab

Refresh this page, and you're done!

First time submitting to our SecureDrop? Start here.

Return visit

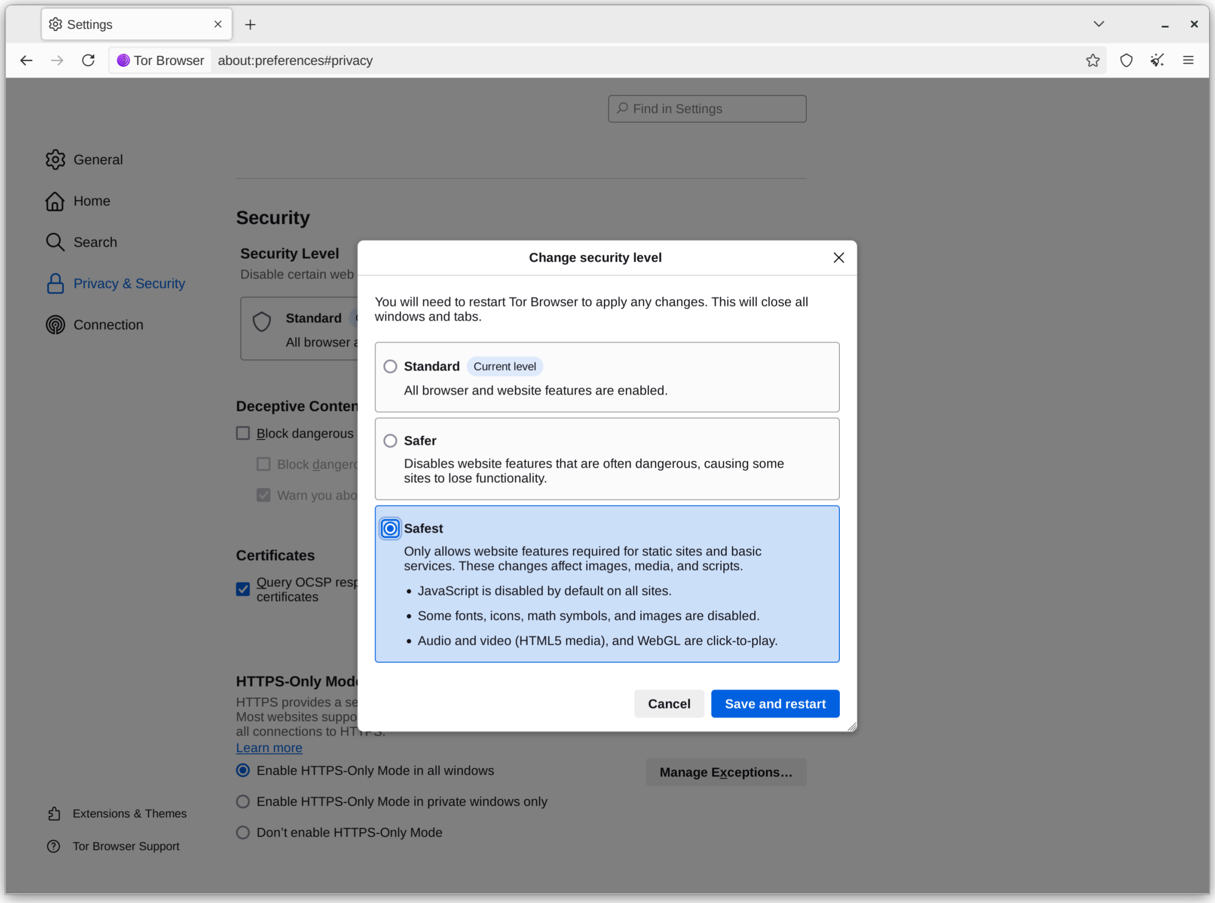
Already have a codename? Check for replies or submit something new.

Powered by **SecureDrop 2.3.0**.

Please note: Sharing sensitive documents may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

1. Click the shield icon in the toolbar
2. Click **Settings…**
3. If the current level is not already set to **Safest**, click **Change…**
4. Select **Safest**
5. Select **Save and restart** for the changes to take effect
6. Navigate back to the Source Interface for the SecureDrop for which you wish to submit



Security

Security Level

Disable certain web

Standard

All browser

Change security level

You will need to restart Tor Browser to apply any changes. This will close all windows and tabs.

○ **Standard** Current level

All browser and website features are enabled.

○ **Safer**

Disables website features that are often dangerous, causing some sites to lose functionality.

● **Safest**

Only allows website features required for static sites and basic services. These changes affect images, media, and scripts.

- JavaScript is disabled by default on all sites.
- Some fonts, icons, math symbols, and images are disabled.
- Audio and video (HTML5 media), and WebGL are click-to-play.

Deceptive Conten

□ Block dangerous

□ Block danger

☑ Warn you abo

Certificates

☑ Query OCSP resp certificates

HTTPS-Only Mod

HTTPS provides a se Most websites suppo all connections to HTTPS.

Learn more

● Enable HTTPS-Only Mode in all windows

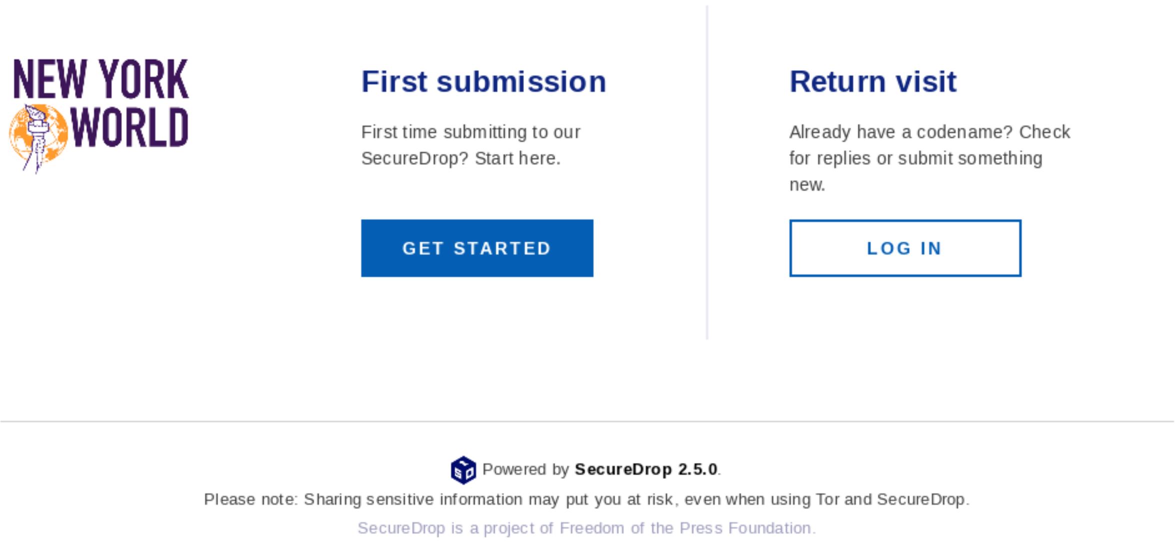
○ Enable HTTPS-Only Mode in private windows only

○ Don't enable HTTPS-Only Mode

Note

The "Safest" setting disables the use of JavaScript on every page you visit using Tor Browser, even after a browser restart. This may cause other websites you visit using Tor Browser to no longer work correctly, until you adjust the Security Level again. We recommend keeping the setting at "Safest" during the entirety of the session in which you access an organization's SecureDrop instance.

Once you return to the SecureDrop page, it should stop displaying the warning. If this is the first time you are using SecureDrop, click the **Get Started** button.



First submission

First time submitting to our SecureDrop? Start here.

Return visit

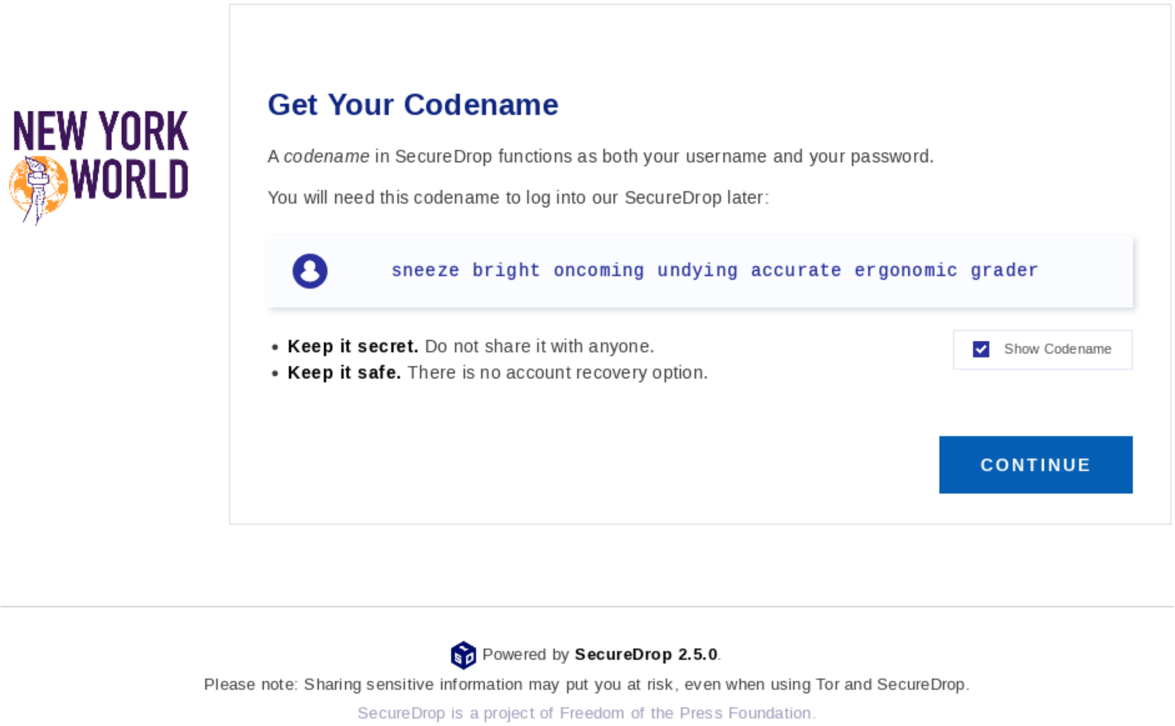
Already have a codename? Check for replies or submit something new.

Powered by **SecureDrop 2.5.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

You should now see a screen that shows the unique codename that SecureDrop has generated for you. Note that your codename will not be the same as the codename shown in the image below. It is extremely important that you both remember this code and keep it secret. After submitting documents, you will need to provide this code to log back in and check for responses.



Get Your Codename

A *codename* in SecureDrop functions as both your username and your password.

You will need this codename to log into our SecureDrop later:

```
sneeze bright oncoming undying accurate ergonomic grader
```

- **Keep it secret.** Do not share it with anyone.
- **Keep it safe.** There is no account recovery option.

Powered by **SecureDrop 2.5.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

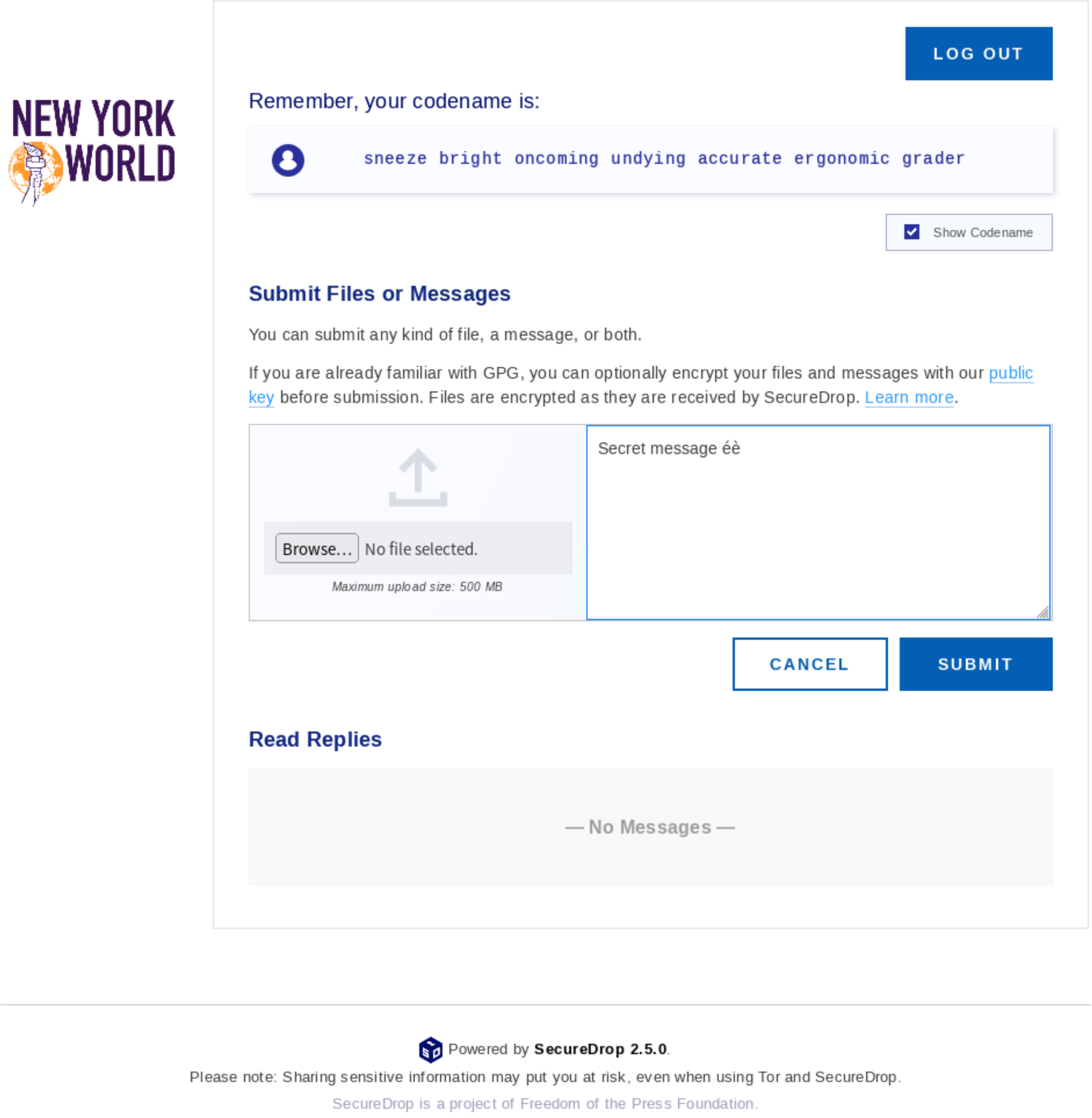
The best way to protect your codename is to memorize it. If you cannot memorize it right away, we recommend writing it down and keeping it in a safe place at first, and gradually working to memorize it over time. Once you have memorized it, you should destroy the written copy.

Tip

For detailed recommendations on best practices for managing your passphrase, check out *Passphrase Best Practices*.

Once you have generated a codename and put it somewhere safe, click **Submit Documents**.

You will next be brought to the submission page, where you may upload a document, enter a message to send to journalists, or both. You can only submit one document at a time, so you may want to combine several files into a ZIP archive if necessary. The maximum submission size is currently 500MB. If the files you wish to upload are over that limit, we recommend that you send a message to the journalist explaining this, so that they can set up another method for transferring the documents.



Remember, your codename is:

```
sneeze bright oncoming undying accurate ergonomic grader
```

Submit Files or Messages

You can submit any kind of file, a message, or both.

If you are already familiar with GPG, you can optionally encrypt your files and messages with our public key before submission. Files are encrypted as they are received by SecureDrop. Learn more.

No file selected.

Maximum upload size: 500 MB

Secret message éè

Read Replies

— No Messages —

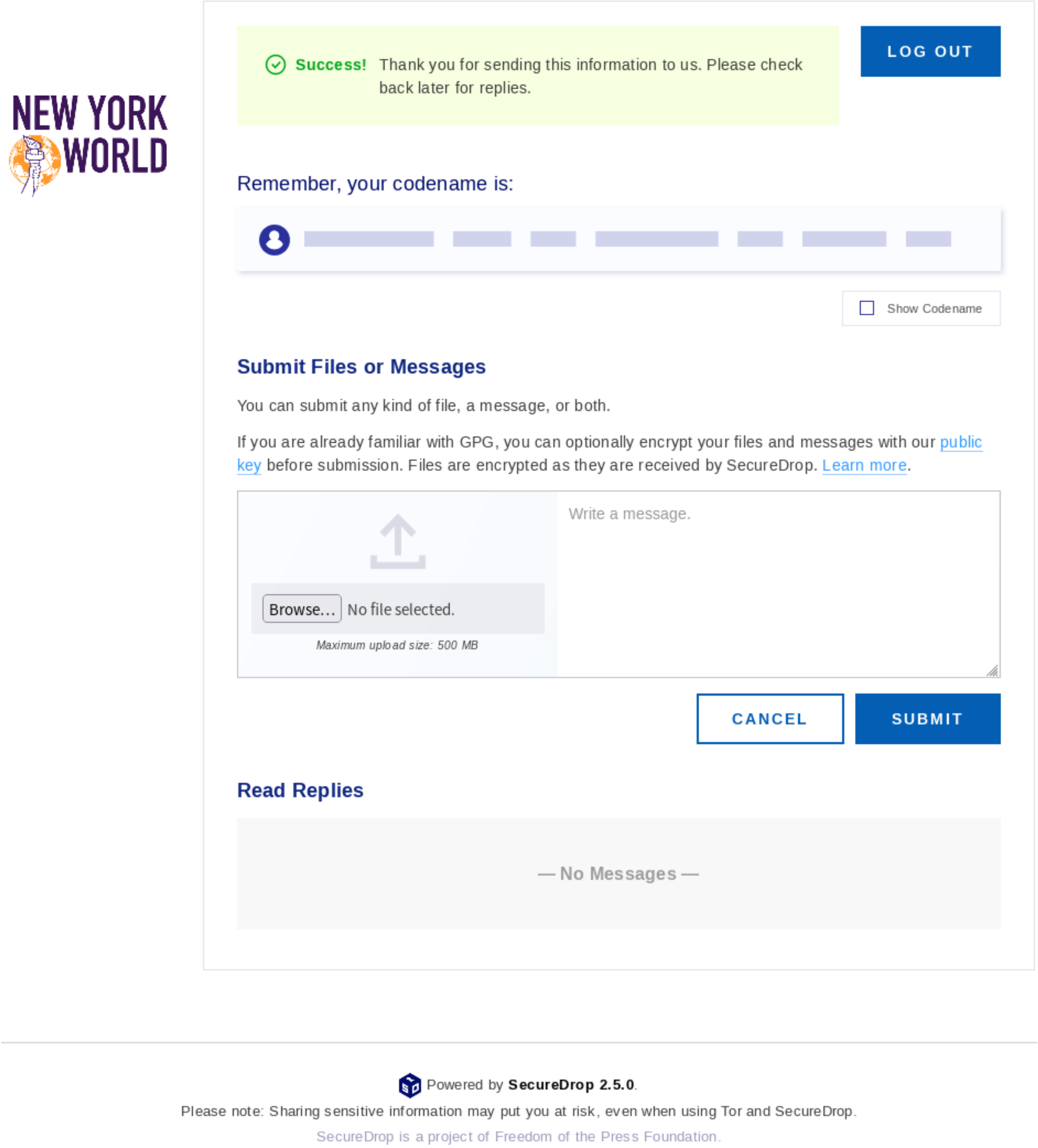
Powered by **SecureDrop 2.5.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

When your submission is ready, click **Submit**.

After clicking **Submit**, a confirmation page should appear, showing that your message and/or documents have been sent successfully. On this page you can make another submission or view responses to your previous messages.



Success! Thank you for sending this information to us. Please check back later for replies.

Remember, your codename is:

□ Show Codename

Submit Files or Messages

You can submit any kind of file, a message, or both.

If you are already familiar with GPG, you can optionally encrypt your files and messages with our public key before submission. Files are encrypted as they are received by SecureDrop. Learn more.

Browse… No file selected.

Maximum upload size: 500 MB

Write a message.

Read Replies

— No Messages —

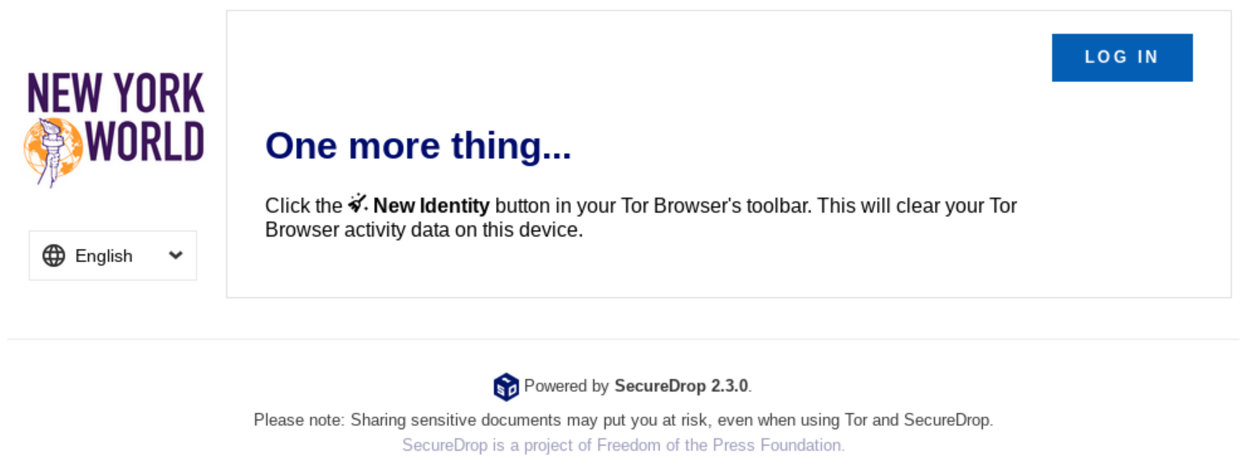
Powered by **SecureDrop 2.5.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

Once you are finished submitting documents, be certain you have saved your secret codename and then click the **Log out** button.

The final step to clearing your session is to restart Tor Browser for optimal security. After logging out, you should see a new page recommending you to click the **New Identity** button in the Tor Browser toolbar.



One more thing...

Click the New Identity button in your Tor Browser's toolbar. This will clear your Tor Browser activity data on this device.

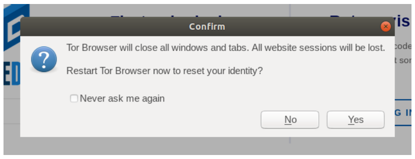
Powered by SecureDrop 2.3.0.

Please note: Sharing sensitive documents may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

You can either close the browser entirely or follow the instructions on the page:

1. Click on the **New Identity** button in the Tor Browser toolbar
2. Click **Yes** in the dialog box that appears to confirm you'd like to restart Tor Browser



Tor Browser will close all windows and tabs. All website sessions will be lost.

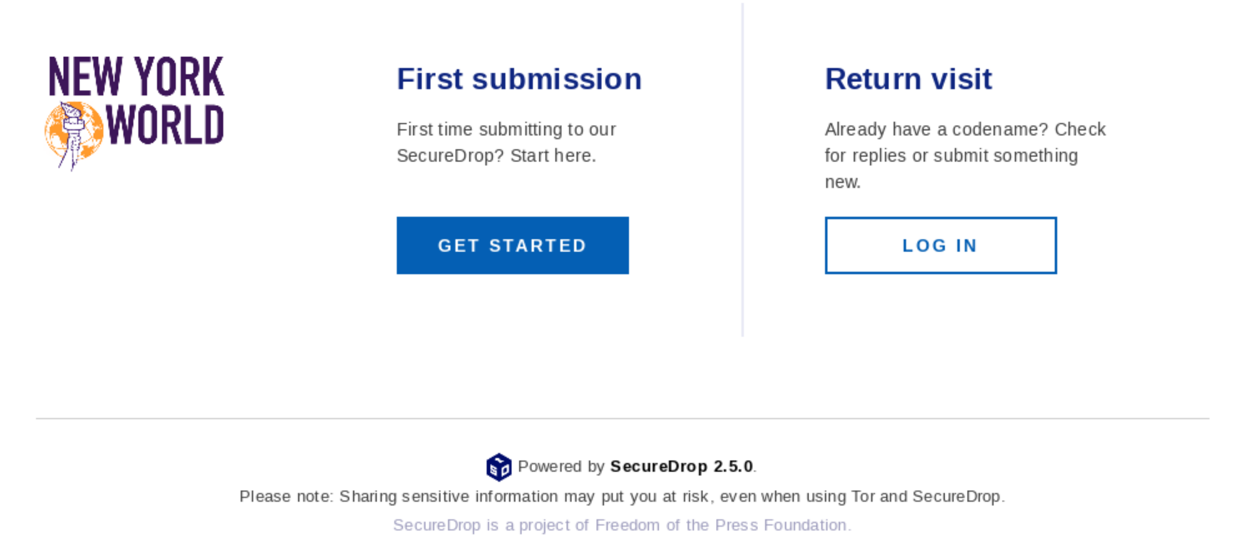
Restart Tor Browser now to reset your identity?

□ Never ask me again

1.13 After You Submit

1.13.1 Continuing the Conversation

If you have already submitted a document and would like to check for responses, click the **Log in** button on the media organization's SecureDrop page.



First submission

First time submitting to our SecureDrop? Start here.

Return visit

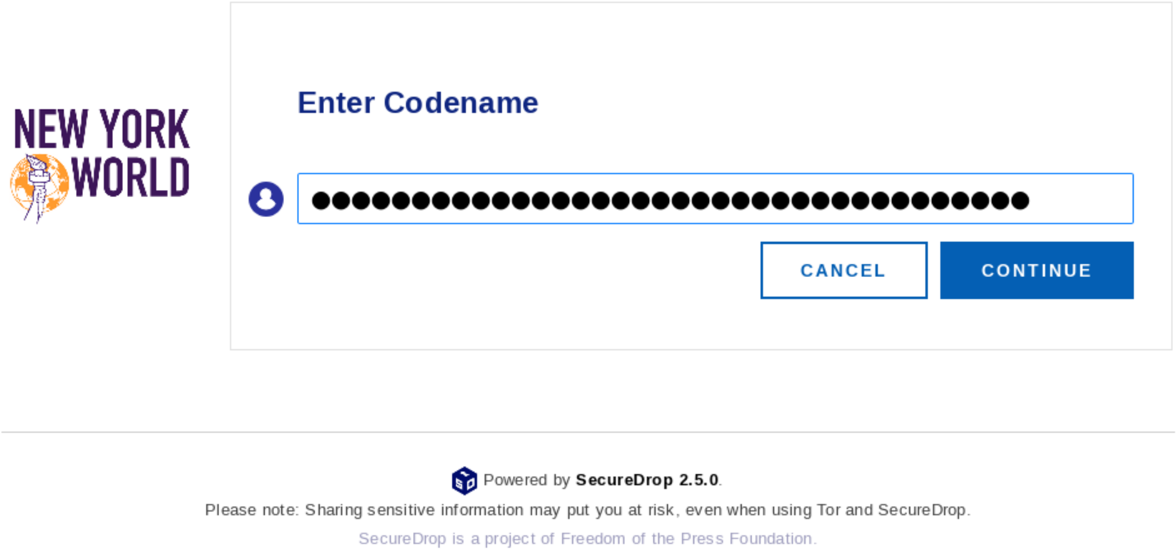
Already have a codename? Check for replies or submit something new.

Powered by SecureDrop 2.5.0.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

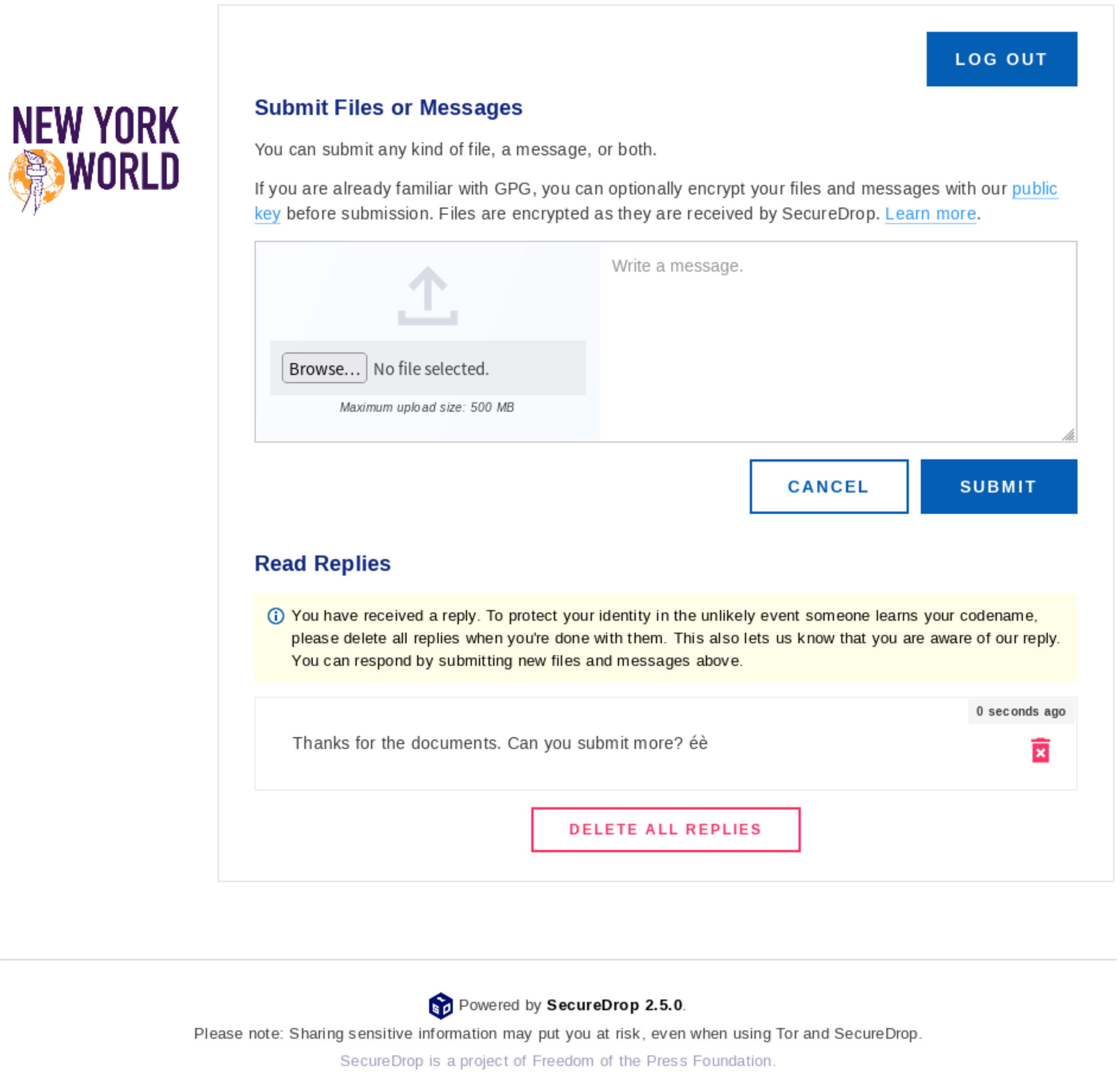
The next page will ask for your secret codename. Enter it and click **Continue**.



Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

If a journalist has responded, their message will appear on the next page. Before leaving the page, you should delete any replies. In the unlikely event that someone learns your codename, this will ensure that they will not be able to see the previous correspondences you had with journalists.



Submit Files or Messages

You can submit any kind of file, a message, or both.

If you are already familiar with GPG, you can optionally encrypt your files and messages with our public key before submission. Files are encrypted as they are received by SecureDrop. Learn more.

Maximum upload size: 500 MB

Read Replies

You have received a reply. To protect your identity in the unlikely event someone learns your codename, please delete all replies when you're done with them. This also lets us know that you are aware of our reply. You can respond by submitting new files and messages above.

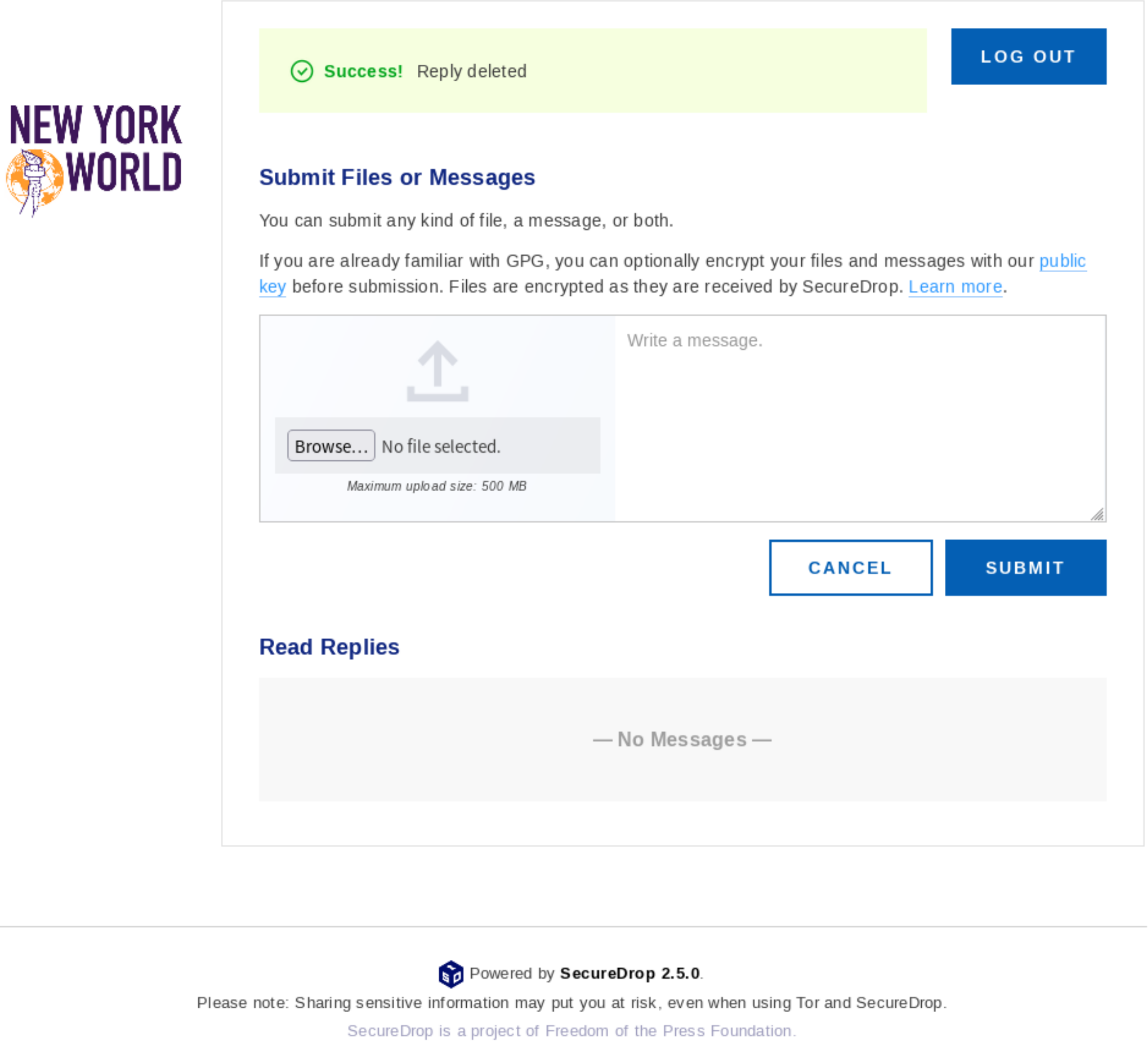
Thanks for the documents. Can you submit more? éè

Powered by SecureDrop 2.5.0.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

After you delete the reply from the journalist, make sure you see the confirmation message: “Reply deleted”.



Success! Reply deleted

Submit Files or Messages

You can submit any kind of file, a message, or both.

If you are already familiar with GPG, you can optionally encrypt your files and messages with our public key before submission. Files are encrypted as they are received by SecureDrop. Learn more.

Read Replies

— No Messages —

Powered by **SecureDrop 2.5.0**.

Please note: Sharing sensitive information may put you at risk, even when using Tor and SecureDrop.

SecureDrop is a project of Freedom of the Press Foundation.

1.14 SecureDrop for Journalists

Note

SecureDrop wants your feedback! Confused by something in our documentation? Let us know by opening an issue on GitHub or in our Gitter channel.

This guide presents an overview of the SecureDrop system for a journalist. It covers the core functions necessary to start working with the platform: logging in securely, viewing documents, editing documents, and interacting with sources.

Journalists will use at least two separate computers to interact with SecureDrop. The first is a *Journalist Workstation*, which connects to the *Journalist Interface*. Journalists download encrypted submissions and copy them to a *Transfer Device* (a thumb drive or DVD). Those submissions are then connected to the airgapped *Secure Viewing Station* (*SVS*) which holds the key to decrypt them. The *SVS* is used to read, print, and otherwise prepare documents for publication. Apart from those deliberately published, decrypted documents are never accessed on an Internet-connected computer.

SecureDrop provides a number of benefits intended to protect journalists. Communications through SecureDrop are encrypted in transit, so messages cannot be easily intercepted and read while they are moving across the Internet, and are also encrypted on the server so if any attacker manages to break into the server, they would not be able to read past messages.

In addition, the decryption key for submissions resides on an air-gapped computer (not connected to the Internet), which makes it harder for an attacker to access.

It also helps in the event of a subpoena or court order. All servers are owned by the individual news organization, so no third-party companies can be secretly subpoenaed. Additionally, SecureDrop limits the amount of metadata it collects and saves, so there's no trail showing exactly when a journalist was speaking with a source, or details that might give the source away.

For full details about what makes SecureDrop a unique and useful tool for Journalists, *see here.*

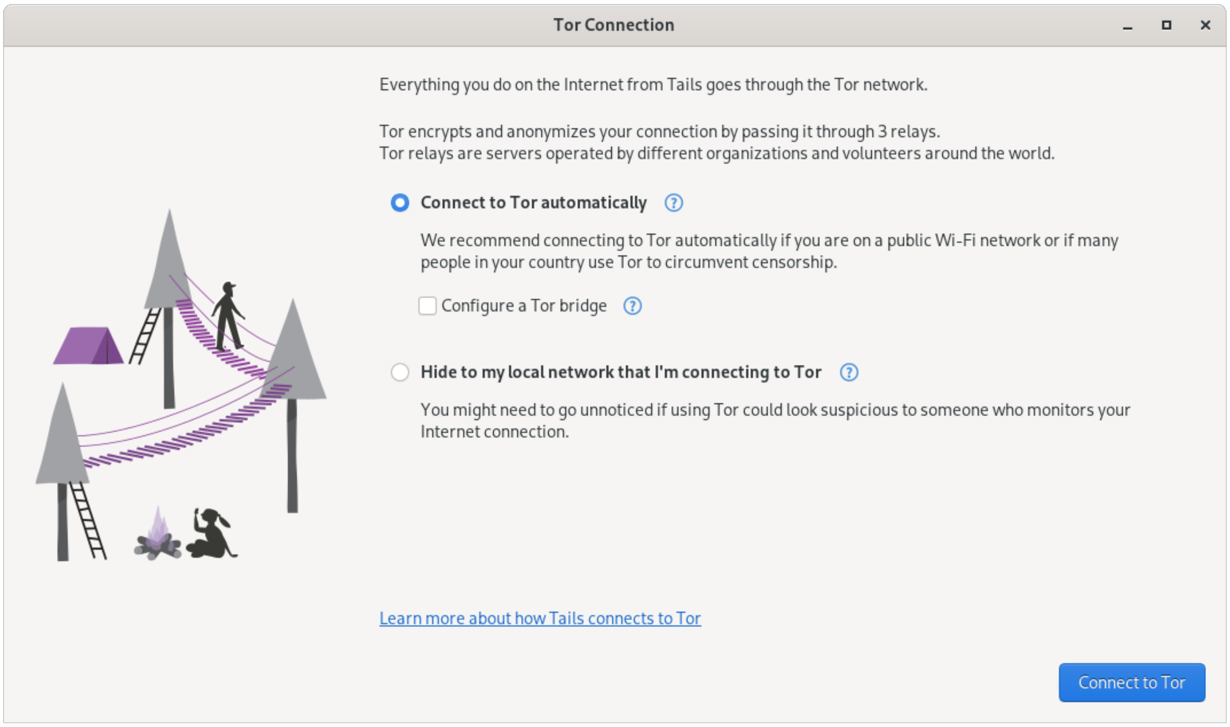
1.15 Using the Journalist Workstation

1.15.1 Connecting to the Tor network in Tails

After you connect to the Internet, the Tor Connection assistant will start.

If you are operating in an environment with a high degree of political freedom, and you are able to access the Tor network reliably, you can accept the defaults:

1. Click **"Connect to Tor automatically (easier)"**
2. Leave the checkbox **"Configure a Tor bridge"** unchecked
3. Click **"Connect 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 organizations and volunteers around the world.

● **Connect 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.

□ Configure a Tor bridge

○ **Hide to my local network that I'm connecting to Tor**

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

Learn more about how Tails connects to Tor

For more information about alternative ways to connect to the Tor network, please see the section "Connecting to the Tor network" in the Tails documentation.

> **Note**
>
> The Tor Connection assistant may display an error message after connecting to the Tor network successfully. If the error message disappears after a few seconds, you can safely ignore it. The error is caused by SecureDrop-specific changes that briefly interrupt Tor connectivity.

1.15.2 Updating Your Workstation

You should keep your SecureDrop workstations updated with:

- **Tails updates**
- **SecureDrop workstation updates**

You should apply Tails updates to your Tails drive as they are released, as they often contain critical security fixes. The *Journalist Workstation* Tails drive, once booted and connected to Tor, will alert you if upgrades are available. For most Tails upgrades, you can simply follow the steps in the Tails Upgrader that appears on screen to update your Tails drive. However, sometimes Tails upgrades are "manual," which means that you should follow the instructions in the Tails Upgrade Documentation to upgrade the drives. Talk to your SecureDrop administrator if you have trouble.

You can also check for and install updates using the "Check for SecureDrop Updates" option from the *SecureDrop Menu*.

Admin and *Journalist Workstations* automatically check for updates on boot. An update window will pop up when updates are needed, and you should simply follow the prompts in the updater to perform the update.

> **Note**
>
> Note that you will need to have a Tails Administrator password configured to complete the update. If you forget to do so, you will need to reboot to enable it.

1.15.3 Connecting to the *Journalist Interface*

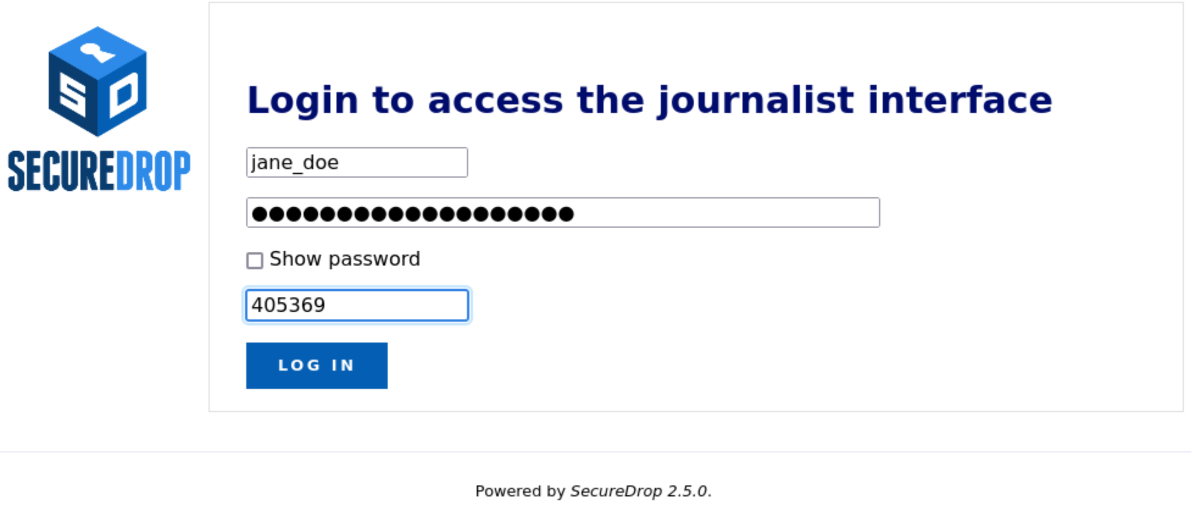
Journalists viewing documents on SecureDrop must connect to the *Journalist Interface* using the Tails operating system on a USB drive. As part of your on-boarding, your admin should have provided you with a Tails drive configured for this purpose, known as the *Journalist Workstation* USB drive.

If you do not have a USB drive clearly identified as the *Journalist Workstation*, ask your administrator for assistance before continuing.

> **Note**
>
> The Tails OS makes using SecureDrop very different from other computing experiences. The added layers of security mean extra steps each time you want to login. With practice, you will become increasingly comfortable with the process.

To use the *Journalist Interface*, you will visit a Tor Onion Service address in Tor Browser. By design, this Onion Service address is only accessible from your *Journalist Workstation*; it will not work in Tor Browser on another computer, unless explicitly configured with an access token.

To visit the *Journalist Interface*, open the *SecureDrop Menu* and select the "Launch Journalist Interface" option. This will open Tor Browser to an ".onion" address. Log in with your username, passphrase, and two-factor authentication token. (If you have been provided with a YubiKey, see *Using YubiKey with the Journalist Interface* for detailed setup and usage information.)



Login to access the journalist interface

jane_doe

●●●●●●●●●●●●●●●●●●●●

□ Show password

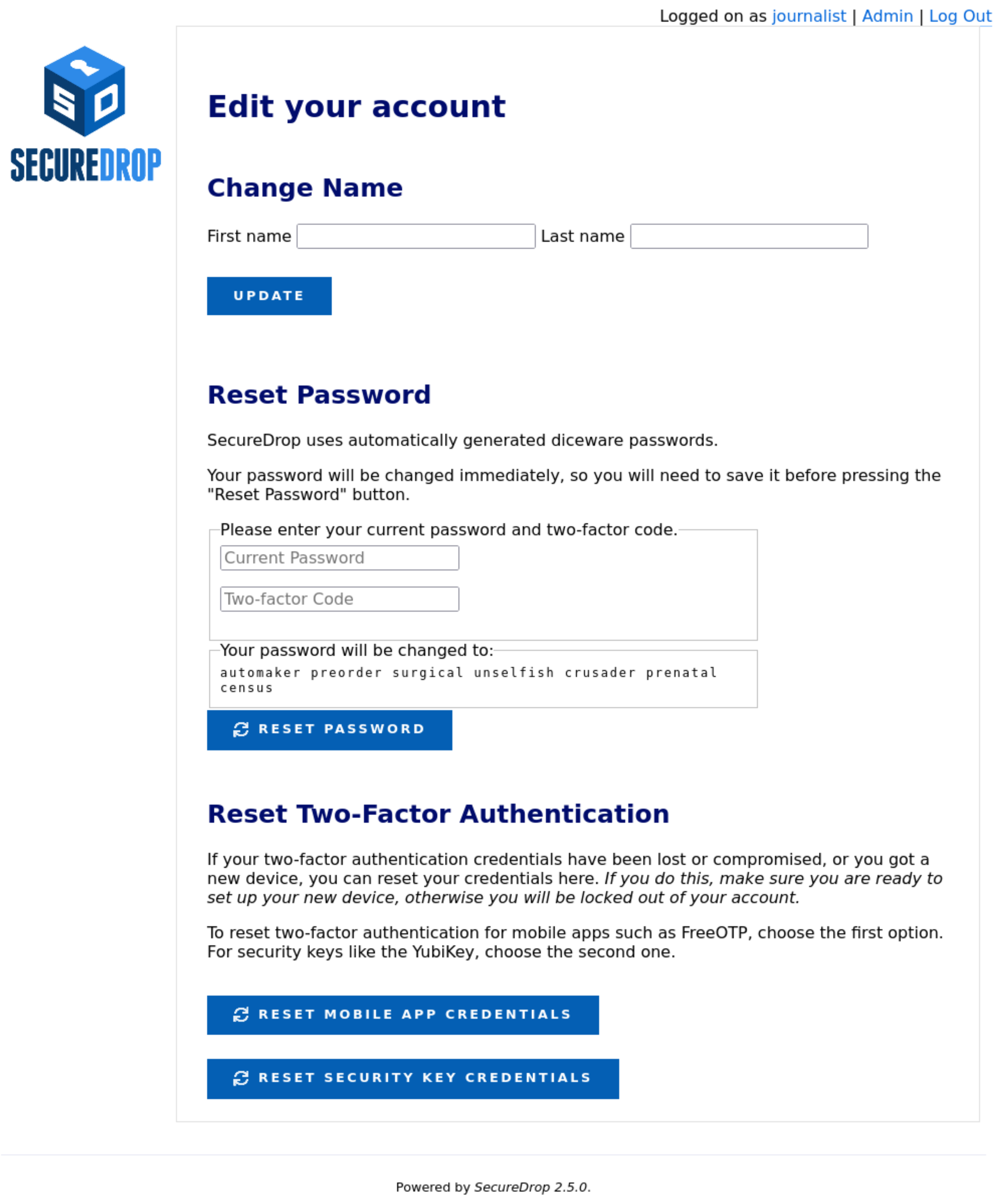
405369

Powered by *SecureDrop 2.5.0*.

Reset Passphrase or Two-factor Authentication Credentials

If necessary, journalists may reset their user passphrase or two-factor authentication token in their user profile. To navigate to your user profile, log in to the *Journalist Interface* and click on the link in the upper right of the screen where it says **Logged on as <your user name>.**

If you have lost or forgotten your passphrase or your two-factor device (i.e. your mobile phone or security key), you will need to contact your SecureDrop admin for assistance.



Logged on as journalist | Admin | Log Out
SECUREDROP
UPDATE
RESET PASSWORD
RESET MOBILE APP CREDENTIALS
RESET SECURITY KEY CREDENTIALS

Edit your account

Change Name

First name [ ] Last name [ ]

Reset Password

SecureDrop uses automatically generated diceware passwords.

Your password will be changed immediately, so you will need to save it before pressing the "Reset Password" button.

Please enter your current password and two-factor code.

Current Password

Two-factor Code

Your password will be changed to:

```
automaker preorder surgical unselfish crusader prenatal
census
```

Reset Two-Factor Authentication

If your two-factor authentication credentials have been lost or compromised, or you got a new device, you can reset your credentials here. *If you do this, make sure you are ready to set up your new device, otherwise you will be locked out of your account.*

To reset two-factor authentication for mobile apps such as FreeOTP, choose the first option. For security keys like the YubiKey, choose the second one.

Powered by *SecureDrop 2.5.0*.

Note

If the QR code for setting up two-factor authentication in your mobile authenticator app is not displayed, it may be blocked by Tor Browser. You can set Tor Browser's security level to **Standard** by clicking on the Shield icon. Alternatively, you can manually type in the two-factor secret (in FreeOTP, use the **Add token** option from the menu).

1.15.4 Daily Journalist Alerts About Submissions

When a SecureDrop has little activity and receives only a few submissions every other week, checking the *Journalist Interface* daily only to find there is nothing is a burden. It is more convenient for journalists to be notified daily via encrypted email about whether or not there has been submission activity in the past 24 hours.

If the email shows submissions were received, the journalist can connect to the *Journalist Interface* to get them.

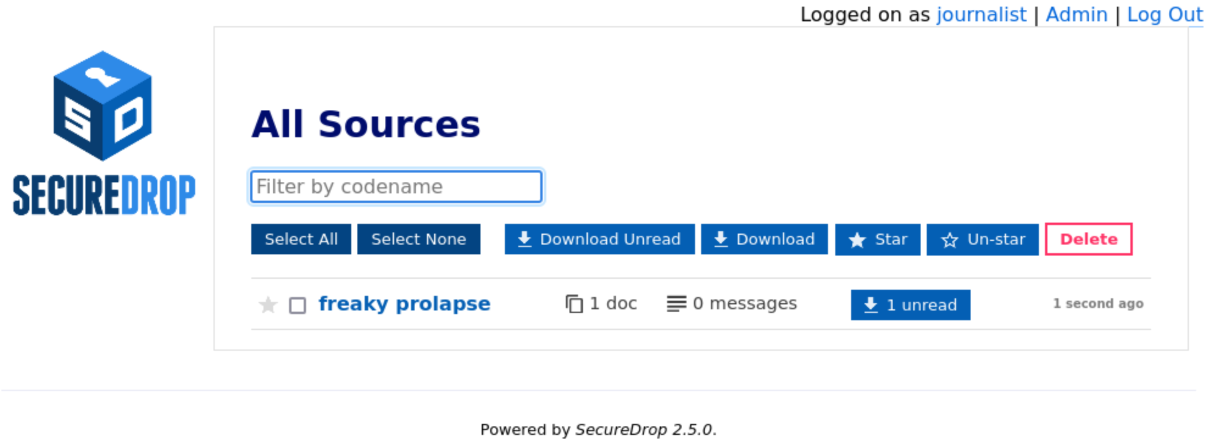
Note

For security reasons, the email will be sent every 24 hours, regardless of whether there are new submissions or not. The subject of the email will always be “Submissions in the past 24h”. To find out whether there were submissions or not, you must decrypt the contents of the email.

This is an optional feature that must be activated *by the administrator*. In the simplest case a journalist provides their email and GPG public key to the admin. If a team of journalist wants to receive these daily alerts, they should share a GPG key and ask the admin to setup a mail alias (SecureDrop does not provide that service) so they all receive the alerts and are able to decrypt them.

1.15.5 Interacting With Sources

If any sources have uploaded documents or sent messages, they will be listed on the homepage by codename.



Logged on as journalist | Admin | Log Out

All Sources

☆ □ freaky prolapse 1 doc 0 messages 1 unread 1 second ago

Powered by *SecureDrop 2.5.0*.

Note

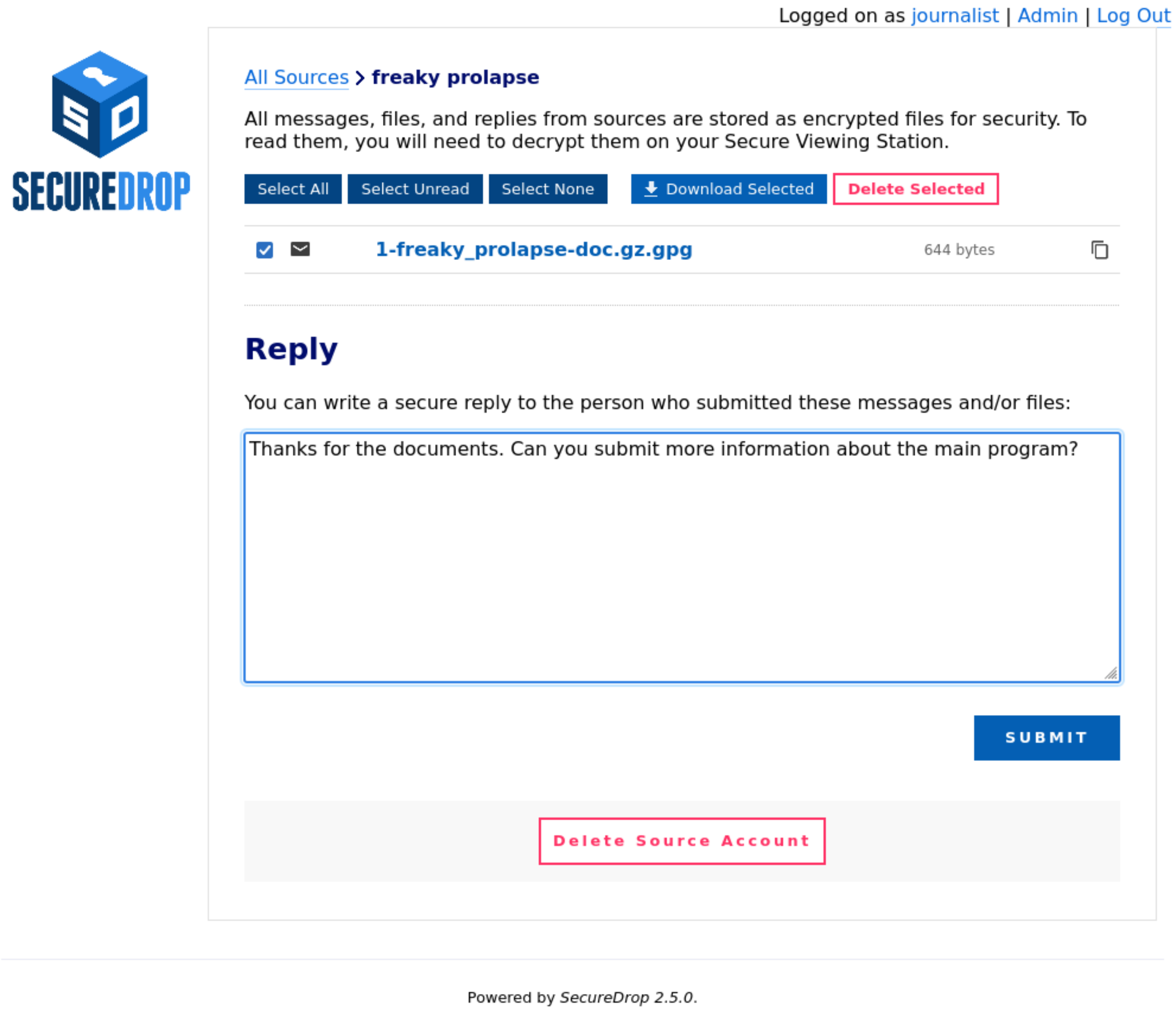
Codenames that journalists see are different than the codenames visible to sources.

Click on a codename to see the dedicated page for that source. You will see all of the messages that they have written and documents that they have uploaded.

Tip

You can also **Star** interesting or promising sources to easily return to them later. All starred sources will be bumped to the top of the list of sources.

If you want to reply to the source, write your message in the text field and click **Submit**.


Logged on as journalist | Admin | Log Out
SECUREDROP
All Sources > freaky prolapse
Select All
Select Unread
Select None
Download Selected
Delete Selected
1-freaky_prolapse-doc.gz.gpg
644 bytes
Reply
SUBMIT
Delete Source Account
Powered by SecureDrop 2.5.0.

All messages, files, and replies from sources are stored as encrypted files for security. To read them, you will need to decrypt them on your Secure Viewing Station.

You can write a secure reply to the person who submitted these messages and/or files:

Thanks for the documents. Can you submit more information about the main program?

Once your reply has been successfully submitted, you will be returned to the source page and see a message confirming that the reply was stored. The source will see your reply the next time they log in with their unique codename.

To minimize the impact of a source codename being compromised, the *Source Interface* encourages the source to delete the reply after reading it. Once a source has read your reply and deleted it from their inbox, a checkmark will appear next to the reply in the interface.

Note

Prior to SecureDrop 0.9.0, replies when deleted from the source inbox would also disappear from the journalist inbox. As such, if there are older conversations, there may be discontinuities in the conversation.

You may also delete replies if you change your mind after sending them.

Documents and messages are encrypted to the SecureDrop installation's *Submission Public Key*. In order to read the messages or look at the documents you will need to transfer them to the *Secure Viewing Station*, which holds the *Submission Private Key*. To recall the conversation history between your organization and sources, you can also download replies and transfer them to the *Secure Viewing Station* for decryption.

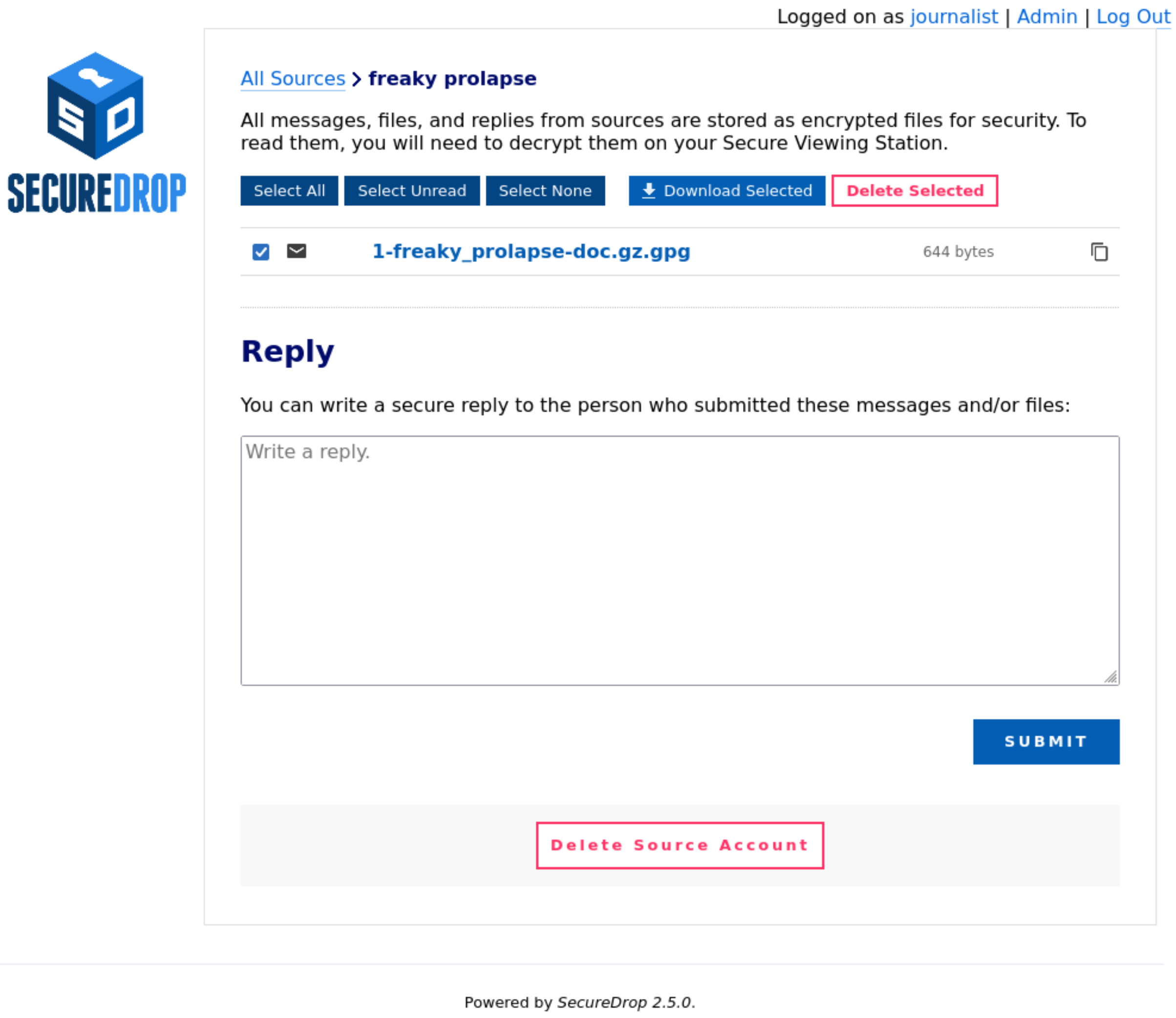
1.16 Using the Secure Viewing Station

1.16.1 Moving Documents to the *Secure Viewing Station*

Step 1: Download the encrypted submission

Documents and messages sent by sources can only be decrypted and viewed on the *Secure Viewing Station*. After clicking on an individual source, you will see a page with any documents or messages the source has sent you. Documents always end with `-doc.gz.gpg`, while messages always end with `-msg.gpg`.

Click on a document or message name to save it, or select a number of documents and save them all at once by clicking **Download Selected**.



Logged on as journalist | Admin | Log Out

All Sources > **freaky prolapse**

All messages, files, and replies from sources are stored as encrypted files for security. To read them, you will need to decrypt them on your Secure Viewing Station.

☑ ✉ 1-freaky_prolapse-doc.gz.gpg 644 bytes

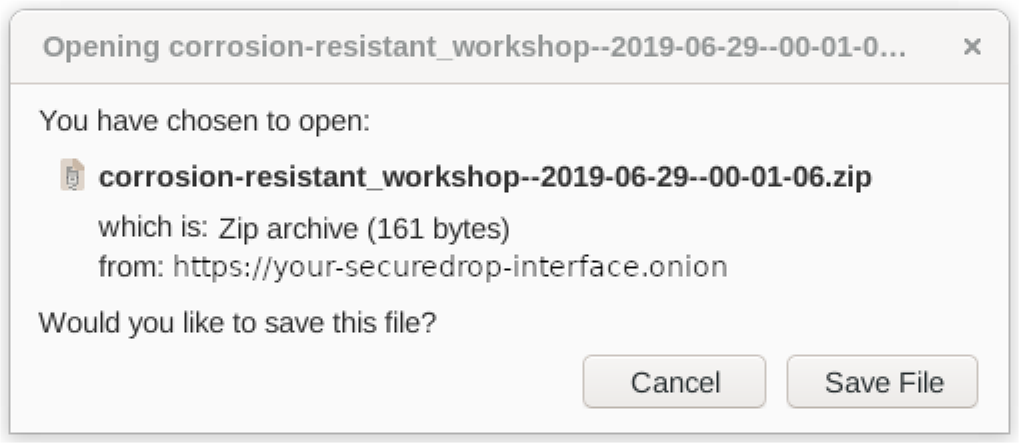
Reply

You can write a secure reply to the person who submitted these messages and/or files:

Write a reply.

Powered by *SecureDrop 2.5.0*.

A dialog box with two choices will appear, **Cancel** and **Save file**.



Opening corrosion-resistant_workshop--2019-06-29--00-01-0…

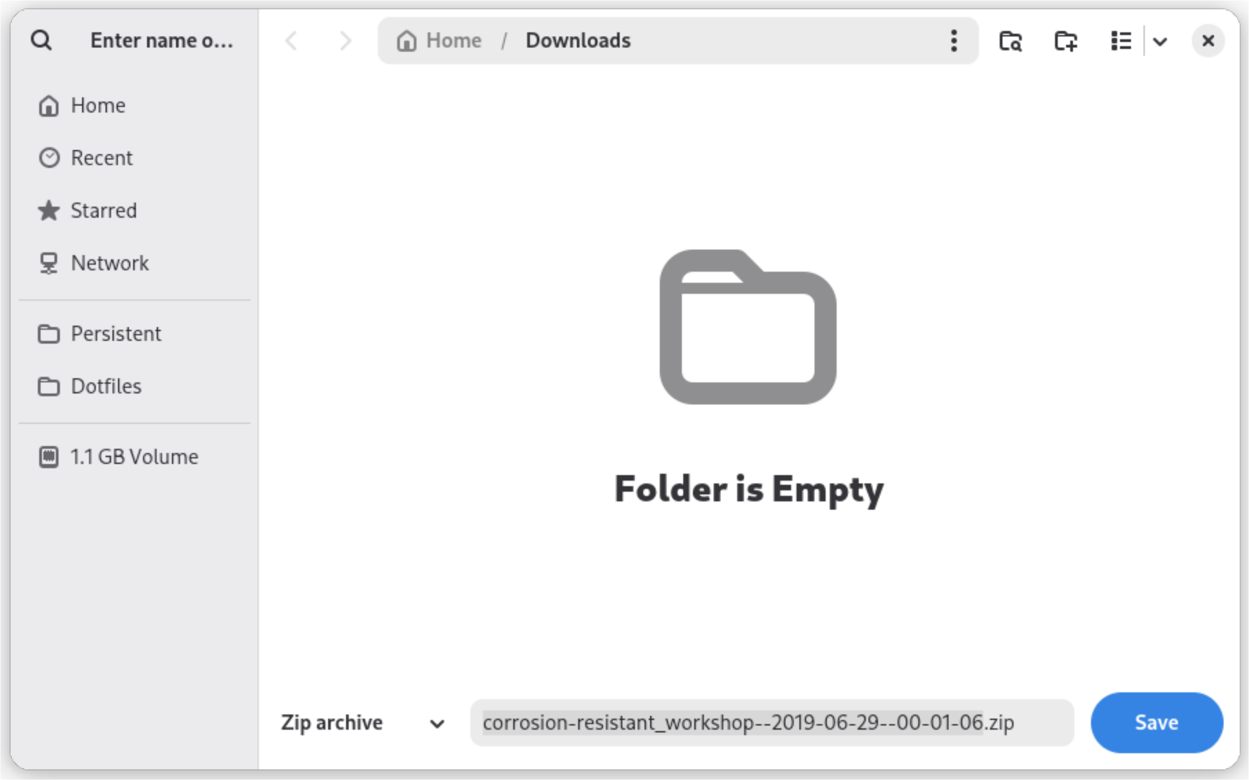
You have chosen to open:

corrosion-resistant_workshop--2019-06-29--00-01-06.zip

which is: Zip archive (161 bytes)
from: https://your-securedrop-interface.onion

Would you like to save this file?

Click **Save file**. In the save dialog, you can select the download location. The default location is the **Downloads** folder. You may also wish to save it to the **Persistent** folder, visible in the shortcuts column. Note that the name may be abbreviated; you can view the full name by hovering the mouse over the shortcut.



corrosion-resistant_workshop--2019-06-29--00-01-06.zip

The difference between these two folders is as follows:

- **Downloads**: Downloads saved to this folder will be stored in memory, which means that they will only be available for the duration of your current Tails session. The full path to this folder is `/home/amnesia/Downloads`.
- **Persistent**: Downloads saved to this folder will be stored on your Tails USB drive in the special persistent volume that is only available if you have unlocked it on the Tails welcome screen. The full path to this folder is `/home/amnesia/Persistent`.

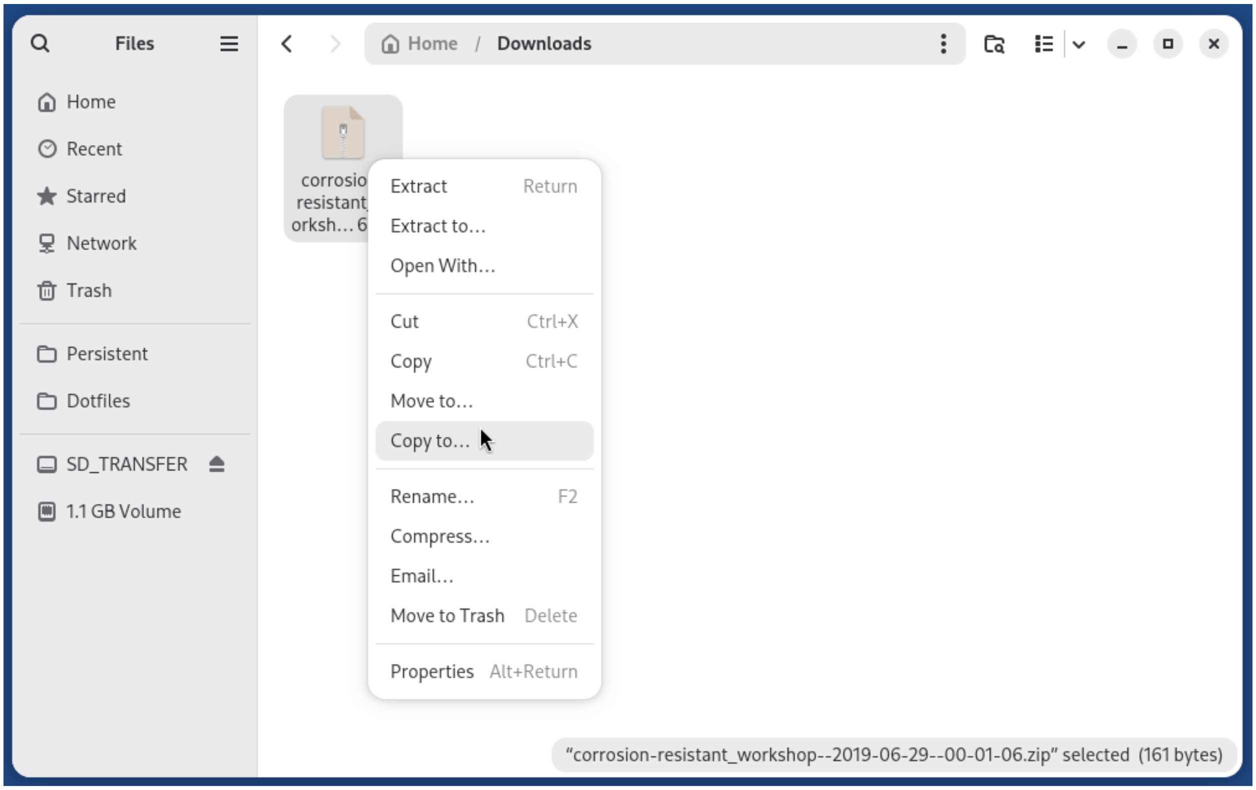
Unless you have a reason to store encrypted submissions on the *Journalist Workstation*, we recommend using the non-persistent “Downloads” folder. In the recommended process, you will now move the submission to the *Secure Viewing Station*, and there is no need to leave a persistent copy behind.

Step 2: Copy the encrypted submission to the *Transfer Device*

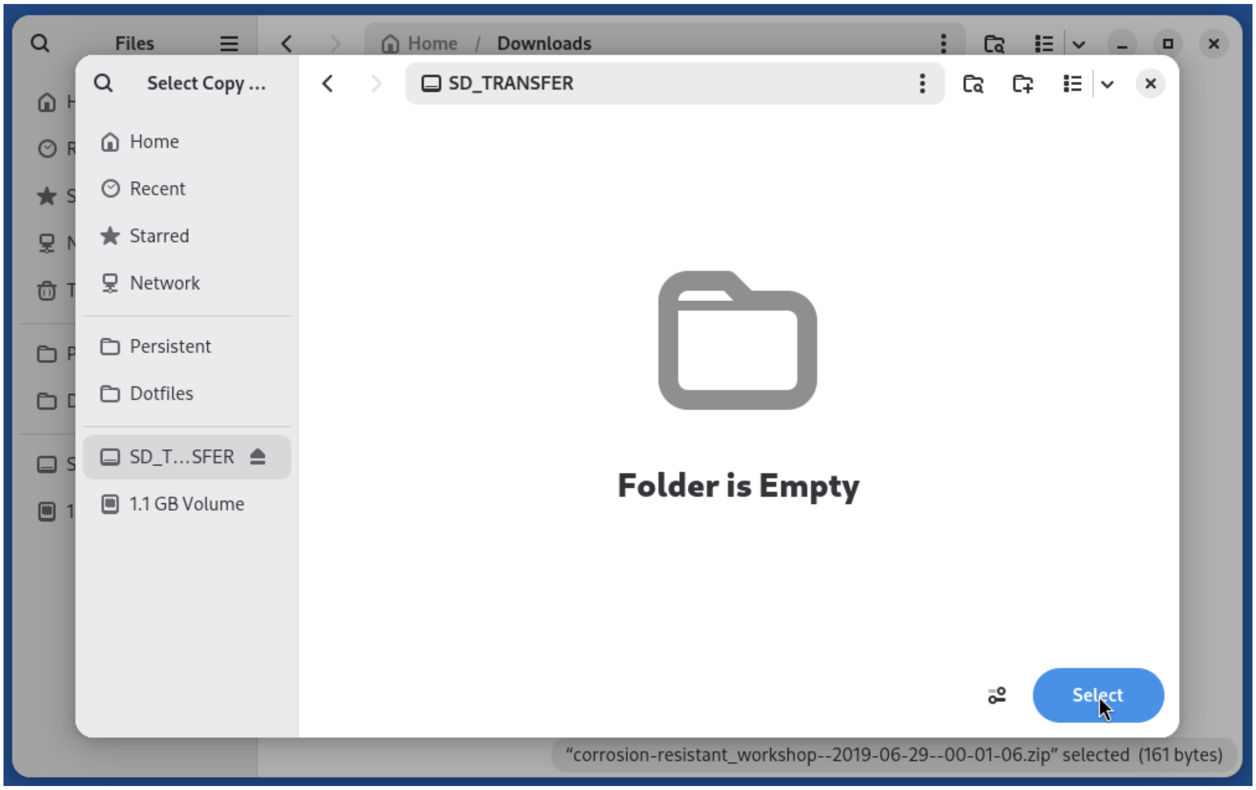
Once downloaded to either folder, move the document to the designated USB stick you intend to use to transfer the documents from your *Journalist Workstation* to the *Secure Viewing Station*. This storage device is known as your *Transfer Device*.

> **Note**
>
> If the *Transfer Device* was set up according to our recommendations, you will be prompted for a decryption passphrase on the *Journalist Workstation* and the *Secure Viewing Station* before being able to use it in a given session. We recommend storing this passphrase in your own personal password manager (e.g., on your smartphone), so that it is readily accessible to you whenever you need it.

You can right-click the file and select **Copy to**, then select the *Transfer Device* in the **Select Copy Destination** dialog.



"corrosion-resistant_workshop--2019-06-29--00-01-06.zip" selected (161 bytes)



Folder is Empty

"corrosion-resistant_workshop--2019-06-29--00-01-06.zip" selected (161 bytes)

This will leave a redundant copy behind in the "Downloads" folder. If you have downloaded the file to the non-persistent "Downloads" folder (as recommended), the redundant copy will disappear when the computer is shut down or rebooted.

"Eject" the *Transfer Device* by clicking the eject icon next to its name in the file manager. Wait for this operation to complete (the eject icon will disappear), then unplug the *Transfer Device*. "Ejecting" the drive in this manner ensures that all write operations are completed before you physically unplug it.

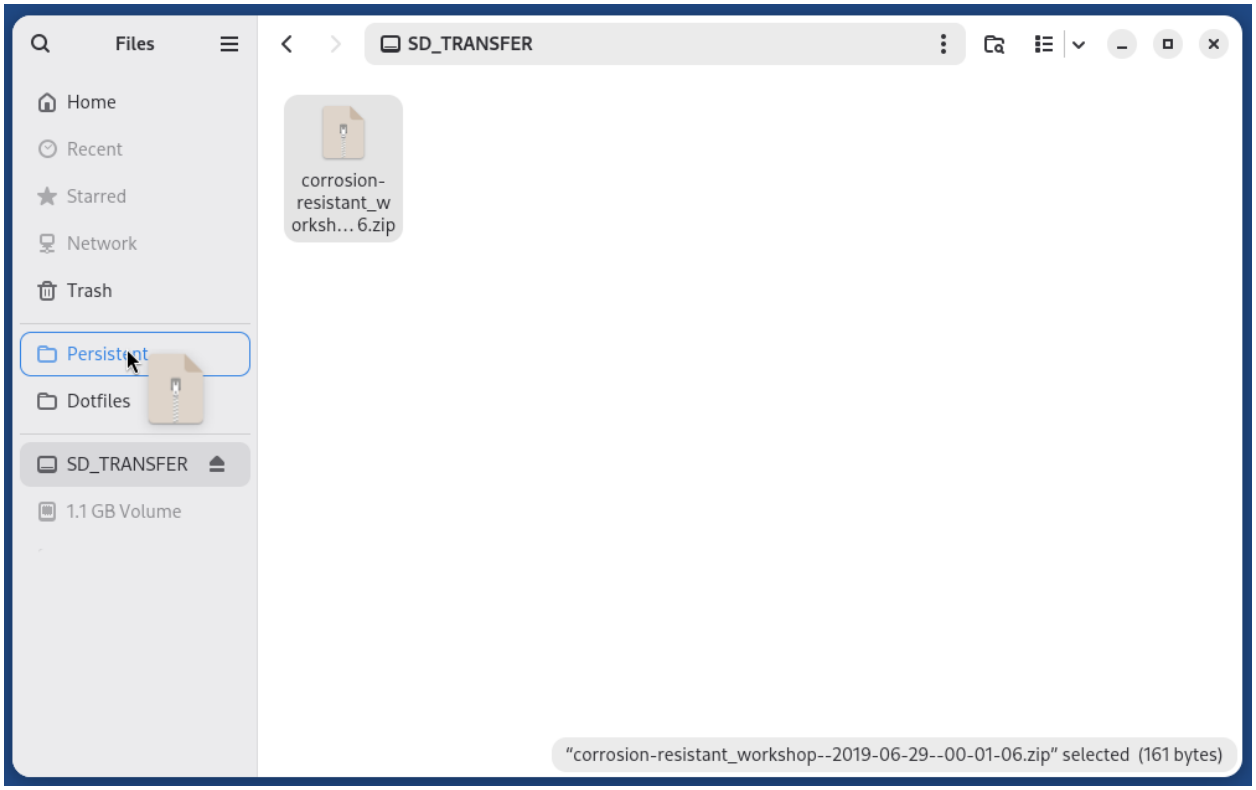
Step 3: Decrypt and view the submission on the *Secure Viewing Station*

Next, boot up the *Secure Viewing Station* using Tails and enter the passphrase for the *Secure Viewing Station* persistent volume. Once you have logged in, plug in the *Transfer Device*.

Note

The *Secure Viewing Station* and *Journalist Workstation* are on separate Tails USB drives.

Click on the **Home** icon on your desktop, then on the *Transfer Device*. Copy the file into your **Persistent** folder. You can do so by opening a new window with the **Persistent** folder and dragging the file from one window to another. A faster method is to drag the file to the **Persistent** shortcut in the list of places.



“corrosion-resistant_workshop--2019-06-29--00-01-06.zip” selected (161 bytes)

Important

Always copy submissions to the **Persistent** folder *before* decrypting them. Otherwise you might accidentally decrypt them on the USB stick, and they could be recoverable in the future.

After successfully copying them to the *Secure Viewing Station*, erase the files from your *Transfer Device*. Ensure you're viewing the *Transfer Device* folder, then right click on the files that need removal and click “Move to Trash”, then navigate to “Trash” folder in the sidebar, and select “Empty Trash”.

To decrypt and view documents or messages, return to your **Persistent** folder. All key actions are initiated by double-clicking:

- Double-clicking archives in ZIP or gzip format will invoke the **File Roller** application to extract the contents to the same location.
- Double-clicking decrypted messages or documents will attempt to open them in a default application suitable for the file type.
- On Tails 4, double-clicking files that end in `.gpg` will attempt to decrypt the contents to the same directory. If you have configured a passphrase for your *Submission Key*, you will be prompted for it.
- On Tails 5, double-clicking the `.gpg` file will launch an application called **Kleopatra**, from which you can decrypt the file and save the result to the same directory.
- On Tails 7.0, 7.1, 7.2, or 7.3, you will need to *first* open **Kleopatra** (**Apps** ▶ **Accessories** ▶ **Kleopatra**) before attempting to double-click any `.gpg` files.

Note

If you are using any of these versions, please contact your *Administrator* about upgrading to Tails 7.4 or later.

- On all other versions of Tails, double-clicking the `.gpg` file will decrypt the file and attempt to open them in a default application suitable for the file type.

If the default application does not work, you can right-click on the document and choose **Open with Other Application…** to try opening the document with LibreOffice Writer, Document Viewer, or another application. You might also need to right-click on a file and choose **Rename…** to rename a document with an incorrect or missing file extension.

Tip

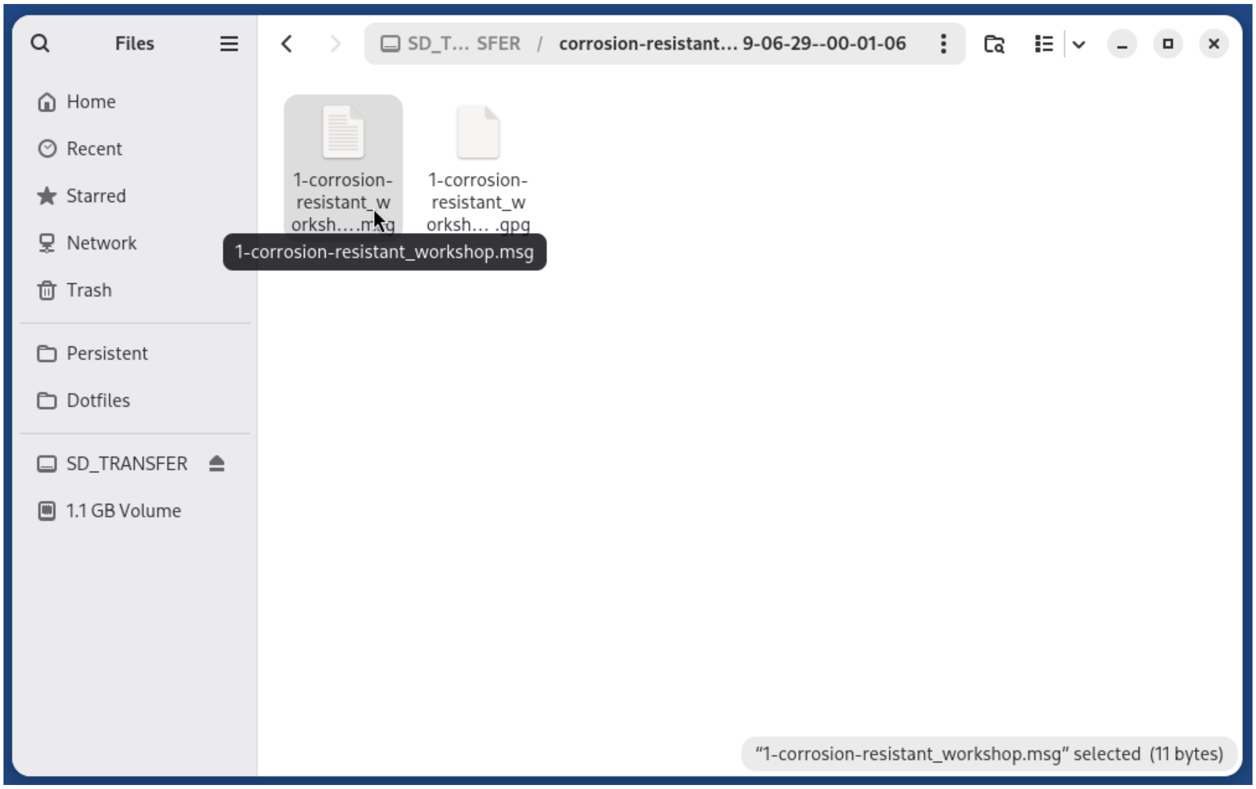
Always extract gzip archives with the *File Roller* application, which is the default when double-clicking the archive. Other methods may not preserve the filename contained in the archive.

For example, an archive called `1-artful_elevation-doc.gz` might contain a file `secrets.docx`, but if you extract the contents by right-clicking the archive and selecting **Extract here**, the extracted file will be called `1-artful_elevation-doc` instead of `secrets.docx`. This may result in problems when attempting to open the file due to the loss of its file extension.

Once you have extracted the archive, navigate to the folder containing the encrypted document message or document (ends with `.gpg`).

Double-click the file to decrypt it. On Tails 5.1 or greater, this will launch **Kleopatra**, from which you can decrypt the file and save the result to the same directory.

The decrypted file will have the same filename, but without `.gpg` at the end.


Files
SD_T… SFER / corrosion-resistant… 9-06-29--00-01-06
Home
Recent
Starred
Network
Trash
Persistent
Dotfiles
SD_TRANSFER
1.1 GB Volume
1-corrosion-resistant_worksh….msg
1-corrosion-resistant_worksh… .gpg
1-corrosion-resistant_workshop.msg

“1-corrosion-resistant_workshop.msg” selected (11 bytes)

You can now double-click on the decrypted file to open it in its default application.

1.17 Working with Documents

This section describes how to organize submissions, handle unusual file formats, safely research submissions, remove metadata, and mitigate risks from submitted malware.

Tip

This is only a very limited introduction. Freedom of the Press Foundation publishes and maintains digital security guides for journalists, many of which relate to these topics, and offers digital security training for news organization staff.

1.17.1 Organizing submissions

Whenever you download submissions using one of the **Download** buttons in the *Journalist Interface*, they will be organized as a ZIP archive with a built-in folder structure, which you can use as a template for organizing submissions on the *Secure Viewing Station*.

Submissions downloaded in this manner from the *list of all sources* will contain a structure like the following:

```
all
├── recessive accreditation
│   ├── 1_2019-07-07
│   │   └── 1-recessive_accreditation-msg.gpg
│   └── 2_2019-07-07
│       └── 2-recessive_accreditation-msg.gpg
└── surviving authentication
    ├── 1_2019-07-07
    │   └── 1-surviving_authentication-doc.gz.gpg
    └── 2_2019-07-07
        └── 2-surviving_authentication-msg.gpg
```

Submissions downloaded in this manner from the screen for an *individual source* will contain a similar structure, but without the parent folder `all`.

A folder like `1_2019-07-07` in the example above will always contain exactly one message or document. The numbers in the folder name (1, 2, etc.) correspond to the numbering in the *Journalist Interface*. The dates (2019-07-07 in the example above) are the day (in year/month/day format) of the last activity related to this source, at the time the archive was downloaded.

If you download messages or documents one at a time in the *Journalist Interface*, they will not be contained in a ZIP file at all. Instead, you will be dealing with individual files like `1-surviving_authentication-doc.gz.gpg`, without a folder structure.

1.17.2 Handling File Formats

SecureDrop accepts submissions of any file type. Tails comes with pre-installed applications for securely working with documents, including an office suite, graphics tools, desktop publishing tools, audio tools, and printing and scanning tools.

For more information, visit the Tails guide to working with sensitive documents.

1.17.3 Pre-Encrypted Submissions

SecureDrop sources can optionally encrypt prior to submitting to SecureDrop. This means that once you decrypt the document as you usually do by double clicking the document in the file manager, there will be another layer of encryption.

Most often, the file will be encrypted to the SecureDrop key. If the file is encrypted to your SecureDrop key, you should be able to double click the file as usual once more in the SVS and it should decrypt.

However, it's also possible the file is encrypted to another key, potentially your personal key. If this occurs, you will get an error message in Tails that reads "Decryption failed. You probably do not have the decryption key". To determine which key was used, if you are comfortable at the command line, you can open the `Terminal`, navigate to the file, and use:

```
gpg --decrypt NAME_OF_FILE
```

replacing `NAME_OF_FILE` with the name of the file you wish to decrypt. This command will tell you what key was used to encrypt the file. If you are not comfortable at the command line, contact your SecureDrop admin or Freedom of the Press Foundation for assistance.

Warning

Do not transfer source material off the *Secure Viewing Station* for decryption. Instead, transfer cryptographic keys *to* the SVS device for decryption and metadata removal.

1.17.4 Researching Submissions

Journalists should take care to research submissions using the Tor Browser, ideally in a new Tails session on your *Journalist Workstation* for highly sensitive submissions.

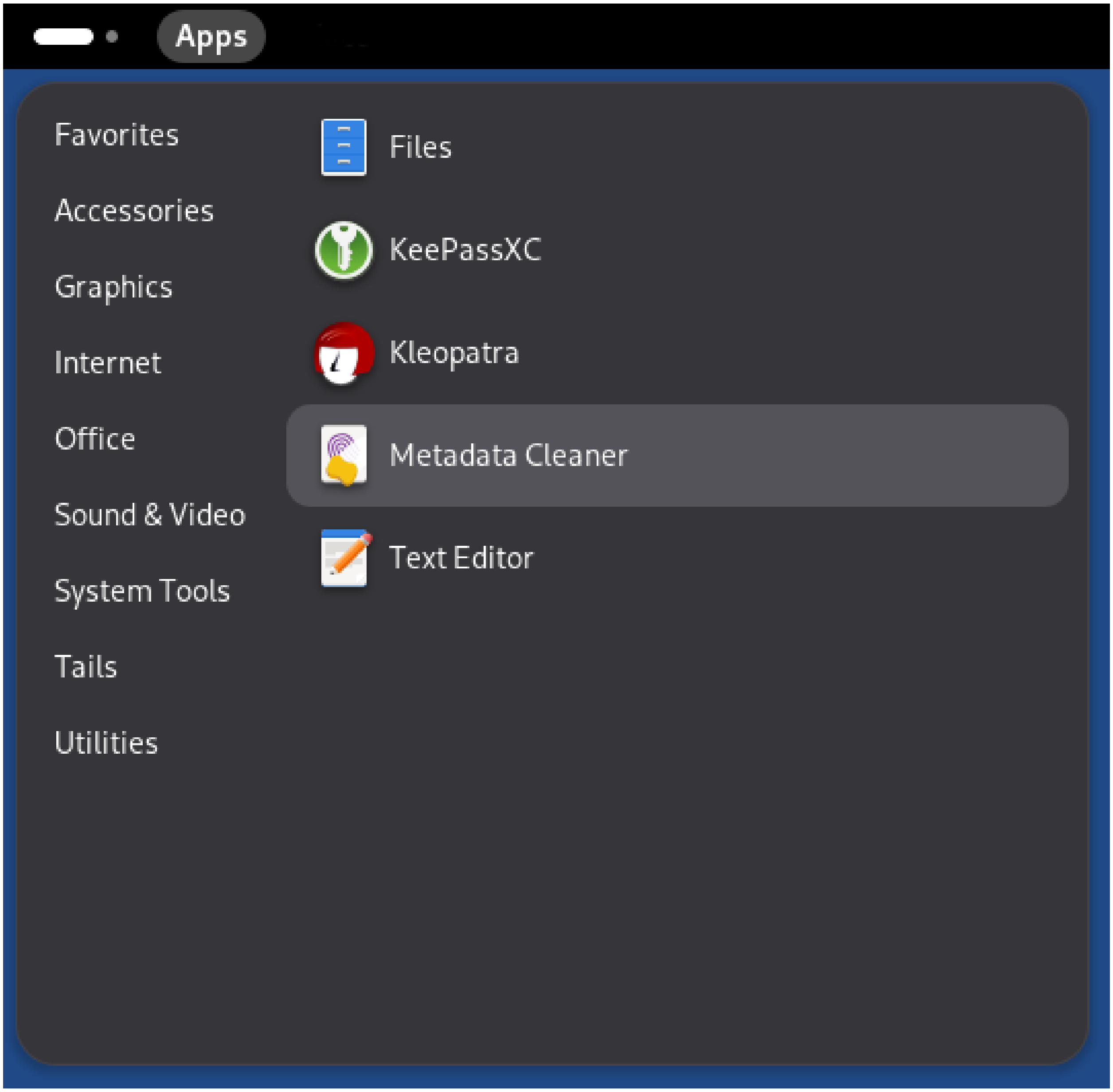
1.17.5 Removing Metadata

Tip

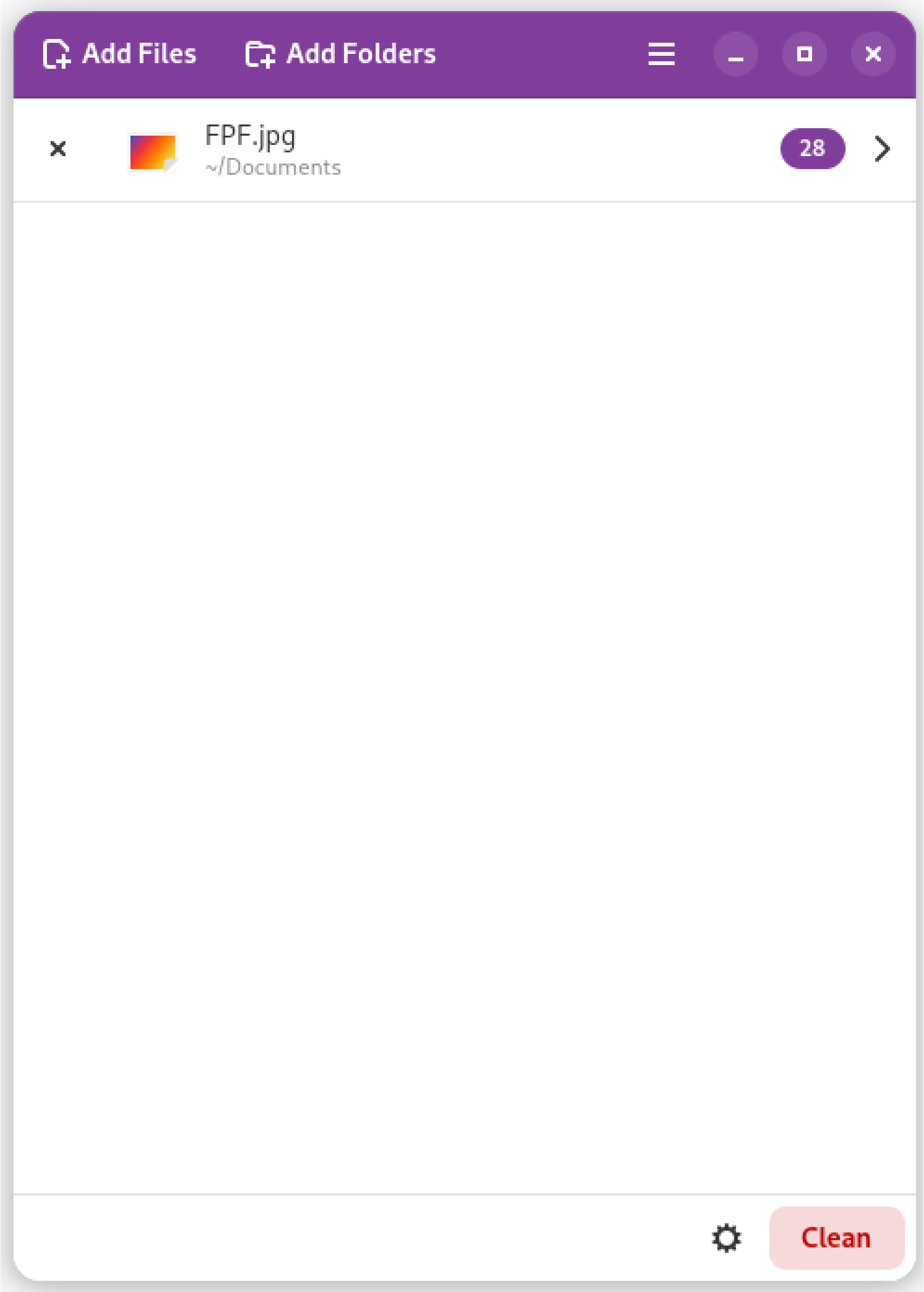
For detailed information about removing metadata from documents, check out this in-depth guide to removing metadata.

Tails comes with the Metadata Anonymisation Toolkit 2 (MAT2) that is used to help strip metadata from a variety of types of files, including png, jpg, OpenOffice/LibreOffice documents, Microsoft Office documents, pdf, tar, tar.bz2, tar.gz, zip, mp3, mp2, mp1, mpa, ogg, and flac. We recommend using this and other tools to work with documents within Tails for as much of your workflow as possible.

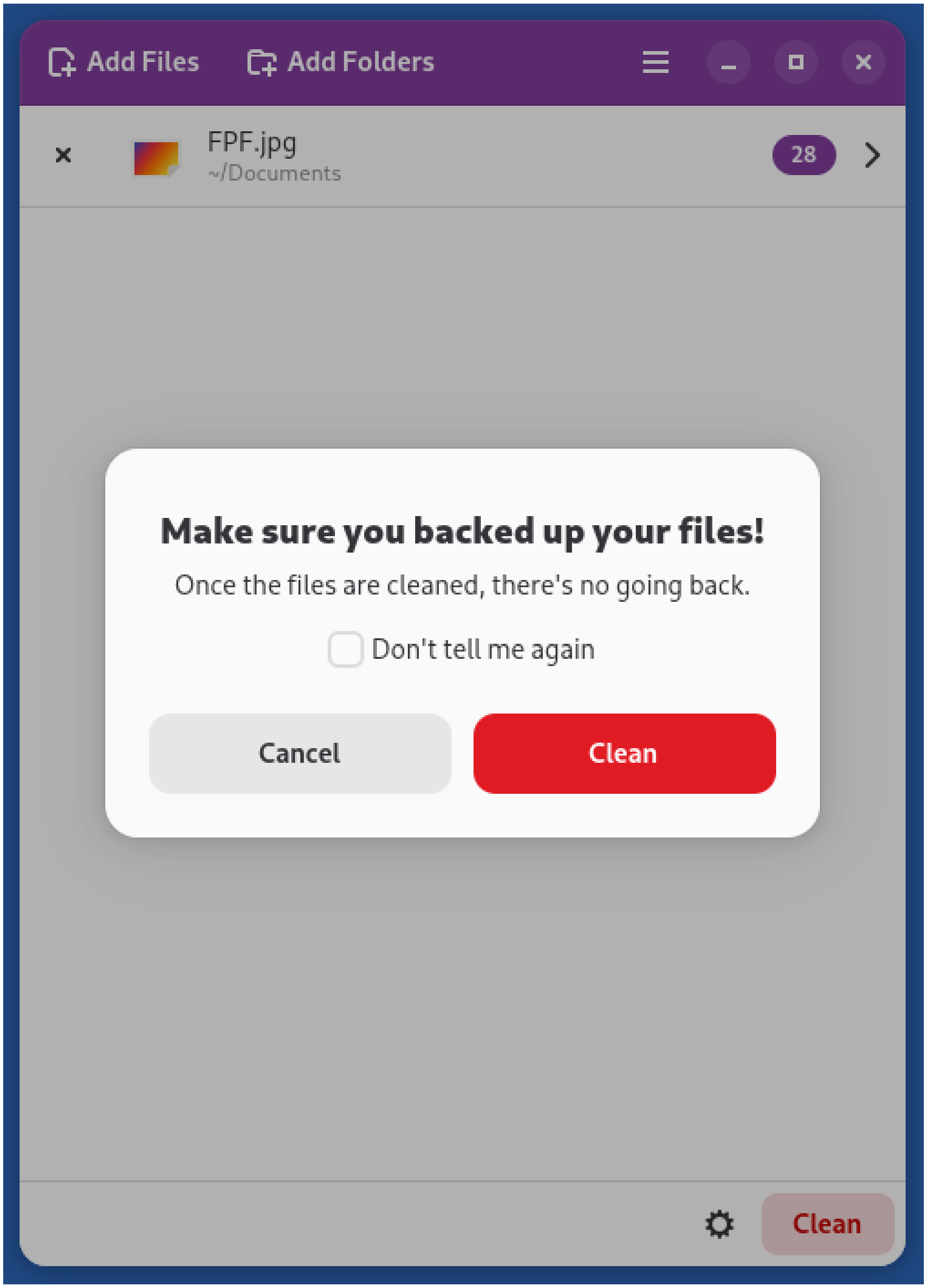
You can use MAT2 via the *Metadata Cleaner* application which is found in the **Accessories** section of the **Apps** menu.



You can load individual files or folders into *Metadata Cleaner* by clicking **Add Files** or **Add Folders**. *Metadata Cleaner* gives you a count of how many metadata parameters are associated with each file and lets you view the metadata.



You can select **Clean** to remove the metadata from the files. Note that this process deletes the original files, leaving only the cleaned versions.

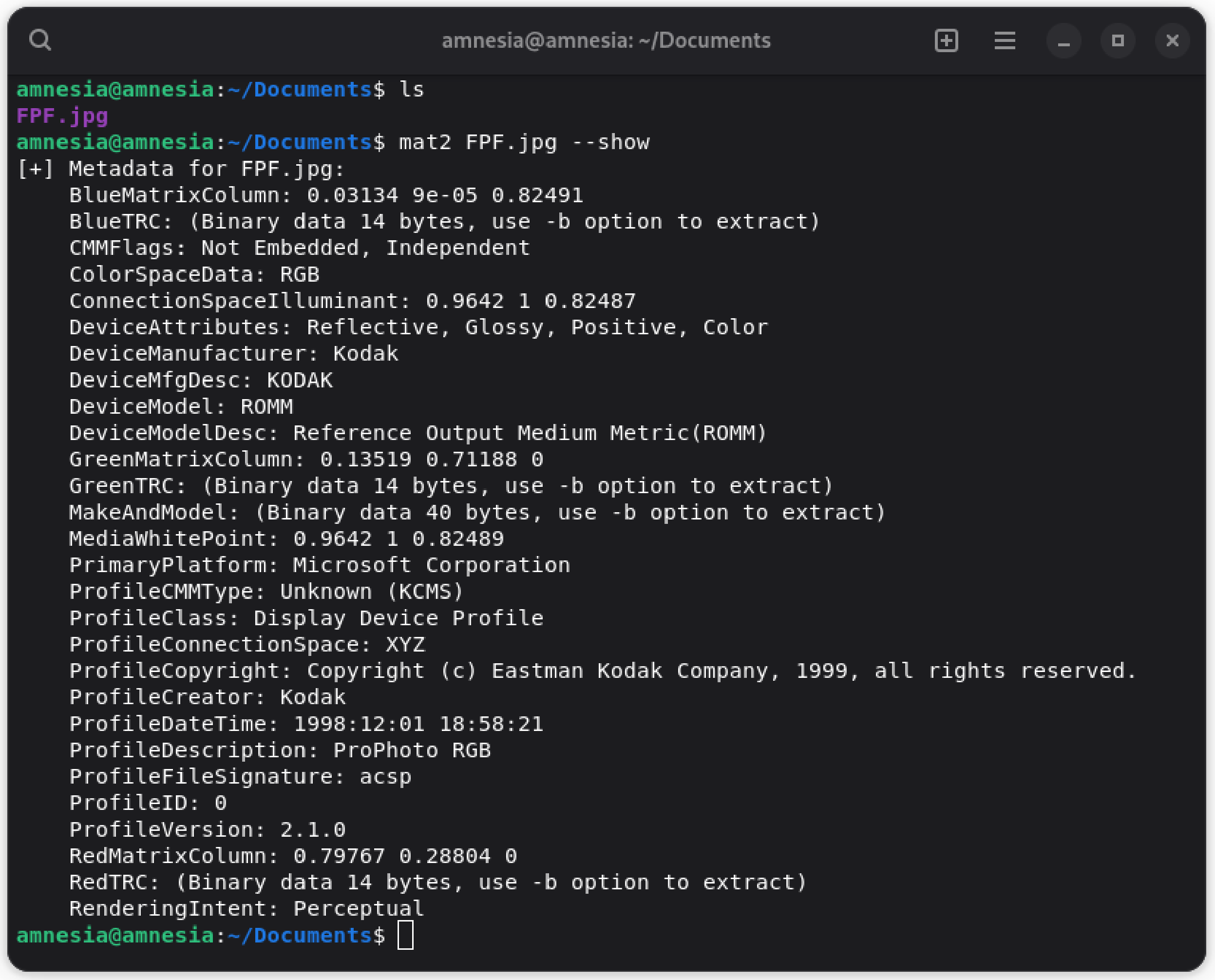


Make sure you backed up your files!

Once the files are cleaned, there's no going back.

□ Don't tell me again

To use MAT2 on the command line, type `man mat2` to see a list of available actions you can take with MAT2. For example, you can view the metadata of a file with `mat2 filename --show`.



```
amnesia@amnesia:~/Documents$ ls
FPF.jpg
amnesia@amnesia:~/Documents$ mat2 FPF.jpg --show
[+] Metadata for FPF.jpg:
    BlueMatrixColumn: 0.03134 9e-05 0.82491
    BlueTRC: (Binary data 14 bytes, use -b option to extract)
    CMMFlags: Not Embedded, Independent
    ColorSpaceData: RGB
    ConnectionSpaceIlluminant: 0.9642 1 0.82487
    DeviceAttributes: Reflective, Glossy, Positive, Color
    DeviceManufacturer: Kodak
    DeviceMfgDesc: KODAK
    DeviceModel: ROMM
    DeviceModelDesc: Reference Output Medium Metric(ROMM)
    GreenMatrixColumn: 0.13519 0.71188 0
    GreenTRC: (Binary data 14 bytes, use -b option to extract)
    MakeAndModel: (Binary data 40 bytes, use -b option to extract)
    MediaWhitePoint: 0.9642 1 0.82489
    PrimaryPlatform: Microsoft Corporation
    ProfileCMMType: Unknown (KCMS)
    ProfileClass: Display Device Profile
    ProfileConnectionSpace: XYZ
    ProfileCopyright: Copyright (c) Eastman Kodak Company, 1999, all rights reserved.
    ProfileCreator: Kodak
    ProfileDateTime: 1998:12:01 18:58:21
    ProfileDescription: ProPhoto RGB
    ProfileFileSignature: acsp
    ProfileID: 0
    ProfileVersion: 2.1.0
    RedMatrixColumn: 0.79767 0.28804 0
    RedTRC: (Binary data 14 bytes, use -b option to extract)
    RenderingIntent: Perceptual
amnesia@amnesia:~/Documents$ 
```

You can create a "clean" version of the file with `mat2 filename`, noting that this does not erase the metadata on the original file but instead creates a new cleaned copy. Use the `--inplace` flag if you wish to delete the original file and leave only a cleaned version.

Note that even after running MAT2, you should carefully inspect files to ensure that all metadata has been wiped, or convert them to a simpler file format (for example, converting a `.xls` file to a `.csv`) to ensure that metadata is not left behind in error.

1.17.6 Risks From Malware

SecureDrop does not scan for or remove malware in submissions you receive. There are important steps you can take to protect yourself:

1. **Keep the version of Tails on your Secure Viewing Station up-to-date.**

   Tails offers more protection against compromise than your everyday computer, and the air-gap prevents potential malware from "phoning home." But if the version of Tails is outdated, an attacker can still attempt to exfiltrate or destroy information.

2. **Print documents from the Secure Viewing Station instead of exporting them digitally, whenever possible.**

   Printing documents prevents the proliferation of malware to your everyday workstation, and eliminates most categories of embedded metadata. Note that printing a document may still preserve watermarks, printer codes, steganographically encoded data, or other information not visible to the naked eye.

3. **Consult with your administrator or your digital security staff before copying files digitally.**

   If you must copy a file in digital form (because of its format, the volume of information, or for other reasons), we recommend taking the time to consult with technical experts within the organization.

   > **Tip**
   >
   > Converting files to simpler formats (e.g., PDF to PNG) can help reduce the risk of malware. Tails provides both graphical and command-line utilities that can be used for this purpose.

4. **Never scan QR codes embedded in documents using a network-connected device.**

   QR codes can contain malicious links that your device will automatically visit. This can alert third-parties to your actions, reveal the identities of your sources, and breach the air gap that is in place with the *Secure Viewing Station*.

   In general, be careful when opening any links provided in a SecureDrop submission. If you are unsure if a link is safe to click, you should consult internally, or contact Freedom of the Press Foundation for assistance.

5. **Don't photograph submissions using your smartphone, and be careful with all digital photography**.

   Many smartphones are configured to back up photographs to cloud services, immediately or intermittently; newer digital cameras have similar functionality. Not all backup settings may be visible to you.

   Any digital photograph will include certain metadata by default, which may reveal sensitive information about your SecureDrop usage patterns (potentially including GPS coordinates) to anyone who gains access to the file.

> **Warning**
>
> If you have not memorized the passphrases to unlock the USB drives for the *Secure Viewing Station* or the *Transfer Device*, you may need to access a password manager on your phone or laptop to do so. We recommend switching any required electronic devices into airplane mode, and securely storing any devices you do not need outside the environment in which you access the *Secure Viewing Station*. This further mitigates the risk of accidentally compromising the air-gap.

Fully mitigating the risks of malware received via SecureDrop is beyond the scope of this documentation. If you have questions, you can contact us at securedrop@freedom.press (GPG encrypted) or via the support portal. Please do **NOT** disclose details about the contents of any submission you have received.

Moving Documents to Your Everyday Workstation

> **Important**
>
> As noted above, SecureDrop does not scan for or remove malware. If the file you received contains malware targeting the operating system and applications running on your everyday workstation, copying it in its original form carries the risk of spreading malware to that computer. Make sure you understand the risks, and consider other methods to export the document (e.g., print).

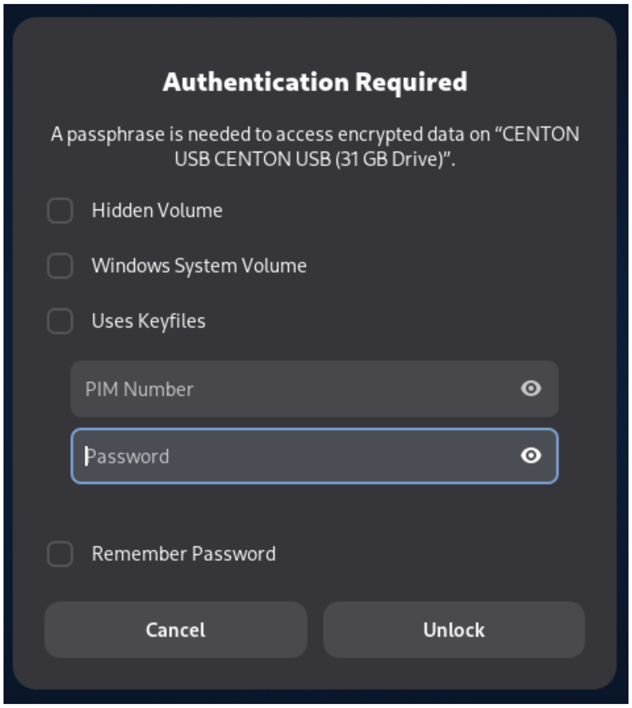
If you must copy a file from your *Secure Viewing Station* to your everyday workstation in digital form, our *recommendation* is that journalists are provided with an *Export Device*, typically a USB drive, which is encrypted using VeraCrypt. These instructions assume that you are following the recommended workflow. If you are unsure, ask your administrator.

Note

VeraCrypt support was added to Tails in version 3.9. We strongly recommend keeping your *Secure Viewing Station* up-to-date with each release of Tails.

To open the *Export Device* on the *Secure Viewing Station*, follow these steps:

1. If your *Export Device* has a physical write protection switch, make sure it is in the *unlocked* position.
2. Plug the *Export Device* into the *Secure Viewing Station*.
3. Enter your passphrase, which we recommend keeping in your own personal password manager (e.g., on your smartphone), not on *KeePassXC*.



Authentication Required

A passphrase is needed to access encrypted data on "CENTON USB CENTON USB (31 GB Drive)".

☐ Hidden Volume

☐ Windows System Volume

☐ Uses Keyfiles

PIM Number

Password

☐ Remember Password

4. Click Unlock.

The *Export Device* should now open in the file manager. If there are still files on the *Export Device* from your last copy operation, delete them by moving them to the Trash, and then selecting **Empty Trash**.

Copy the file or files you want to access on your everyday workstation to the *Export Device* using the file manager.

Decrypting and Preparing to Publish

Note

To decrypt a VeraCrypt drive on a Windows or Mac workstation, you need to have the *VeraCrypt* software installed. If you are unsure if you have the software installed or how to use it, ask your administrator, or see the Freedom of the Press Foundation guide for working with VeraCrypt.

To access the *Export Device* on your everyday workstation, follow these steps:

1. If your *Export Device* has a physical write protection switch, make sure it is in the *locked* position.

2. Plug the *Export Device* into your everyday workstation.
3. Launch the *VeraCrypt* application.
4. Click **Select Device** and select the *Export Device*, then click **OK**.
5. Click **Mount**.
6. Enter the passphrase for your *Export Device*. You should find this in your own personal password manager.
7. Open the *Export Device* in your operating system's file manager, and copy the contents of interest to your everyday workstation.

As a security precaution, we recommend deleting the files on the *Export Device* after each copy operation. If you are using write protection, you have to perform this step on the *Secure Viewing Station* to get the security benefits of write protection.

When you are done, switch back to the *VeraCrypt* window, and click **Dismount**.

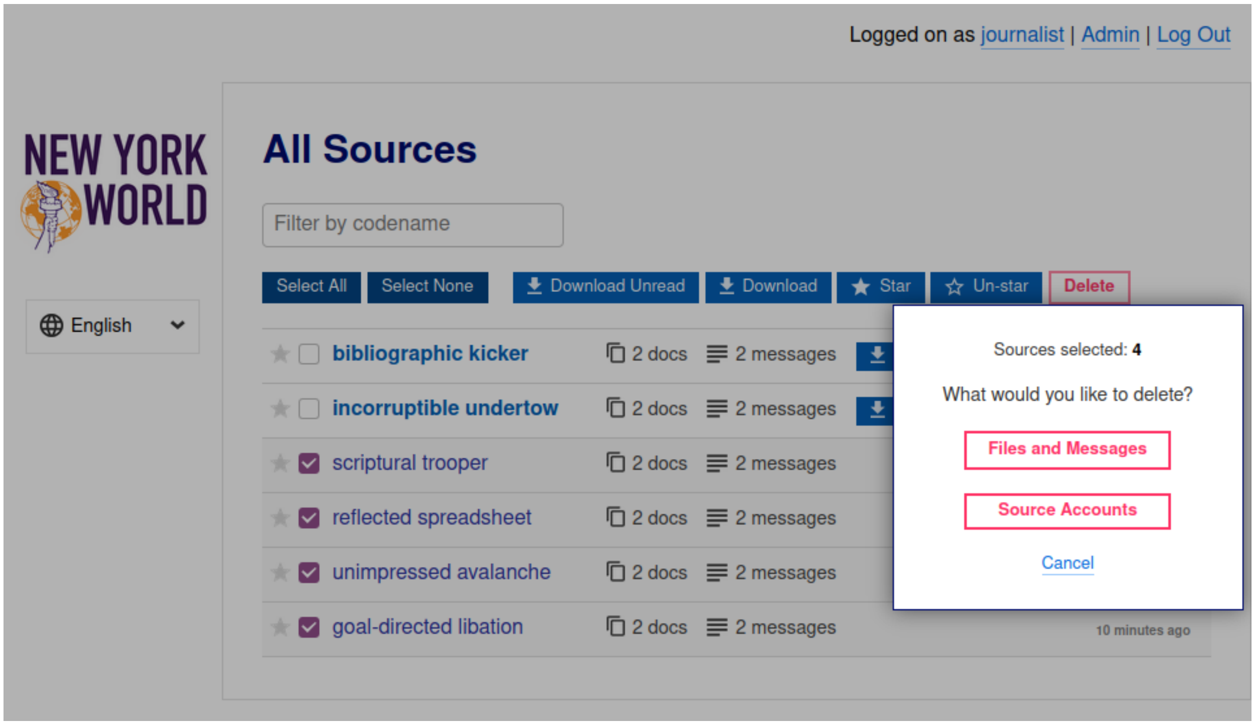
You are now ready to write articles and blog posts, edit video and audio, and begin publishing important, high-impact work!

> **Tip**
>
> Check out our SecureDrop *Promotion Guide* to read about encouraging sources to use SecureDrop.

Deleting submissions and source accounts

As part of routine SecureDrop usage, we recommend that you establish data retention practices consistent with your organization's threat model, data lifecycle and data retention policies. Regularly deleting submissions and source accounts can mitigate risks in the event that your SecureDrop servers or a source's account details are compromised.

To delete sources, first select them in the list of all sources in the *Journalist Interface*, then click the **Delete** button. You will be given a choice to delete all messages and files for the selected sources, or to delete the source accounts.



	Source	Docs	Messages
☆ □	bibliographic kicker	2 docs	2 messages
☆ □	incorruptible undertow	2 docs	2 messages
☆ ☑	scriptural trooper	2 docs	2 messages
☆ ☑	reflected spreadsheet	2 docs	2 messages
☆ ☑	unimpressed avalanche	2 docs	2 messages
☆ ☑	goal-directed libation	2 docs	2 messages

10 minutes ago

Sources selected: **4**

What would you like to delete?

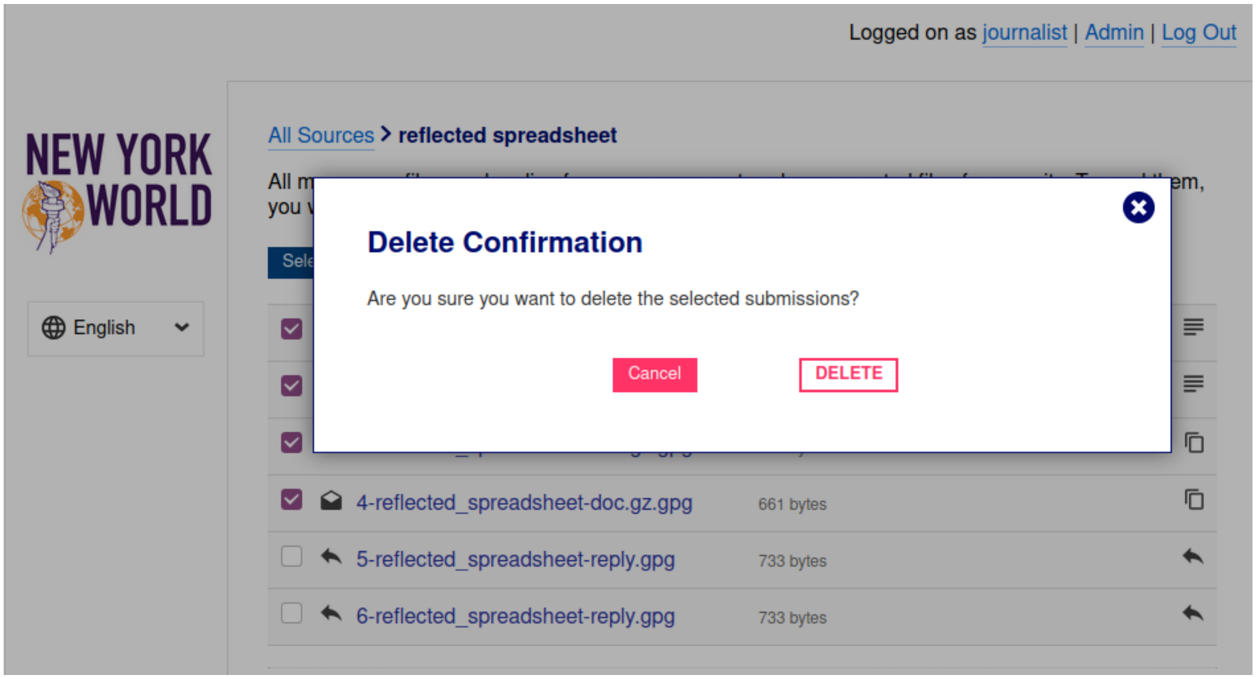
If you delete messages and files for a source, the source will continue to appear in the list of sources in the *Journalist Interface*, and they will still be able to log into the *Source Interface* using their codename. Consider using this option as part of regular deletion of reviewed submissions, especially if you are not sure that all communication with the source has concluded.

> **Note**
>
> If you delete all messages and files, that includes all replies you have sent to the source, even if the source has not seen them yet. You will still be able to send new replies.

If you delete the entire source account, the source will not be able to log in again using their codename, and all information about them will be destroyed. Consider using this option if it is clear that all communication with the source has concluded, or if the source has requested that all information about them and their submissions should be removed.

You can more selectively delete source submissions and journalist replies by clicking the source's two-word designation in the list of all sources. You will see a list of source messages (filenames end with `-msg.gpg`), file submissions (filenames end with `-doc.gz.gpg`) and journalist replies (filenames end with `--reply.gpg`).

Select the source data you wish to delete, then click the **Delete** button. You will be prompted for confirmation.



Logged on as journalist | Admin | Log Out
NEW YORK WORLD
English
All Sources > reflected spreadsheet
Cancel
DELETE

Delete Confirmation

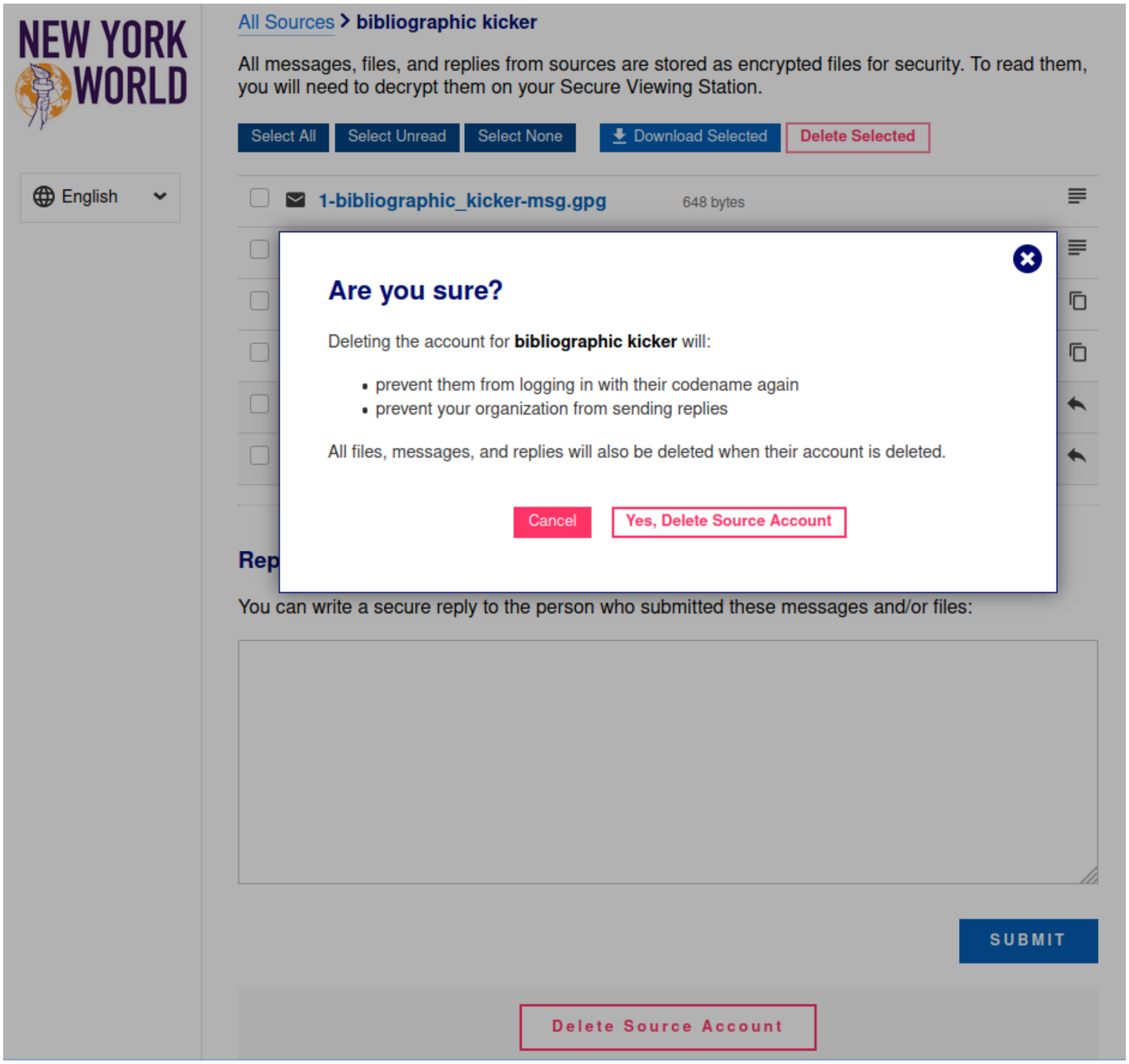
Are you sure you want to delete the selected submissions?

☑ 4-reflected_spreadsheet-doc.gz.gpg 661 bytes

□ 5-reflected_spreadsheet-reply.gpg 733 bytes

□ 6-reflected_spreadsheet-reply.gpg 733 bytes

From the same page, you also have the option to delete the entire source account. To do so, click the button labeled **Delete Source Account** at the bottom of the page. You will be prompted for confirmation.



All messages, files, and replies from sources are stored as encrypted files for security. To read them, you will need to decrypt them on your Secure Viewing Station.

Are you sure?

Deleting the account for **bibliographic kicker** will:

- prevent them from logging in with their codename again
- prevent your organization from sending replies

All files, messages, and replies will also be deleted when their account is deleted.

You can write a secure reply to the person who submitted these messages and/or files:

1.18 SecureDrop for Administrators

Note

SecureDrop wants your feedback! Confused by something in our documentation? Let us know by opening an issue on GitHub or in our Gitter channel.

SecureDrop servers are managed by a systems administrator.

For larger newsrooms, there may be a team of systems admins, but at least one person within the organization will need to serve as the administrator. In some situations, such as smaller news organizations where a journalist has the technical capacity to administer systems, one person can serve as both Journalist and Administrator. When possible, we advise having a dedicated staff member serving the role of SecureDrop Administrator.

The admin uses a dedicated *Admin Workstation* running Tails, connects to the *Application* and *Monitor Servers* over authenticated onion services, and manages them using Ansible.

If you are considering becoming a SecureDrop administrator, below are some attributes that will be important to have:

- Experience with managing Linux-based systems from the command line.
- Proficiency with network hardware such as firewalls and switches (e.g. pfSense).
- Experience with configuration management tools such as Ansible, Salt, Chef, or Puppet.
- Ability to use and configure secure communication tools such as GPG.

We consider the first two requirements and the second two preferred attributes.

This Admin Guide will walk you through the entire experience, from planning to installation to deployment, and will also provide reference materials to help ensure that your servers remain up-to-date and in proper working order.

1.19 Responsibilities

The SecureDrop architecture contains multiple machines and hardened servers. While many of the installation and maintenance tasks have been automated, a skilled Linux admin is required to responsibly run the system.

1.19.1 Responsibilities of SecureDrop administrators

As a SecureDrop administrator, it is your responsibility to:

- *install SecureDrop*
- *manage users*
- *manage the system configuration*
- *ensure that servers, firewall and workstations are kept up-to-date*
- *monitor OSSEC alerts*
- *monitor the SecureDrop team's release and security-related communications*
- apply available firmware updates to all SecureDrop hardware
- ensure that the SecureDrop environment is physically secure and monitored
- investigate and respond to security incidents
- schedule and perform required maintenance tasks, such as operating system upgrades
- ensure that SecureDrop users adhere to the documented processes for checking SecureDrop, communicating with sources, and reviewing documents
- verify the integrity of SecureDrop code
- avoid the installation of unsupported code or patches
- *decommission SecureDrop after it is no longer in use*

1.19.2 Responsibilities of the SecureDrop team

The SecureDrop team employed by Freedom of the Press Foundation (FPF) and the SecureDrop community maintain and develop the SecureDrop software, which is offered as open source software, free of charge, and at your own risk.

FPF offers *paid priority support services*. We are happy to provide assistance with installing the system, with training of administrators and journalists, and with investigation of technical issues and incidents.

Note

Each SecureDrop instance is hosted and operated independently. Freedom of the Press Foundation does not offer systems administration, hosting or "remote hands" services.

When the SecureDrop team becomes aware of a security vulnerability in SecureDrop or its software dependencies, we assess the impact of the vulnerability in the context of existing security mitigations and *our threat model*. Based on this assessment, we prioritize technical work and external communications.

For high severity issues that require technical changes to SecureDrop, we will issue a point release as soon as possible. As part of issuing a release or advisory, we will post further details on the SecureDrop website and to the support portal.

In rare circumstances when a technical fix is extremely time sensitive, we may provide signed patches to impacted SecureDrop instances. Even in these cases, we ask that you never install code provided to you that is not signed using the current SecureDrop release key.

When in doubt how to resolve an issue, please avoid following technical instructions that have not been vetted by the SecureDrop team. If you encounter bugs, please report them. For sensitive matters, you can contact us via the SecureDrop Support Portal or via our contact form.

1.19.3 Managing Users

Admins are responsible for managing user credentials and encouraging best practices. (See *Passphrases* and *Passphrase Best Practices*.) The admin will also have access to the *Journalist Interface*, via her own username, passphrase, and two-factor authentication method (using a smartphone application or YubiKey).

See *User Management* for more information on adding and managing users.

1.19.4 Managing the System Configuration

Admins are responsible for configuring and maintaining the system. Several tools are available to support this:

- *The Admin Interface* allows the admin to manage users and configure web interface features such as organizations logos and submission preferences
- *Server SSH access* is also available, to allow administrators to troubleshoot server issues and perform manual updates.
- *The securedrop-admin utility* is used via the *Admin Workstation* to configure and install SecureDrop, to perform operations including server backups and restores, and to update the server configuration after installation.

1.19.5 Keeping the System Updated

The admin is responsible for ensuring that updates are applied to SecureDrop. Where possible, updates are applied automatically, but some update operations require manual intervention.

Updates: Servers

The admin should be aware of all SecureDrop updates and take any required manual action if requested in the SecureDrop Release Blog (RSS feed). We also recommend registering with the SecureDrop Support Portal to stay apprised of upcoming releases.

Most often, the SecureDrop servers will automatically update via `apt`. However, occasionally you will need to run `securedrop-admin install` or take other manual steps. If you are onboarded to the support portal, we will let you know in advance of major releases if manual intervention will be required.

Updates: Network Firewall

Given all traffic first hits the network firewall as it faces the non-Tor public network, the admin should ensure that critical security patches are applied to the firewall.

Because of recent changes to the frequency and scope of security updates, we do not recommend the use of pfSense Community Edition (CE). pfSense Plus continues to receive necessary security updates on a regular basis, and is provided with the purchase of most Netgate firewalls. If you wish to use a custom firewall or alternate option, we recommend using an OPNSense-based solution.

If you're using one of the network firewalls recommended by FPF, you can subscribe to email updates from the Netgate homepage or follow the Netgate blog to be alerted when releases occur. If critical security updates need to be applied, you can do so through the firewall's pfSense WebGUI.

Refer to our *Keeping pfSense up to Date* documentation or the official pfSense Upgrade Docs for further details on how to update the suggested firewall.

No matter which vendor you go with, you should make it a priority to stay informed of potential updates to your network firewall.

Updates: Workstations

The admin should keep all SecureDrop workstations updated with:

- **Tails updates** for each *Admin Workstation*, *Journalist Workstation*, and *Secure Viewing Station*; and
- **SecureDrop workstation updates** for each *Admin Workstation* and *Journalist Workstation*.

You should apply Tails updates to your Tails drives as they are released, as they often contain critical security fixes. Subscribe to the Tails RSS Feed to be alerted of new releases. The online Tails drives, once booted and connected to Tor, will alert you if upgrades are available. Follow the Tails Upgrade Documentation on how to upgrade the drives.

Admin and *Journalist Workstations* automatically check for updates on boot. An update window will pop up when updates are needed, and you should simply follow the prompts in the updater to perform the update.

Note

Note that you will need to have a Tails Administrator password configured to complete the update. If you forget to do so, you will need to reboot to enable it.

1.19.6 Monitoring OSSEC Alerts

SecureDrop uses OSSEC to monitor the servers for unusual activity caused by system configuration issues or security breaches. The admin should decrypt and read all OSSEC alerts. Report any suspicious events to FPF through the SecureDrop Support Portal. See the *OSSEC Guide* for more information on common OSSEC alerts.

Warning

Do not post logs or alerts to public forums without first carefully examining and redacting any sensitive information.

1.19.7 Monitoring SecureDrop-related communications

Release announcements and security advisories are posted to the SecureDrop blog, which is also available as an RSS feed. You can also follow us on our social media accounts (Twitter and Mastodon).

We strongly recommend *joining the SecureDrop support portal*. As a member of the support portal, you will receive email notifications related to all major announcements, and you can open tickets in case of technical issues. Membership is free of charge.

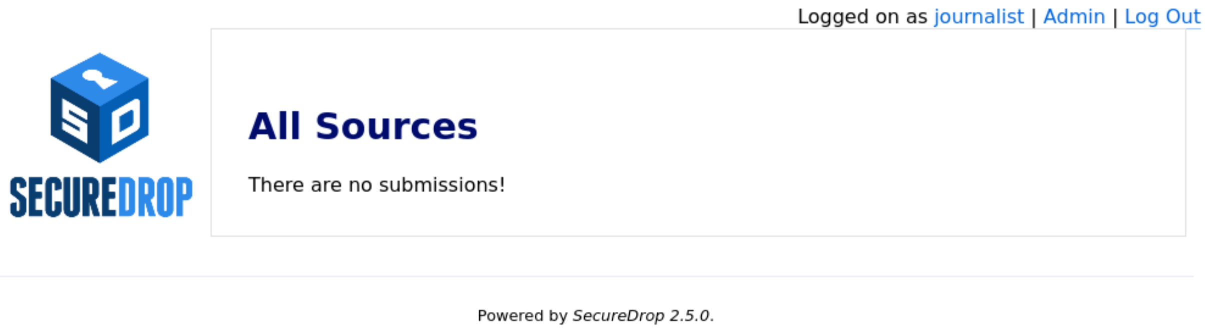
1.20 The Admin Interface

The *Admin Interface* is an extended version of the *Journalist Interface*, that allows you to manage users and configure the appearance and behaviour of your instance's web interfaces.

1.20.1 Logging in

To log in to the *Admin Interface*, start the *Admin Workstation* with persistence enabled. Open the *SecureDrop Menu* and select the "Launch Journalist Interface" option. Tor Browser will start and load the login page for the *Journalist Interface*. Use your username, passphrase, and two-factor authentication token to log in.

By default, you will be logged in to the *Journalist Interface*'s source list page.



Logged on as journalist | Admin | Log Out

All Sources

There are no submissions!

Powered by SecureDrop 2.5.0.

In the course of normal administration operations you should not need to view source communications, but if you do, you can find information on managing submissions in the *journalist guide*.

Note

If you have lost your login information or your two-factor authentication is no longer valid, you can create another account with admin privileges via the command line on the *Application Server*. See *here* for more information.

1.20.2 User Management

You can use the *Admin Interface* to add and remove users, and to reset their credentials if necessary. To open the *Admin Interface*, click **Admin** in the upper right corner of the *Journalist Interface*.

Adding Users

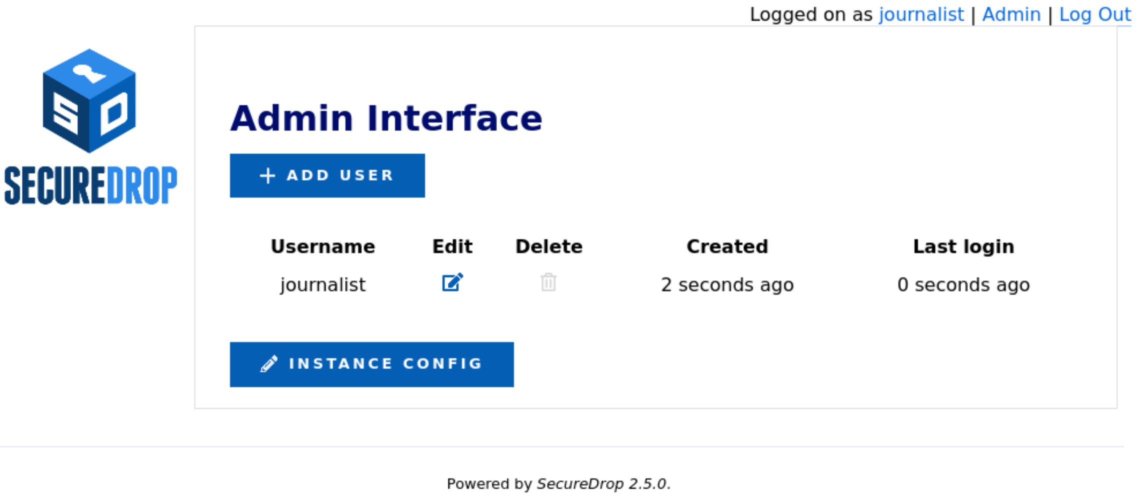
After logging in, you can add new user accounts for the journalists at your organization who will be checking the system for submissions. Make sure the journalist is physically in the same room as you when you do this, as they will have to be present to enable two-factor authentication. SecureDrop supports the use of either a smartphone authenticator app or a Yubikey for two-factor authentication. If an app is to be used, the journalist should install it before proceeding with the account setup.

Tip

We recommend using FreeOTP (available for Android and for iOS) to generate two-factor codes because it is Free Software. However, if it does not work for you for any reason, alternatives exist:

- Google Authenticator for Android and iOS (proprietary)
- authenticator for the desktop (Free Software)

1. Click **Admin** in the top right corner of the page to load the *Admin Interface*.

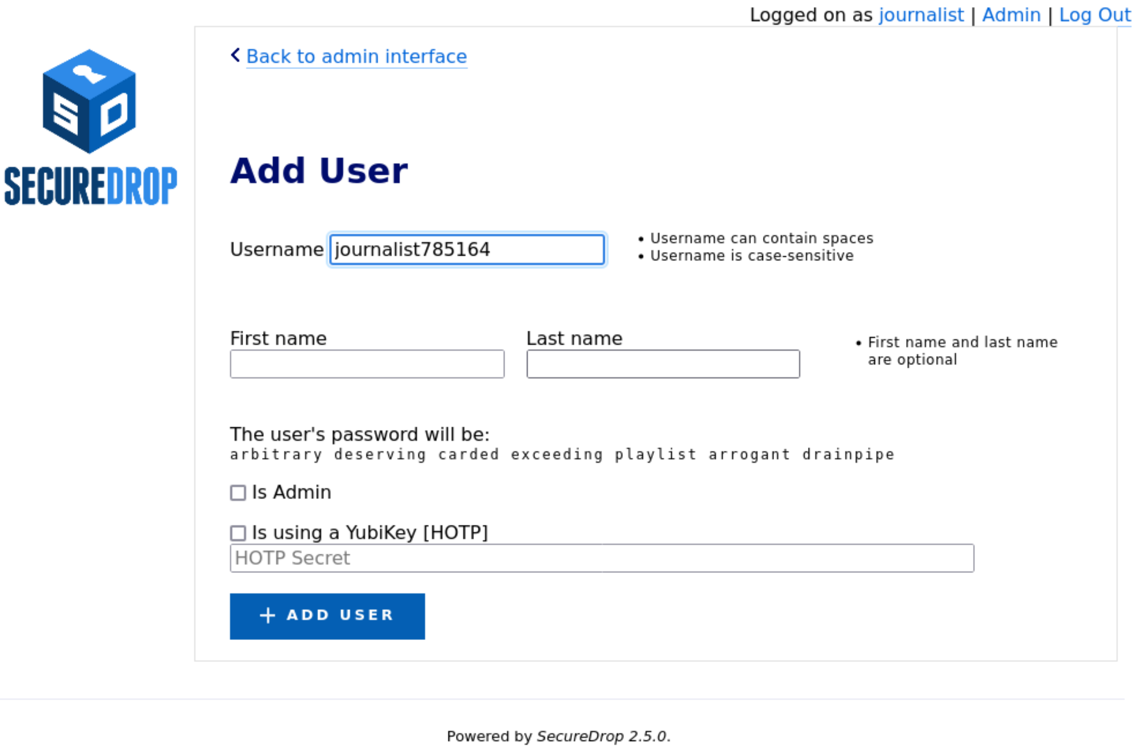


Admin Interface

Username	Edit	Delete	Created	Last login
journalist			2 seconds ago	0 seconds ago

Powered by *SecureDrop 2.5.0*.

2. Click **Add User** to add a new user.


Logged on as journalist | Admin | Log Out
SECUREDROP
‹ Back to admin interface
+ ADD USER

Add User

Username journalist785164

- Username can contain spaces
- Username is case-sensitive

First name

Last name

- First name and last name are optional

The user's password will be:
`arbitrary deserving carded exceeding playlist arrogant drainpipe`

□ Is Admin

□ Is using a YubiKey [HOTP]

HOTP Secret

Powered by *SecureDrop 2.5.0*.

3. Hand the keyboard over to the journalist so they can create their own username.
4. Once they're done entering a username for themselves, have them save their pre-generated Diceware passphrase

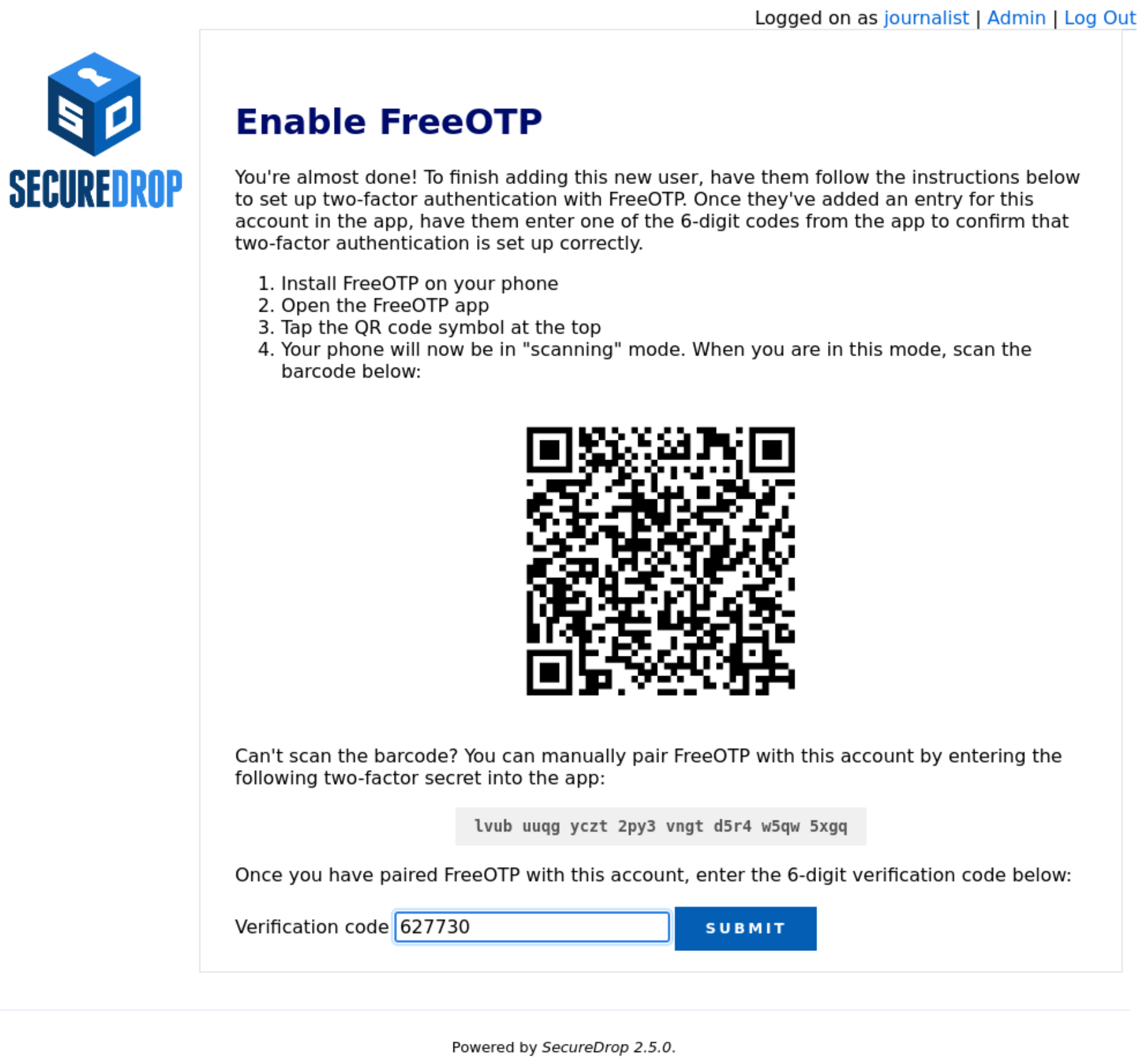
to their password manager.

5. If the new account should also have admin privileges, allowing them to add or delete other journalist accounts, select **Is Admin**.
6. Finally, set up two-factor authentication for the account, following one of the two procedures below for your chosen method.

> **Note**
>
> The username **deleted** is reserved, as it is used to mark accounts which have been deleted from the system.

FreeOTP

1. If the journalist is using FreeOTP or another app for two-factor authentication, click **Add User** to proceed to the next page.



Logged on as journalist | Admin | Log Out

Enable FreeOTP

You're almost done! To finish adding this new user, have them follow the instructions below to set up two-factor authentication with FreeOTP. Once they've added an entry for this account in the app, have them enter one of the 6-digit codes from the app to confirm that two-factor authentication is set up correctly.

1. Install FreeOTP on your phone
2. Open the FreeOTP app
3. Tap the QR code symbol at the top
4. Your phone will now be in "scanning" mode. When you are in this mode, scan the barcode below:

Can't scan the barcode? You can manually pair FreeOTP with this account by entering the following two-factor secret into the app:

```
lvub uuqg yczt 2py3 vngt d5r4 w5qw 5xgq
```

Once you have paired FreeOTP with this account, enter the 6-digit verification code below:

Verification code 627730

Powered by *SecureDrop 2.5.0*.

2. Next, the journalist should open FreeOTP on their smartphone and scan the barcode displayed on the screen.
3. If they have difficulty scanning the barcode, they can tap on the icon at the top that shows a plus and the symbol of a

key and use their phone's keyboard to input the two-factor secret into the `Secret` input field, without whitespace.

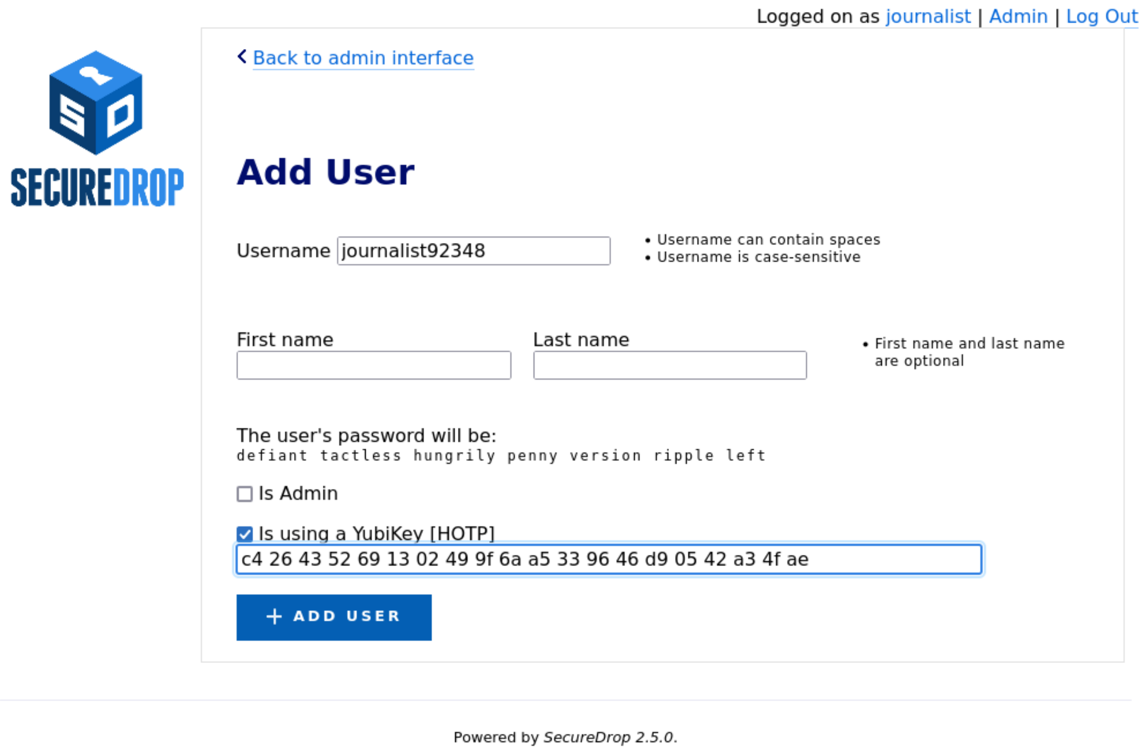
4. Inside the FreeOTP app, a new entry for this account will appear on the main screen, with a six-digit number that recycles to a new number every thirty seconds. The journalist should enter the six-digit number in the **Verification code** field at the bottom of the **Enable FreeOTP** form and click **Submit**.

If two-factor authentication was set up successfully, you will be redirected back to the *Admin Interface* and will see a confirmation that the two-factor code was verified.

> **Note**
>
> If the QR code for setting up two-factor authentication in your mobile authenticator app is not displayed, it may be blocked by Tor Browser. You can set Tor Browser's security level to **Standard** by clicking on the Shield icon. Alternatively, you can manually type in the two-factor secret (in FreeOTP, use the **Add token** option from the menu).

YubiKey

1. If the journalist wishes to use a YubiKey for two-factor authentication, select **Is using a YubiKey**. You will then need to enter their YubiKey's OATH-HOTP Secret Key. For more information on how to retrieve this key, read the *YubiKey Setup Guide*.



Logged on as journalist | Admin | Log Out

‹ Back to admin interface

Add User

Username journalist92348

- Username can contain spaces
- Username is case-sensitive

First name

Last name

- First name and last name are optional

The user's password will be:
`defiant tactless hungrily penny version ripple left`

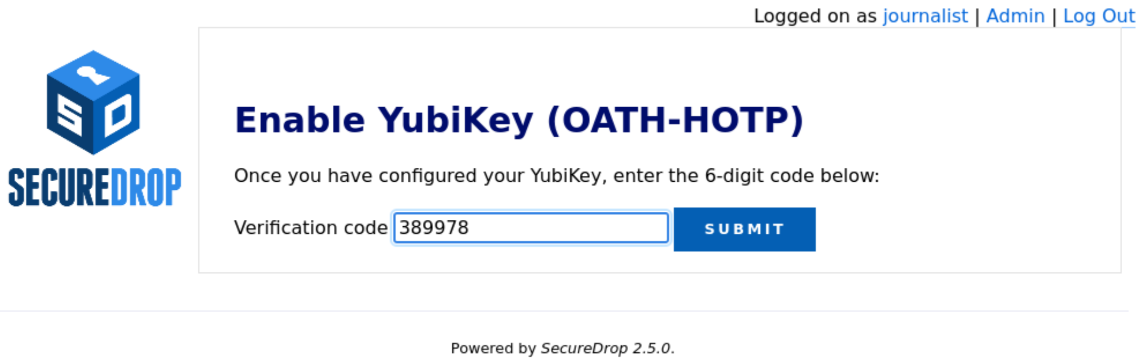
☐ Is Admin

☑ Is using a YubiKey [HOTP]

c4 26 43 52 69 13 02 49 9f 6a a5 33 96 46 d9 05 42 a3 4f ae

Powered by *SecureDrop 2.5.0*.

2. Once you've entered the Yubikey's OATH-HOTP Secret Key, click **Add User**. On the next page, have the journalist authenticate using their YubiKey, by inserting it into a USB port on the workstation and pressing its button.



Logged on as journalist | Admin | Log Out

Enable YubiKey (OATH-HOTP)

Once you have configured your YubiKey, enter the 6-digit code below:

Verification code 389978

Powered by *SecureDrop 2.5.0*.

3. If everything was set up correctly, you will be redirected back to the *Admin Interface*, where you should see a flashed message that says "The two-factor code for user *new username* was verified successfully.".

The journalist will require their username, passphrase, and two-factor authentication method whenever they check SecureDrop. Make sure that they have memorised their username and passphrase, or stored them in their password manager, and that they can keep their two-factor authentication device secure.

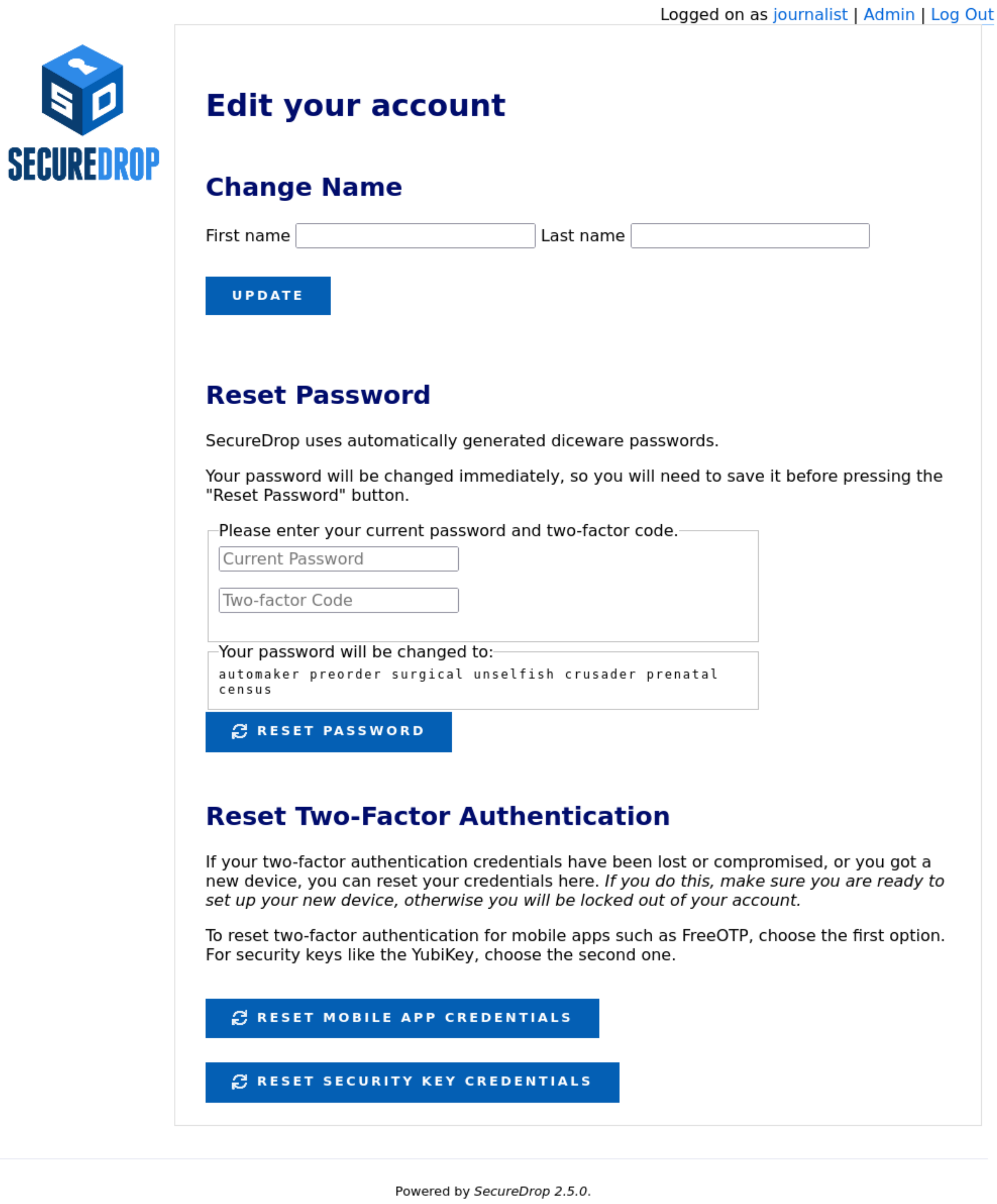
Passphrases and Two-Factor Resets

Warning

Both of these operations will lock a user out of their SecureDrop account. Users should be physically present when their passphrase or two-factor authentication method is reset. If this is not possible, store the passphrase and/or two-factor authentication secret in your own password manager before securely transmitting them to the user in question, and delete them once the user has confirmed they can successfully log in.

Even while following *passphrase best practices*, your journalists may occasionally lock themselves out of their accounts. This can happen if, for example, they lose their two-factor device or if they forget the passphrase to their password manager. When this happens, you can reset their account as follows:

1. Log in as an administrator to the *Journalist Interface*
2. Select *Admin* at the top right to open the *Admin Interface*
3. Find the user's account name and select **Edit**



Logged on as journalist | Admin | Log Out

Edit your account

Change Name

First name ______ Last name ______

Reset Password

SecureDrop uses automatically generated diceware passwords.

Your password will be changed immediately, so you will need to save it before pressing the "Reset Password" button.

Please enter your current password and two-factor code.

Current Password

Two-factor Code

Your password will be changed to:

```
automaker preorder surgical unselfish crusader prenatal
census
```

Reset Two-Factor Authentication

If your two-factor authentication credentials have been lost or compromised, or you got a new device, you can reset your credentials here. *If you do this, make sure you are ready to set up your new device, otherwise you will be locked out of your account.*

To reset two-factor authentication for mobile apps such as FreeOTP, choose the first option. For security keys like the YubiKey, choose the second one.

Powered by *SecureDrop 2.5.0*.

Next, you can either rotate their passphrase or reset two-factor authentication for their account.

To change their passphrase to the randomly-generated passphrase shown:

1. Have the journalist enter their current passphrase and two-factor code.
2. Make sure the new passphrase is saved in a password manager.
3. Click **Reset Password**

To reset two-factor authentication:

1. Click the button that corresponds to the user's chosen two-factor authentication method:
    - Click **Reset Mobile App Credentials** for accounts using FreeOTP or a similar authentication app
    - Click **Reset Security Key Credentials** for accounts using a Yubikey
2. Follow the on-screen instructions to complete the process and verify their new two-factor authentication credentials.

Off-boarding Users

See *our guide to off-boarding users from SecureDrop*.

1.20.3 Instance Configuration

The Instance Configuration section of the *Admin Interface* allows you to:

- update the organization name and logo displayed on the *Source* and *Journalist Interfaces*
- set submission preferences for the *Source Interface*
- send test OSSEC alerts.

Updating the Organization Name

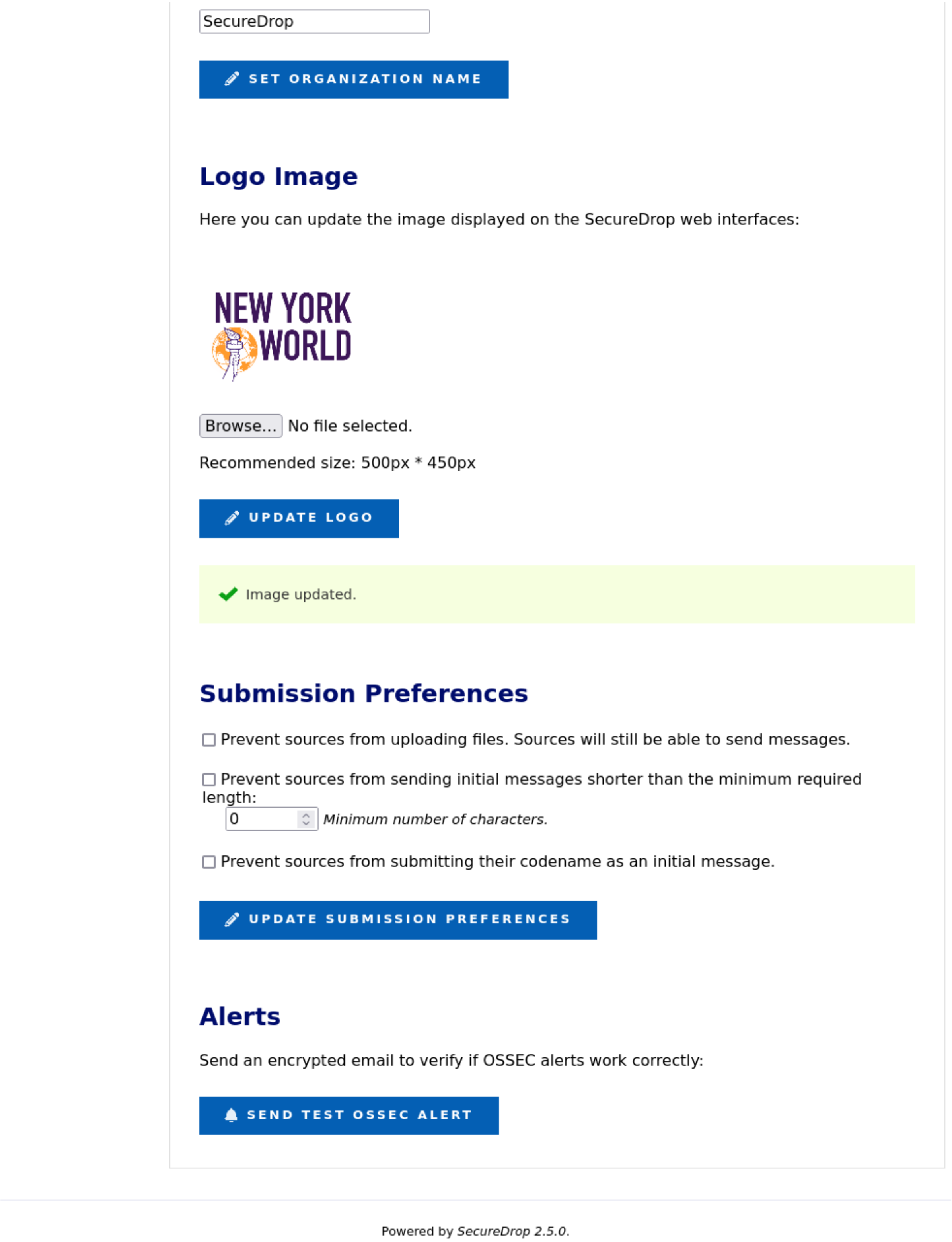
Your organization name is used in page titles and logo ALT text on the *Source Interface* and *Journalist Interface*. By default, it's set to `SecureDrop`. To change it, enter your desired name in the Organization Name field and click **Set Organization Name**.

Updating the Logo Image

You can update the system logo shown on the web interfaces of your SecureDrop instance via the *Admin Interface*. We recommend a size of `500px x 450px`. Only PNG-format images are supported. To update the logo image:

1. Copy the logo image to your admin workstation
2. Click **Browse** and select the image from your workstation's filesystem
3. Click **Update Logo** to upload and set the new logo

You should see a message appear indicating the change was a success.



SecureDrop

Logo Image

Here you can update the image displayed on the SecureDrop web interfaces:

No file selected.

Recommended size: 500px * 450px

✓ Image updated.

Submission Preferences

□ Prevent sources from uploading files. Sources will still be able to send messages.

□ Prevent sources from sending initial messages shorter than the minimum required length:
0 *Minimum number of characters.*

□ Prevent sources from submitting their codename as an initial message.

Alerts

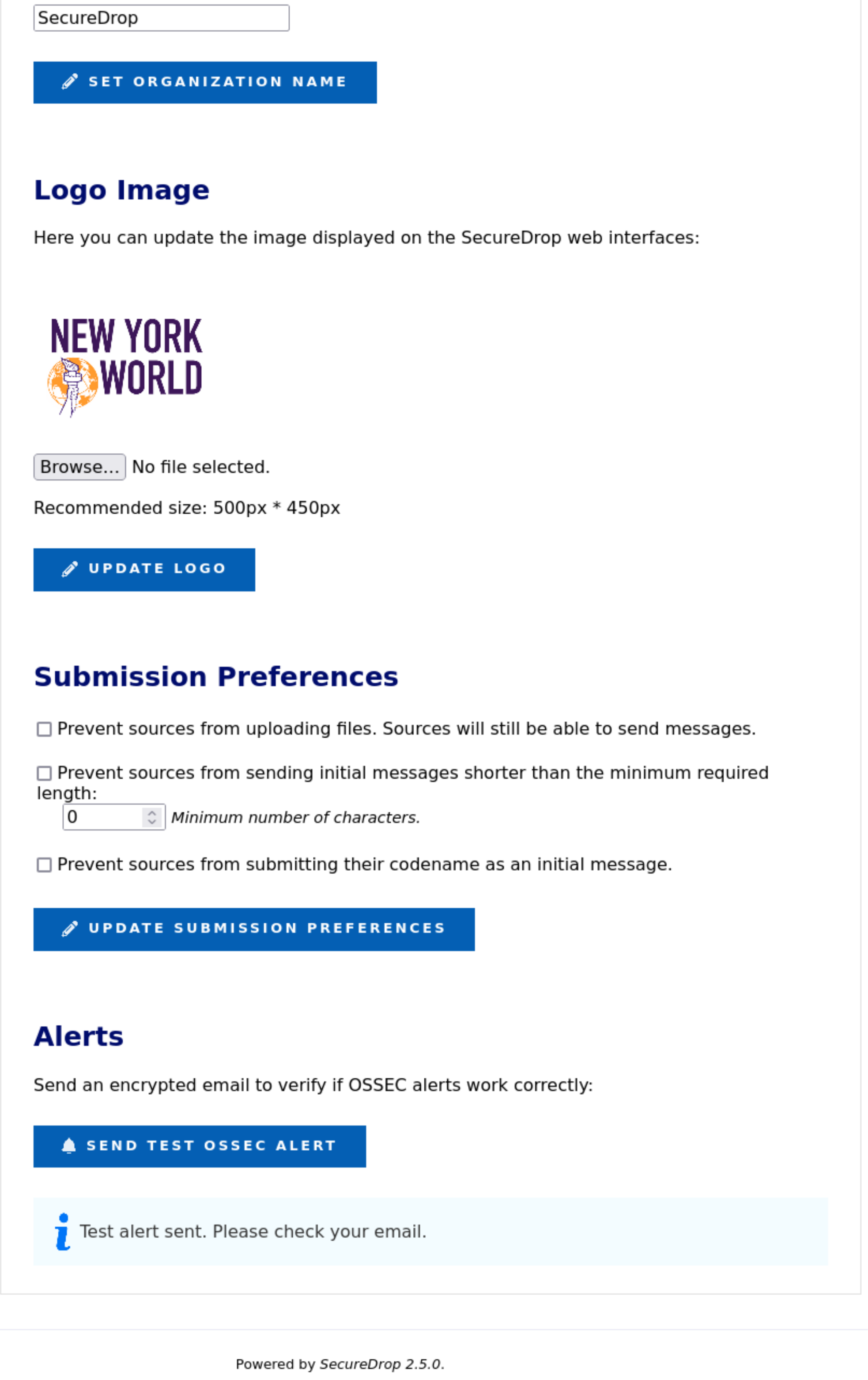
Send an encrypted email to verify if OSSEC alerts work correctly:

Powered by *SecureDrop 2.5.0*.

It may be necessary to hold the Shift key while pressing the Reload button in the browser, which will force it to purge the cached version of the logo in order to see the new one.

Testing OSSEC Alerts

To verify that the OSSEC monitoring system's functionality, you can send a test OSSEC alert by clicking **Send Test OSSEC Alert**.



SecureDrop

Logo Image

Here you can update the image displayed on the SecureDrop web interfaces:

No file selected.

Recommended size: 500px * 450px

Submission Preferences

☐ Prevent sources from uploading files. Sources will still be able to send messages.

☐ Prevent sources from sending initial messages shorter than the minimum required length:
0 *Minimum number of characters.*

☐ Prevent sources from submitting their codename as an initial message.

Alerts

Send an encrypted email to verify if OSSEC alerts work correctly:

Test alert sent. Please check your email.

Powered by *SecureDrop 2.5.0.*

You should receive an OSSEC alert email at the address specified during the installation of SecureDrop. The email may take several minutes to arrive. If you don't receive it, refer to the *OSSEC Guide* for information on troubleshooting steps.

Submission Preferences

The Submission Preferences subsection allows you to restrict the types of submissions accepted by your instance.

Disabling Document Uploads

By default, SecureDrop supports both text submissions and document uploads. If you only want to receive text messages, you can disable uploads as follows:

1. Check the **Prevent sources from uploading documents** checkbox
2. Click **Update Submission Preferences**

This change will be applied immediately on the *Source Interface*. Documents that were previously uploaded will still be available via the *Journalist Interface*.

Preventing Short Initial Messages

By default, SecureDrop does not apply a minimum length requirement to messages. If your instance is experiencing a high volume of short one-time messages with no actionable content, or if you would like to indicate to sources that their initial message should include enough information for journalists to respond to them effectively, you can set an initial message length as follows:

1. Check the **Prevent sources from sending initial messages shorter than the minimum required length** checkbox
2. Enter the desired minimum length in the field below the checkbox
3. Click **Update Submission Preferences**

This change will be applied immediately on the Source Interface. Initial messages that are too short will be rejected, with an error message informing sources of the requirement. This requirement will not be applied to initial messages that also include a document, or to subsequent messages in the conversation.

To remove the requirement, uncheck the checkbox and click **Update Submission Preferences**.

Preventing Initial Messages Containing the Source's Codename

Sources should never need to share their seven-word codename with journalists. If your instance is receiving one-time messages consisting of the source's codename, you can optionally reject those messages, before they are stored, as follows:

1. Check the **Prevent sources from submitting their codename as an initial message** checkbox
2. Click **Update Submission Preferences**

This change will be applied immediately on the Source Interface. Initial messages that contain the source's codename will be rejected, with an error message reminding sources to protect their codename and keep it secret. To remove this restriction, uncheck the checkbox and click **Update Submission Preferences**.

1.21 Logging in via SSH

1.21.1 Server SSH Access

Generally, you should avoid directly SSHing into the servers in favor of using the *Admin Interface* or `securedrop-admin`. However, in some cases, you may need to SSH in order to troubleshoot and fix a problem that cannot be resolved via these tools.

You can access your *Application Server* and *Monitor Server* via SSH by using either the `ssh app` or `ssh mon` commands (respectively) from an *Admin Workstation*.

For quick access, use the "SSH into the App Server" and "SSH into the Monitor Server" options in the *SecureDrop Menu*.

In this section we cover basic commands you may find useful when you SSH into the *Application Server* and *Monitor Server*.

Tip

When you SSH into either SecureDrop server, you will be dropped into a `tmux` session. `tmux` is a screen multiplexer - it allows you to tile panes, preserve sessions to keep your session alive if the network connection fails, and more. Check out this tmux tutorial to learn how to use `tmux`.

Tip

If you want a refresher of the Linux command line, we recommend this resource to cover the fundamentals.

Shutting Down the Servers

```
sudo shutdown now -h
```

Rebooting the Servers

```
sudo reboot
```

1.21.2 Investigating Logs

Consult our *Investigating Logs* topic guide for locations of the most relevant log files you may want to examine as part of troubleshooting, and for how to enable error logging for the *Source Interface*.

Note

You can use the `securedrop-admin` tool to extract logs to send to Freedom of the Press Foundation for analysis. Run the following command on your *Admin Workstation*:

```
securedrop-admin logs
```

This command will produce encrypted tarballs containing logs from each server. See the command output for more information.

1.21.3 Immediately Apply a SecureDrop Update

SecureDrop will update and reboot once per day. However, once a SecureDrop update is announced, you can opt to fetch the update immediately.

Important

Except where otherwise indicated, make sure to update both your *Application Server* and your *Monitor Server*.

To update your servers immediately, you can SSH into each server (via `ssh app` and `ssh mon`) and run the following commands:

```
sudo apt update
sudo unattended-upgrades
```

Note

Depending on the nature of the update (e.g., if the `tor` package is upgraded and you are using SSH-over-Tor), your SSH connection may be interrupted, and you may have to reconnect to see the full output.

1.21.4 Application Server

Adding Users (CLI)

After the provisioning of the first admin account, we recommend using the Admin Interface web application for adding additional journalists and admins.

However, you can also add users via `./manage.py` in `/var/www/securedrop/` as described *during first install*. You can use this command line method if the web application is unavailable.

Restart the Web Server

If you make changes to your Apache configuration, you may want to restart the web server to apply the changes:

```
sudo systemctl restart apache2
```

Cleaning up deleted submissions

When submissions are deleted through the web interface, their database records are deleted and their encrypted files are securely wiped. For large files, secure removal can take some time, and it's possible, though unlikely, that it can be interrupted, for example by a server reboot. In older versions of SecureDrop this could leave a submission file present without a database record.

As of SecureDrop 1.0.0, automated checks send OSSEC alerts when this situation is detected, recommending you run `manage.py list-disconnected-fs-submissions` to see the files affected. As with any `manage.py` usage, you would run the following on the admin workstation:

```
ssh app
sudo -u www-data bash
cd /var/www/securedrop
./manage.py list-disconnected-fs-submissions
```

You then have the option of running:

```
./manage.py delete-disconnected-fs-submissions
```

to clean them up. As with any potentially destructive operation, it's recommended that you *back the system up* before doing so.

There is also the inverse scenario, where a database record could point to a file that no longer exists. This would usually only have happened as a result of disaster recovery, where perhaps the database was recovered from a failed hard drive, but some submissions could not be. The OSSEC alert in this case would recommend running:

```
./manage.py list-disconnected-db-submissions
```

To clean up the affected records you would run (again, preferably after a backup):

```
./manage.py delete-disconnected-db-submissions
```

Even when submissions are completely removed from the application server, their encrypted files may still exist in backups. We recommend that you delete old backup files with `shred`, which is available on Tails.

1.21.5 Monitor Server

Restart OSSEC

If you make changes to your OSSEC monitoring configuration, you will want to restart OSSEC via OSSEC's control script, `ossec-control`:

```
sudo /var/ossec/bin/ossec-control restart
```

1.22 The `securedrop-admin` Utility

1.22.1 Using `securedrop-admin`

The `securedrop-admin` command-line utility is used from the *Admin Workstation* to perform common server administration tasks, including:

- configuring and installing SecureDrop
- backing up and restoring the servers (see *Backing Up and Restoring Servers*)
- retrieving server logs for troubleshooting (see *Investigating Logs*)
- updating the SecureDrop code and Tails configuration on the *Admin Workstation*
- updating your SecureDrop servers' configuration post-install.

To use `securedrop-admin`:

1. Boot the *Admin Workstation* with persistence enabled and an admin password set
2. Open a terminal via **Apps** ▶ **System Tools** ▶ **Console**

You can list all available `securedrop-admin` actions using the command `securedrop-admin --help`

Note

If your team has multiple admins, each with their own *Admin Workstation*, you must take steps to manually synchronize any configuration changes made via `securedrop-admin` with each other. See *Managing Configuration Updates with Multiple Admins*

1.22.2 Updating the Server Configuration

There are two primary reasons why you may want to update the system configuration:

- to change SecureDrop server configuration options. **Example:** You want to change the time of day at which the servers are automatically rebooted (default: 4:00 AM).
- to restore a valid configuration state on your servers. **Example:** Another admin has directly modified the iptables rules during troubleshooting, and you want to reinstate the correct rules.

In both cases, follow these steps:

1. Boot the *Admin Workstation* and unlock its persistent volume.
2. Determine the current version of *securedrop-admin* you have installed on your *Admin Workstation* by running:

   ```
   apt-cache policy securedrop-admin
   ```

   If the version is the same as the version number displayed in the footer of your *Source Interface*, you are running the applicable version of the SecureDrop code on your workstation, and can proceed to the next step.

   If the versions differ, **it is not safe to proceed**. Follow the upgrade instructions associated with the release notes for the most recent release of SecureDrop. Apply all available updates, including for the Tails operating system.

1. Run `securedrop-admin sdconfig`. This will display the current configuration, one line at a time, and allow you to change it. At this point, any changes you make are only saved on this *Admin Workstation*, to the following file:

   `~/.config/securedrop-admin/site-specific`

2. Run `securedrop-admin install`. This will apply the configuration to your *Application* and *Monitor Server*, and enforce the canonical state of the server configuration.

Note

If you see an error running `securedrop-admin install`, and believe it may be an intermittent issue (for example, due to losing network connectivity to the servers), it is safe to run the `securedrop-admin install` command again. If you see the same issue consistently, then you will need to troubleshoot it.

If you see the error message "timeout (62s) waiting for privilege escalation prompt", try deleting the Ansible control path directory on your *Admin Workstation* (`rm -rf ~/.ansible/cp`) to reset the connection to the servers, then re-run the `securedrop-admin install`.

If you encounter other errors, we encourage you to submit a bug report, or to contact us at securedrop@freedom.press (GPG encrypted).

1.22.3 Updating Localization for the *Source Interface* and the *Journalist Interface*

The *Source Interface* and *Journalist Interface* are translated in the following languages:

https://github.com/freedomofpress/securedrop/blob/develop/securedrop/i18n.rst

At any time during and after initial setup, you can choose from a list of supported languages to display using the codes shown in parentheses.

> **Note**
>
> With a *Source Interface* displayed in French (for example), sources submitting documents are likely to expect a journalist fluent in French to be available to read the documents and follow up in that language.

To add or remove locales from your instance, you'll need to *update your system configuration* as outlined above.

When you reach the prompt starting with "Space separated list of additional locales to support", you will see a list of languages currently supported. Refer to the list above to see which languages correspond to which language codes. For example:

```
Space separated list of additional locales to support (ru nl pt_BR fr_FR tr it_IT zh_
↪Hant sv hi ar en_US de_DE es_ES nb_NO): nl fr_FR es_ES
```

You'll need to list all languages you now want to support, adding or removing languages as needed. Locale changes will be applied after the next reboot.

1.22.4 Managing Configuration Updates with Multiple Admins

Organizations with multiple admins should set up a way to synchronize any changes one admin makes to the server configuration, as by default those changes are stored only on their individual *Admin Workstation*.

Configuration changes will be flagged by OSSEC and will generate alerts, but if other admins don't regularly review OSSEC alerts they may miss important changes, such as an update to the *Submission Public Key*. If they subsequently run `securedrop-admin install` from their *Admin Workstation*, they will revert the server configuration to an older version.

The simplest approach to keeping workstations in sync is to inform other admins of changes as you make them, for example via a secure Signal group chat. Any such communications should happen over a platform that provides E2EE, as you may need to share sensitive information.

Configuration information is stored on the *Admin Workstation* under `~/.config/securedrop-admin`:

- `~/.config/securedrop-admin/site-specific` contains settings written by `securedrop-admin sdconfig` - if it is changed other admins should be notified.
- The *Submission Public Key* and *OSSEC Alert Public Key* should be present under `~/.config/securedrop-admin`. If these keys are rotated, the public keys should be updated on other *Admin Workstations*.
- Onion service information is stored in several files:

  ```
  ~/.config/securedrop-admin/app-ssh.auth_private
  ~/.config/securedrop-admin/mon-ssh.auth_private
  ~/.config/securedrop-admin/app-journalist.auth_private
  ~/.config/securedrop-admin/app-sourcev3-ths
  ~/.config/securedrop-admin/tor_v3_keys.json
  ```

  If onion service addresses are changed, the files listed above should be shared securely with other administrators - preferably in person using an encrypted transfer USB, as they can be used to access the servers directly via SSH over Tor.

1.23 Frequently Asked Questions

Some initial troubleshooting steps for common scenarios follow. If you continue to have trouble after following these steps, you can contact the SecureDrop team for further assistance.

1.23.1 Generic Troubleshooting Tips

When troubleshooting, ensure you are on the latest version of SecureDrop in your *Admin Workstation*. This is done by accepting the update when prompted at boot in the GUI that appears.

1.23.2 I can't SSH into my servers over Tor from my Admin Workstation. What do I do?

At any point after the successful installation of SecureDrop, if you cannot SSH into your Admin Workstation, you should first perform the following troubleshooting steps:

1. **Ensure that you are connected to Tor.** You can do this by browsing to any site in Tor Browser in your *Admin Workstation*.
2. **Ensure your servers are online.** Visit the *Admin Interface* to check your *Application Server* is online, and you can trigger a *test OSSEC alert* to verify your *Monitor Server* is online.
3. **Ensure that SSH aliases and onion service authentication are configured:**
   - First, ensure that the correct configuration files are present in `~/.config/securedrop-admin`:
     - `app-ssh.auth_private`
     - `mon-ssh.auth_private`
     - `app-journalist.auth_private`
     - `app-sourcev3-ths`
     - `tor_v3_keys.json`
   - Then, run `securedrop-admin localconfig`. This will ensure your local Tails environment is configured properly.
4. **Confirm that your SSH key is available**: During the install, you configured SSH public key authentication using `ssh-copy-id`. Ensure this key is available using `ssh-add -L`. If you see the output "This agent has no identities." then you need to add the key via `ssh-add` prior to SSHing into the servers.

1.23.3 I got a unusual error when running `securedrop-admin install`. What do I do?

If the error message is not informative, try running it again. The Tor connection can be flaky and can cause apparent errors, but there is no negative impact of re-rerunning `securedrop-admin install` more than once. The command will simply check which tasks have been completed, and pick up where it left off. However, if the same issue persists, you will need to investigate further.

1.24 Installation Overview

1.24.1 Installation Support

Any organization can install SecureDrop for free and also make modifications because the project is open source.

Because the installation and operation are complex, and because SecureDrop can only be as secure as the operational security practices followed by its users, Freedom of the Press Foundation will also help organizations install SecureDrop and train journalists and administrators.

If you would like to work with Freedom of the Press Foundation on your SecureDrop installation, please reach out to us. We do ask news organizations that can afford to pay for installation support, training and maintenance to do so.

As part of priority support agreements and on a pro-bono basis for smaller news organizations, Freedom of the Press Foundation will visit your offices, help set up SecureDrop and train journalists to use it. (For pro-bono support, we request that our travel costs are covered.)

1.24.2 Setting Expectations

SecureDrop is a technical tool. It is designed to protect journalists and sources, but no tool can guarantee safety. This guide will instruct you in installing and configuring SecureDrop, but it does not explain how to use it safely and effectively. Put another way: at the end of this guide, you will have built a car; you will not know how to drive. The *Deployment Guide* contains best practices for working with SecureDrop. Make sure to read it after completing the installation.

Setting up SecureDrop is a multi-step process, where each step builds on the steps that come before it. It's important that you treat the installation as a complete process, making sure not to skip any portions of the install guide or jump ahead to later content.

Once you have all the necessary hardware, *setting up SecureDrop* will take at least a day's work.

We recommend that you set aside at least a week to *complete and test* your setup.

1.24.3 Tracking your progress

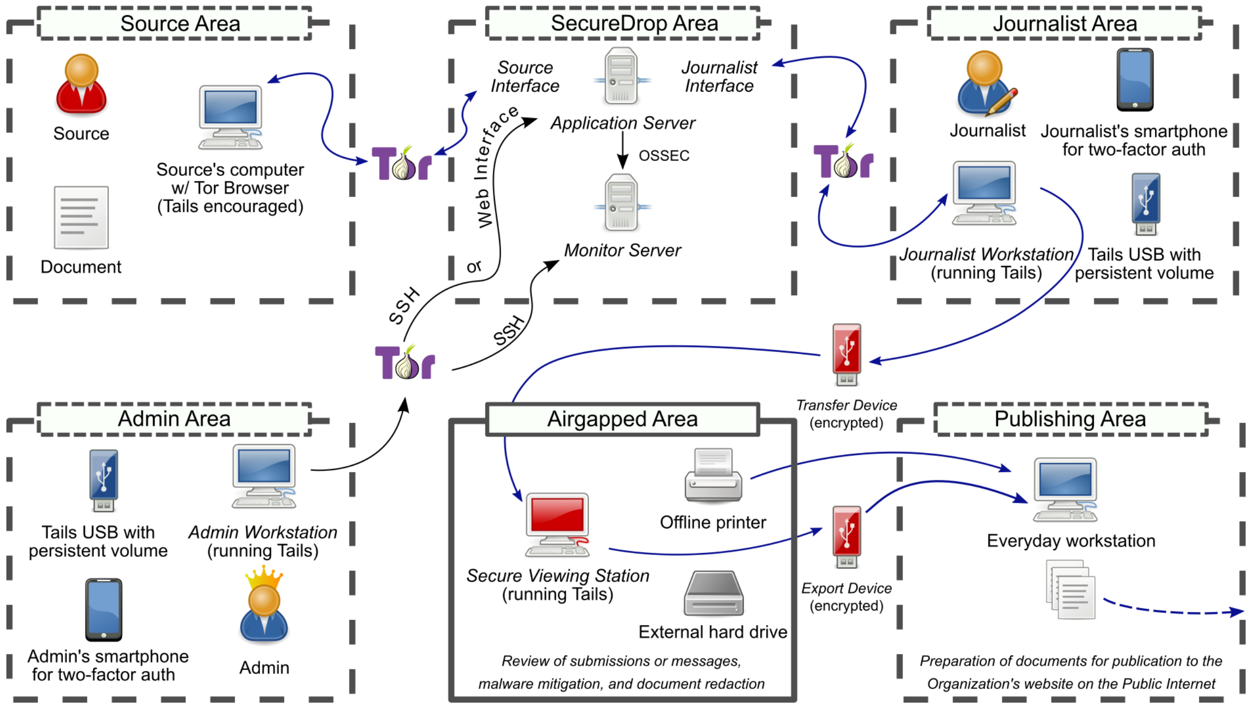
To assist in the installation process, we offer a SecureDrop Installation Worksheet, which you can print out and complete as you go. Only complete this worksheet on paper, never electronically.

It is **critical** that you destroy this worksheet when your installation is complete and all of your passphrases have been safely stored in a password manager.

Warning

Remember to destroy the SecureDrop Installation Worksheet after the installation is complete.

1.24.4 Technical Summary


Source Area
Source
Source's computer w/ Tor Browser (Tails encouraged)
Document
SecureDrop Area
Source Interface
Journalist Interface
Application Server
OSSEC
Monitor Server
Web Interface
or
SSH
SSH
Journalist Area
Journalist
Journalist's smartphone for two-factor auth
Journalist Workstation (running Tails)
Tails USB with persistent volume
Transfer Device (encrypted)
Admin Area
Tails USB with persistent volume
Admin Workstation (running Tails)
Admin's smartphone for two-factor auth
Admin
Airgapped Area
Offline printer
Secure Viewing Station (running Tails)
External hard drive
Review of submissions or messages, malware mitigation, and document redaction
Export Device (encrypted)
Publishing Area
Everyday workstation
Preparation of documents for publication to the Organization's website on the Public Internet

This installation guide will walk you through the process of setting up the computers and services needed for a functional SecureDrop.

During this process, you'll set up the following devices:

- ***Secure Viewing Station*:**
  A physically-secured and air-gapped laptop running the Tails operating system from a USB stick, that journalists use to decrypt and view submitted documents.
- ***Application Server*:**
  An Ubuntu server running two segmented Tor hidden services. The source connects to the *Source Interface*, a public-facing Tor Onion Service, to send messages and documents to the journalist. The journalist connects to the *Journalist Interface*, an authenticated Tor Onion Service, to download encrypted documents and respond to sources.
- ***Monitor Server*:**
  An Ubuntu server that monitors the *Application Server* with OSSEC and sends email alerts.

As an administrator, you will also require a computer to connect to SecureDrop and perform administrative tasks via SSH or the *Journalist Interface*. This computer is referred to as the *Admin Workstation*, and must be capable of running the Tails operating system. The *Admin Workstation* may also be used as a *Journalist Workstation* if necessary.

Before you begin the installation, you will want to be sure to familiarize yourself with the *glossary* and the *passphrases* involved in SecureDrop's operations. You may wish to leave these documents open in other tabs for reference as you work.

When running commands or editing configuration files that include filenames, version numbers, usernames, hostnames, or IP addresses, make sure to use the appropriate values for your instance.

Once you're familiar with SecureDrop, have made your plan, ensured your organization is ready to follow through, and assembled the necessary hardware, you're ready to begin.

Note

The SecureDrop installation guide includes documentation on setting up Tails-based *Admin Workstation* and *Journalist Workstation* USB sticks. It is strongly recommended that these be used in preference to other undocumented solutions.

1.25 Passphrases

Each individual with a role (admin or journalist) at a given SecureDrop instance must generate and retain a number of strong, unique passphrases. The document is an overview of the passphrases, keys, two-factor secrets, and other credentials that are required for each role in a SecureDrop installation.

Note

We encourage each end user to use KeePassXC, an easy-to-use password manager included in Tails, to generate and retain strong and unique passphrases. The SecureDrop code repository includes a template that you can use to initialize this database for an *Admin Workstation* or a *Journalist Workstation*. For more information, see the *KeePassXC setup instructions*.

Tip

For best practices on managing passphrases, see *Passphrase Best Practices*.

1.25.1 Admin

The admin will be using the *Admin Workstation* with Tails to connect to the *Application Server* and the *Monitor Server* using Tor and SSH. The tasks performed by the admin will require the following set of credentials and passphrases:

- A passphrase for the persistent volume on the Admin Live USB.
- Additional credentials, which we recommend adding to Tails' KeePassXC password manager during the installation:
  - The *Application Server* and *Monitor Server* admin username and password (required to be the same for both servers).
  - The network firewall username and password.
  - The SSH private key and, if set, the key's passphrase.
  - The *OSSEC Alert Public Key*.
  - The admin's personal GPG public key, if you want to potentially encrypt sensitive files to it for further analysis.
  - The account details for the destination email address for OSSEC alerts.
  - The onion services values required to connect to the *Application* and *Monitor Servers*.

The admin will also need to have a way to generate two-factor authentication codes.

Tip

We recommend using FreeOTP (available for Android and for iOS) to generate two-factor codes because it is Free Software. However, if it does not work for you for any reason, alternatives exist:

- Google Authenticator for Android and iOS (proprietary)
- authenticator for the desktop (Free Software)

And the admin will also have the following two credentials:

- The secret code for the *Application Server*'s two-factor authentication.
- The secret code for the *Monitor Server*'s two-factor authentication.

1.25.2 Journalist

The journalist will be using the *Journalist Workstation* with Tails to connect to the *Journalist Interface*. The tasks performed by the journalist will require the following set of passphrases:

- A passphrase for the persistent volume on the Tails device.
- A passphrase for the KeePassXC password manager, which unlocks the passphrase for logging into the *Journalist Interface*.

The journalist will also need to have a two-factor authenticator, such as an Android or iOS device with FreeOTP installed, or a YubiKey. This means the journalist will also have the following credential:

- The secret code for the *Journalist Interface*'s two-factor authentication.

Secure Viewing Station

The journalist will be using the *Secure Viewing Station* with Tails to decrypt and view submitted documents. The tasks performed by the journalist will require the following passphrases:

- A passphrase for the persistent volume on the Tails device.

The backup that is created during the installation of SecureDrop is also encrypted with the application's GPG key. The backup is stored on the persistent volume of the Admin Live USB.

Transfer Device and *Export Device*

As noted in the *setup guide*, we recommend using encrypted USB drives for transferring files to the *Secure Viewing Station*, and for exporting them from the *SVS* in situations where using a secure printer or a similar analog conversion is not an option.

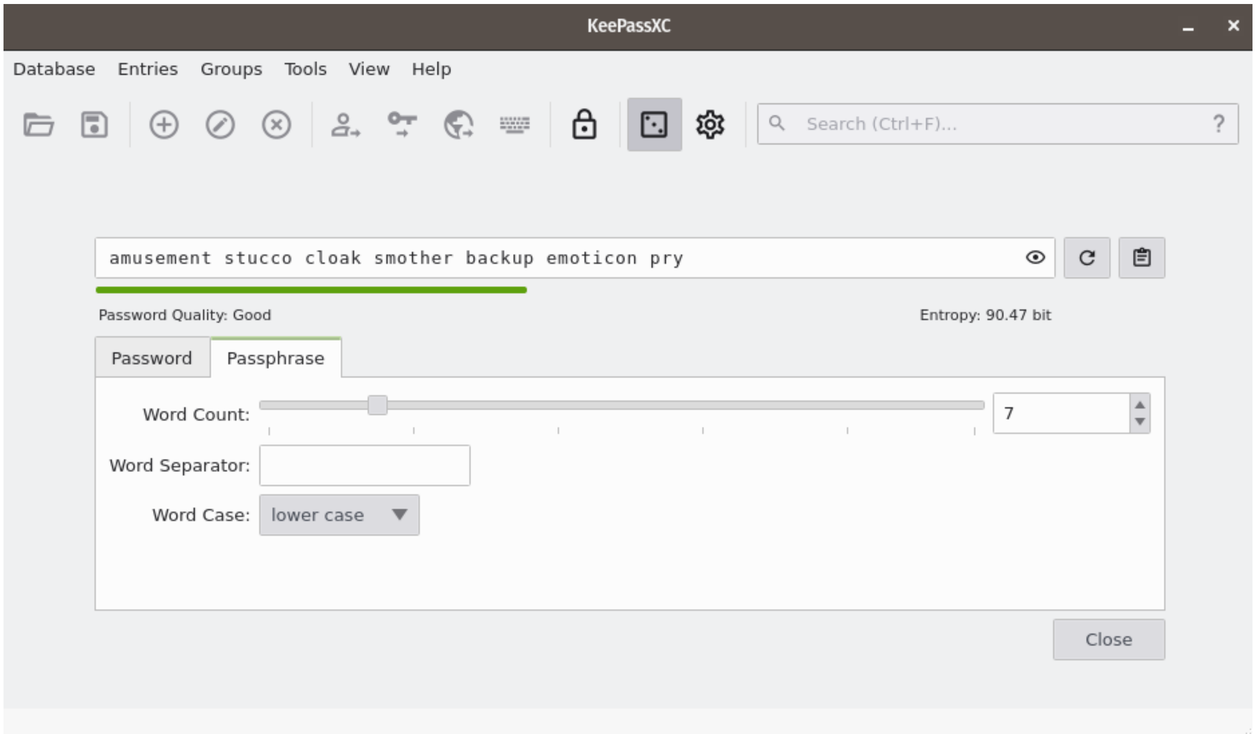
For every copy operation, the user will need to enter the USB drive's encryption passphrase at least twice (on the computer they're copying from, and on the computer they're copying to). To make it easy for them to find the passphrase, we recommend storing it in the journalist's own existing password manager, which should be accessible using their smartphone.

1.25.3 How to Generate a Strong, Unique Passphrase

We recommend using a unique, 7-word passphrase for each case described above. You can create these passphrases either by using physical dice or with KeePassXC, a password manager included with Tails.

Using KeePassXC to Generate a Passphrase

To create a random passphrase using KeePassXC, launch the application, then click the **dice icon**. Then click the **Passphrase** tab and set the **Word Count** to 7. You can optionally set a **Word Separator**, for example a space or hyphen.



amusement stucco cloak smother backup emoticon pry

Password Quality: Good

Entropy: 90.47 bit

Word Count: 7

Word Separator:

Word Case: lower case

1.26 Hardware

This document outlines the required hardware components necessary to successfully install and operate a SecureDrop instance, and recommends some specific components that we have found to work well. If you have any questions, please email securedrop@freedom.press.

1.26.1 Hardware Overview

For an installation of SecureDrop, you must acquire:

- 2 computers with memory and hard drives to use as the SecureDrop servers.
- Mouse, keyboard, monitor (and necessary dongle or adapter) for installing the servers.
- At least 2 dedicated physical computers that can boot to Tails: one computer for the *Secure Viewing Station*, and one or more computers for the *Admin Workstation(s)/Journalist Workstation(s)*.
- Dedicated airgapped hardware for the mouse, keyboard, and monitor (only if you are using a desktop for the *Secure Viewing Station*).
- A dedicated network firewall with at least 4 NICs.
- At least 3 ethernet cables.
- Plenty of USB sticks: 1 drive for the Template Tails stick, 1 drive for each Secure Viewing Station, 1 drive for each *Transfer Device*, 1 drive for each *Export Device*, and 1 drive for each admin and journalist.

Additionally, you may want to consider the following purchases:

- a printer without wireless network support, to use in combination with the *Secure Viewing Station*.
- an external storage drive to expand the storage capacity of the *Secure Viewing Station*.
- an external hard drive for server backups.
- a USB drive to store *backups of your Tails workstation drives*.
- a security key for HOTP authentication, such as a YubiKey, if you want to use hardware-based two-factor authentication instead of a mobile app.
- a USB drive with a physical write protection switch, or a USB write blocker, if you want to mitigate the risk of introducing malware from your network to your *Secure Viewing Station* during repeated use of an *Export Device*.
- CD-R/DVD-R writers, if you want to use CD-Rs/DVD-Rs as transfer or export media, and a CD shredder that can destroy media consistent with your threat model.

In the sections that follow, we provide additional details on most of these items.

Tip

While a printer is not required, we highly recommend it. Printing documents is generally far safer than copying them in digital form. See our *guide to working with documents* for more information.

1.26.2 Advice for users on a tight budget

If you cannot afford to purchase new hardware for your SecureDrop instance, we encourage you to consider re-purposing existing hardware to use with SecureDrop. If you are comfortable working with hardware, this is a great way to set up a SecureDrop instance for cheap.

Since SecureDrop's throughput is significantly limited by the use of Tor for all connections, there is no need to use top of the line hardware for any of the servers or the firewall. In our experience, relatively recent recycled Dell desktops or servers are adequate for the SecureDrop servers, and recycled ThinkPad laptops work well for the *Admin Workstation/Journalist Workstation*.

Please note that very old laptops or desktops may not work for the workstations. Since the release of Tails 3.0, 32-bit computers are no longer supported.

Additionally, we recommend against re-purposing Apple Macintosh laptops and desktops. Recent Apple computers, which have M-series CPUs, are completely unsupported by Tails and will not work. Older computers with Intel CPUs may work, but are likely to experience compatibility issues.

If you choose to use recycled hardware, you should of course consider whether or not it is trustworthy; making that determination is outside the scope of this document.

1.26.3 Required Hardware

Servers

These are the core components of a SecureDrop instance.

- *Application Server*: 1 physical server to run the SecureDrop web services.
- *Monitor Server*: 1 physical server which monitors activity on the *Application Server* and sends email notifications to an admin.
- *Network Firewall*: 1 physical computer that is used as a dedicated firewall for the SecureDrop servers.

An acceptable alternative that requires more technical expertise is to *configure an existing hardware firewall*.

We are often asked if it is acceptable to run SecureDrop on cloud servers (e.g. Amazon EC2, DigitalOcean, etc.) or on dedicated servers in third-party datacenters instead of on dedicated hardware hosted in the organization. This request is generally motivated by a desire for cost savings and/or convenience. However: we consider it **critical** to have dedicated physical machines hosted within the organization for both technical and legal reasons:

- While the documents are stored encrypted at rest (via PGP) on the SecureDrop *Application Server*, the documents hit server memory unencrypted (unless the source used the GPG key provided to encrypt the documents first before submitting), and are then encrypted in server memory before being written to disk. If the machines are compromised then the security of source material uploaded from that point on cannot be assured. The machines are hardened to prevent compromise for this reason. However, if an attacker has physical access to the servers either because the dedicated servers are located in a datacenter or because the servers are not dedicated and may have another virtual machine co-located on the same server, then the attacker may be able to compromise the machines. In addition, cloud servers are trivially accessible and manipulable by the provider that operates them. In the context of SecureDrop, this means that the provider could access extremely sensitive information, such as the plaintext of submissions or the encryption keys used to identify and access the onion services.
- In addition, attackers with legal authority such as law enforcement agencies may (depending on the jurisdiction) be able to compel physical access, potentially with a gag order attached, meaning that the third party hosting your servers or VMs may be legally unable to tell you that law enforcement has been given access to your SecureDrop servers.

One of the core goals of SecureDrop is to avoid the potential compromise of sources through the compromise of third-party communications providers. Therefore, we consider the use of virtualization for production instances of SecureDrop to be an unacceptable compromise and do not support it. Instead, dedicated servers should be hosted in a physically secure location in the organization itself. While it is technically possible to modify SecureDrop's automated installation process to work on virtualized servers (for example, we do so to support our CI pipeline), doing so in order to run it on cloud servers is at your own risk and without our support or consent.

Workstations

These components are necessary to do the initial installation of SecureDrop and to process submissions using the air-gapped workflow.

Secure Viewing Station (SVS)

1 physical computer used as an air-gap to decrypt and view submissions retrieved from the *Application Server*.

The chosen hardware should be solely used for this purpose. This system must have a removable wireless card, which will need to be completely removed before use. It must also have a removable storage device, such as a solid state drive (SSD) or a hard disk drive (HDD), which likewise needs to be removed prior to using the system. You will only ever boot directly to the *Secure Viewing Station* USB drive.

Admin/Journalist Workstation(s)

At least 1 physical computer that is used as a workstation for SecureDrop admins and/or journalists.

Each Admin and Journalist will have their own bootable Tails USB with an encrypted persistent partition that they will use to access SecureDrop. You will need at least one *workstation* to boot the Tails USBs, and may need more depending on: the number of admins/journalists you wish to grant access to SecureDrop, whether they can share the same workstation due to availability requirements, geographic distribution, etc.

USB Drive(s)

At least 2 USB drives to use as a bootable Tails USB for the *SVS* and the *Admin Workstation*/*Journalist Workstation*.

If only one person is maintaining the system, you may use the same Tails instance as both the *Admin Workstation* and the *Journalist Workstation*; otherwise, we recommend buying 1 drive for each admin and each journalist.

You will also need 2 additional drives for use as a *Transfer Device* and *Export Device*.

We also recommend buying an additional USB drive for making regular backups of your Tails workstations.

One thing to consider is that you are going to have *a lot* of USB drives to keep track of, so you should consider how you will label or identify them and buy drives accordingly. Drives that are physically larger are often easier to label (e.g. with tape, printed sticker or a label from a labelmaker).

Two-factor Device

Two-factor authentication is used when connecting to different parts of the SecureDrop system. Each admin and each journalist needs a two-factor device. We currently support two options for two-factor authentication:

- Your existing smartphone with an app that computes TOTP codes (e.g. FreeOTP for Android and for iOS).
- A dedicated hardware dongle that computes HOTP codes (e.g. a YubiKey).

Tip

We recommend using FreeOTP (available for Android and for iOS) to generate two-factor codes because it is Free Software. However, if it does not work for you for any reason, alternatives exist:

- Google Authenticator for Android and iOS (proprietary)
- authenticator for the desktop (Free Software)

Transfer Device(s) and Export Device(s)

Journalists need physical media (known as the *Transfer Device*) to transfer encrypted submissions from the *Journalist Workstation* to the *Secure Viewing Station*, to decrypt and view them there. If they deem a submission to be newsworthy, they may need physical media (known as the *Export Device*) to copy it to their everyday workstation.

Our standard recommendation is to use USB drives, in combination with volume-level encryption and careful data hygiene. Our documentation, including the *journalist guide*, is based on this approach. We also urge the use of a secure printer or similar analog conversions to export documents from the *Secure Viewing Station*, whenever possible.

You may want to consider enforcing write protection on USB drives when only read access is needed, or you may want to implement a workflow based on CD-Rs or DVD-Rs instead. We encourage you to evaluate these options in the context of your own threat model.

Please find some notes regarding each of these methods below, and see our recommendations in the *setup guide* for additional background.

USB drives

We recommend using one or multiple designated USB drives as the *Transfer Device(s)*, and one or multiple designated USB drives as the *Export Device(s)*. Whether one or multiple drives are appropriate depends on the number of journalists accessing the system, and on whether the team is distributed or not.

Our documentation explains how the *Transfer Device* can be encrypted using LUKS, and how the *Export Device* can be encrypted using VeraCrypt (which works across platforms). We have not evaluated hardware-based encryption options; if you do select a hardware solution, make sure that both devices work in Tails, and that the *Export Device* also works on the operating system(s) used by journalists accessing the *Secure Viewing Station*.

USB drives with write protection (optional)

When it is consistently applied and correctly implemented in hardware, write protection can prevent the spread of malware from the computers used to read files stored on a *Transfer Device* or an *Export Device*.

It is especially advisable to enable write protection before attaching an *Export Device* to an everyday workstation that lacks the security protections of the Tails operating system. For defense in depth, you may also want to enable write protection before attaching a *Transfer Device* to the *Secure Viewing Station*.

The two main options to achieve write protection of USB drives are:

- drives with a built-in physical write protection switch
- a separate USB write blocker device as used in forensic applications.

DVD-Rs or CD-Rs

Single-use, write-once media can be used to realize a transfer and export workflow that is always one-directional: files are transferred to the *Secure Viewing Station* and the media used to do so are destroyed; files are exported from the *Secure Viewing Station* and the media used to do so are destroyed.

If you want to realize such a workflow, we recommend purchasing separate drives for each computer that will write to or read from the media, to minimize the risks from malware compromising any one drive's firmware.

You will also need a stack of blank DVD/CD-Rs, which you can buy anywhere, and a method to securely destroy media after use. Depending on your threat model, this can be very expensive; a cheap shredder can be purchased for less than $50, while shredders designed for use in Sensitive Compartmented Information Facilities (SCIFs) sell for as much as $3,000.

Monitor, Keyboard, Mouse

You will need these to do the initial installation of Ubuntu on the *Application* and *Monitor Servers*.

Depending on your setup, you may also need these to work on the *SVS*.

1.26.4 Optional Hardware

This hardware is not *required* to run a SecureDrop instance, but most of it is still recommended.

Offline Printer

We highly recommend purchasing a printer for your *Secure Viewing Station* and using it as the preferred method to make copies of documents received via SecureDrop.

By printing a submission, even a non-technical user can effectively mitigate many of the complex risks associated with malware or hidden metadata embedded in files received via SecureDrop. Your organization may also already have robust procedures in place for destroying sensitive printed documents.

Important

To maintain the integrity of the air-gap, this printer should be dedicated to use with the *Secure Viewing Station*, connected via a wired connection, and should not have any wireless communication capabilities.

While printing is notable for what it strips away, it is also important to remember what it preserves: QR codes or links that journalists may scan or type in; printer tracking information included in a scanned document; other visually encoded information. See the *Risks From Malware* section in the Journalist Guide for further guidance on this subject.

Offline Storage

The *SVS* is booted from a Tails USB drive, which has an encrypted persistent volume but typically has a fairly limited storage capacity since it's just a USB drive. For installations that expect to receive a large volume of submissions, we recommend buying an external hard drive or solid state drive that can be used to store submissions that have been transferred from the *Application Server* to the *SVS*.

Important

Like all storage media associated with SecureDrop, this drive should be encrypted and protected with a secure passphrase. We recommend using the tools built into Tails to encrypt the drive using LUKS.

If you are planning to use hardware RAID and/or hardware-based encryption, we recommend that you research Tails compatibility before a procurement decision.

Backup Storage

It's useful to run periodic backups of the servers in case of failure. We recommend buying an external hard drive to store server backups.

Because this drive will be connected to the *Admin Workstation* to perform backups, it should *not* be the same drive used for *Offline Storage*.

Important

Like all storage media associated with SecureDrop, this drive should be encrypted and protected with a secure passphrase. We recommend using the tools built into Tails to encrypt the drive using LUKS.

If you are planning to use hardware RAID and/or hardware-based encryption, we recommend that you research Tails compatibility before a procurement decision.

Labeling Equipment

As you have probably noticed by now, a SecureDrop installation has a plethora of components. Some of these components can be hard to tell apart; for example, if you buy 3 of the same brand of USB sticks to use for the Admin Workstation, Journalist Workstation, and Secure Viewing Station, they will be indistinguishable from each other unless you label them. We recommend buying some labeling equipment up front so you can label each component as you provision it during the installation process.

There is a multitude of options for labeling equipment. We've had good results with small portable labelmakers, such as the Brother P-Touch PT-210 or the Epson LabelWorks LW-300. We like them because they produce crisp, easy-to-read labels, and it's easy to customize the size of the label's text, which is great for clearly labeling both large components (like computers) and small components (like USB sticks).

If you do not have a label maker available but have an inkjet printer available to you, it may also be possible to print and cut out labels using adhesive-backed paper and some scissors. These are some labels designed by our team which may be used for labeling:

- `Admin Workstation Label`
- `Journalist Workstation Label`
- `Secure Viewing Station Label`
- `Firewall Label`
- `Application Server Label`
- `Monitor Server Label`
- `Admin TAILS USB Drive Label`
- `Journalist TAILS USB Drive Label`
- `Secure Viewing Station TAILS USB Drive Label`
- `File Transfer USB Drive Label`

1.26.5 SecureBoot

SecureBoot is a feature available on most systems that, when enabled, does not allow any operating system to boot that has not been signed by a trusted key. By only booting to operating systems that are properly signed, you can be sure that the OS itself has not been corrupted or tampered with, at least at the boot level.

While preparing your hardware for a SecureDrop installation, you will want to make sure SecureBoot is enabled for the Workstations, and disabled for the Servers.

For instructions on how to enable or disable the SecureBoot feature for your device, please consult the manufacturer's manual for BIOS settings, as they differ for each make and model.

SecureBoot for Workstations

The **Secure Viewing Station**, **Admin Workstation**, and **Journalist Workstation** should all have SecureBoot enabled.

Some systems, including recent ThinkPads, require you to specifically enable the Third-Party UEFI Certificate Authority within the SecureBoot settings to boot to Tails. If your system has SecureBoot enabled but is not booting to the device you select in the boot menu, go to the BIOS settings and look for the Third-Party CA Option.

On ThinkPads, this can be found within the BIOS by going to **Security** ▸ **SecureBoot** ▸ **Allow Microsoft 3rd Party UEFI CA**, and setting the switch to the on position.

SecureBoot for Servers

SecureBoot must be disabled on the server hardware. During the installation, SecureDrop installs a hardened, security-focused version of the Linux kernel (grsec) that does not support SecureBoot. If SecureBoot is enabled on either of the servers during the install, you will receive a pre-install error reminding you that it must be turned off before the installation can proceed.

1.26.6 Specific Hardware Recommendations

Application and Monitor Servers

We recommend using NUCs for the servers and routinely test new models for compatibility. NUCs ("Next Unit of Computing") are comparatively inexpensive, compact, quiet, and low-power devices, which makes them suitable for deployment in a wide range of environments. Originally produced by Intel, ASUS has taken over production beginning with the 13th generation.

There are a variety of models to choose from. We currently recommend the 11th through 13th generation NUC models listed below.

Note

If using non-recommended hardware, ensure you remove as much extraneous hardware as physically possible from your servers. This could include: speakers, cameras, microphones, fingerprint readers, wireless, and Bluetooth cards.

Note

If using non-recommended hardware, you may require drivers that are not available in the kernel that ships by default in the version of Ubuntu Server we recommend. In this event, you may need to select the Hardware Enablement Kernel (HWE) during boot, which supports more recent hardware. To do so, select the "Boot and Install with the HWE Kernel" option in the boot menu for Ubuntu Server.

NUCs typically come as kits, and some assembly is required. You will need to purchase the RAM and hard drive separately for each NUC and insert both into the NUC before it can be used. We recommend:

- 2x 240GB SSDs (2.5" or M.2, depending on your choice of kit)
- 1x memory kit of compatible 2x8GB sticks - You can put one 8GB memory stick in each of the servers.

14th-gen NUC

We have tested and can recommend the ASUS NUC14RVH. It provides both 22x80 and 22x42 M.2 ports for NVMe SSD storage, as well as a 2.5 inch drive bay for a SATA hard drive or SSD (if using this slot, we recommend choosing an SSD).

The NUC14's AX211 wireless hardware is not removable. Before installation of the RAM and storage, we recommend that you disconnect the wireless antennae leads from the AX211 component. They're the wires highlighted in the red box in the picture. Cover the free ends with electrical tape after disconnecting them.

Note

The wireless card is located underneath the NVMe port

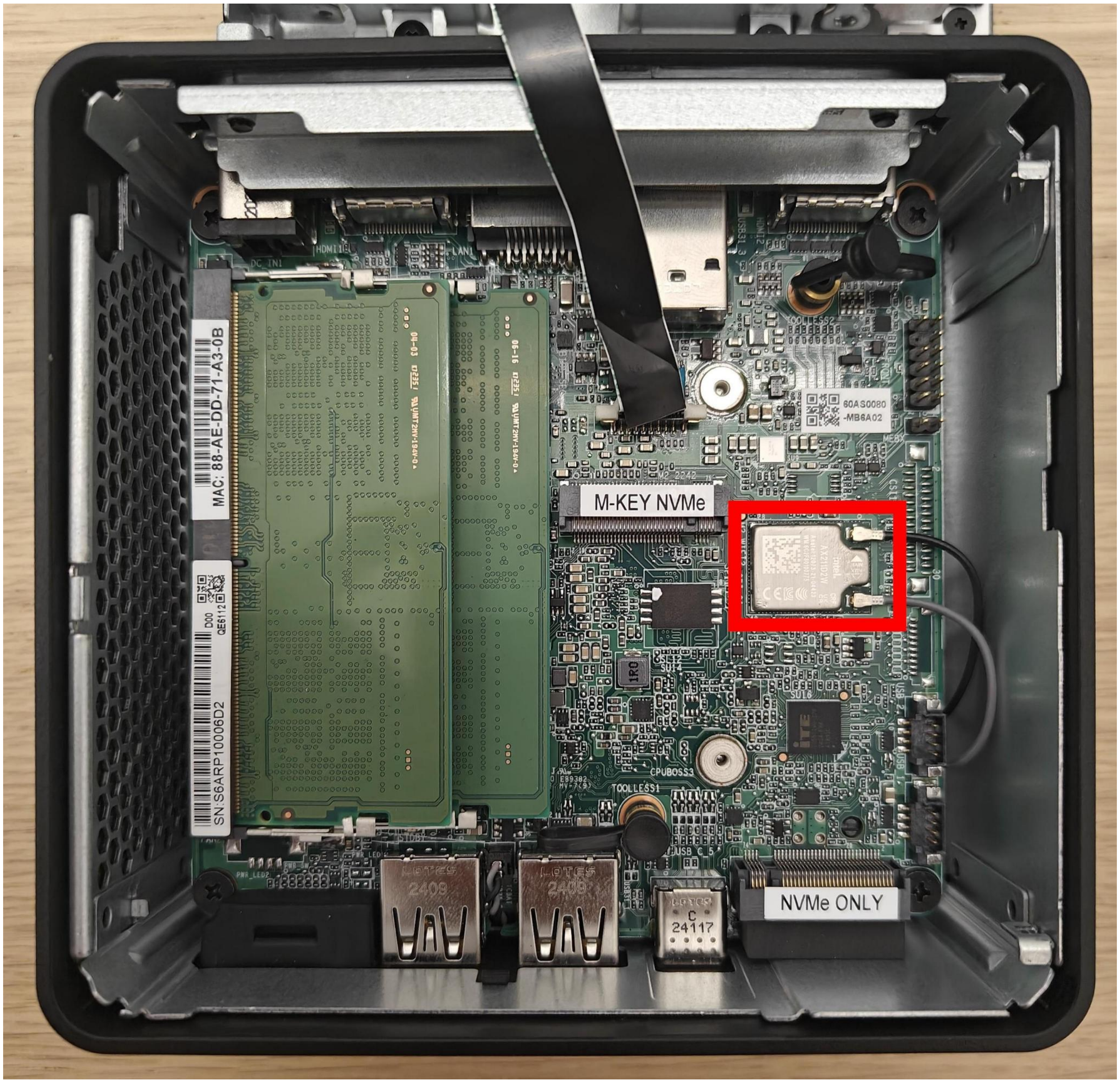


Fig. 1: The location of the wireless card within the NUC14

13th-gen NUC

We have tested and can recommend the ASUS NUC13ANHi5. It provides two M.2 SSD storage options: a 22x80 port for an NVMe drive, and a 22x42 port for a SATA drive. It also has a 2.5 inch drive bay for a SATA hard drive or SSD (if using this slot, we recommend choosing an SSD).

The NUC13's AX211 wireless hardware is removable. Doing so requires the use of a 5mm nut driver. Before installation of the RAM and storage, we recommend that you remove the wireless card and disconnect the wireless antennae leads from the AX211 component. Be sure to cover the free ends with electrical tape after disconnecting them.

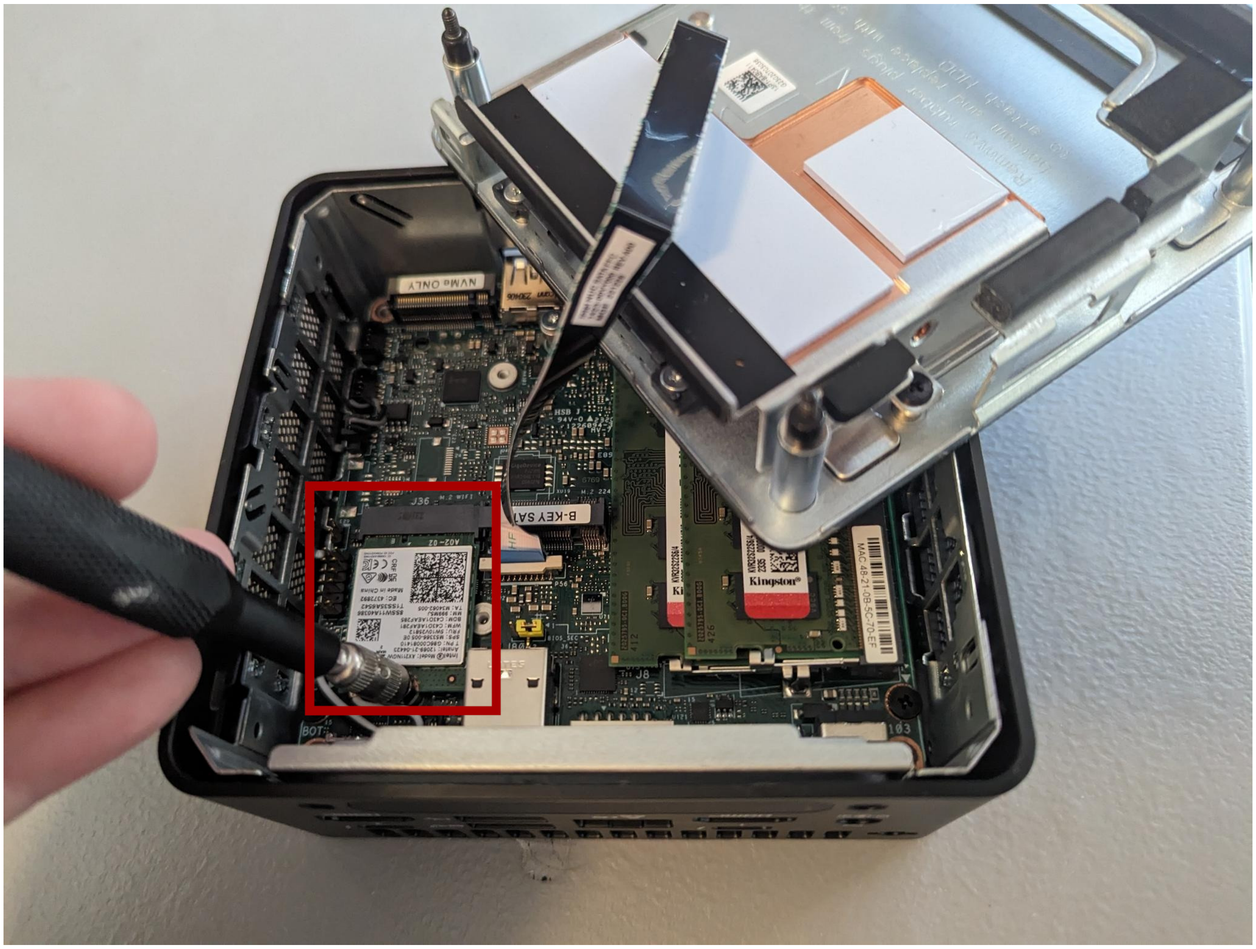


Fig. 2: The location of the wireless card within the NUC13

Note

The wireless card is located underneath the 22x80 NVMe port

12th-gen NUC

We have tested and can recommend the NUC12WSKi5. It provides two M.2 SSD storage options: a 22x80 port for an NVMe drive, and a 22x42 port for a SATA drive.

The NUC12's AX211 wireless hardware is removable. Doing so requires the use of a 5mm nut driver. Before installation of the RAM and storage, we recommend that you remove the wireless card and disconnect the wireless antennae leads from the AX211 component. Be sure to cover the free ends with electrical tape after disconnecting them.

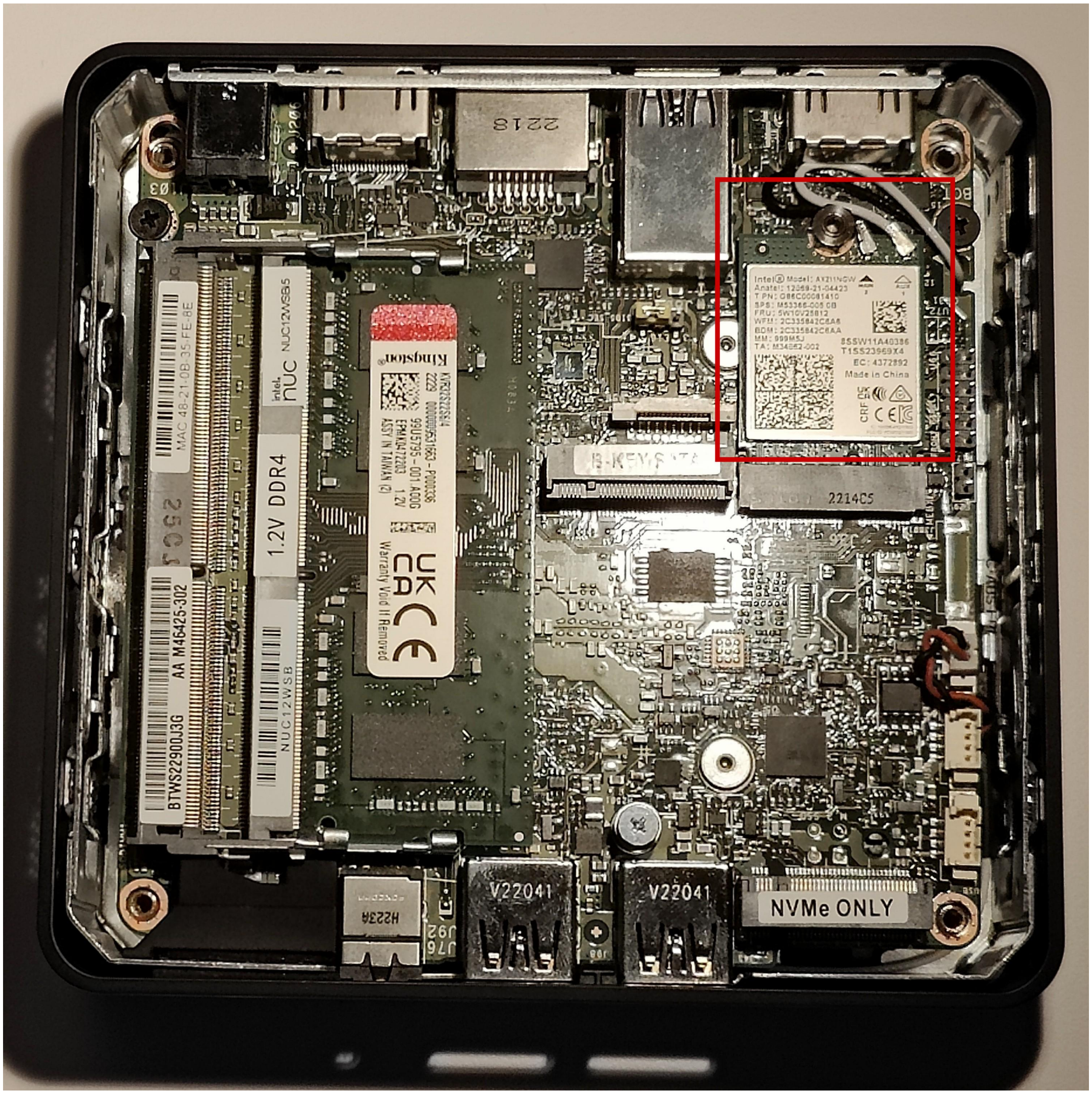
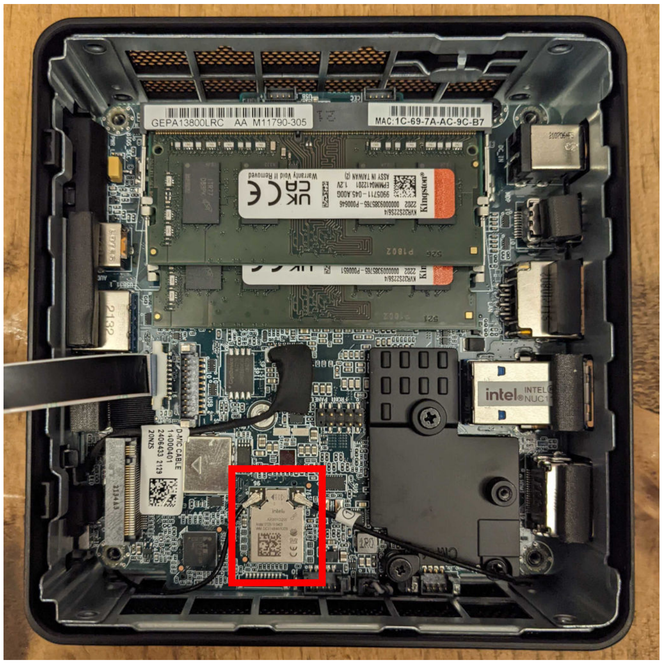


Fig. 3: The location of the wireless card within the NUC12

11th-gen NUC

We have tested and can recommend the Intel NUC11PAHi3. It provides two storage options: M.2 SSD storage and a 2.5” secondary storage option (SSD or HDD).

The NUC11’s AX201 wireless hardware is not removable. Before installation of the RAM and storage, we recommend that you disconnect the wireless antennae leads from the AX201 component. They’re the black wires highlighted in the red box in the picture. Cover the free ends with electrical tape after disconnecting them.



Before the initial OS installation, boot into the BIOS by pressing **F2** at startup and adjust the system configuration:

- Under **Advanced** ▶ **Onboard Devices**, disable all onboard devices other than LAN: HD audio, microphone, Thunderbolt, WLAN, Bluetooth, SD card controller, and enhanced consumer infrared.
- Under **Boot** ▶ **Secure Boot**, disable **Secure Boot** using the drop-down menu.

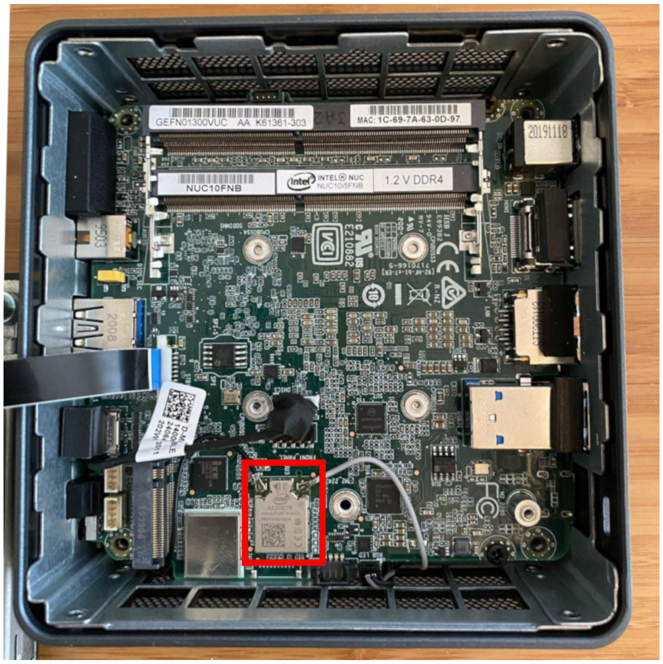
Note

Unlike some previous generation NUCs we recommended, the NUC11PAHi3 does not support SGX. However, if you use a different type of 11th generation NUC that does have SGX support, disable it under **Security** ▶ **Security Features**, as it is not used by SecureDrop but may be targeted by active CPU exploits.

10th-gen NUC

We previously recommended the NUC10i5FNH, however it is now end-of-life so we recommend replacing it with a version that the manufacturer supports. While SecureDrop will most likely continue working in the short-term, we will no longer be testing on this hardware. The instructions below are included only for reference and will be removed in the near future.

The NUC10's AX201 wireless hardware is not removable. Before installation of the RAM and storage, we recommend that you disconnect the wireless antennae leads from the AX201 component. They're the black and gray wires highlighted in the red box in the picture. Cover the free ends with electrical tape after disconnecting them.



Before the initial OS installation, boot into the BIOS by pressing **F2** at startup and adjust the system configuration:

- Under **Advanced ▶ Onboard Devices**, disable all onboard devices other than LAN: HD audio, microphone, Thunderbolt, WLAN, Bluetooth, SD card controller, and enhanced consumer infrared.
- Under **Security ▶ Security Features**, disable SGX support, which is not used by SecureDrop and may be targeted by active CPU exploits.
- Under **Boot ▶ Secure Boot**, uncheck the **Secure Boot** checkbox.

8th-gen NUC

We previously recommended the NUC8i5BEK, however it is now end-of-life so we recommend replacing it with a version that the manufacturer supports. While SecureDrop will most likely continue working in the short-term, we will no longer be testing on this hardware.

7th-gen NUC

We previously recommended the NUC7i5BNH, however it is now end-of-life so we recommend replacing it with a version that the manufacturer supports. While SecureDrop will most likely continue working in the short-term, we will no longer be testing on this hardware.

Journalist Workstation and Admin Workstation

Both the *Journalist Workstation* and the *Admin Workstation* must be compatible with the Tails operating system. Compare any hardware you want to procure or allocate for this purpose against the list of known issues maintained by the Tails project, but please be advised that the list is far from exhaustive.

We advise against using Macs, as there are many Tails compatibility issues both with older and with newer models. Instead, we recommend the ThinkPad T series. The ThinkWiki is an excellent, independently maintained resource for verifying general Linux compatibility of almost any ThinkPad model.

For any Tails workstation, we recommend at least 8GB of RAM.

Secure Viewing Station (SVS)

The *Secure Viewing Station* is a machine that is kept offline and only ever used together with the Tails operating system. This machine will be used to generate the GPG keys used by SecureDrop to encrypt submissions, as well as decrypt and view submissions. Since this machine will never touch the Internet or run an operating system other than Tails, it does not need a hard drive or network device; in fact, we recommend removing these components if they are already present.

As with the workstations, one good option is to buy a Linux-compatible laptop from the Lenovo ThinkPad series. It's possible to re-purpose old laptops from other manufacturers, as long as the wireless components are removable.

If you are purchasing a new laptop for use as a *Secure Viewing Station*, you will want to ensure you are purchasing a model with a removable wireless card and removable storage. We have tested the following laptops with removable components, and can confirm compatibility within Tails:

- Framework 13 laptop (Intel)
- Lenovo Thinkpad T14 (2nd generation)

For other models, we recommend that you check the service manual for the specific generation/model of laptop. For example, according to the service manual for the Thinkpad X1 Carbon, it uses a standard removable M.2-based wireless card.

Just as with the servers, you can also use a NUC for the *SVS*. As noted before, NUCs do not ship with a storage drive, and older models can be configured without any wireless components. However, NUCs *do* contain an IR receiver, which we recommend taping over with opaque masking tape.

If you choose to use a NUC, you must use a model that offers wireless as an **option** (described as something like `M.2 22×30 slot and wireless antenna pre-assembled (for wireless card support)`). If a model is advertised as having "integrated wireless" (most newer NUC models), this means the wireless components are not physically removable, and these machines are not a suitable choice for the *SVS*.

Tails USBs

We *strongly recommend* getting USB 3.0-compatible drives to run Tails from. The transfer speeds are significantly faster than USB 2.0, which means a live operating system booting from one will be much faster and more responsive.

You will need *at least* an 8GB drive to run Tails with an encrypted persistent partition. We recommend getting something in the 32-128GB range so you can handle large amounts of submissions without hassle. Anything more than that is probably overkill.

Transfer Device(s) and Export Device(s)

For USB drives with physical write protection, we have tested the Kanguru SS3 on Tails, and it works well with and without encryption.

If you want to use a setup based on CD-Rs or DVD-Rs, we've found the CDR/DVD writers from Samsung and LG to work reasonably well; you can find some examples here.

Please see our recommendations in the *setup guide* for additional background.

Network Firewall

We recommend a 4 NIC network firewall and currently provide setup instructions for pfSense and OPNSense. Suitable models include:

- the Protectli Vault 4-Port, running OPNSense configured with coreboot.
- the Netgate SG-4100 running pfSense Plus.
- the Netgate SG-6100 running pfSense Plus. This device is overspecced for SecureDrop's purposes, but can be used if the other cheaper firewalls can't be procured.

Printers

Careful consideration should be given to the printer used with the *SVS*. Most printers today have wireless functionality (WiFi or Bluetooth connectivity) which should be **avoided** because it could be used to compromise the air-gap.

Unfortunately, it is difficult to find printers that work with Tails, and it is increasingly difficult to find non-wireless printers at all. To assist you, we have compiled the following partial list of air-gap-safe printers that have been tested and are known to work with Tails:

Printer Model	Testing Date	Tails Versions	Printer Type
HP DeskJet F4200	06/2017	3.0	Color Inkjet
HP DeskJet 1112	06/2017	3.0	Color Inkjet
HP DeskJet 1110	08/2017	3.1	Color Inkjet
HP LaserJet 400 M401n	06/2015	1.4	Monochrome Laser
HP DeskJet 6940	04/2015	1.3.2	Monochrome Inkjet

Note

We've documented both the HP DeskJet F4200 and HP LaserJet 400 M401n with screenshots of the installation process, in our section on *Setting Up a Printer in Tails*. While the F4200 installed automatically, the 400 M401n required that we set "Make and model" to "HP LaserJet 400 CUPS+Gutenprint v5.2.9" when manually configuring the drivers.

If you know of another model of printer that fits our requirements and works with Tails, please submit a pull request to add it to this list.

Monitor, Keyboard, Mouse

We don't have anything specific to recommend when it comes to displays. You should make sure you know what monitor cable you need for the servers, since you will need to connect them to a monitor to do the initial Ubuntu installation.

You should use a wired (USB) keyboard and mouse, not wireless.

Hardware End-of-Life

No matter what hardware you decide to use, it's important to be mindful of how long it will continue to receive security updates. Given the security requirements for a SecureDrop instance, any hardware that is no longer receiving security updates from the manufacturer will become more and more vulnerable over time. Once your hardware has reached its end-of-life (EOL), we recommend upgrading to newer, supported hardware.

For the hardware we recommend, you can find a list of end-of-life dates below:

Hardware	End-of-Life (EOL)
ASUS NUC14RVH	Not yet confirmed
ASUS NUC13ANHi5	Not yet confirmed
Intel NUC12WSKi5	April 05, 2026
Intel NUC11PAHi3	September 30, 2026
Intel NUC10i5FNH	June 25, 2024
Intel NUC8i5BEK	March 26, 2024
Intel NUC7i5BNH	April 30, 2023
Thinkpad T420 (SVS)	Already EOL; use only for airgapped SVS
Thinkpad T Series	EOL dates vary; consult with manufacturer
TekLager APU4D4	Not yet confirmed
Netgate SG-4100	Not yet confirmed (will be 2 years after sales stop)
Netgate SG-6100	Not yet confirmed (will be 2 years after sales stop)

1.27 Minimum requirements for the SecureDrop environment

- The *Application* and *Monitor Servers* should be dedicated physical machines, not virtual machines.
- A trusted location to host the servers. The servers should be hosted in a location that is owned or occupied by the organization to ensure that their legal department can not be bypassed with gag orders.
- The SecureDrop servers should be on a separate internet connection or completely segmented from the corporate network, such as a dedicated subnet with DENY rules for all traffic to and from the corporate LAN.
- All traffic from the corporate network should be blocked at the SecureDrop's point of demarcation.
- Video monitoring should be recorded of the server area and the organizations safe.
- Journalists should ensure that while using the air-gapped viewing station they are in an area without video cameras.
- An established monitoring plan and incident response plan. Who will receive the OSSEC alerts and what will their response plan be? These should cover technical outages and a compromised environment plan.

1.28 Create USB Boot Drives

1.28.1 Overview

For the initial SecureDrop setup, you will need three USB drives.

Two of them will be used for the Tails operating system, for creating the *Admin Workstation* and *Secure Viewing Station*.

The other USB drive will have the Ubuntu Server installer, which is needed to install the underlying server OS for your *Application* and *Monitor Servers*.

Important

As soon as you create a new drive, be sure to *label it immediately*. USB drives all look alike and you're going to be juggling a whole bunch of them throughout this installation. Label immediately. Always.

1.28.2 Tails Introduction

Tails is a privacy-enhancing live operating system that runs on removable media, such as a DVD or a USB stick. It sends all your Internet traffic through Tor, does not touch your computer's hard drive, and securely wipes unsaved work on shutdown.

Most of the work of installing, administering, and using SecureDrop is done from computers using Tails, so the first thing you need to do is set up several USB drives with the Tails operating system. To get started, you'll need two Tails drives: one for the *Admin Workstation* and one for the *Secure Viewing Station*. *Later*, you'll set up a bunch more Tails drives for your journalists and backups, but for now you just need two.

Install Tails

The Tails website has detailed and up-to-date instructions on how to download and verify Tails, and how to create a bootable Tails USB drive.

Follow the instructions at these links and then return to this page:

- Download and verify the Tails image file
- Install onto a USB drive

Important

Make sure you verify the Tails .img file using one of the methods described on the Tails website.

You will need to create 2 Tails USBs to perform the SecureDrop installation:

1. The *Secure Viewing Station* Tails USB.
2. The *Admin Workstation* Tails USB.

Tip

This process will take some time, most of which will be spent waiting around.

Enable Persistent Storage

By default, everything you save while running Tails will be securely erased and discarded when you power off or reboot your system.

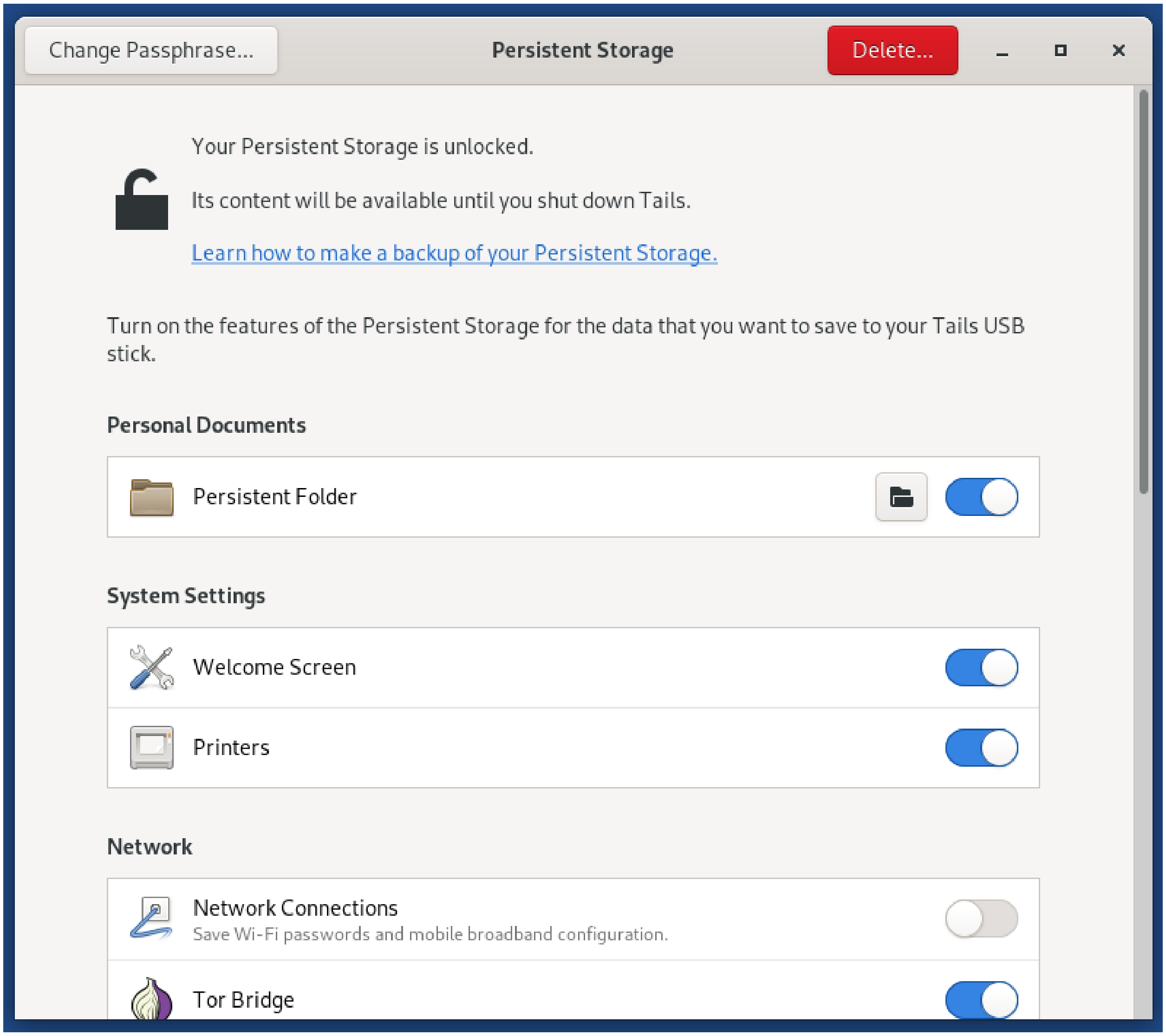
Because we will need to keep certain settings and files saved between sessions, you will need to enable persistence.

Creating an encrypted persistent volume will allow you to securely save information and settings in the free space that is left on your Tails drive. You will need to create a persistent storage on each Tails drive. Each drive's persistent storage partition needs its own unique, complex passphrase that's easy to write down or remember.

For instructions on how to generate a strong passphrase, see *the Passphrases page*.

Please use the instructions on the Tails website to make the persistent volume on each Tails drive you create. When creating the persistence volume, you will be asked to select from a list of features, such as 'Personal Data'. You should enable **all** features by selecting each item in the list.

Beginning with Tails 5.8, a Persistent Storage application is provided which will allow you to enable or disable features without requiring a restart. You can also use this tool to change the passphrase of the persistent volume (provided you still know the original passphrase).



Your Persistent Storage is unlocked.

Its content will be available until you shut down Tails.

Learn how to make a backup of your Persistent Storage.

Turn on the features of the Persistent Storage for the data that you want to save to your Tails USB stick.

Personal Documents

Persistent Folder: ●

System Settings

Welcome Screen: ●

Printers: ●

Network

Network Connections: ○
Save Wi-Fi passwords and mobile broadband configuration.

Tor Bridge: ●

Some other things to keep in mind:

- Right now, you need to create a persistent volume on both the *Admin Workstation* Tails drive and the *Secure Viewing Station* Tails drive.
- Each journalist will need their own Tails drive with their own persistent volume secured with their own passphrase — but *that comes later*.

Note

Tails doesn't always completely shut down and reboot properly when you click "restart", so if you notice a significant delay, you may have to manually power off and restart your computer for it to work properly.

Warning

Make sure that you never use the *Secure Viewing Station* Tails drive on a computer connected to the Internet or a local network. This Tails drive will only be used on the air-gapped *Secure Viewing Station*.

1.28.3 Ubuntu Introduction

Note

Installing Ubuntu is simple and may even be something you are very familiar with, but it is **strongly** encouraged that you read and follow this documentation exactly as there are some “gotchas” that may cause your SecureDrop setup to break.

The SecureDrop *Application Server* and *Monitor Server* run **Ubuntu Server 24.04.3 LTS (Noble Numbat)**. To install Ubuntu on the servers, you must first download and verify the Ubuntu installation media.

Download the Ubuntu Installation Media

The installation media and the files required to verify it are available on the Ubuntu Releases page. You will need to download the following files:

- ubuntu-24.04.3-live-server-amd64.iso
- SHA256SUMS
- SHA256SUMS.gpg

Alternatively, you can use the command line:

```
cd ~/Downloads
curl -OOO https://releases.ubuntu.com/24.04.3/{ubuntu-24.04.3-live-server-amd64.iso,
↪SHA256SUMS{,.gpg}}
```

Verify the Ubuntu Installation Media

You should verify the Ubuntu image you downloaded hasn’t been modified by a malicious attacker or otherwise corrupted. To do so, check its integrity with cryptographic signatures and hashes.

First, download both *Ubuntu Image Signing Keys* and verify their fingerprints.

```
gpg --recv-key --keyserver hkps://keyserver.ubuntu.com \
"C598 6B4F 1257 FFA8 6632 CBA7 4618 1433 FBB7 5451" \
"8439 38DF 228D 22F7 B374 2BC0 D94A A3F0 EFE2 1092"
```

Note

It is important you type this out correctly. If you are not copy-pasting this command, double-check you have entered it correctly before pressing enter.

Again, when passing the full public key fingerprint to the `--recv-key` command, GPG will implicitly verify that the fingerprint of the key received matches the argument passed.

Caution

If GPG warns you that the fingerprint of the key received does not match the one requested **do not** proceed with the installation. If this happens, please email us at securedrop@freedom.press.

Next, verify the `SHA256SUMS` file.

```
gpg --keyid-format long --verify SHA256SUMS.gpg SHA256SUMS
```

Move on to the next step if you see "Good Signature" in the output, as below. Note that any other message (such as "Can't check signature: no public key") means that you are not ready to proceed.

```
gpg: Signature made Thu 11 Feb 2021 02:07:58 PM EST
gpg:                using RSA key 843938DF228D22F7B3742BC0D94AA3F0EFE21092
gpg: Good signature from "Ubuntu CD Image Automatic Signing Key (2012) <cdimage@ubuntu.
↪com>" [unknown]
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 8439 38DF 228D 22F7 B374  2BC0 D94A A3F0 EFE2 1092
```

The next and final step is to verify the Ubuntu image.

```
sha256sum -c <(grep ubuntu-24.04.3-live-server-amd64.iso SHA256SUMS)
```

If the final verification step is successful, you should see the following output in your terminal.

```
ubuntu-24.04.3-live-server-amd64.iso: OK
```

Caution

If you do not see the line above it is not safe to proceed with the installation. If this happens, please contact us at securedrop@freedom.press.

Create the Ubuntu Installation Media

The Ubuntu website has detailed instructions on how to to create a bootable Ubuntu Server USB drive.

Follow the instructions at the link below for your operating system, then return to this page:

- Create a bootable Ubuntu USB drive on Mac
- Create a bootable Ubuntu USB drive on Windows
- Create a bootable Ubuntu USB drive on Linux

1.29 Set Up the *Secure Viewing Station*

The *Secure Viewing Station* is the computer where journalists read and respond to SecureDrop submissions. Once submissions are encrypted on the *Application Server*, only the *Secure Viewing Station* has the key to decrypt them. The *Secure Viewing Station* is never connected to the internet or a local network, and only ever runs from a dedicated Tails drive. Journalists download encrypted submissions using their *Journalist Workstation*, copy them to a *Transfer Device* (a USB drive or a DVD) and physically transfer the *Transfer Device* to the *Secure Viewing Station*.

We recommend storing your *Secure Viewing Station* in a secure area on-site, and ensuring it does not leave this area. If you have journalists working outside of your premises, you may want to consider setting up a *remote Secure Viewing Station*.

Since the *Secure Viewing Station* never uses a network connection or an internal hard drive, we recommend that you physically remove any internal storage devices or networking hardware such as wireless cards or Bluetooth adapters. If the machine has network ports you can't physically remove, you should clearly cover these ports with labels noting not to use them. For an even safer approach, fill a port with epoxy to physically disable it. We also recommend you remove the speakers from the device (or just cut the audio cables if that's easier). This is to prevent exfiltration of data from the airgap via ultrasonic audio, which cannot be heard by humans. If you have questions about repurposing hardware for the *Secure Viewing Station*, contact the Freedom of the Press Foundation.

The steps below assume you have already *created a Tails USB drive with Persistent Storage enabled*. If that is not the case, please review the previous page in the installation guide, then return here once the new Tails drive is ready.

The Tails drive should be clearly labeled "SecureDrop Secure Viewing Station". If it's not labeled, label it right now, then boot it on the *Secure Viewing Station*. After it loads, you should see the Tails Welcome Screen.

Enter your passphrase to unlock the persistent storage, then press **Unlock**. Before starting Tails, set an administration password for use with this Tails session. To do so, click the **+** button under "Additional Settings". Click **Administration Password** in the list of settings. Enter the password twice, click **Add**, then click **Start Tails**.

Note

The Tails administration password is a one-time password. It is reset every time you shut down Tails. Pick a password you will be able to remember for the length of this session.

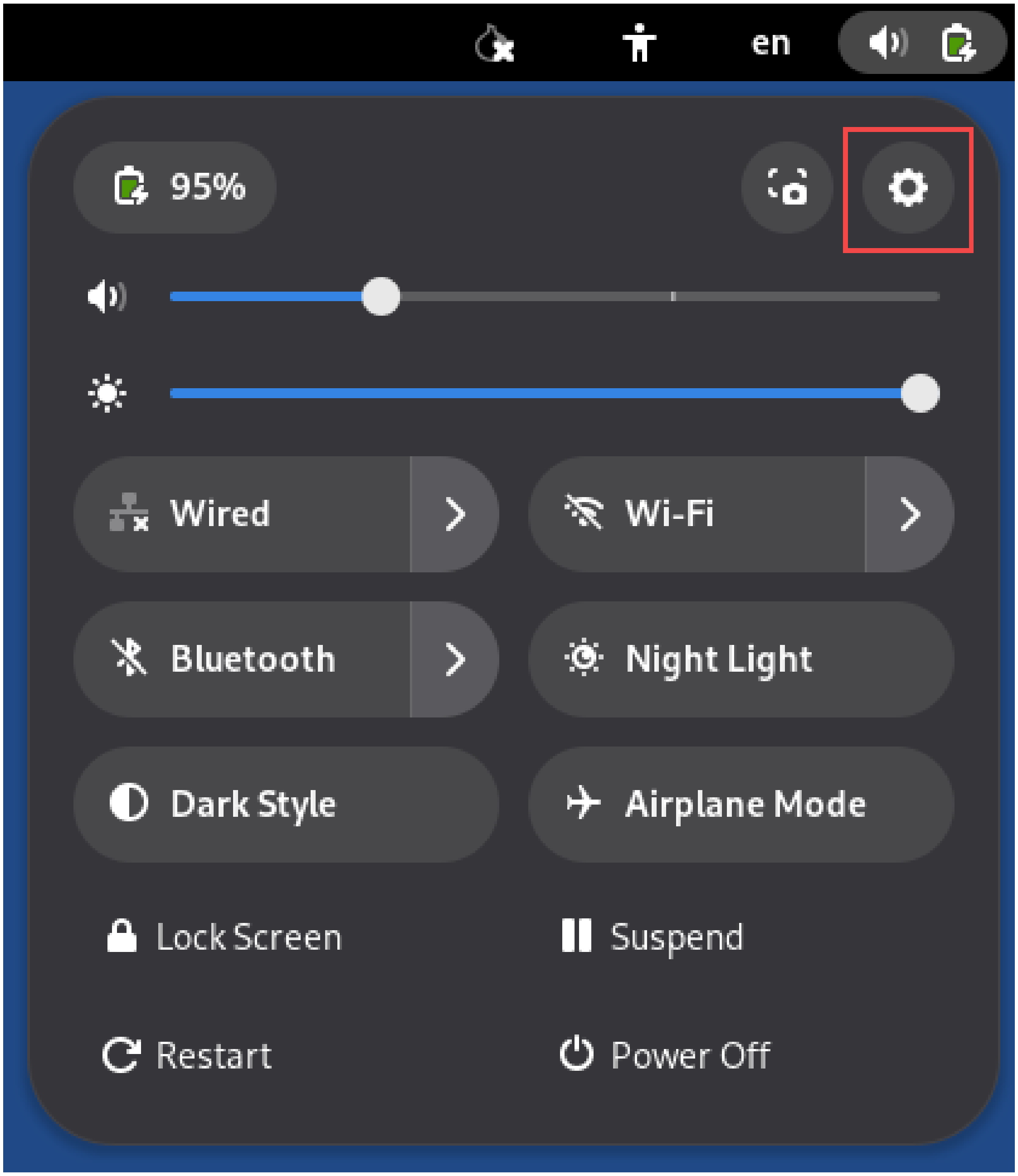
We will now prepare the *Secure Viewing Station*.

1.29.1 Correct the System Time

After booting up Tails on the *Secure Viewing Station*, you will need to manually set the system time before you create the *SecureDrop Submission Key*. This operation requires the Tails administration password to be set (see above).

To set the system time:

1. Click the upper right down arrow in the menu bar and select the gear icon:



2. Select the **Details** section, then click **Date & Time**.
3. Click **Unlock**. Type in the admin password you set when you started up Tails.
4. Set the correct time, region and city.
5. Click **Lock**, exit Settings and wait for the system time to update in the top panel.

1.30 Set Up the *Transfer Device* and the *Export Device*

Journalists copy submissions from their *Journalist Workstation* to the *Secure Viewing Station* using the *Transfer Device*.

For exporting submissions from the *Secure Viewing Station*, we recommend using a secure printer or a similar analog conversion process wherever possible. For cases where an electronic file transfer is necessary, we recommend setting up an *Export Device*, separate from the *Transfer Device*.

Important

Understand the security risks of working with files in digital form

After downloading a submission on the *Journalist Workstation*, a journalist will copy it to the *Transfer Device* and carry it to the air-gapped *Secure Viewing Station* to decrypt and review it. If the journalist then copies the decrypted file in its original form to an Internet-connected computer, they may expose themselves, their colleagues, or their sources to significant risks, e.g.:

- A submission may be infected with malware targeting your newsroom.
- If your *Secure Viewing Station* has not been updated in a while, it may have software vulnerabilities an attacker can exploit, e.g., to exfiltrate the *Submission Private Key* alongside a legitimate submission.
- The submission may contain metadata identifying the source which has not yet been cleaned up.

These risks are not specific to SecureDrop. They're inherent to dealing with tips sent in digital form.

This is why we place the strongest emphasis on always picking the most secure available export method for a given submission. Printing documents or re-recording audio and video files can eliminate most categories of malware and metadata (QR code malware and tracking dots being the most notable exceptions).

If and when you do need to copy decrypted files in electronic form, the recommendations below are intended to establish a baseline of security. Please consider these recommendations in the context of your own threat model, and do not hesitate to contact us via securedrop@freedom.press (GPG encrypted) if we can help.

1.30.1 Choose media types and encryption

You will need to decide what storage media to use for the *Transfer Device* and the *Export Device*, and which encryption scheme to apply to each device. There are many options to consider: USB flash drives, write-once media like CD-Rs and DVD-Rs, external hard drives, and so on.

The following recommendation is intended to balance security, usability and cost considerations, and you may want to modify it based on your threat model:

- Use USB flash drives for both the *Transfer Device* and the *Export Device*.
- Encrypt the *Transfer Device* using LUKS, which works in the Tails environment and in other Linux environments.
- Encrypt the *Export Device* using VeraCrypt, which works across platforms.

If you follow this recommendation, it is important that the contents of the *Transfer Device* and the *Export Device* are always wiped after a copy operation is completed.

Note

You may want to purchase a USB device with a physical write protection switch for the *Export Device*, to enforce write protection whenever it is attached to an Internet-connected everyday workstation. This ensures that malware cannot spread from infected computers in your network to the *Secure Viewing Station*.

Another option is to purchase a hardware USB write blocker as used in forensics, and enforce its usage whenever the *Export Device* is attached to an Internet-connected workstation.

Write-once media like CDs and DVDs can be a reasonable alternative to this setup. If you implement a workflow based on CDs or DVDs, it is crucial that they are destroyed immediately after use. While you can find CD/DVD destroyers at a relatively low cost, those built to the highest standards of security sell in the $2,500 to $3,000 price range as of 2019.

1.30.2 Decide how to manage encryption passphrases

Because files are copied between multiple computers, KeePassXC in Tails is not necessarily the most convenient option for managing the encryption passphrases for your *Transfer Device* or your *Export Device*. While Tails itself gives you the option to "remember" passphrases, this option does not work across reboots.

A simple alternative is to make sure that every journalist stores the *Transfer Device* and *Export Device* passphrases in their own password manager, which ideally will synchronize to their smartphone. See the Freedom of the Press Foundation guide for choosing a password manager if you are not currently using one.

Tip

The user will have to enter this passphrase repeatedly. For this reason, we recommend using diceware instead of random character sequences that are difficult to type. If your password manager does not support generating diceware passphrases, see the EFF guide for information on how to do it yourself.

1.30.3 Create USB *Transfer Device*

The easiest and recommended option for a *Transfer Device* is a USB drive. If you have a large team of journalists you may want to *create several* of these. Here we'll just walk through making one *Transfer Device*[1].

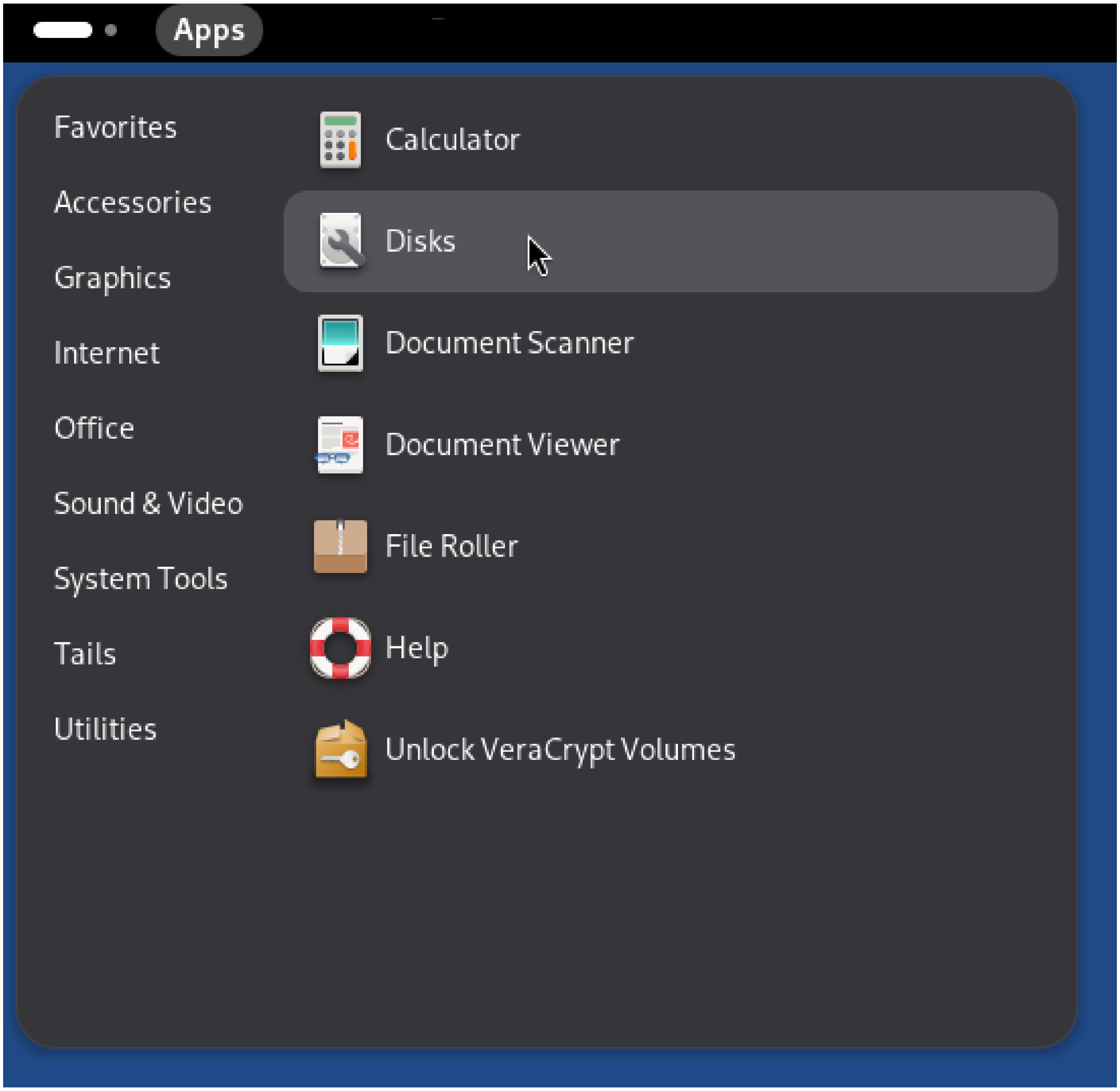
Note

This process will destroy all data currently on the drive.

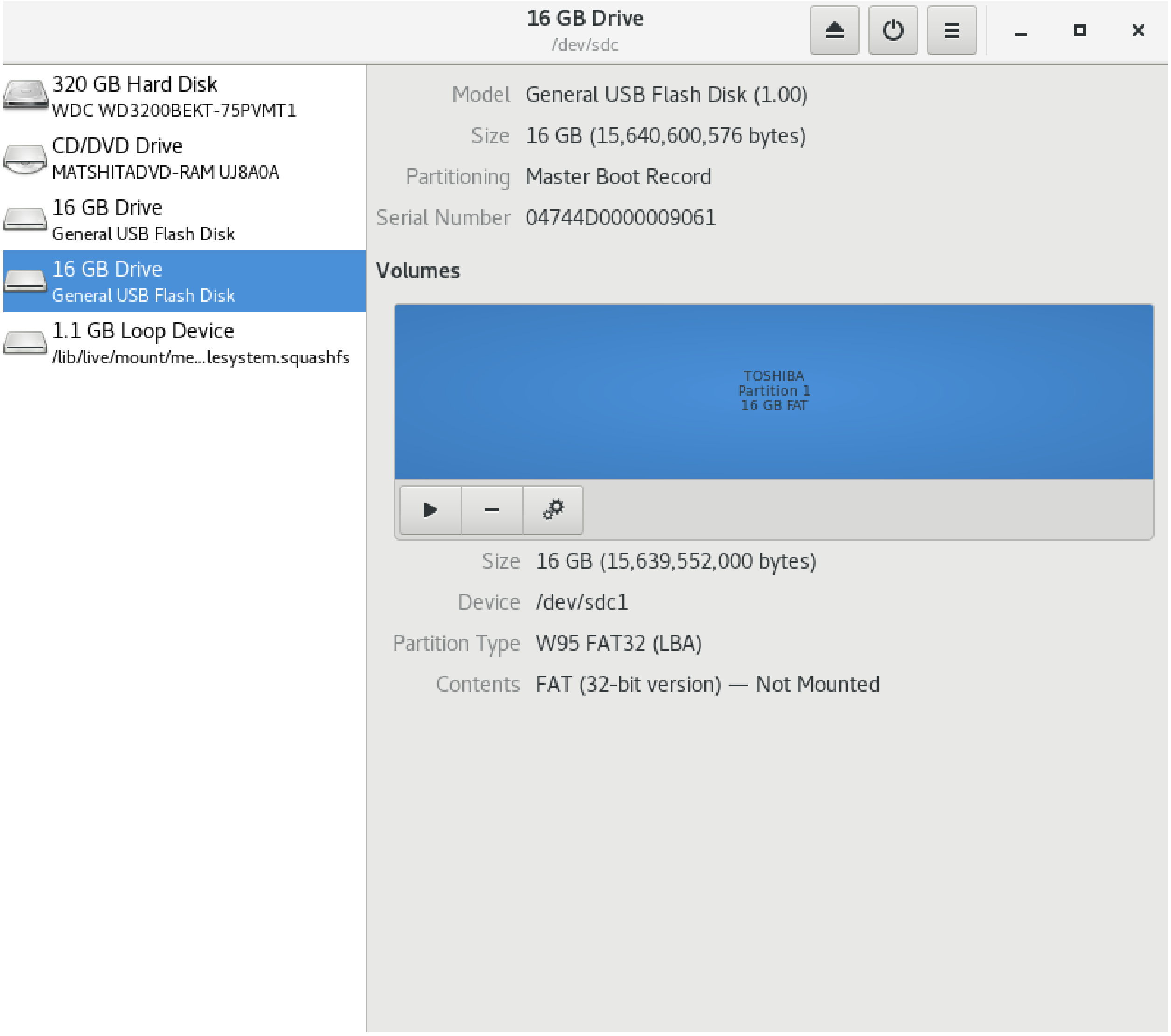
First, label your USB drive "SecureDrop Transfer Device".

On the *Secure Viewing Station*, open the **Apps** menu in the top left corner and select **Utilities** then **Disks**:

[1] Tails screenshots were taken on Tails 4.0.0. Please make an issue on GitHub if you are using the most recent version of Tails and the interface is different from what you see here.



Connect your *Transfer Device* then pick your device in the menu on the left. Since we're going to destroy all the data on this drive, it's important that you pick the right drive. It should be named something that sounds similar to the manufacturer's label on the outside of the drive, and it will only appear after you plug it in. Double check that you have clicked on the correct drive:



320 GB Hard Disk
WDC WD3200BEKT-75PVMT1

CD/DVD Drive
MATSHITADVD-RAM UJ8A0A

16 GB Drive
General USB Flash Disk

16 GB Drive
General USB Flash Disk

1.1 GB Loop Device
/lib/live/mount/me...lesystem.squashfs

Model	General USB Flash Disk (1.00)
Size	16 GB (15,640,600,576 bytes)
Partitioning	Master Boot Record
Serial Number	04744D0000009061

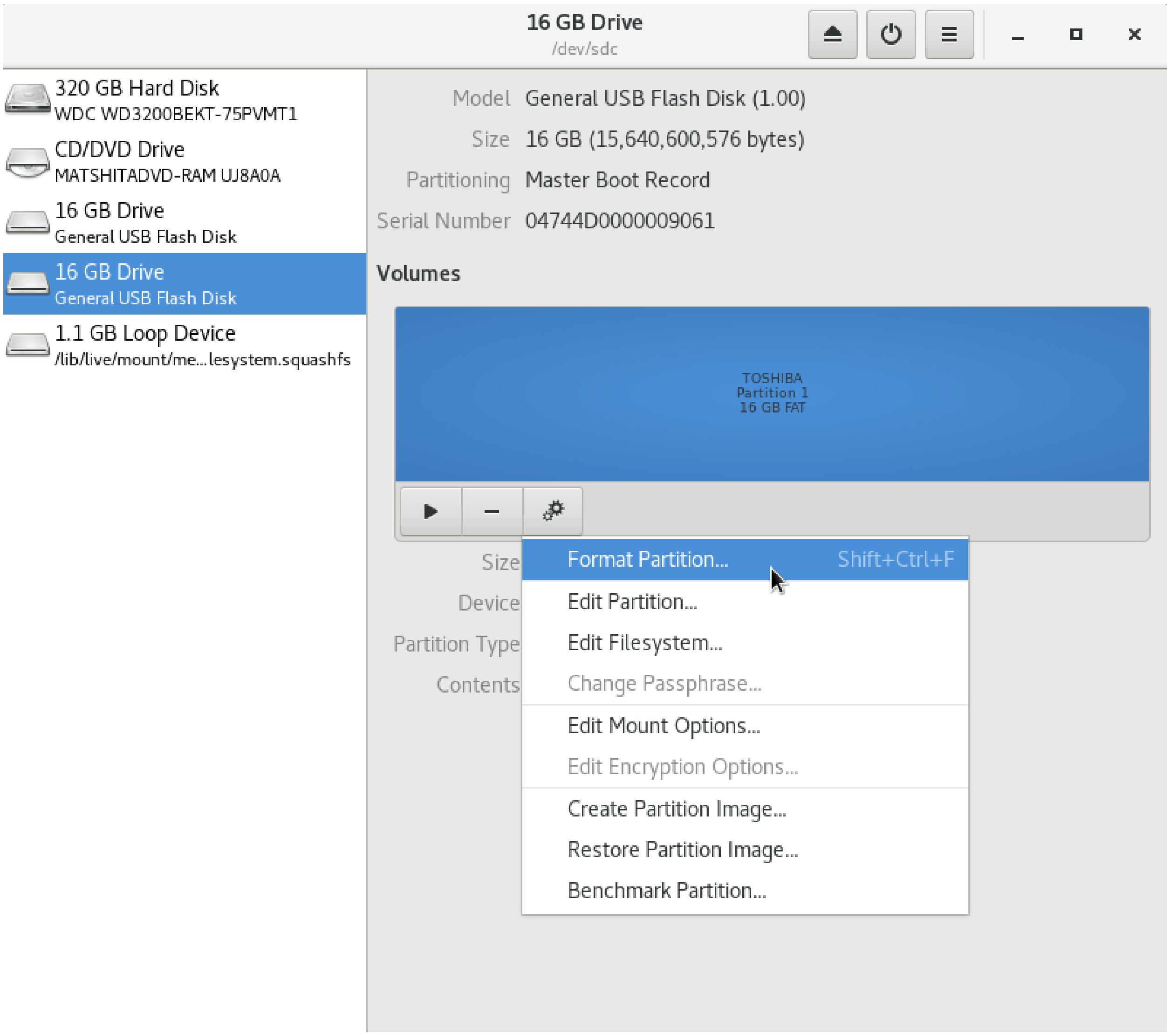
Volumes

Size	16 GB (15,639,552,000 bytes)
Device	/dev/sdc1
Partition Type	W95 FAT32 (LBA)
Contents	FAT (32-bit version) — Not Mounted

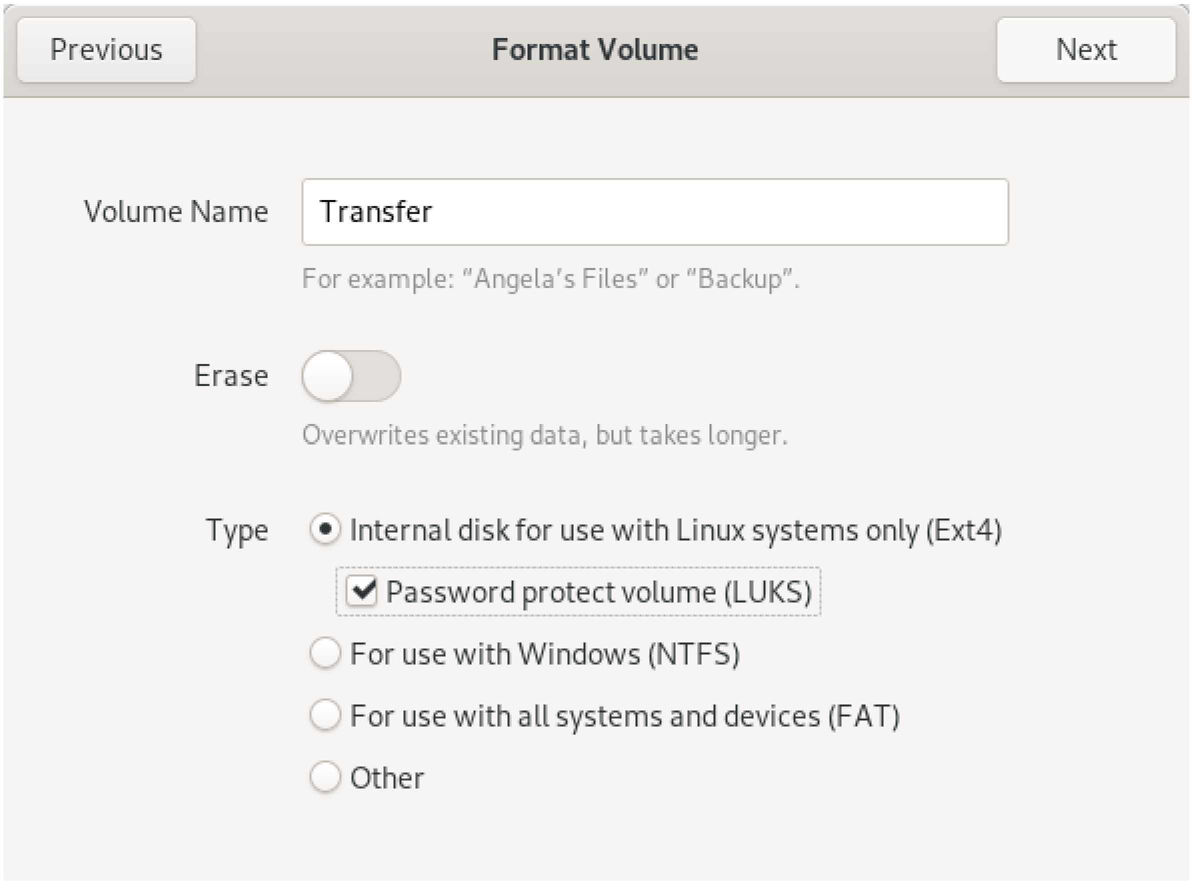
Once you're sure you have the right drive, click the interlocking gears, then **Format Partition…**.

Note

If there are multiple existing partitions on the drive, you should first click the "-" icon on the left of the interlocking gears icon to delete each partition, and then create another partition that fills all free space with the options as shown below.



Give the partition on your *Transfer Device* a descriptive name like “Transfer Device” and select the options as in the following screenshot:



Volume Name: Transfer

For example: "Angela's Files" or "Backup".

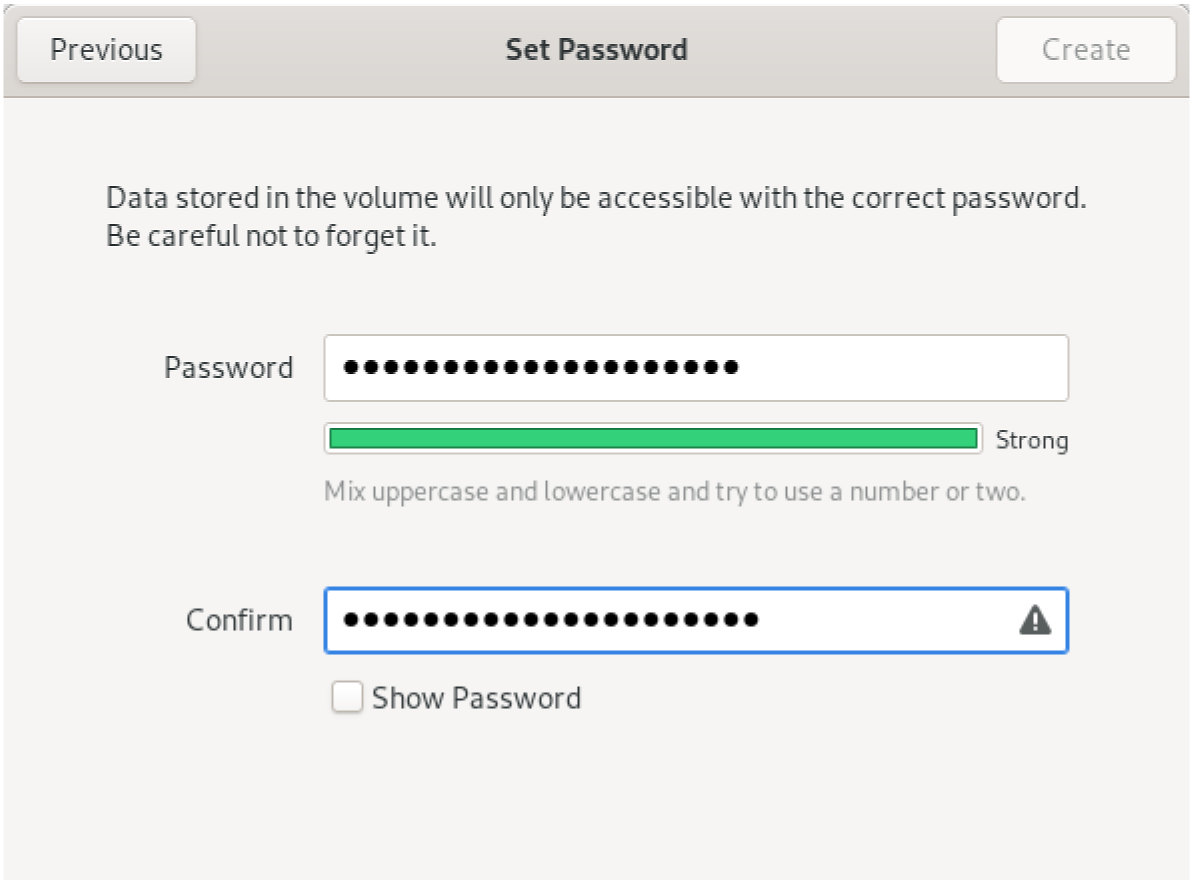
Erase ○

Overwrites existing data, but takes longer.

Type

- ● Internal disk for use with Linux systems only (Ext4)
  - ☑ Password protect volume (LUKS)
- ○ For use with Windows (NTFS)
- ○ For use with all systems and devices (FAT)
- ○ Other

You will then be prompted to set a password. As noted earlier, we recommend storing this passphrase in the password manager for every user who will copy files using the *Transfer Device*, not in KeePassXC. Because users will have to type in this passphrase every time they mount the *Transfer Device* in Tails, we recommend using a diceware passphrase.



Data stored in the volume will only be accessible with the correct password. Be careful not to forget it.

Mix uppercase and lowercase and try to use a number or two.

After typing in the passphrase, click **Format** to continue. The Disks utility will ask you if you are sure: click **Format** to continue. After a few seconds, your new *Transfer Device* should be ready for use. If you haven't already, make sure to label it.

1.30.4 Create a USB *Export Device*

We recommend using a fully encrypted USB drive for copying files off the *Secure Viewing Station*. This is even more important than for the *Transfer Device*, as the risk of accidentally leaving decrypted files on the *Export Device* is significant.

Because the *Export Device* will need to be mounted on both Tails and the journalist's everyday workstation, you will need to use an encryption scheme that works on both operating systems.

We recommend the use of VeraCrypt. It is actively maintained cross-platform software that has been independently audited and is free to use.

VeraCrypt-encrypted media can be opened in the Tails operating system and on common Linux distributions without installing additional software. To open VeraCrypt media on Windows or Mac workstations, or to create VeraCrypt drives, you need to install the VeraCrypt software. The guide by Freedom of the Press Foundation provides instructions for encrypting storage media using VeraCrypt.

Warning

If you plan to use your *Export Device* with computers running macOS 15 ("Sequoia") or later, you must also perform the VeraCrypt setup on that version of macOS.

Keep in mind that each journalist using a Windows or Mac workstation will need to have the VeraCrypt software installed on their computer to access the encrypted *Export Device*.

Note

We recommend against installing the VeraCrypt software on the *Journalist Workstation*, the *Admin Workstation* or the *Secure Viewing Station*. The software installed in the persistent volume of these Tails drives should be kept to a minimum. You do not need to install the software to *decrypt* VeraCrypt drives on these workstations, and you can *create* them from another computer.

Larger organizations may want to consider setting up a controlled environment for creating VeraCrypt-encrypted *Export Devices* and providing them to journalists, to ensure that each drive is provisioned in a secure manner.

As with the *Transfer Device*, we recommend storing the passphrase in the password manager of each user who will use a given *Export Device*.

Hardware-encrypted USB drives can be a reasonable alternative to VeraCrypt. We cannot currently offer a specific recommendation, but please bear in mind that the drive must work across platforms (including Tails). We recommend selecting a vendor that has fully opened the source code and specifications of their devices and encouraged third party audits.

Limiting write access

If you re-use the same *Export Device* for multiple copy operations, there is the risk of introducing malware to the *Secure Viewing Station* from your network. Depending on your threat model, there are steps you may want to take to mitigate that risk.

One option is to restrict write access to the *Export Device* before it is plugged into a device other than the *Secure Viewing Station*. Some USB flash drives come with a physical write protection switch, and write blockers are used in forensics to ensure storage media are not modified during examination.

Full-size SD cards also come with physical write protection switches. However, this write protection is fully host-based (the host operating system can choose to ignore it), and should therefore be considered less secure against sophisticated malware.

Tip

For defense in depth, consider implementing a similar write protection strategy for the *Transfer Device* (enabling write protection before attaching the *Transfer Device* to the *Secure Viewing Station*).

Please see our *guide to working with documents* for additional recommendations regarding malware mitigation.

1.31 Generate the *Submission Key*

When a document or message is submitted to SecureDrop by a source, it is automatically encrypted with the *Submission Key*. The private part of this key is only stored on the *Secure Viewing Station* which is never connected to the Internet. SecureDrop submissions can only be decrypted and read on the *Secure Viewing Station*.

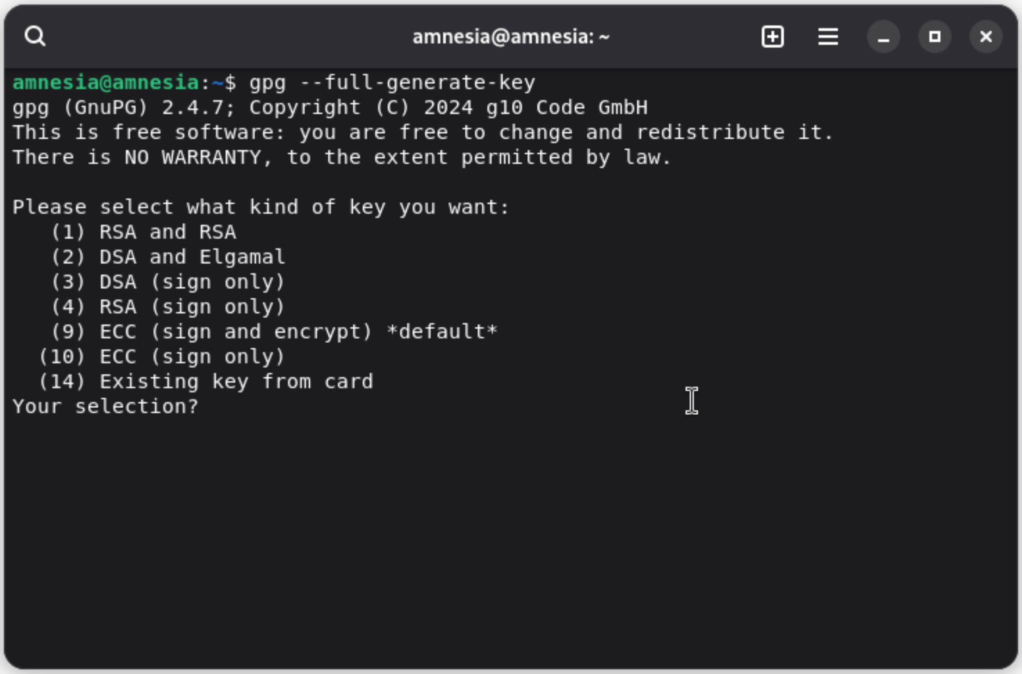
We will now generate the *Submission Key*. If you aren't still logged into your *Secure Viewing Station* from the previous step, boot it using its Tails USB stick, with persistence enabled.

Important

Do not follow these steps before you have fully configured the *Secure Viewing Station* according to the *instructions*. The private key you will generate in the following steps is one of the most important secrets associated with your SecureDrop installation. This procedure is intended to ensure that the private key is protected by the air-gap throughout its lifetime.

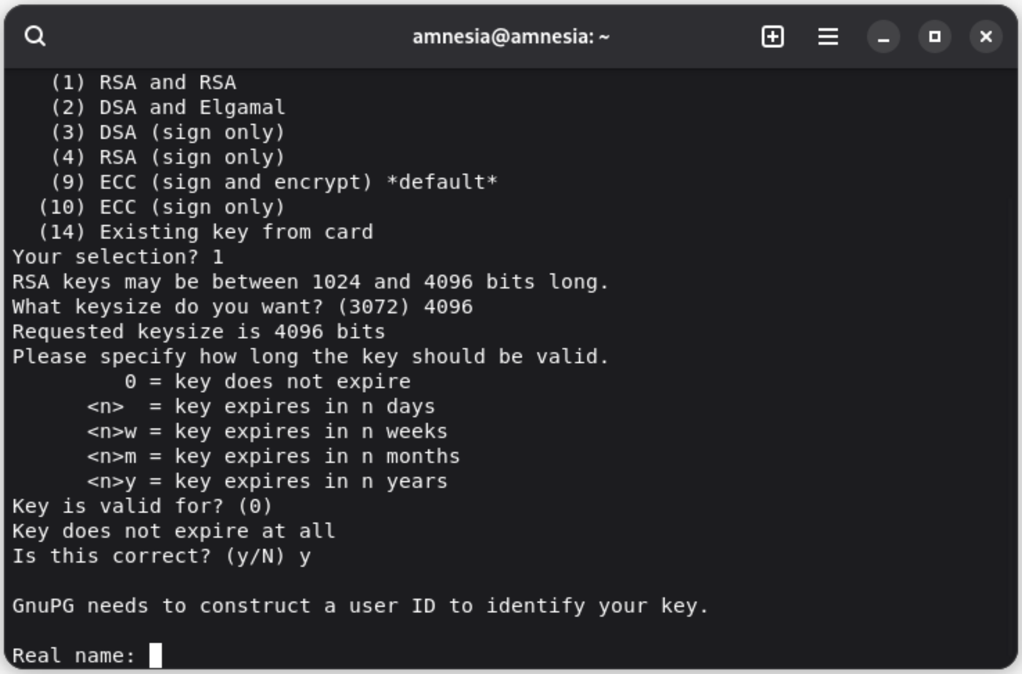
1.31.1 Create the Key

1. Navigate to **Apps** ▶ **System Tools** ▶ **Console** to open a terminal.
2. In the terminal, run `gpg --full-generate-key`:



```
amnesia@amnesia:~$ gpg --full-generate-key
gpg (GnuPG) 2.4.7; Copyright (C) 2024 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
   (1) RSA and RSA
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
   (9) ECC (sign and encrypt) *default*
  (10) ECC (sign only)
  (14) Existing key from card
Your selection?
```

3. When it says **Please select what kind of key you want**, choose "*(1) RSA and RSA (default)*".
4. When it asks **What keysize do you want?**, type `4096`.
5. When it asks **Key is valid for?**, press Enter. This means your key does not expire.
6. It will let you know that this means the key does not expire at all and ask for confirmation. Type **y** and hit Enter to confirm.

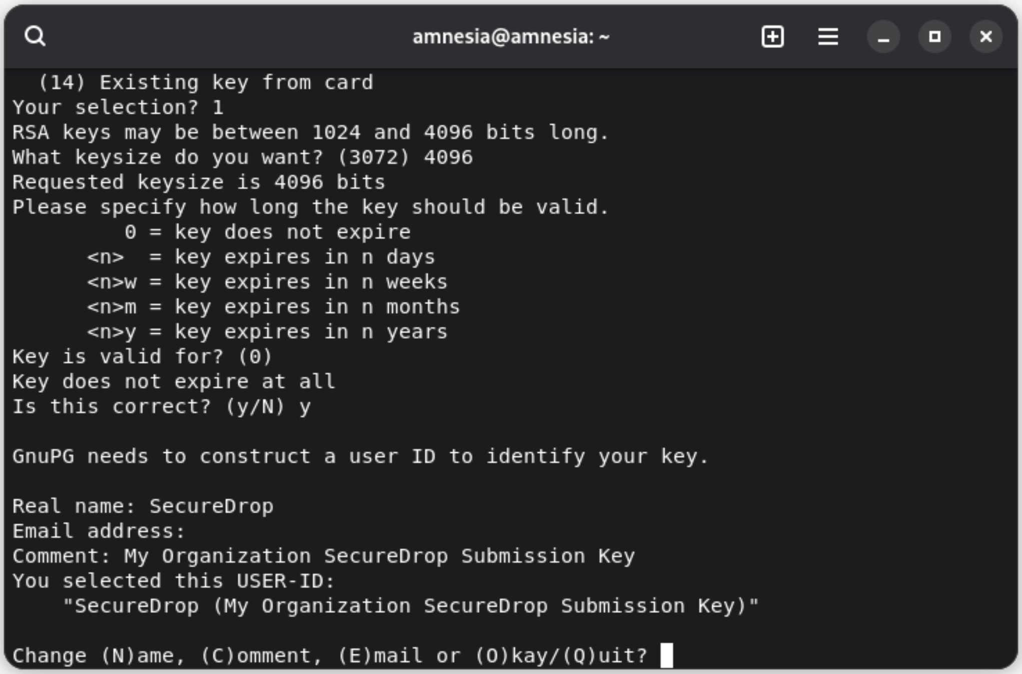


```
   (1) RSA and RSA
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
   (9) ECC (sign and encrypt) *default*
  (10) ECC (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: 
```

7. **Next it will prompt you for user ID setup. Use the following options:**

    - **Real name**: “SecureDrop”
    - **Email address**: leave this field blank
    - **Comment**: `[Your Organization's Name] SecureDrop Submission Key`

8. GPG will confirm these options. Verify that everything is written correctly. Then type `O` for `(O)kay` and hit enter to continue:



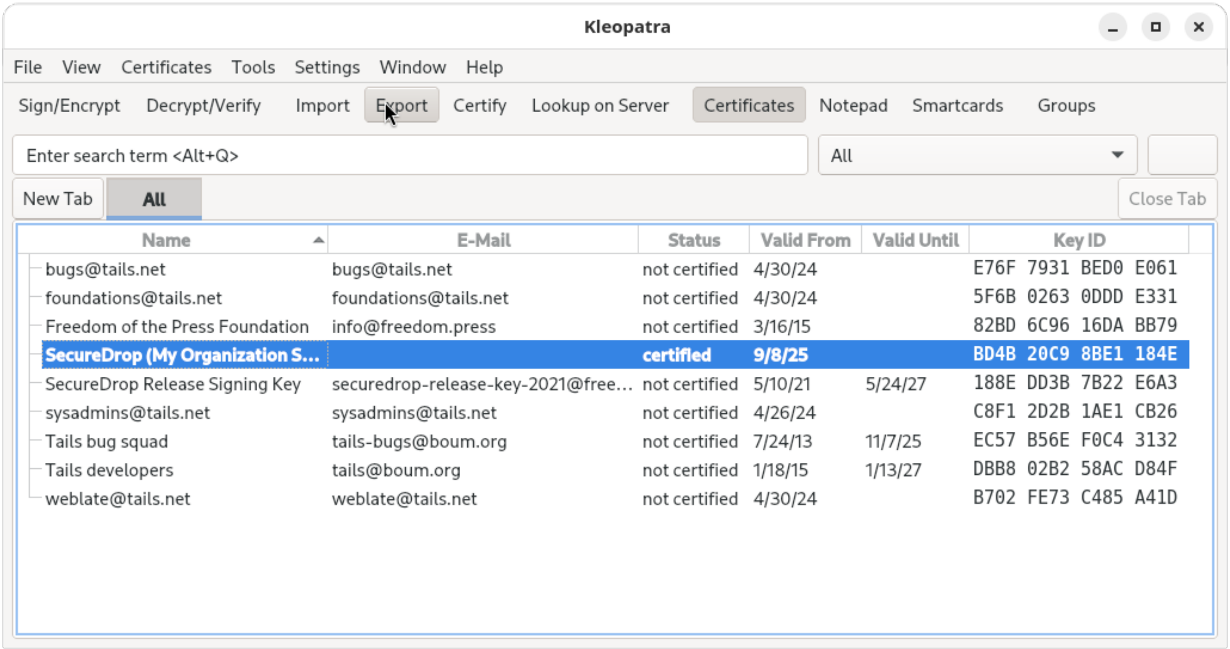
```
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: SecureDrop
Email address:
Comment: My Organization SecureDrop Submission Key
You selected this USER-ID:
    "SecureDrop (My Organization SecureDrop Submission Key)"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit?
```

9. A box will pop up (twice) asking you to type a passphrase. Since the key is protected by the encryption on the Tails persistent volume, it is safe to simply click **OK** without entering a passphrase.
10. The software will ask you if you are sure. Click **Yes, protection is not needed**.
11. Wait for the key to finish generating.

1.31.2 Export the *Submission Public Key*

Navigate to **Apps** ▶ **Accessories** ▶ **Kleopatra** to open a graphical interface to manage GPG keys. Once Kleopatra opens you will find a list of keys, including the SecureDrop Submission Key you just created.

Click to select the key, then click the “Export…” button in the toolbar above.

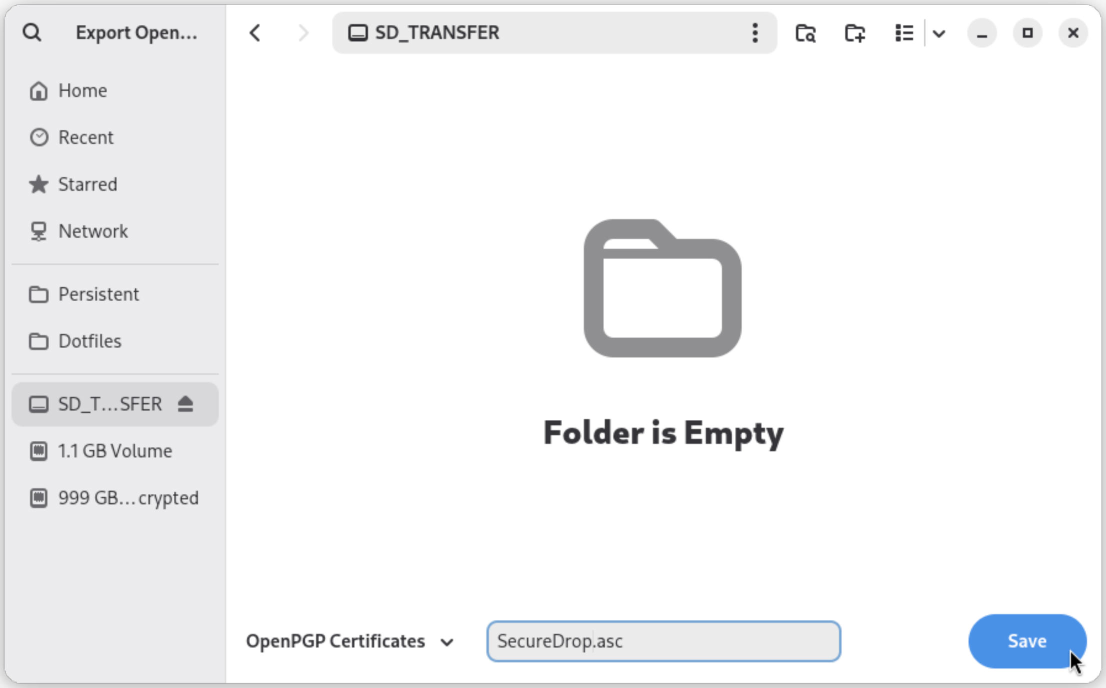

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards Groups
Enter search term <Alt+Q>
All
New Tab
All
Close Tab

Name	E-Mail	Status	Valid From	Valid Until	Key ID
bugs@tails.net	bugs@tails.net	not certified	4/30/24		E76F 7931 BED0 E061
foundations@tails.net	foundations@tails.net	not certified	4/30/24		5F6B 0263 0DDD E331
Freedom of the Press Foundation	info@freedom.press	not certified	3/16/15		82BD 6C96 16DA BB79
SecureDrop (My Organization S…		**certified**	**9/8/25**		**BD4B 20C9 8BE1 184E**
SecureDrop Release Signing Key	securedrop-release-key-2021@free…	not certified	5/10/21	5/24/27	188E DD3B 7B22 E6A3
sysadmins@tails.net	sysadmins@tails.net	not certified	4/26/24		C8F1 2D2B 1AE1 CB26
Tails bug squad	tails-bugs@boum.org	not certified	7/24/13	11/7/25	EC57 B56E F0C4 3132
Tails developers	tails@boum.org	not certified	1/18/15	1/13/27	DBB8 02B2 58AC D84F
weblate@tails.net	weblate@tails.net	not certified	4/30/24		B702 FE73 C485 A41D

Save the key to the *Transfer Device* by changing the location to `/media/amnesia/Transfer Device`, then set the filename to `SecureDrop.asc`. Once that is set, click the *Save* button to finish exporting the key to the transfer device.

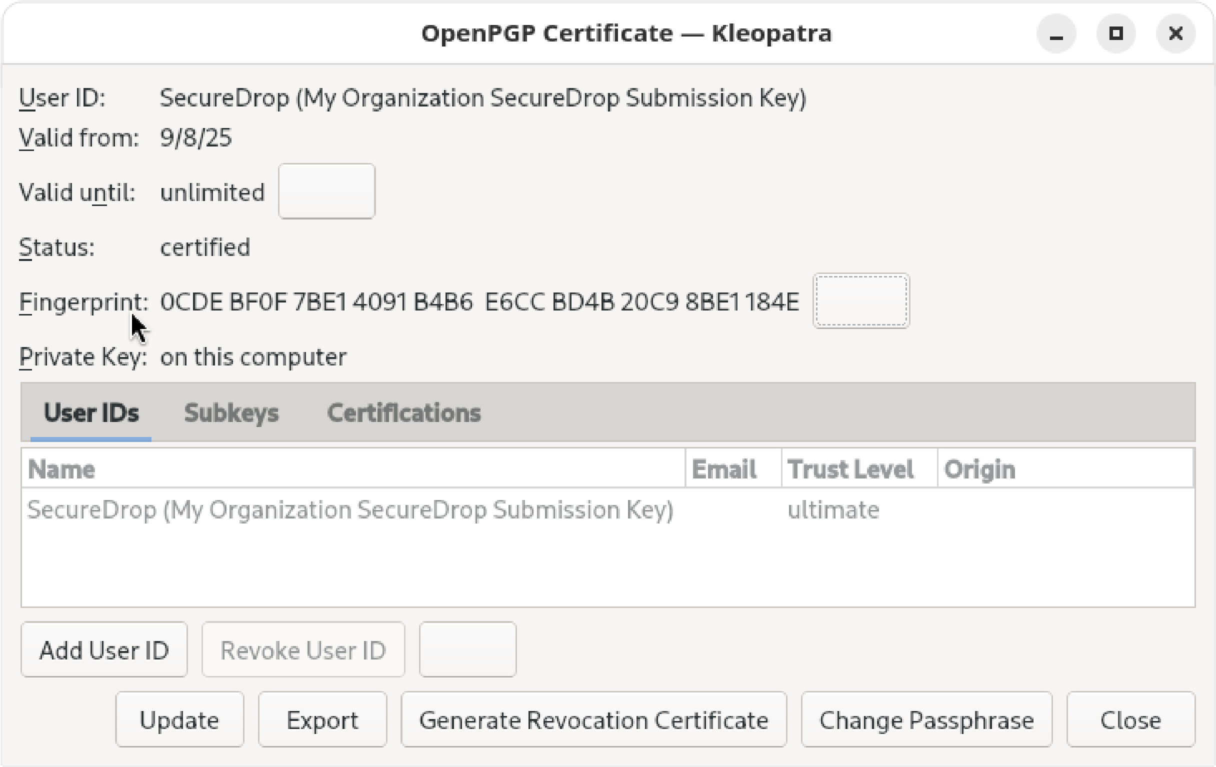
Note

This is the public key only.



SecureDrop.asc

After exporting the public key, you will be returned back to the list of keys. You'll need to provide the fingerprint of the *Submission Key* during the installation. Go ahead and double-click on the *Submission Key*, then write down the 40 hexadecimal digits under *Fingerprint*.



User ID: SecureDrop (My Organization SecureDrop Submission Key)
Valid from: 9/8/25
Valid until: unlimited
Status: certified
Fingerprint: 0CDE BF0F 7BE1 4091 B4B6 E6CC BD4B 20C9 8BE1 184E
Private Key: on this computer

Name	Email	Trust Level	Origin
SecureDrop (My Organization SecureDrop Submission Key)		ultimate	

Note

Your fingerprint will be different from the one in the example screenshot.

At this point, you are done with the *Secure Viewing Station* for now. You can shut down Tails, grab the *Admin Workstation* Tails USB, and move over to your regular workstation.

1.32 Create the Admin Passphrase Database

We provide a KeePassXC password database template to make it easier for admins and journalists to generate strong, unique passphrases and store them securely. Once you have set up Tails with persistence and have cloned the repo, you can set up your personal password database using this template.

Note

Earlier versions of Tails used KeePassX instead of KeePassXC. The provided template is compatible with both.

You can find the template in `tails_files/securedrop-keepassx.kdbx` in the SecureDrop repository that you just cloned. To use the template:

- Copy the template to the Persistent folder - from a terminal, run the command:

```
cp ~/securedrop/tails_files/securedrop-keepassx.kdbx \
   ~/Persistent/Passwords.kdbx
```

- Open the KeePassXC program which is already installed on Tails

- Select **Database ▶ Open database**, and navigate to the location of **~/Persistent/Passwords.kdbx**, select it, and click **Open**
- Leave the password blank and click **OK**. If you receive an "Unlock failed" prompt, click **Retry with empty password**.
- Edit entries as required.
- Select **Database ▶ Save Database** to save your changes.

The next time you use KeepassXC, the database at `~/Persistent/Passwords.kdbx` will be selected by default.

KeePassXC will show a warning every time you attempt to open a database without entering a password. Because your persistent volume is encrypted, setting up this additional password is not strictly required. It provides some additional protection, e.g., if a computer is left running, at the cost of convenience.

For passwordless access without warnings, you can protect the database using a key file, via **Database ▶ Database settings ▶ Security ▶ Add additional protection ▶ Add Key File ▶ Generate**. This key file has to be stored in your Persistent folder and it must be selected when you open the database.

After configuring the password database, restart KeePassXC once to verify that you are able to access it as expected.

Warning

You will not be able to access your passwords if you forget the peristent storage password or the location of the key file used to protect the database.

In case you wish to manually create a database, the suggested password fields in the template are:

Admin:

- Admin account username
- App Server SSH Onion URL
- Email account for sending OSSEC alerts
- Monitor Server SSH Onion URL
- Network Firewall Admin Credentials
- *OSSEC Alert Public Key*
- SecureDrop Login Credentials

Journalist:

- Auth Value: Journalist Interface
- Onion URL: Journalist Interface
- Personal GPG Key
- SecureDrop Login Credentials

Secure Viewing Station:

- SecureDrop GPG Key

Backup:

- This section contains clones of the above entries in case a user accidentally overwrites an entry.

1.33 Set Up the *Admin Workstation*

Earlier, you should have created the *Admin Workstation* Tails USB along with a persistent volume for it. Now, we are going to add a couple more features to the *Admin Workstation* to facilitate SecureDrop's setup.

If you have not switched to and booted the *Admin Workstation* Tails USB on your regular workstation, do so now.

1.33.1 Start Tails with Persistence Enabled

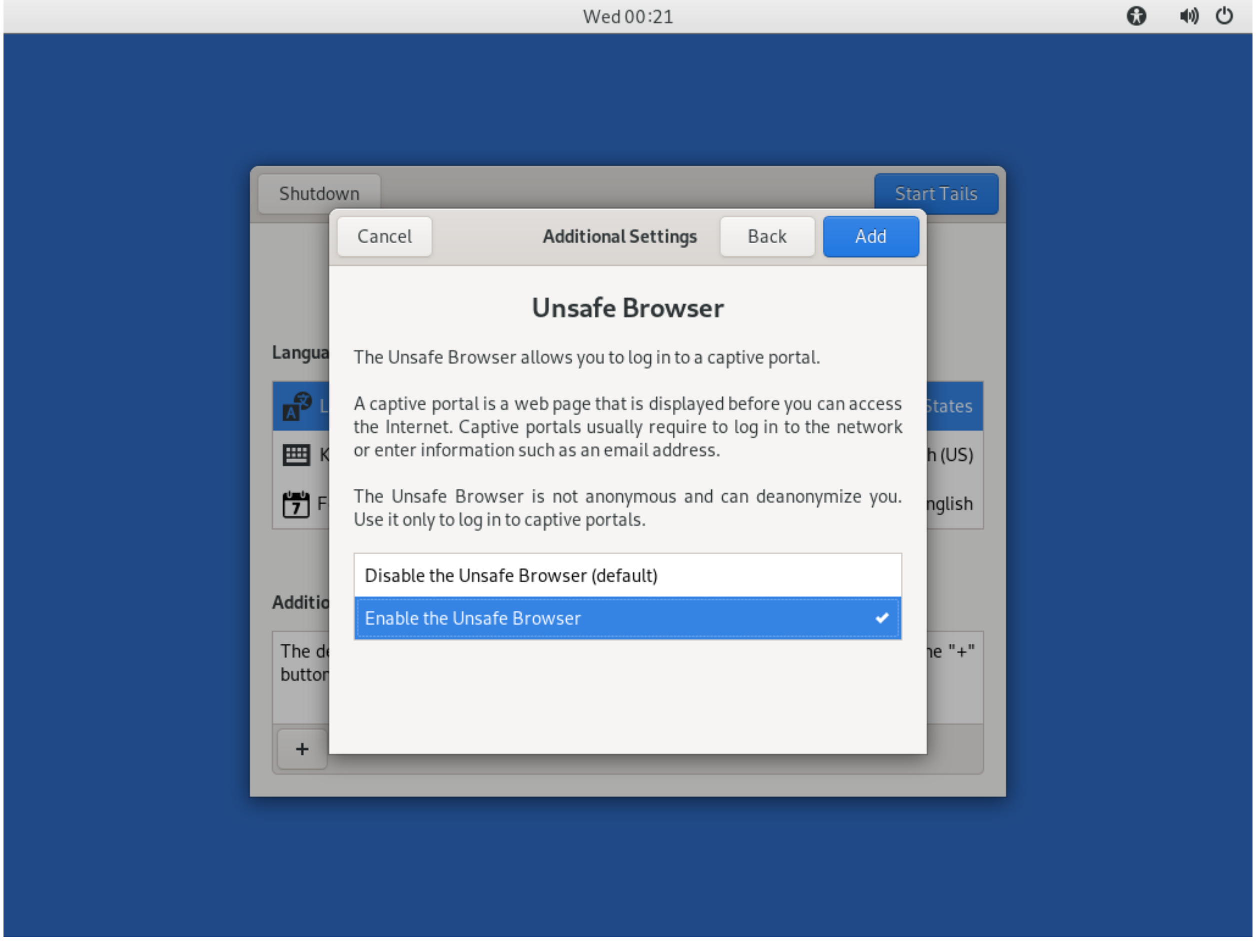
After you boot the *Admin Workstation* Tails USB on your normal workstation, you should see a "Welcome to Tails" screen with a field labeled "Encrypted Persistent Storage". Enter your password and click **Unlock**. Do not click **Start Tails** yet. Under "Additional Settings" click **+**.

Click **Administration password**, enter a password for use with this specific Tails session, and click **Add**.

Note

The Tails administration password is a one-time password. It will reset every time you shut down Tails.

During the installation, you will need the unsafe browser to access the firewall configuration. If you are using Tails 5.8 or newer, the unsafe browser is enabled automatically. If you are using an eariler version, you can enable it by clicking "Unsafe Browser" and then clicking **Add**:



Unsafe Browser

The Unsafe Browser allows you to log in to a captive portal.

A captive portal is a web page that is displayed before you can access the Internet. Captive portals usually require to log in to the network or enter information such as an email address.

The Unsafe Browser is not anonymous and can deanonymize you. Use it only to log in to captive portals.

○ Disable the Unsafe Browser (default)
● Enable the Unsafe Browser ✓

Click **Start Tails**. After Tails finishes booting, make sure you're connected to the Internet and that the Tor status onion icon is not crossed out , consulting the icons in the upper right corner of the screen.

1.33.2 Download the SecureDrop Repository

The rest of the SecureDrop-specific configuration is assisted by files stored in the SecureDrop Git repository. We're going to be using this again once SecureDrop is installed, but you should download it now. To get started, open a terminal . You will use this Terminal throughout the rest of the install process.

Start by running the following commands to download the git repository.

```
cd ~/
git clone https://github.com/freedomofpress/securedrop.git
```

Note

Since the repository is fairly large and Tor can be slow, this may take a few minutes.

Caution

Do not download SecureDrop Git repository as a Zip file, or any other means. Only download by using the given git command.

Verify the Release Tag

Important

It is crucial for the integrity of your installation that you carefully follow the instructions below. By following these steps, you will verify if your copy of the codebase has been approved by the SecureDrop development team.

Download and verify the **SecureDrop Release Signing Key** using the following command:

```
gpg --keyserver hkps://keys.openpgp.org --recv-key \
"2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
```

If you are not copy-pasting this command, we recommend you double-check you have entered it correctly before pressing enter. GPG will implicitly verify that the fingerprint of the key received matches the argument passed.

If GPG warns you that the fingerprint of the key received does not match the one requested, do **not** proceed with the installation. If this happens, please contact us at securedrop@freedom.press.

Note

If the `--recv-key` command fails, first double-check that Tails is connected to Tor. Once you've confirmed that you're successfully connected to Tor, try re-running the `--recv-key` command a few times.

If the command still fails, the *keys.openpgp.org* keyserver may be down. In that case, we recommend downloading the key from the SecureDrop website:

```
cd ~/
torify curl -LO https://securedrop.org/securedrop-release-key.asc
```

Before importing it, inspect the key's fingerprint using the following command. The `--dry-run` option ensures that the key is not imported just yet:

```
gpg --with-fingerprint --import-options import-show --dry-run \
  --import securedrop-release-key.asc
```

Compare the fingerprint in the output with the fingerprint at the beginning of this section. If the fingerprints match, you can safely import the key, using the following command:

```
gpg --import securedrop-release-key.asc
```

If you encounter any difficulties verifying the integrity of the release key, do **not** proceed with the installation. Instead, please contact us at securedrop@freedom.press.

Once you have imported the release key, verify that the current release tag was signed with the release signing key:

```
cd ~/securedrop/
git fetch --tags
git tag -v 2.13.0
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Important

If you do not see the message above, signature verification has failed and you should **not** proceed with the installation. If this happens, please contact us at securedrop@freedom.press.

Verify that each character of the fingerprint matches what is on the screen of your workstation. If it does, you can check out the new release:

```
git checkout 2.13.0
```

Important

If you see the warning `refname '2.13.0' is ambiguous` in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

1.33.3 Install SecureDrop Package and Dependencies

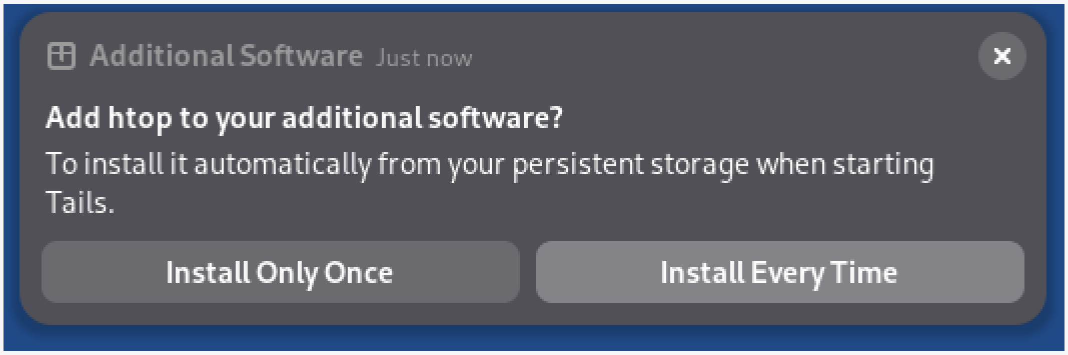
A SecureDrop *Admin Workstation* must have the `securedrop-admin` package and dependencies installed before installing the servers. To install these packages, from the base of the SecureDrop repository that you cloned previously (`~/securedrop/`), run the following command:

```
sudo apt update
./securedrop-admin tails-bootstrap
```

The package installation will take approximately 10 minutes or longer, depending on network speed and computing power. Once the installation is complete, you will be prompted to reboot the workstation. Please do so.

Note

The apt persistence feature will prompt to install the package automatically from persistent storage on each boot. Click **Install Every Time**:



Additional Software Just now

Add htop to your additional software?

To install it automatically from your persistent storage when starting Tails.

Note

Occasionally this command times out due to network latency issues. You should be able to re-run the command and complete the setup.

Important

The setup command should only be run as the `amnesia` user, **not** as root. Contact the SecureDrop team if the package installation encounters repeated errors.

1.34 Set Up the Network Firewall

Now that you've set up your password manager, you can move on to setting up the Network Firewall. You should stay logged in to the *Admin Workstation* to access the Network Firewall's web interface for configuration.

Unfortunately, due to the wide variety of firewalls that may be used, we do not provide specific instructions to cover every type or variation in software or hardware. However, if you have the necessary expertise, we provide *abstract firewall rules* that can be implemented with iptables, Cisco IOS etc. We recommend that you use a firewall with at least four physical interfaces.

The documentation linked below describes the configuration procedure for pfSense- and OPNSense-based firewalls. One option not covered in this guide is to build your own network firewall and install OPNSense on it. However, for most installations, we recommend buying a dedicated firewall appliance with your firewall OS of choice pre-installed.

Please note that we no longer recommend the use of pfSense Community Edition (CE) due to changes in the frequency and scope of security updates made available there. pfSense Plus continues to receive necessary security updates on a regular basis, and is provided with the purchase of most Netgate firewalls.

We currently recommend three firewalls in our *Hardware Guide*:

- The Netgate SG-4100, a pfSense-based firewall with 6 network interfaces: 2 WAN ports and 4 LAN ports.
- The Netgate SG-6100, a pfSense-based firewall with 8 network interfaces: 4 WAN ports and 4 LAN ports.
- The Protectli Vault 4-Port (with coreboot), an OPNSense-based open-source hardware firewall with 4 configurable network interfaces.

1.34.1 Configuration: pfSense

If you are using a pfSense-based firewall such as the recommended SG-4100, follow the instructions to *Configure a pfSense firewall for use with SecureDrop*.

1.34.2 Configuration: OPNSense

If you are using an OPNSense-based firewall such as the recommended APu4D4, follow the instructions to *Configure an OPNSense firewall for use with SecureDrop*.

1.34.3 Configuration: Other Firewalls

If you are using a firewall based on an OS not listed above, you should still set it up use the same overall configuration and ruleset as defined for the supported models.

The *Application* and *Monitor Servers* should be set up on separate subnets configured on separate physical NICs, with the *Admin Workstation* also on a separate subnet if possible. Including the WAN connection, a minimum of 4 NICs must be available.

The abstract ruleset required by SecureDrop can be described as follows:

- Disable DHCP (in case the firewall is providing a DHCP server by default)
- Disallow all traffic by default (inbound or outbound)
- Allow UDP OSSEC (port 1514) from *Application Server* to *Monitor Server*
- Allow TCP ossec agent auth (port 1515) from *Application Server* to *Monitor Server*
- Allow TCP/UDP DNS from *Application Server* and *Monitor Server* to the IPs of known name servers
- Allow UDP NTP from *Application Server* and *Monitor Server* to all
- Allow TCP any port from *Application Server* and *Monitor Server* to all (this is needed for making connections to the Tor network)
- Allow TCP 80/443 from *Admin Workstation* to all (in case there is a need to access the web interface of the firewall)
- Allow TCP SSH from *Admin Workstation* to *Application Server* and *Monitor Server*
- Allow TCP any port from *Admin Workstation* to all

This can be implemented with iptables, Cisco IOS etc. if you have the necessary expertise.

1.35 Setting Up a pfSense Network Firewall

1.35.1 Before You Begin

First, consider how the firewall will be connected to the Internet. You will need to provision several unique subnets, which should not conflict with the network configuration on the WAN interface. If you are unsure, consult your local system administrator.

Many firewalls, including the recommended pfSense-based devices, automatically set up the LAN interface on `192.168.1.1/24`. This particular private network is also a very common choice for home and office routers. If you are connecting the firewall to a router with the same subnet (common in a small office, home, or testing environment), you will probably be unable to connect to the network at first. However, you will be able to connect from the LAN to the pfSense WebGUI configuration wizard, and from there you will be able to configure the network so it is working correctly.

Configuring Your Firewall

Since our recommended firewalls have at least 4 NICs, we will refer to the relevant ports as WAN[1], LAN[1], LAN2, and LAN3. (Bracketed numbers may be present on the physical ports' labels but not in the pfSense UI.) In this case, we can now use a dedicated port on the network firewall for each component of SecureDrop (*Application Server*, *Monitor Server*, and *Admin Workstation*).

Depending on your network configuration, you should define the IP and subnet values your instance will use before continuing. We recommend the default values below:

IP and subnet definitions:

- Admin Subnet: `10.20.1.0/24`
- Admin Gateway: `10.20.1.1`
- Admin Workstation (LAN[1]): `10.20.1.2`
- Application Subnet: `10.20.2.0/24`
- Application Gateway: `10.20.2.1`
- Application Server (LAN2): `10.20.2.2`
- Monitor Subnet: `10.20.3.0/24`
- Monitor Gateway: `10.20.3.1`
- Monitor Server (LAN3) : `10.20.3.2`

1.35.2 Initial Configuration

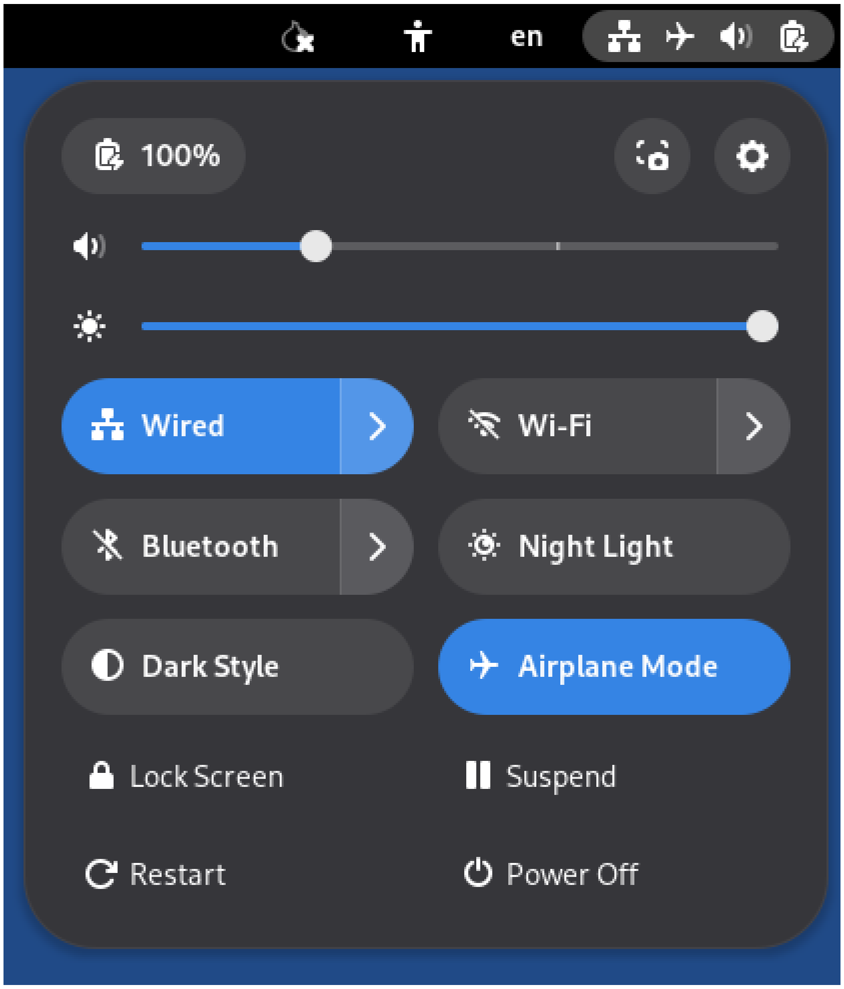
Unpack the firewall, connect the power, and power on the device.

We will use the pfSense WebGUI to do the initial configuration of the network firewall.[1]

Connect to the pfSense WebGUI

1. If you have not already done so, boot the *Admin Workstation* into Tails using its designated USB drive.
2. Connect the *Admin Workstation* to the LAN[1] interface. You should see a popup notification in Tails that says "Connection Established". If you click on the network icon in the upper right of the Tails Desktop, you should see that the Wired Connection is active:

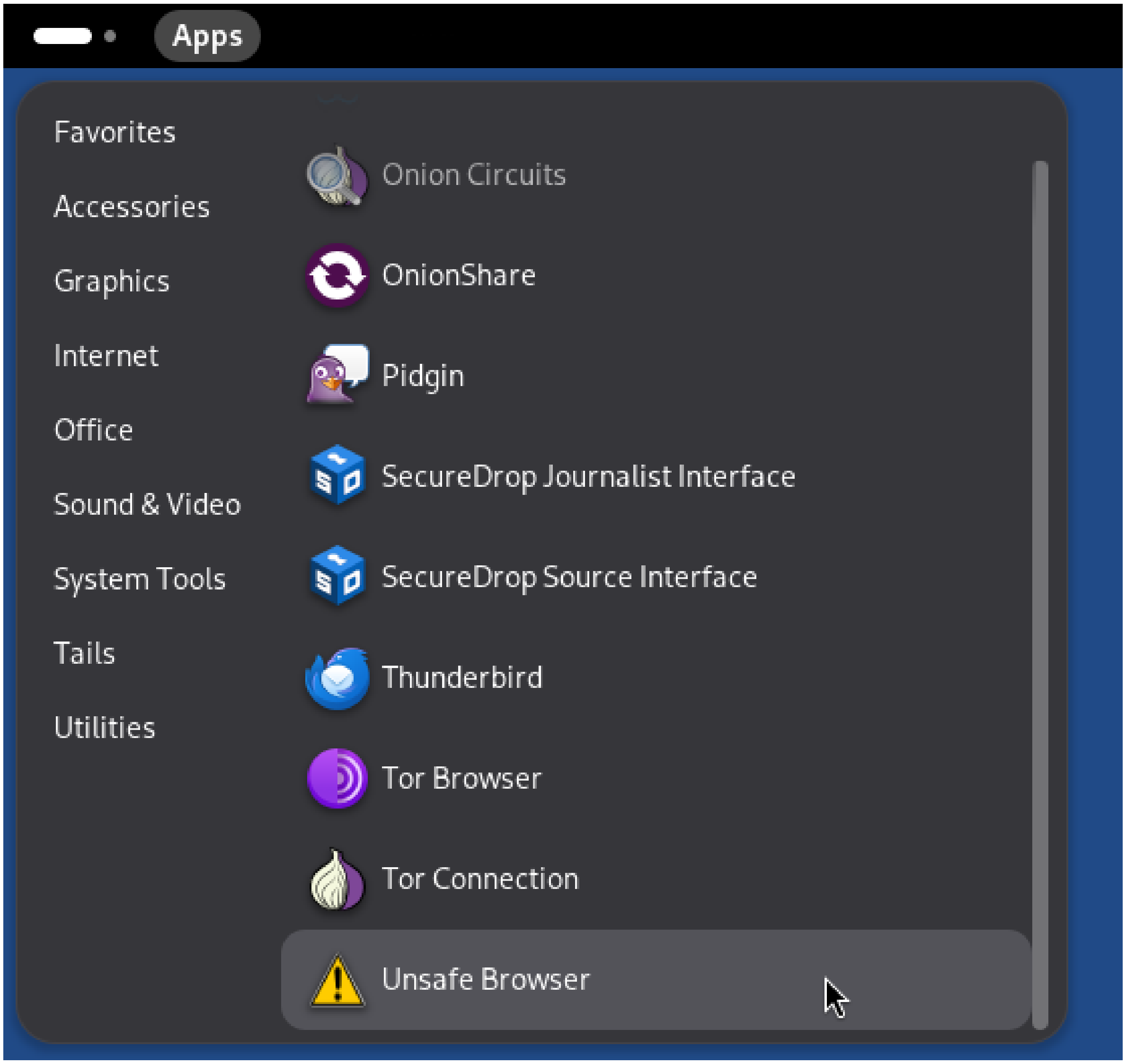
[1] Tails screenshots are current as of Tails 5.0. Please make an issue on GitHub if you are using the most recent version of Tails and the interface is different from what you see here.



Warning

Make sure your *only* active connection is the one you just established with the network firewall. If you are connected to another network at the same time (e.g. a wireless network), you may encounter problems trying to connect the pfSense WebGUI.

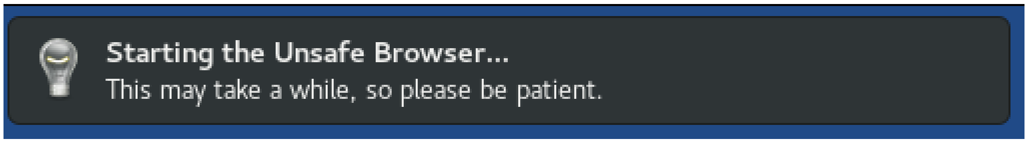
3. Launch the **Unsafe Browser** from the menu bar: **Apps** ▶ **Internet** ▶ **Unsafe Browser**.



Note

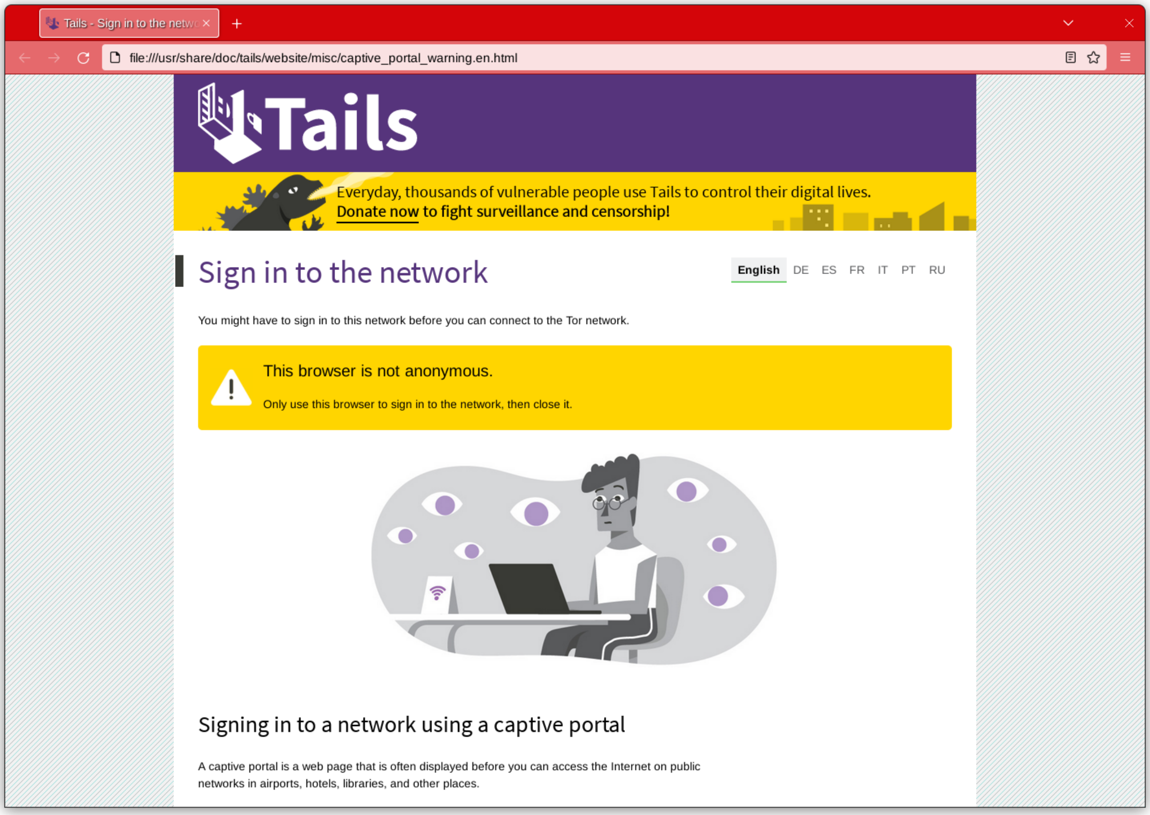
The *Unsafe Browser* is, as the name suggests, **unsafe** (its traffic is not routed through Tor). However, it is the only option because Tails intentionally disables LAN access in the **Tor Browser**.

4. You will see a pop-up notification that says "Starting the Unsafe Browser…"



Starting the Unsafe Browser...
This may take a while, so please be patient.

5. After a few seconds, the Unsafe Browser should launch. The window has a bright red border to remind you to be careful when using it. You should close it once you're done configuring the firewall and use Tor Browser for any other web browsing you might do on the *Admin Workstation*.



Tails - Sign in to the netw
file:///usr/share/doc/tails/website/misc/captive_portal_warning.en.html
Tails
Everyday, thousands of vulnerable people use Tails to control their digital lives.
Donate now to fight surveillance and censorship!
English DE ES FR IT PT RU

Sign in to the network

You might have to sign in to this network before you can connect to the Tor network.

This browser is not anonymous.

Only use this browser to sign in to the network, then close it.

Signing in to a network using a captive portal

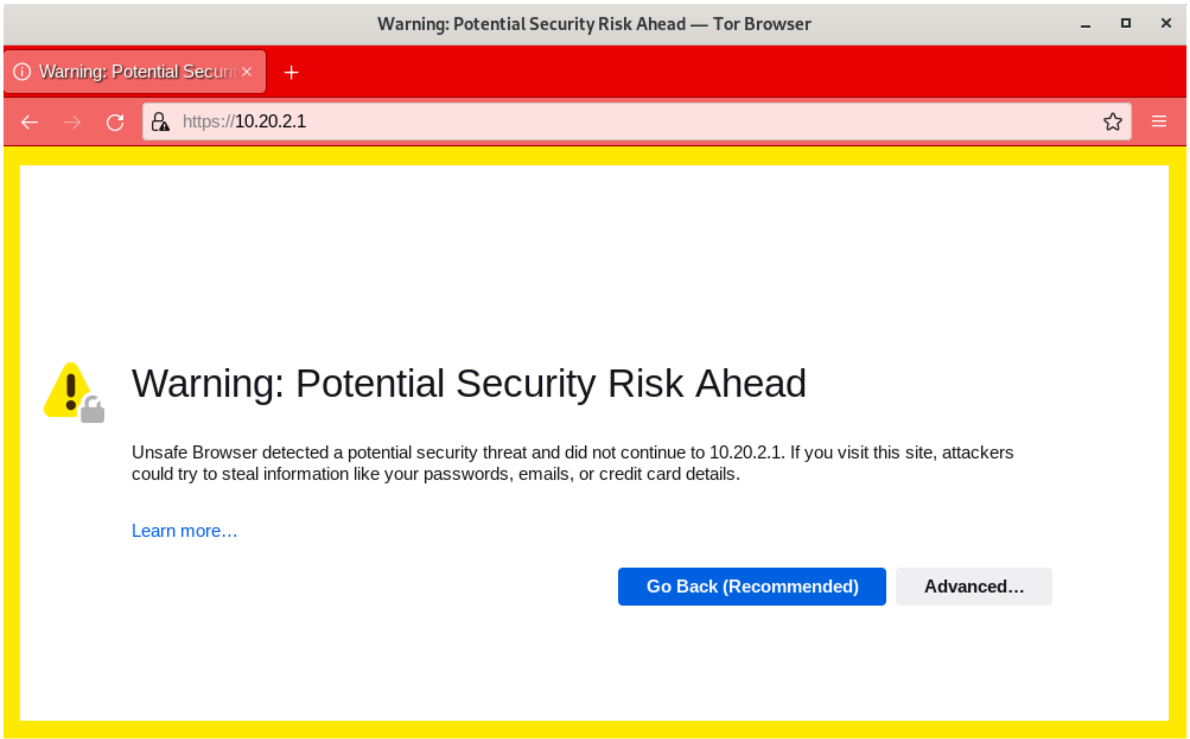
A captive portal is a web page that is often displayed before you can access the Internet on public networks in airports, hotels, libraries, and other places.

6. Navigate to the pfSense WebGUI in the *Unsafe Browser*: `https://192.168.1.1`

Note

If you have trouble connecting, go to your network settings and make sure that you have an IPv4 address in the `192.168.1.1/24` range. You may need to turn on DHCP, else you can manually configure a static IPv4 address of `192.168.1.x` with a subnet mask of `255.255.255.0`. However, make sure not to configure your Tails device to have the same IP as the firewall (`192.168.1.1`).

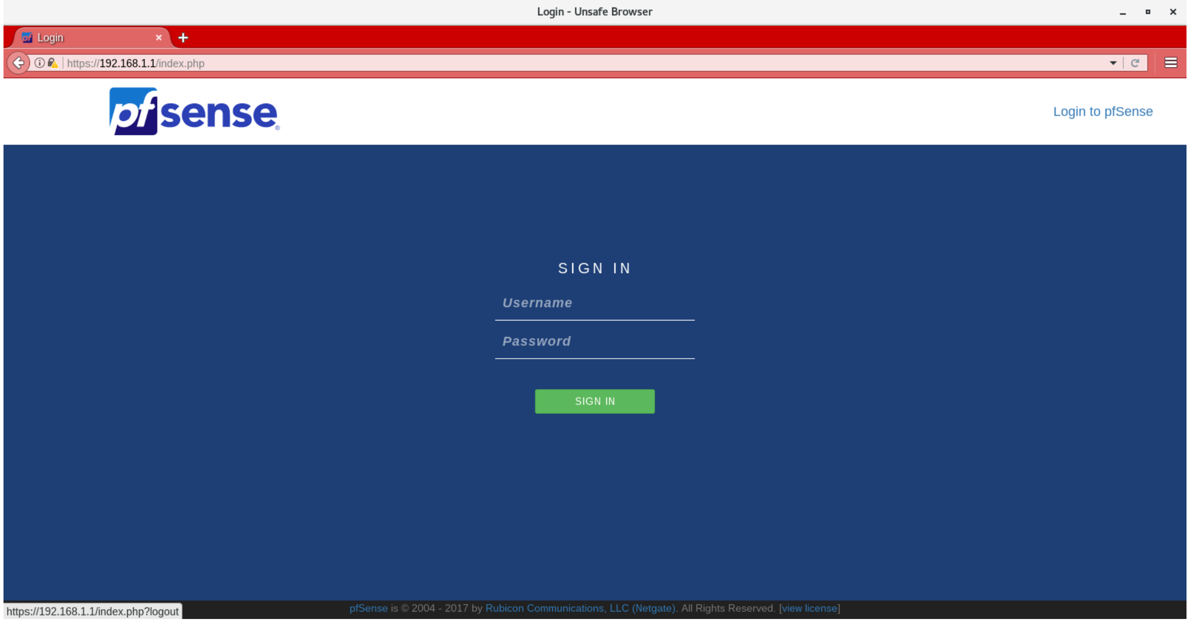
7. The firewall uses a self-signed certificate, so you will see a "Potential Security Risk Ahead" warning when you connect. This is expected. You can safely continue by clicking **Advanced**, then **Accept the Risk and Continue**.


Warning: Potential Security Risk Ahead — Tor Browser
Warning: Potential Securi
https://10.20.2.1
Learn more…
Go Back (Recommended)
Advanced…

Warning: Potential Security Risk Ahead

Unsafe Browser detected a potential security threat and did not continue to 10.20.2.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

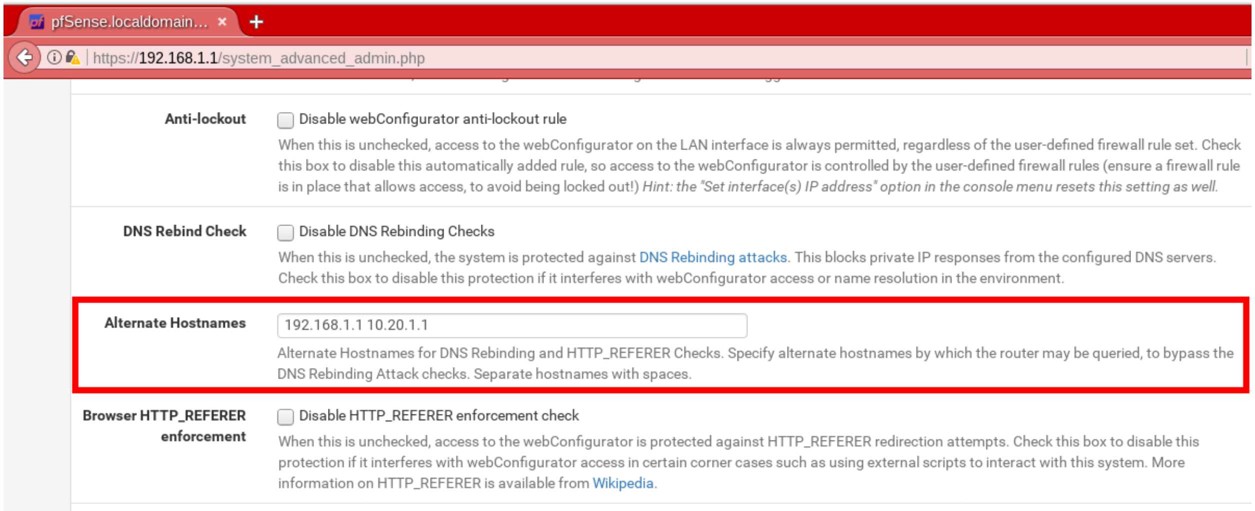
8. You should see the login page for the pfSense GUI. Log in with the default username and passphrase (`admin` / `pfsense`).



pfSense is © 2004 - 2017 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

Alternate Hostnames

Before you can set up the hardware firewall, you will need to set the **Alternate Hostnames** setting after logging in. You will see the Setup Wizard but you should exit out of it by navigating to **System** ▶ **Advanced**. In the **Alternate Hostnames** dialog box, add `192.168.1.1` as well as the IP address of the *Admin Gateway*. If you decide against using our recommended defaults for the *Admin Gateway*, you should include that value here. After saving these settings you should be able to go back to **System** and select **Setup Wizard**.



Anti-lockout □ Disable webConfigurator anti-lockout rule

When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

DNS Rebind Check □ Disable DNS Rebinding Checks

When this is unchecked, the system is protected against DNS Rebinding attacks. This blocks private IP responses from the configured DNS servers. Check this box to disable this protection if it interferes with webConfigurator access or name resolution in the environment.

Alternate Hostnames 192.168.1.1 10.20.1.1

Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks. Specify alternate hostnames by which the router may be queried, to bypass the DNS Rebinding Attack checks. Separate hostnames with spaces.

Browser HTTP_REFERER enforcement □ Disable HTTP_REFERER enforcement check

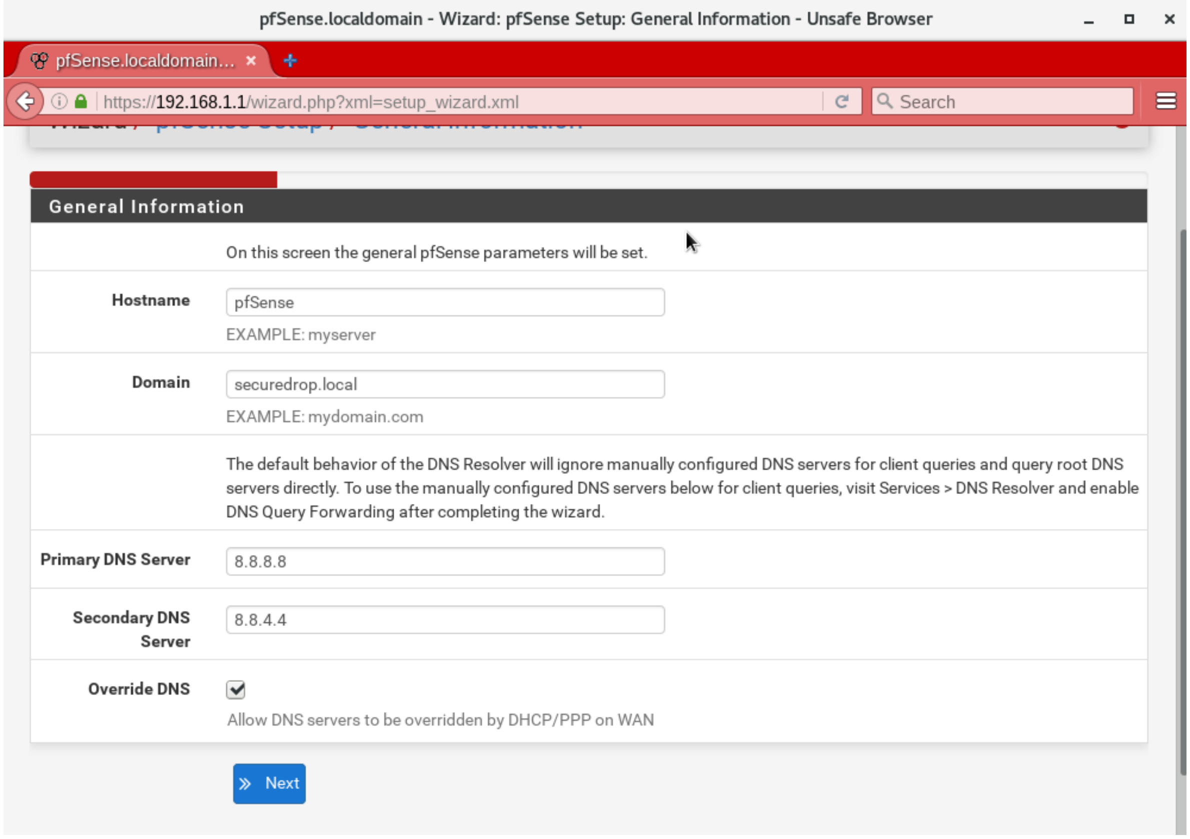
When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from Wikipedia.

Note

If you are using a different IP for the Admin Gateway you should enter that IP in the Alternate Hostname field. Failure to do so will result in an error with the text “An HTTP_REFERER was detected other than what is defined in System -> Advanced”. If you see this error you may have to do a factory reset of the firewall via the serial console.

Setup Wizard

1. If you’re setting up a brand new (or recently factory reset) router, logging in to the pfSense WebGUI will automatically start the Setup Wizard. Click **Next**, then **Next** again. Don’t sign up for a pfSense Gold subscription (unless you want to).
2. On the “General Information” page, we recommend leaving your hostname as the default (pfSense). There is no relevant domain for SecureDrop, so we recommend setting this to `securedrop.local` or something similar. Use your preferred DNS servers. If you don’t know what DNS servers to use, we recommend using Google’s DNS servers: `8.8.8.8` and `8.8.4.4`. Click Next.



pfSense.localdomain - Wizard: pfSense Setup: General Information - Unsafe Browser

https://192.168.1.1/wizard.php?xml=setup_wizard.xml

General Information

On this screen the general pfSense parameters will be set.

Hostname: pfSense
EXAMPLE: myserver

Domain: securedrop.local
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

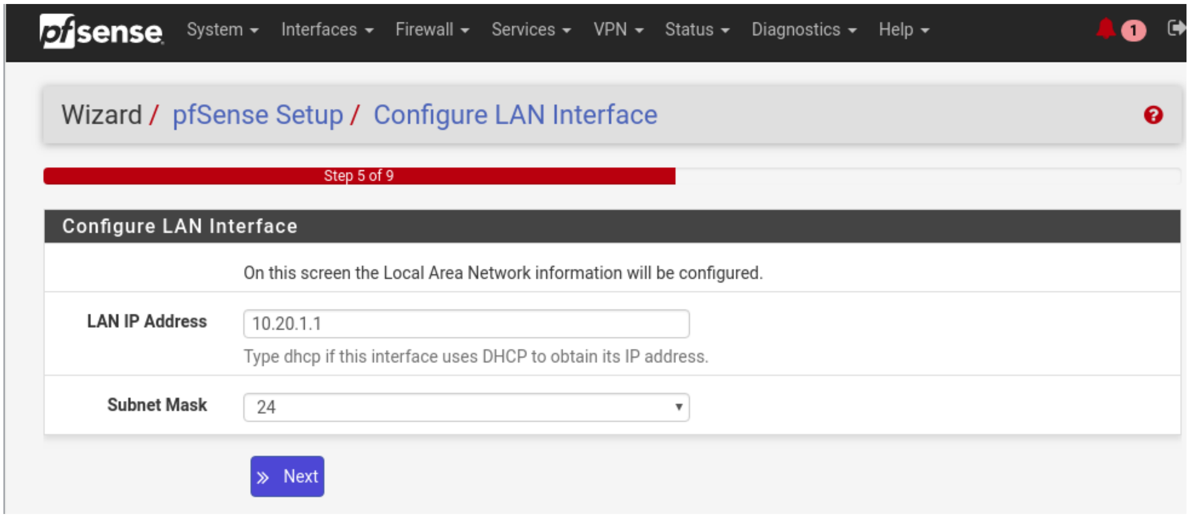
Override DNS: ☑
Allow DNS servers to be overridden by DHCP/PPP on WAN

3. Leave the defaults for "Time Server Information". Click **Next**.

4. On "Configure WAN Interface", enter the appropriate configuration for your network. Consult your local sysadmin if you are unsure what to enter here. For many environments, the default of DHCP will work and the rest of the fields can be left blank. Click **Next**.

   - If your firewall is behind another firewall or NAT device, you will need to deselect the **Block private networks from entering via WAN** option to allow traffic to and from your upstream network.

5. For "Configure LAN Interface", use the IP address of the *Admin Gateway* (`10.20.1.1`) and the subnet mask (`/24`) of the *Admin Subnet*. Click **Next**.



Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

On this screen the Local Area Network information will be configured.

LAN IP Address: 10.20.1.1
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

6. Set a strong admin passphrase. We recommend generating a strong passphrase with KeePassXC, and saving it in the Tails Persistent folder using the provided KeePassXC database template. Click **Next**.
7. Click Reload. Once the reload completes and the web page refreshes, click the corresponding “here” link to “continue on to the pfSense webConfigurator”.

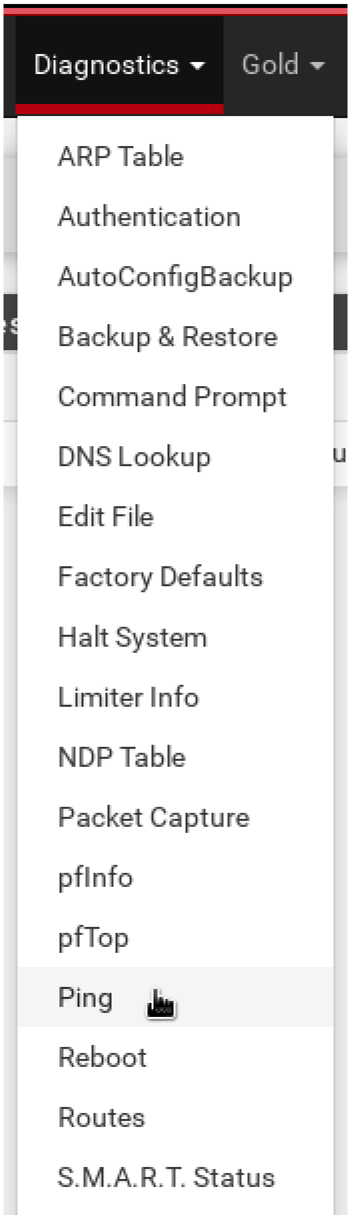
At this point, since you (probably) changed the LAN[1] subnet settings from their defaults, you will no longer be able to connect after reloading the firewall and the next request will probably time out. This is not an error - the firewall has reloaded and is working correctly. To connect to the new LAN[1] interface, unplug and reconnect your network cable to get a new network address assigned via DHCP. Note that if you used a subnet with fewer addresses than `/24`, the default DHCP configuration in pfSense may not work. In this case, you should assign the Admin Workstation a static IP address that is known to be in the subnet to continue.

Now the WebGUI will be available on the Admin Gateway address. Navigate to `https://<Admin Gateway IP>` in the *Unsafe Browser*, and login as before except with the new passphrase you just set for the pfSense WebGUI. Once you’ve logged in to the WebGUI, you are ready to continue configuring the firewall.

Connect Interfaces and Test

Now that the initial configuration is completed, you can connect the WAN port without potentially conflicting with the default LAN[1] settings (as explained earlier). Connect the WAN port to the external network. You can watch the WAN entry in the Interfaces table on the pfSense WebGUI homepage to see as it changes from down (red arrow pointing down) to up (green arrow pointing up). This usually takes several seconds. The WAN’s IP address will be shown once it comes up.

Finally, test connectivity to make sure you are able to connect to the Internet through the WAN. The easiest way to do this is to use ping (**Diagnostics** → **Ping** in the WebGUI). Enter an external hostname or IP that you expect to be up (e.g. `google.com`) and click “Ping”.



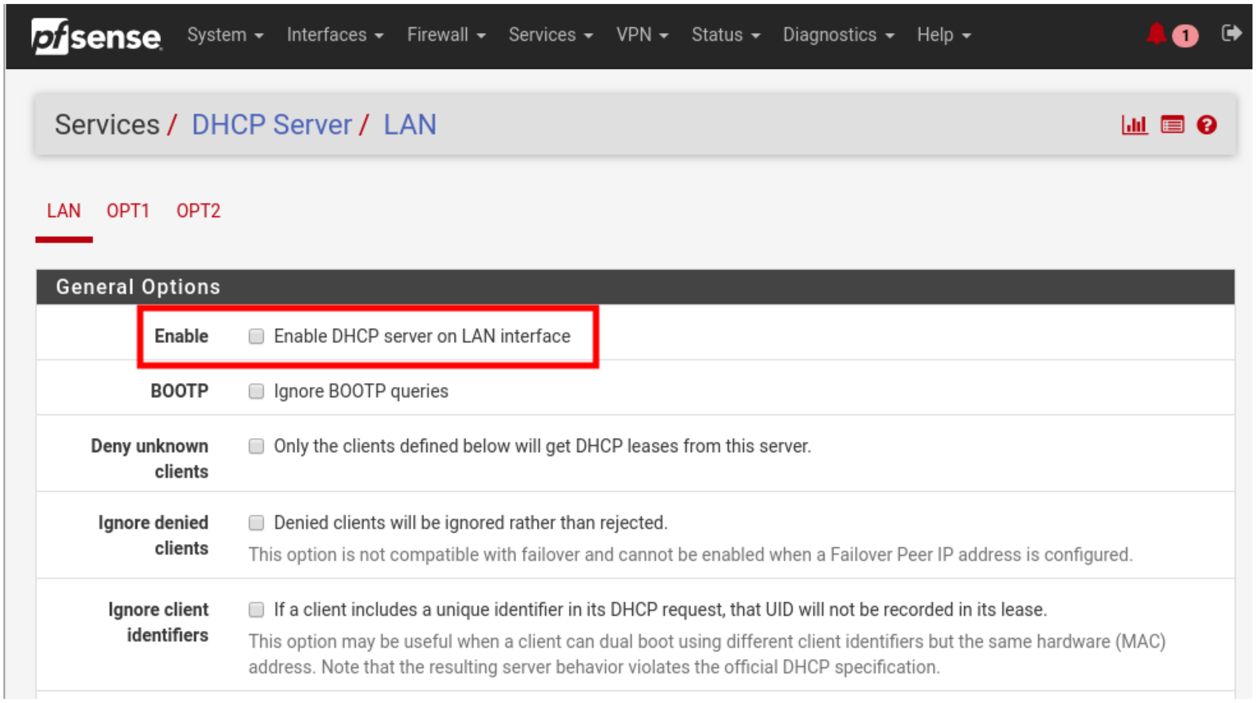
1.35.3 Disable DHCP on the LAN

pfSense runs a DHCP server on the LAN[1] interface by default. At this stage in the documentation, the *Admin Workstation* likely has an IP address assigned via that DHCP server.

In order to tighten the firewall rules as much as possible, we recommend disabling the DHCP server and assigning a static IP address to the Admin Workstation instead.

Disable DHCP Server on the Firewall

To disable DHCP, navigate to **Services** ► **DHCP Server** in the pfSense WebGUI. Uncheck the box labeled **Enable DHCP server on LAN interface**, scroll down, and click the **Save** button.



Services / DHCP Server / LAN

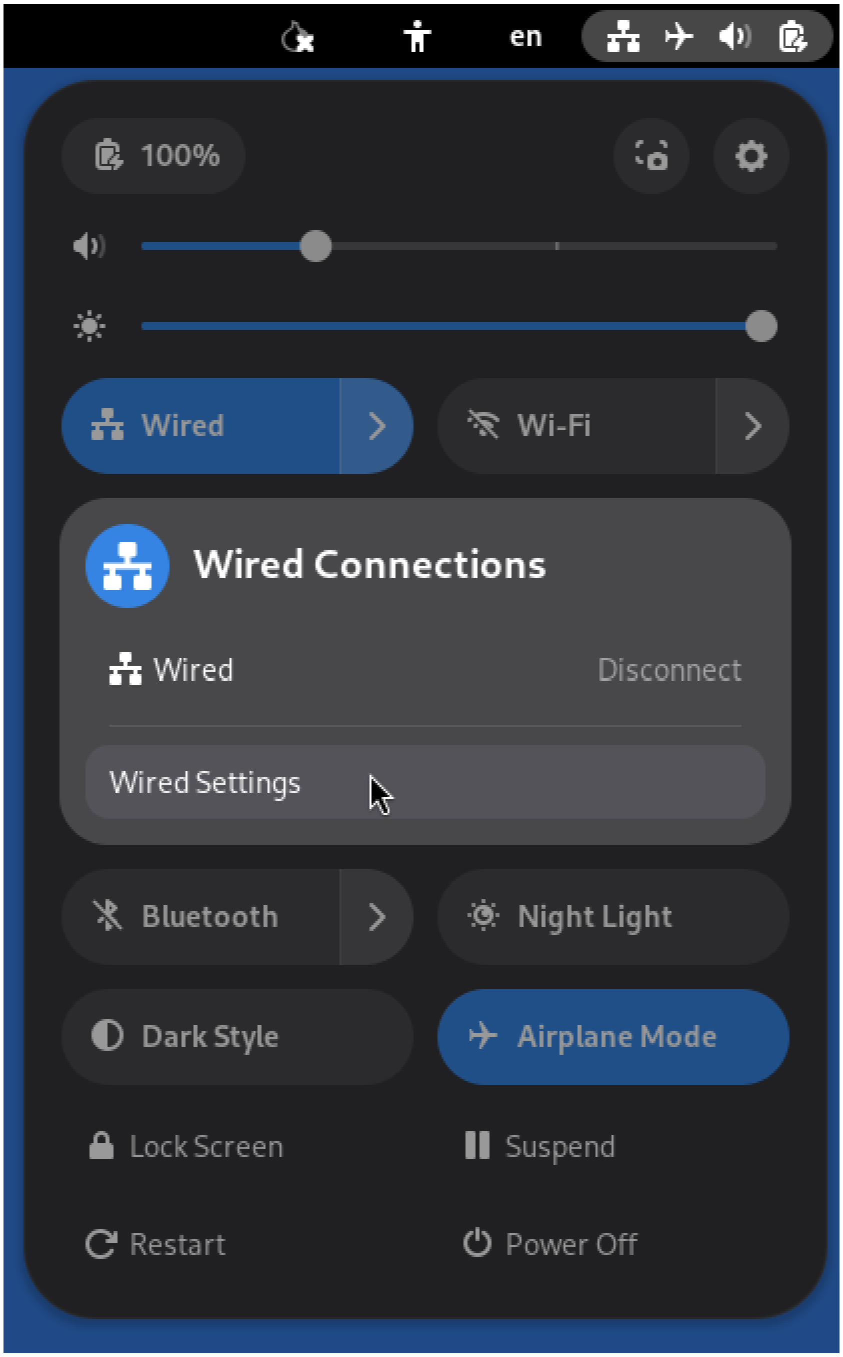
General Options

Enable	□ Enable DHCP server on LAN interface
BOOTP	□ Ignore BOOTP queries
Deny unknown clients	□ Only the clients defined below will get DHCP leases from this server.
Ignore denied clients	□ Denied clients will be ignored rather than rejected. This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore client identifiers	□ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease. This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

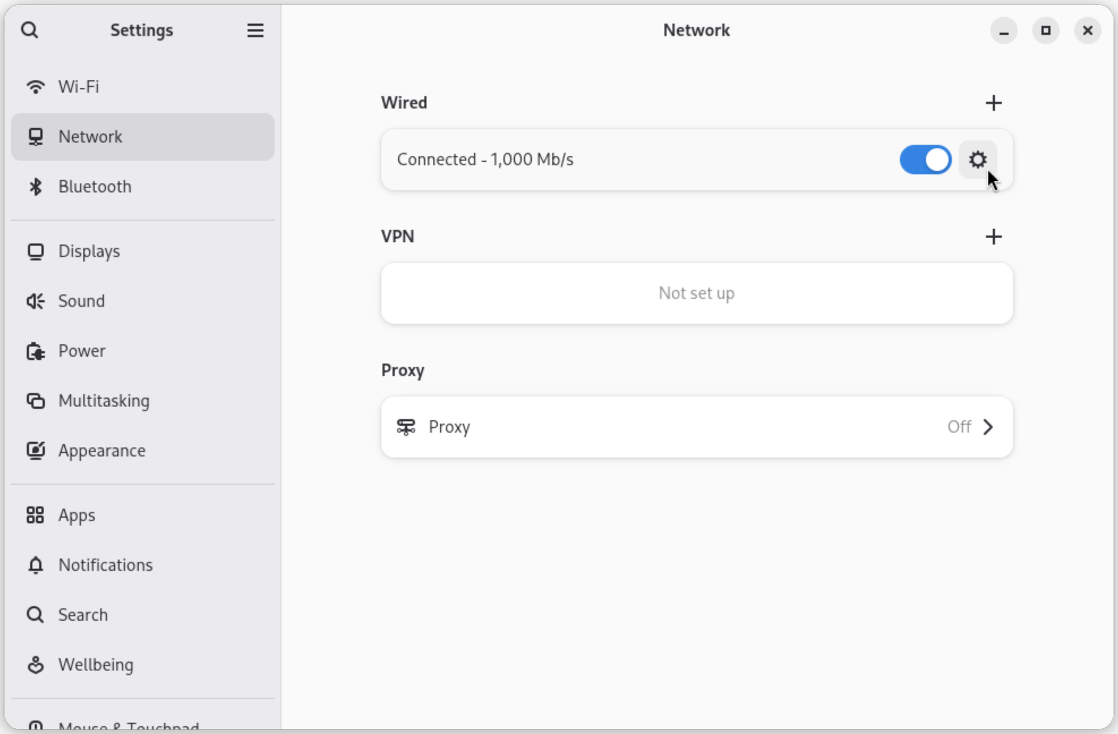
Assign a Static IP Address to the *Admin Workstation*

Now you will need to assign a static IP to the *Admin Workstation*.

You can easily check your current IP address by *clicking* the top right of the menu bar, clicking on the **Wired Connection** and then clicking **Wired Settings**.



From here you can click on the cog beside the wired network connection:



Wired

Connected - 1,000 Mb/s

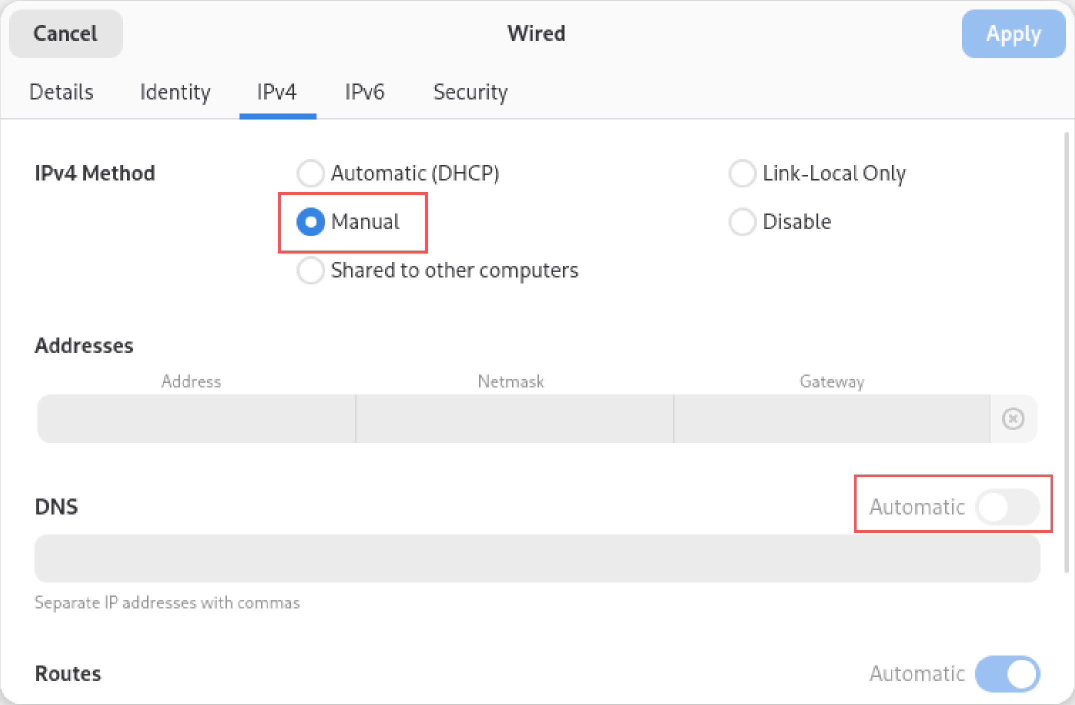
VPN

Not set up

Proxy

Proxy Off

This will take you to the network settings. Change to the **IPv4** tab. Ensure that **IPv4 Method** is set to **Manual**, and that the **Automatic** switch for **DNS** is in the “off” position, as highlighted in the screenshot below:



IPv4 Method ○ Automatic (DHCP) ○ Link-Local Only
● Manual ○ Disable
○ Shared to other computers

Addresses

Address	Netmask	Gateway

DNS Automatic ○

Separate IP addresses with commas

Routes Automatic ●

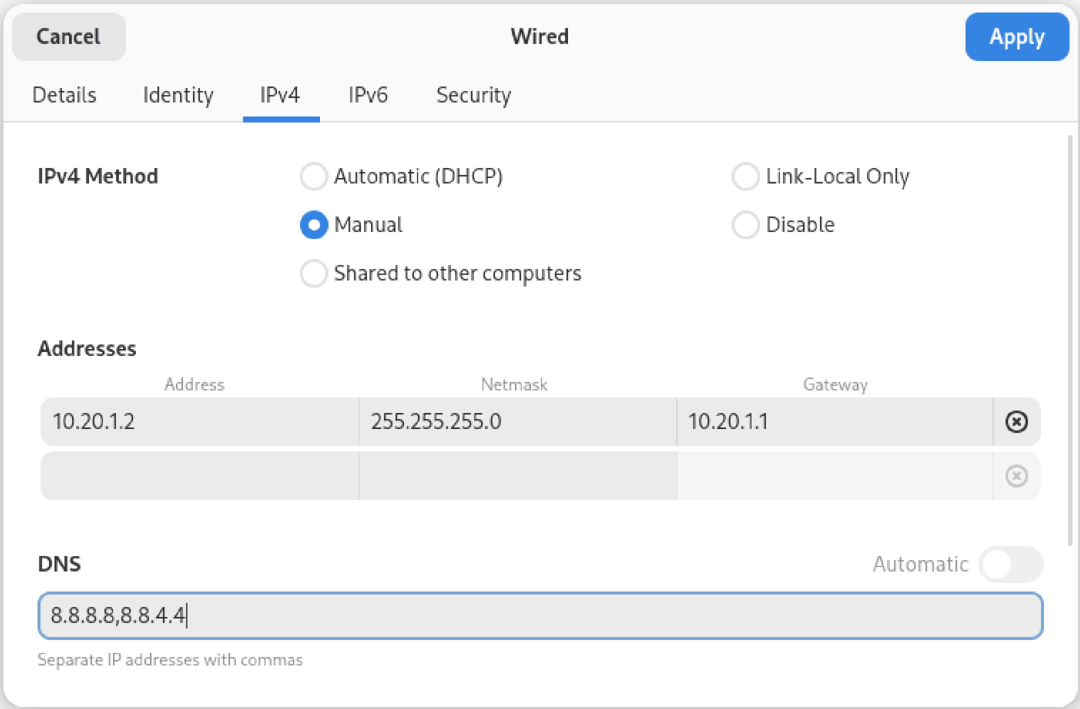
Note

The Unsafe Browser will not launch when using a manual network configuration if it does not have DNS servers configured. This is technically unnecessary for our use case because we are only using it to access IP addresses on the LAN, and do not need to resolve anything with DNS. Nonetheless, you should configure some DNS servers here so you can continue to use the Unsafe Browser to access the WebGUI in future sessions.

We recommend keeping it simple and using the same DNS servers that you used for the network firewall in the setup wizard.

Fill in the static networking information for the *Admin Workstation*:

- Address: `10.20.1.2`
- Netmask: `255.255.255.0`
- Gateway : `10.20.1.1`



IPv4 Method

○ Automatic (DHCP)
○ Link-Local Only
● Manual
○ Disable
○ Shared to other computers

Addresses

Address	Netmask	Gateway
10.20.1.2	255.255.255.0	10.20.1.1

DNS — Automatic ○

8.8.8.8,8.8.4.4

Separate IP addresses with commas

Click **Apply**. If the network does not come up within 15 seconds or so, try disconnecting and reconnecting your network cable to trigger the change. You will need you have succeeded in connecting with your new static IP when you are able to connect using the Tor Connection assistant, and you see the message "Connected to Tor successfully".

Troubleshooting: DNS Servers and the Unsafe Browser

After saving the new network configuration, you may still encounter the "No DNS servers configured" error when trying to launch the Unsafe Browser. If you encounter this issue, you can resolve it by disconnecting from the network and then reconnecting, which causes the network configuration to be reloaded.

To do this, click the network icon in the system toolbar, and click **Disconnect** under the name of the currently active network connection, which is displayed in bold. After it disconnects, click the network icon again and click the name of the connection to reconnect. You should see a popup notification that says "Connection Established", and the Tor Connection assistant should show the message "Connected to Tor successfully".

For the next step, SecureDrop Configuration, you will manually configure the firewall for SecureDrop, using screenshots as a reference.

1.35.4 SecureDrop Configuration

SecureDrop uses the firewall to achieve two primary goals:

1. Isolating SecureDrop from the existing network, which may be compromised (especially if it is a venerable network in a large organization like a newsroom).
2. Isolating the *Application Server* and the *Monitor Server* from each other as much as possible, to reduce attack surface.

In order to use the firewall to isolate the *Application Server* and the *Monitor Server* from each other, we need to connect them to separate interfaces, and then set up firewall rules that allow them to communicate.

Set Up the Firewall Rules

Since there are a variety of firewalls with different configuration interfaces and underlying sets of software, we cannot provide a set of network firewall rules to match every use case.

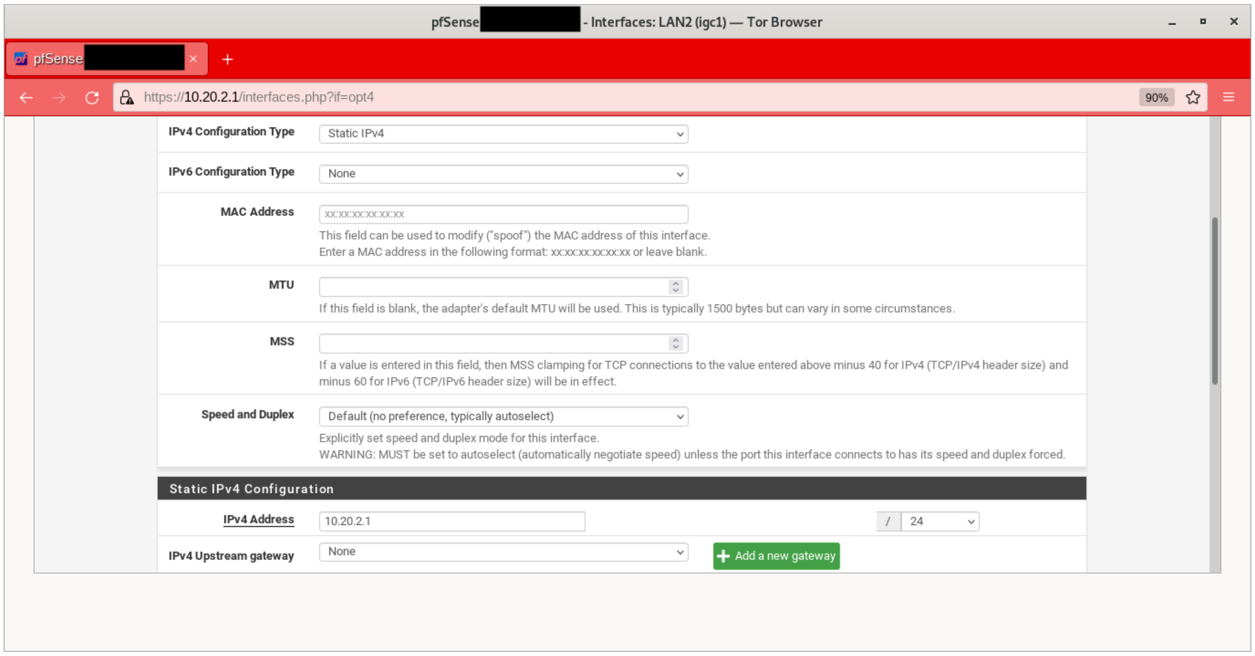
The easiest way to set up your firewall rules is to look at the screenshots of a correctly configured firewall and edit the interfaces, aliases, and firewall rules on your firewall to match them.

Set Up LAN2

We set up the LAN[1] interface during the initial configuration. We now need to set up the LAN2 interface for the *Application Server*. Start by connecting the *Application Server* to the LAN2 port. Then use the WebGUI to configure the LAN2 interface. Go to **Interfaces ▶ LAN2**, and check the box to **Enable Interface**. Use these settings:

- IPv4 Configuration Type: Static IPv4
- IPv4 Address: `10.20.2.1` (Application Gateway IP)

Make sure that the CIDR routing prefix is correct (`/24`). Leave everything else as the default. **Save** and **Apply Changes**.



pfSense[redacted] - Interfaces: LAN2 (igc1) — Tor Browser

pfSense[redacted]

https://10.20.2.1/interfaces.php?if=opt4

IPv4 Configuration Type: Static IPv4

IPv6 Configuration Type: None

MAC Address: xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS:

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex: Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address: 10.20.2.1 / 24

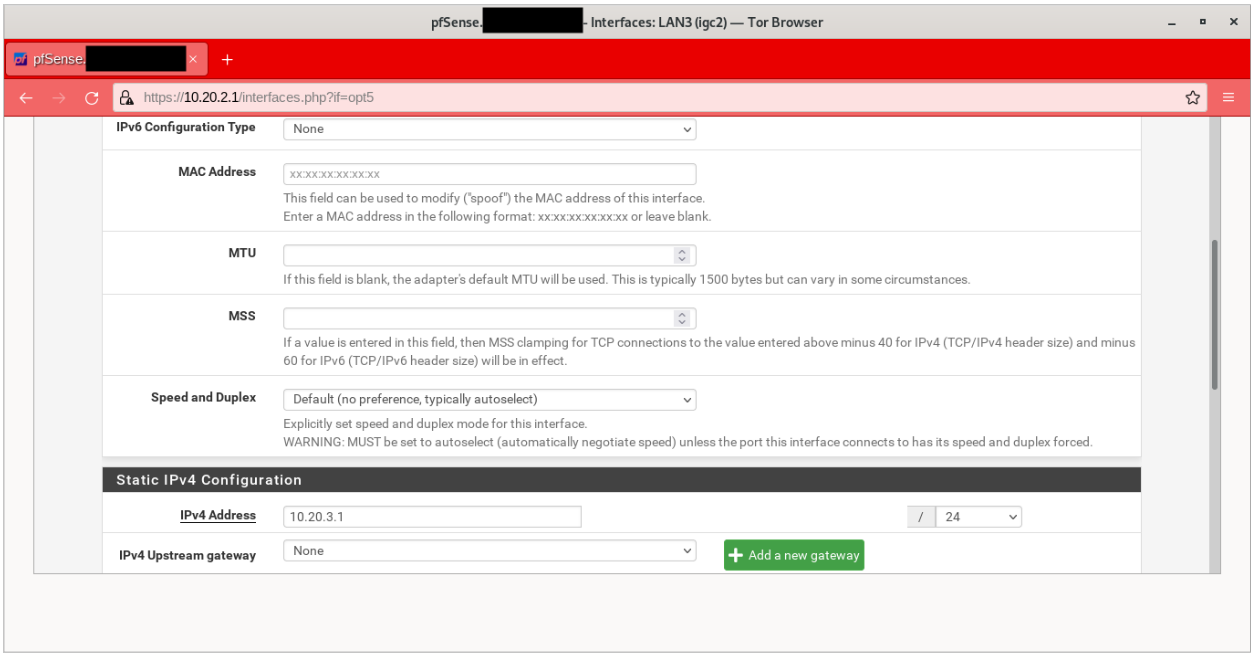
IPv4 Upstream gateway: None

Set Up LAN3

Next, you will have to enable the LAN3 interface. Go to **Interfaces ▶ LAN3**, and check the box to **Enable Interface**. LAN3 interface is set up similarly to how we set up LAN2 in the previous section. Use these settings:

- IPv4 Configuration Type: Static IPv4
- IPv4 Address: `10.20.3.1` (Monitor Gateway IP)

Make sure that the CIDR routing prefix is correct (`/24`). Leave everything else as the default. **Save** and **Apply Changes**.



pfSense.[redacted] - Interfaces: LAN3 (igc2) — Tor Browser

pfSense.[redacted]

https://10.20.2.1/interfaces.php?if=opt5

IPv6 Configuration Type	None
MAC Address	xx:xx:xx:xx:xx:xx This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

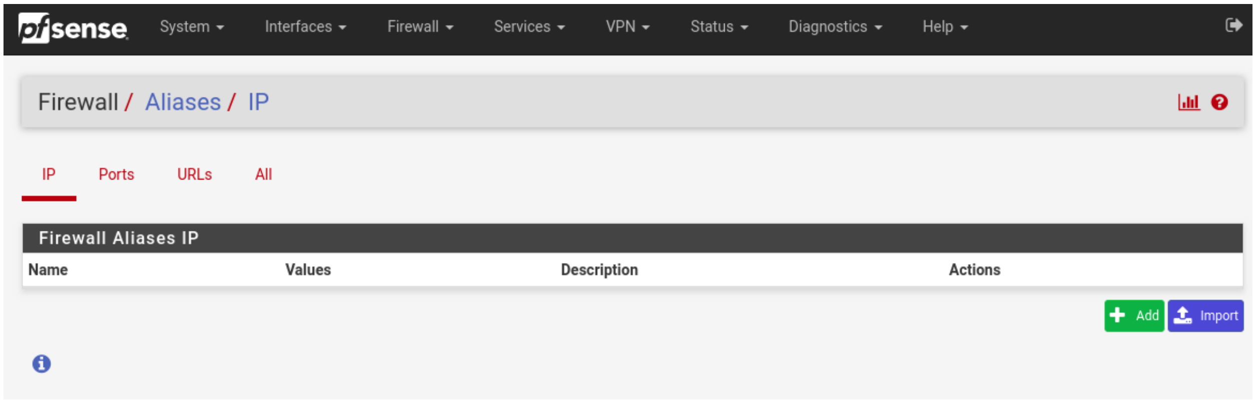
Static IPv4 Configuration

IPv4 Address	10.20.3.1 / 24
IPv4 Upstream gateway	None

Use Screenshots of Firewall Configuration

Here are some example screenshots of a working pfSense firewall configuration. You will add the firewall rules until they match what is shown on the screenshots.

First, we will configure IP and port aliases. Navigate to **Firewall ▶ Aliases** and you should see a screen with no currently defined IP aliases:



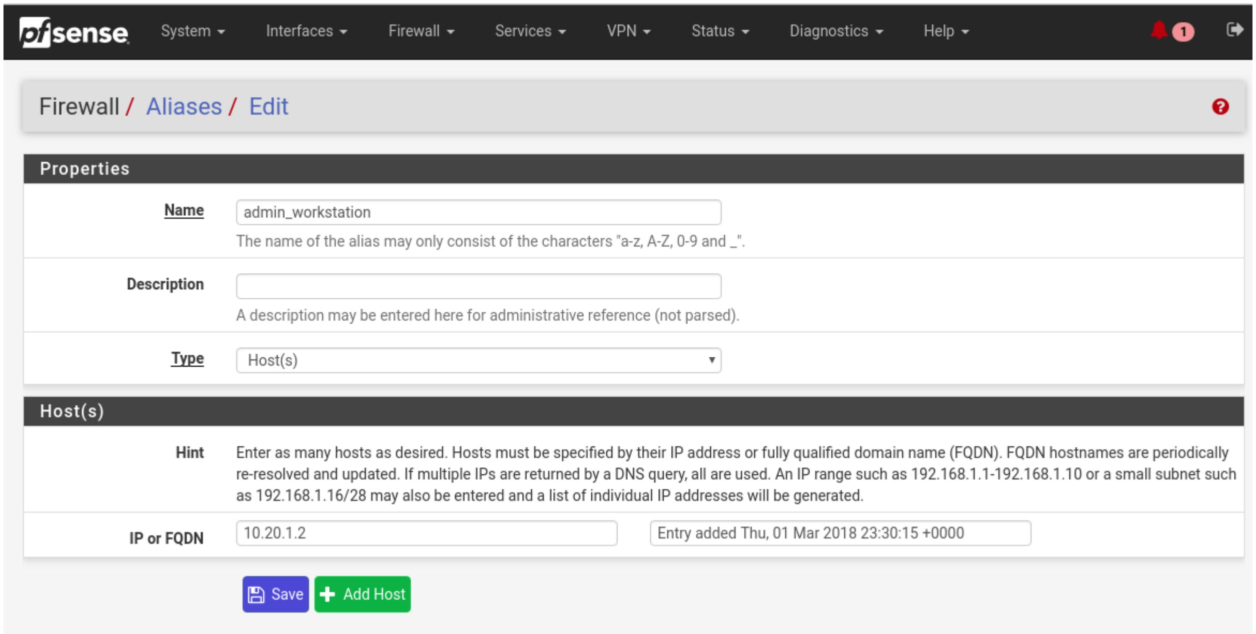
Firewall / Aliases / IP

Firewall Aliases IP

Name	Values	Description	Actions

Next you will click **Add** to add each IP alias. You should leave the **Type** as **Host**. Make aliases for the following:

- `admin_workstation`: `10.20.1.2`
- `app_server`: `10.20.2.2`
- `external_dns_servers`: `8.8.8.8, 8.8.4.4`
- `monitor_server`: `10.20.3.2`
- `local_servers`: `app_server, monitor_server`



Firewall / Aliases / Edit

Properties

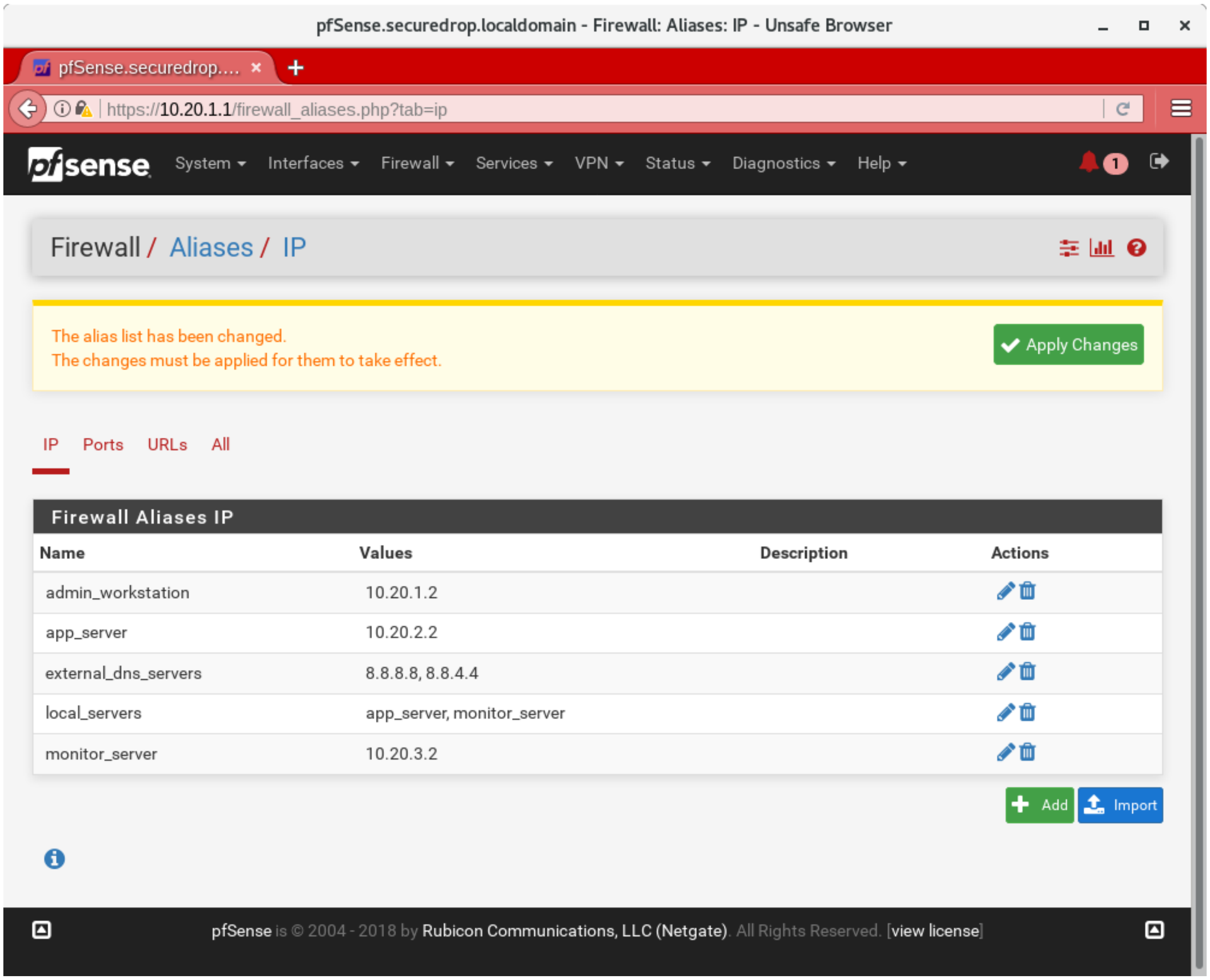
Name	admin_workstation The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	 A description may be entered here for administrative reference (not parsed).
Type	Host(s)

Host(s)

Hint	Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.	
IP or FQDN	10.20.1.2	Entry added Thu, 01 Mar 2018 23:30:15 +0000

Click **Save** to add the alias.

Keep adding aliases until the screenshot matches what is shown here:



pfSense.securedrop.localdomain - Firewall: Aliases: IP - Unsafe Browser
pfSense.securedrop....
https://10.20.1.1/firewall_aliases.php?tab=ip
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Aliases / IP

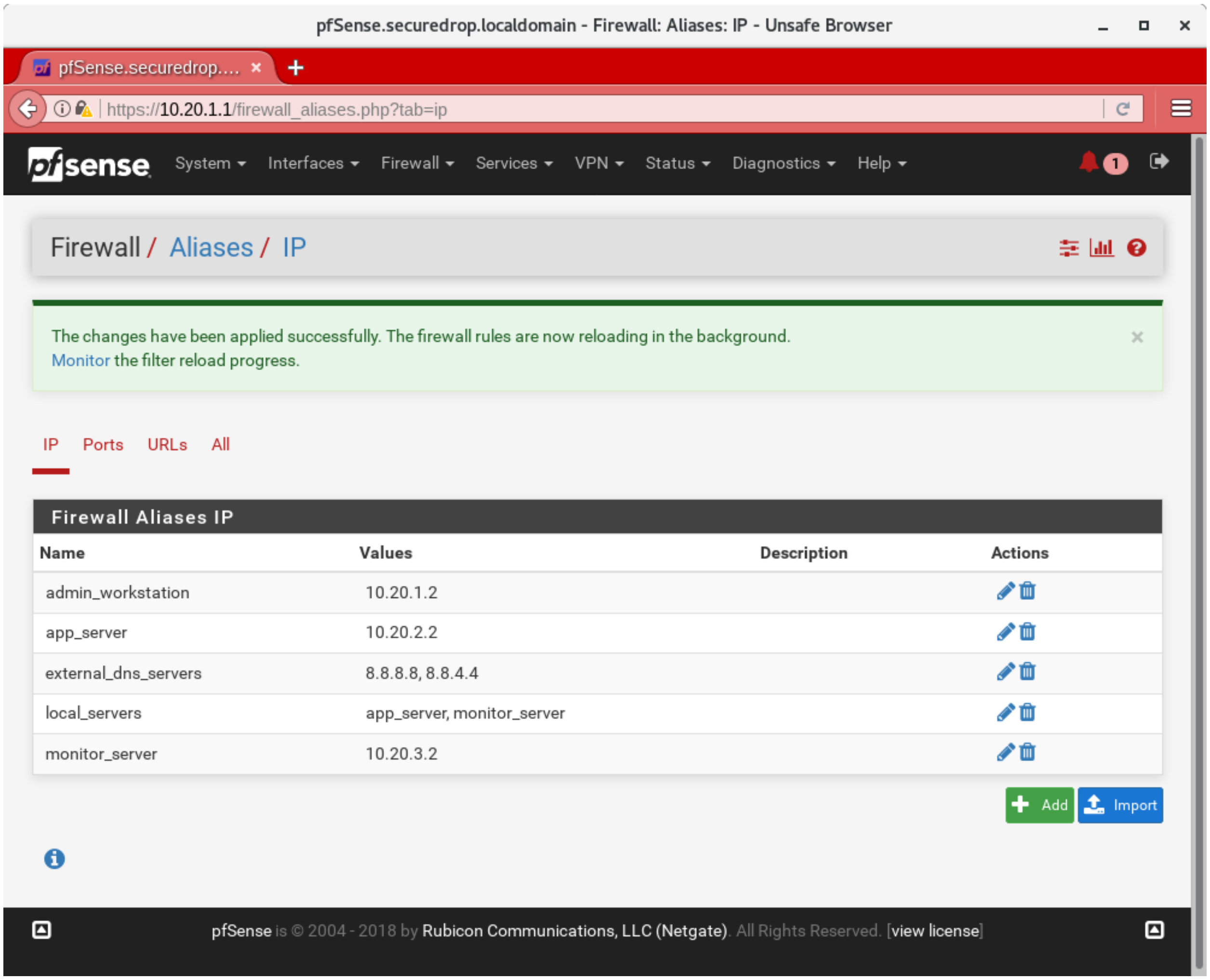
The alias list has been changed.
The changes must be applied for them to take effect.

Firewall Aliases IP

Name	Values	Description	Actions
admin_workstation	10.20.1.2		
app_server	10.20.2.2		
external_dns_servers	8.8.8.8, 8.8.4.4		
local_servers	app_server, monitor_server		
monitor_server	10.20.3.2		

pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

Finally, click **Apply Changes**. This will save your changes. You should see a message “The changes have been applied successfully”:



pfSense.securedrop.localdomain - Firewall: Aliases: IP - Unsafe Browser
pfSense.securedrop....
https://10.20.1.1/firewall_aliases.php?tab=ip
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Aliases / IP
IP
Ports
URLs
All
Add
Import
pfSense is © 2004 - 2018 by Rubicon Communications, LLC (Netgate). All Rights Reserved. [view license]

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

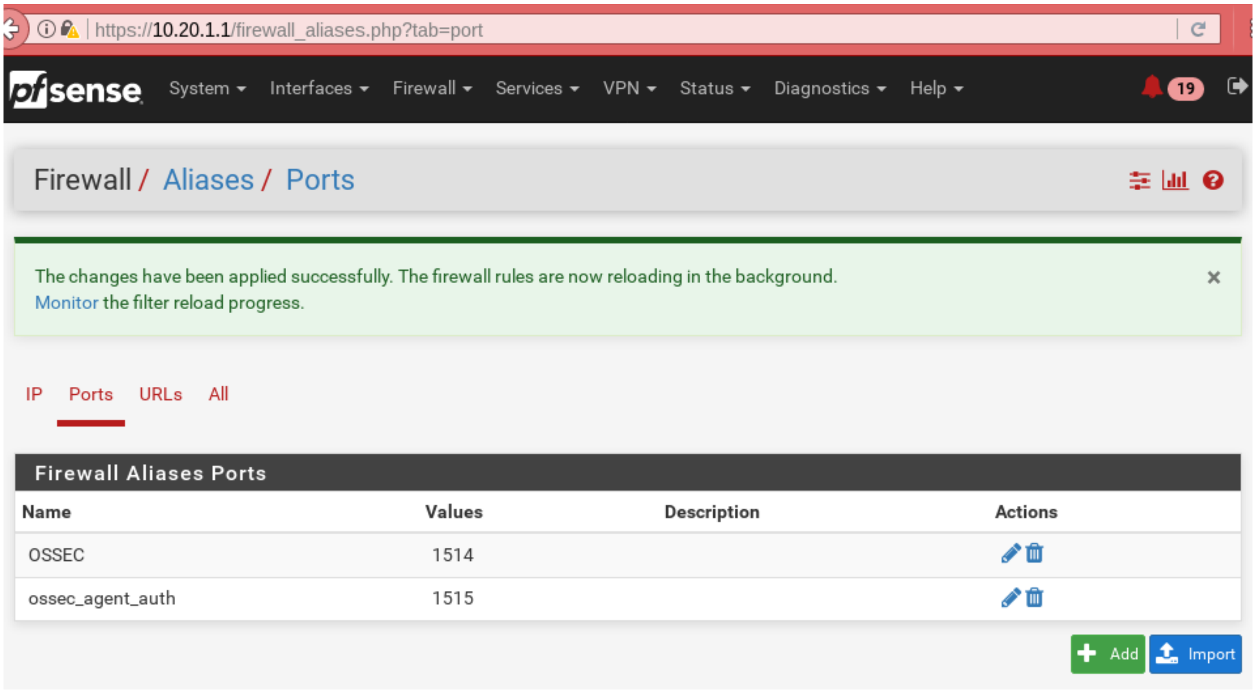
Firewall Aliases IP

Name	Values	Description	Actions
admin_workstation	10.20.1.2		
app_server	10.20.2.2		
external_dns_servers	8.8.8.8, 8.8.4.4		
local_servers	app_server, monitor_server		
monitor_server	10.20.3.2		

Next click "Ports" for the port aliases, and add the following ports:

- OSSEC: 1514
- ossec_agent_auth: 1515

Your configuration should match this screenshot:



https://10.20.1.1/firewall_aliases.php?tab=port

Firewall / Aliases / Ports

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Firewall Aliases Ports

Name	Values	Description	Actions
OSSEC	1514		
ossec_agent_auth	1515		

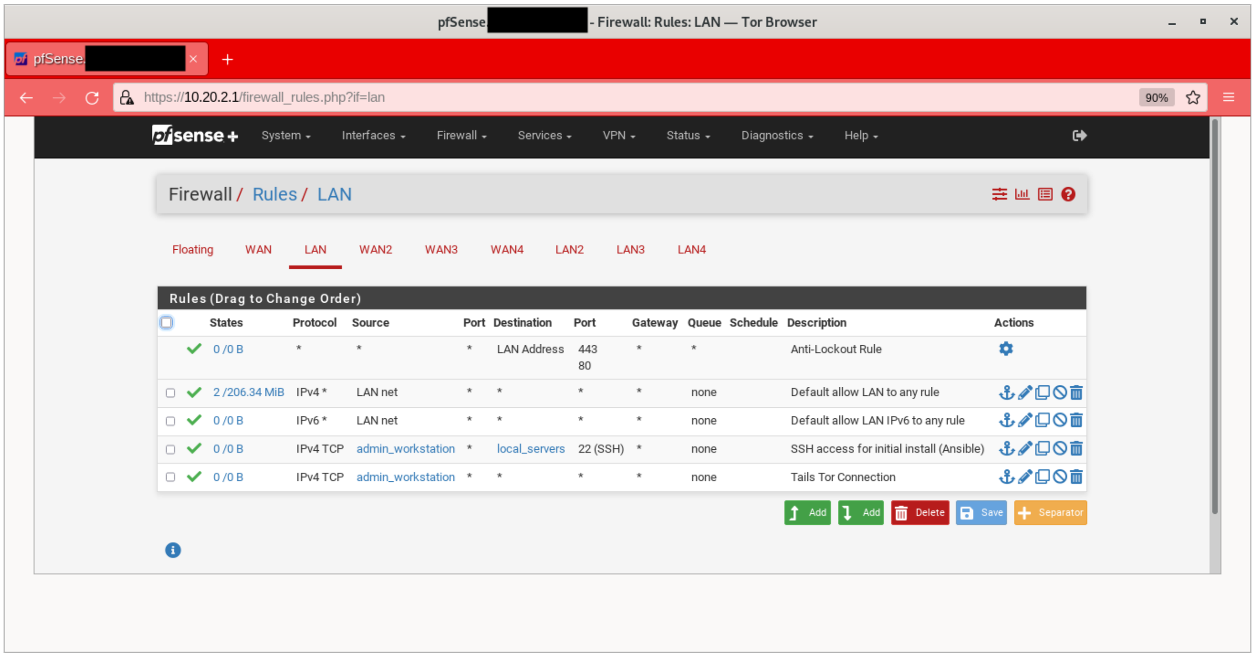
Next we will configure firewall rules for each interface. Navigate to **Firewall ▶ Rules** to add firewall rules for the LAN1, LAN2, and LAN3 interfaces.

Warning

Be sure not to delete the Anti-Lockout Rule on the LAN1 interface. Deleting this rule will lock you out of the pfSense WebGUI.

Add or remove rules until they match the following screenshots by clicking **Add** to add a rule.

LAN[1] interface:



pfSense [redacted] - Firewall: Rules: LAN — Tor Browser

pfSense [redacted]

https://10.20.2.1/firewall_rules.php?if=lan

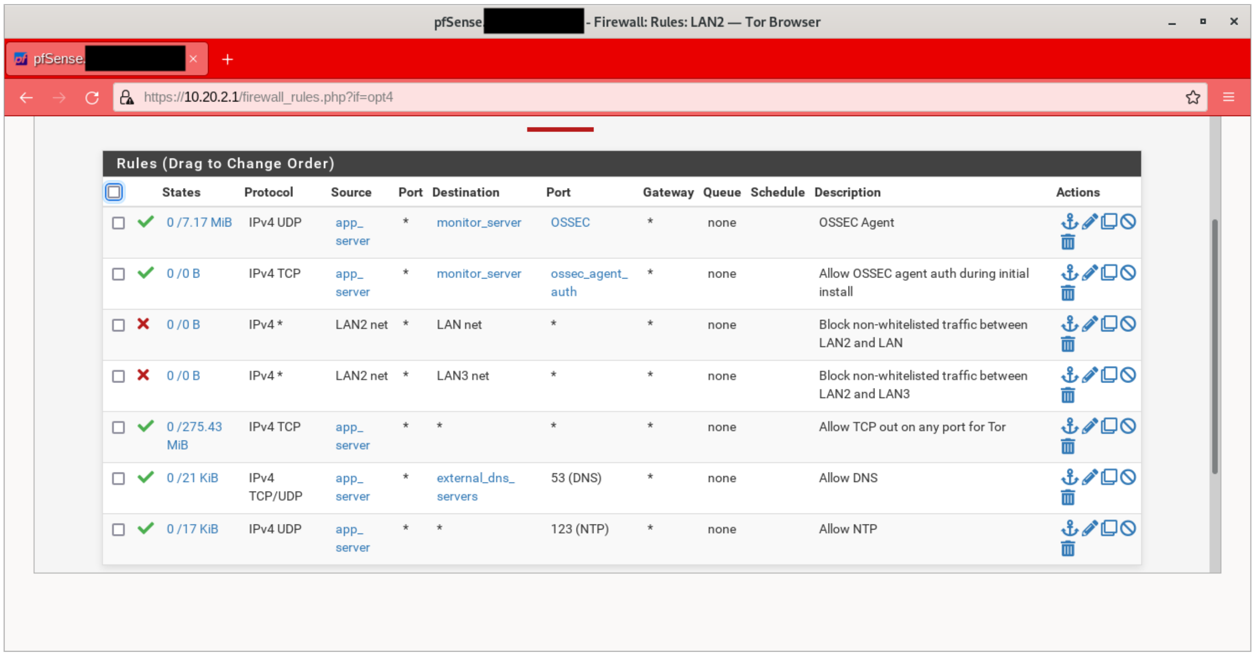
Firewall / Rules / LAN

Floating WAN LAN WAN2 WAN3 WAN4 LAN2 LAN3 LAN4

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0 /0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
□	✓	2 /206.34 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	
□	✓	0 /0 B	IPv4 TCP	admin_workstation	*	local_servers	22 (SSH)	*	none		SSH access for initial install (Ansible)	
□	✓	0 /0 B	IPv4 TCP	admin_workstation	*	*	*	*	none		Tails Tor Connection	

LAN2 interface:



pfSense [redacted] - Firewall: Rules: LAN2 — Tor Browser

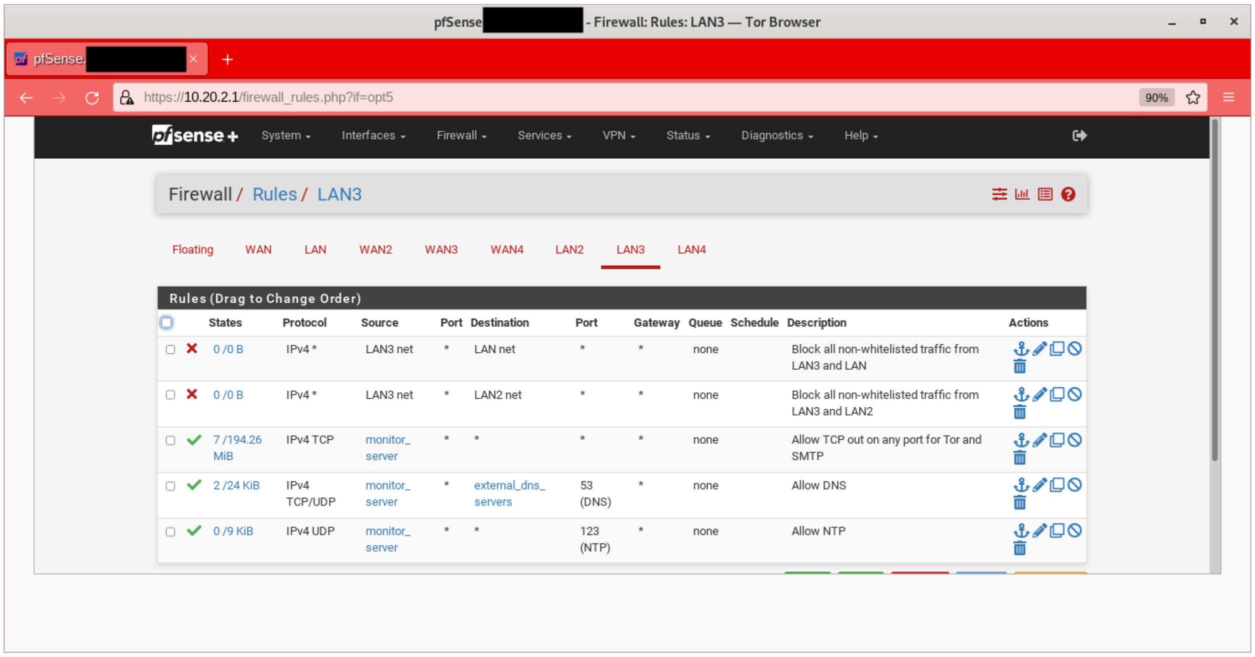
pfSense [redacted]

https://10.20.2.1/firewall_rules.php?if=opt4

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /7.17 MiB	IPv4 UDP	app_server	*	monitor_server	OSSEC	*	none		OSSEC Agent	
□	✓	0 /0 B	IPv4 TCP	app_server	*	monitor_server	ossec_agent_auth	*	none		Allow OSSEC agent auth during initial install	
□	✗	0 /0 B	IPv4 *	LAN2 net	*	LAN net	*	*	none		Block non-whitelisted traffic between LAN2 and LAN	
□	✗	0 /0 B	IPv4 *	LAN2 net	*	LAN3 net	*	*	none		Block non-whitelisted traffic between LAN2 and LAN3	
□	✓	0 /275.43 MiB	IPv4 TCP	app_server	*	*	*	*	none		Allow TCP out on any port for Tor	
□	✓	0 /21 KiB	IPv4 TCP/UDP	app_server	*	external_dns_servers	53 (DNS)	*	none		Allow DNS	
□	✓	0 /17 KiB	IPv4 UDP	app_server	*	*	123 (NTP)	*	none		Allow NTP	

LAN3 interface:



pfSense[redacted] - Firewall: Rules: LAN3 — Tor Browser

https://10.20.2.1/firewall_rules.php?if=opt5

Firewall / Rules / LAN3

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0 /0 B	IPv4 *	LAN3 net	*	LAN net	*	*	none		Block all non-whitelisted traffic from LAN3 and LAN	
□	✗	0 /0 B	IPv4 *	LAN3 net	*	LAN2 net	*	*	none		Block all non-whitelisted traffic from LAN3 and LAN2	
□	✓	7 /194.26 MiB	IPv4 TCP	monitor_server	*	*	*	*	none		Allow TCP out on any port for Tor and SMTP	
□	✓	2 /24 KiB	IPv4 TCP/UDP	monitor_server	*	external_dns_servers	53 (DNS)	*	none		Allow DNS	
□	✓	0 /9 KiB	IPv4 UDP	monitor_server	*	*	123 (NTP)	*	none		Allow NTP	

Finally, click **Apply Changes**. This will save your changes. You should see a message “The changes have been applied successfully”. Once you’ve set up the firewall, exit the Unsafe Browser, and continue with the “Keeping pfSense up to date” section below.

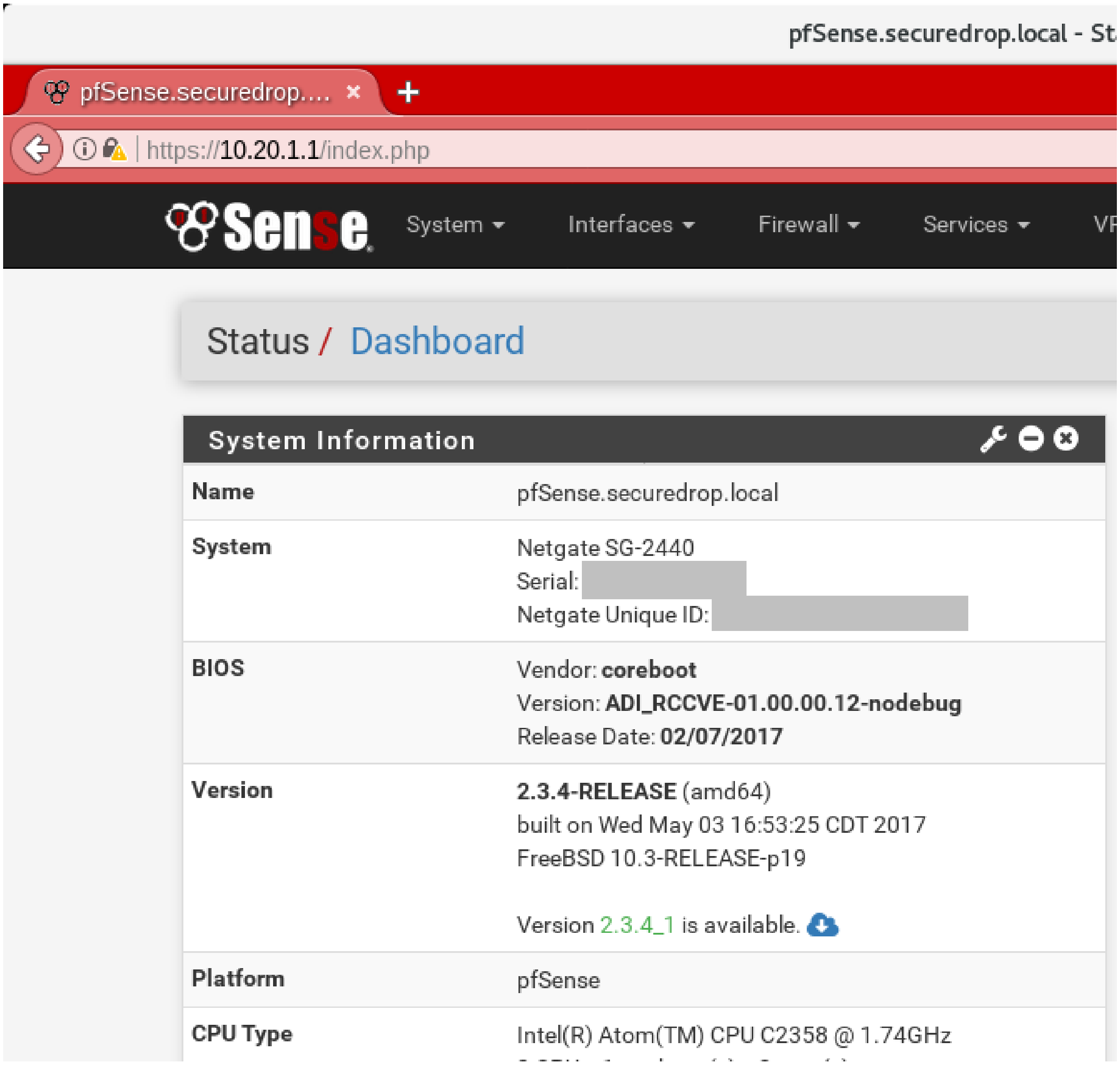
1.35.5 Tips for Setting Up pfSense Firewall Rules

Here are some general tips for setting up pfSense firewall rules:

1. Create aliases for the repeated values (IPs and ports).
2. pfSense is a stateful firewall, which means that you don’t need corresponding rules to allow incoming traffic in response to outgoing traffic (like you would in, e.g. iptables with `--state ESTABLISHED,RELATED`). pfSense does this for you automatically.
3. You should create the rules *on the interface where the traffic originates*.
4. Make sure you delete the default “allow all” rule on the LAN interface. Leave the “Anti-Lockout” rule enabled.
5. Any traffic that is not explicitly passed is logged and dropped by default in pfSense, so you don’t need to add explicit rules (iptables `LOGNDROP`) for that.
6. Since some of the rules are almost identical except for whether they allow traffic from the *Application Server* or the *Monitor Server*, you can use the “add a new rule based on this one” button to save time creating a copy of the rule on the other interface.
7. If you are troubleshooting connectivity, the firewall logs can be very helpful. You can find them in the WebGUI in *Status* → *System Logs* → *Firewall*.

1.35.6 Keeping pfSense up to Date

Periodically, the pfSense project maintainers release an update to the pfSense software running on your firewall. You will be notified by the appearance of text saying that there is a new version in the **Version** section of the “Status: Dashboard” page (the home page of the WebGUI).



Status / Dashboard

System Information

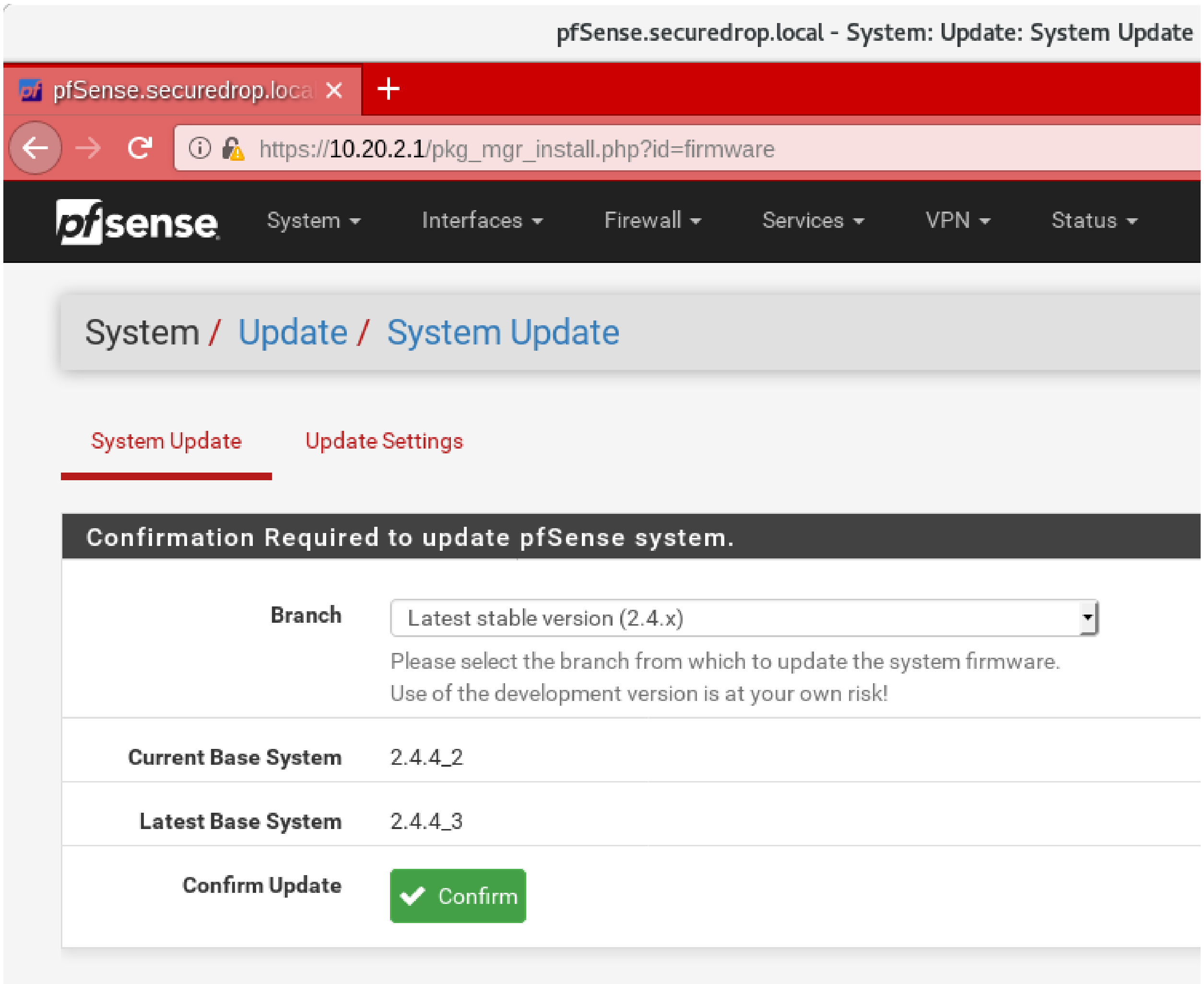
Name	pfSense.securedrop.local
System	Netgate SG-2440 Serial: [redacted] Netgate Unique ID: [redacted]
BIOS	Vendor: **coreboot** Version: **ADI_RCCVE-01.00.00.12-nodebug** Release Date: **02/07/2017**
Version	**2.3.4-RELEASE** (amd64) built on Wed May 03 16:53:25 CDT 2017 FreeBSD 10.3-RELEASE-p19 Version 2.3.4_1 is available.
Platform	pfSense
CPU Type	Intel(R) Atom(TM) CPU C2358 @ 1.74GHz

If you see that an update is available, we recommend installing it. Most of these updates are for minor bugfixes, but occasionally they can contain important security fixes. You should keep apprised of updates yourself by checking the pfSense Blog posts with the "releases" tag.

Note

You can subscribe to email updates on https://www.netgate.com.

To install the update, click the Download icon next to the update then click the "Confirm" button:



pfSense.securedrop.local - System: Update: System Update

https://10.20.2.1/pkg_mgr_install.php?id=firmware

System / Update / System Update

Confirmation Required to update pfSense system.

Branch: Latest stable version (2.4.x)

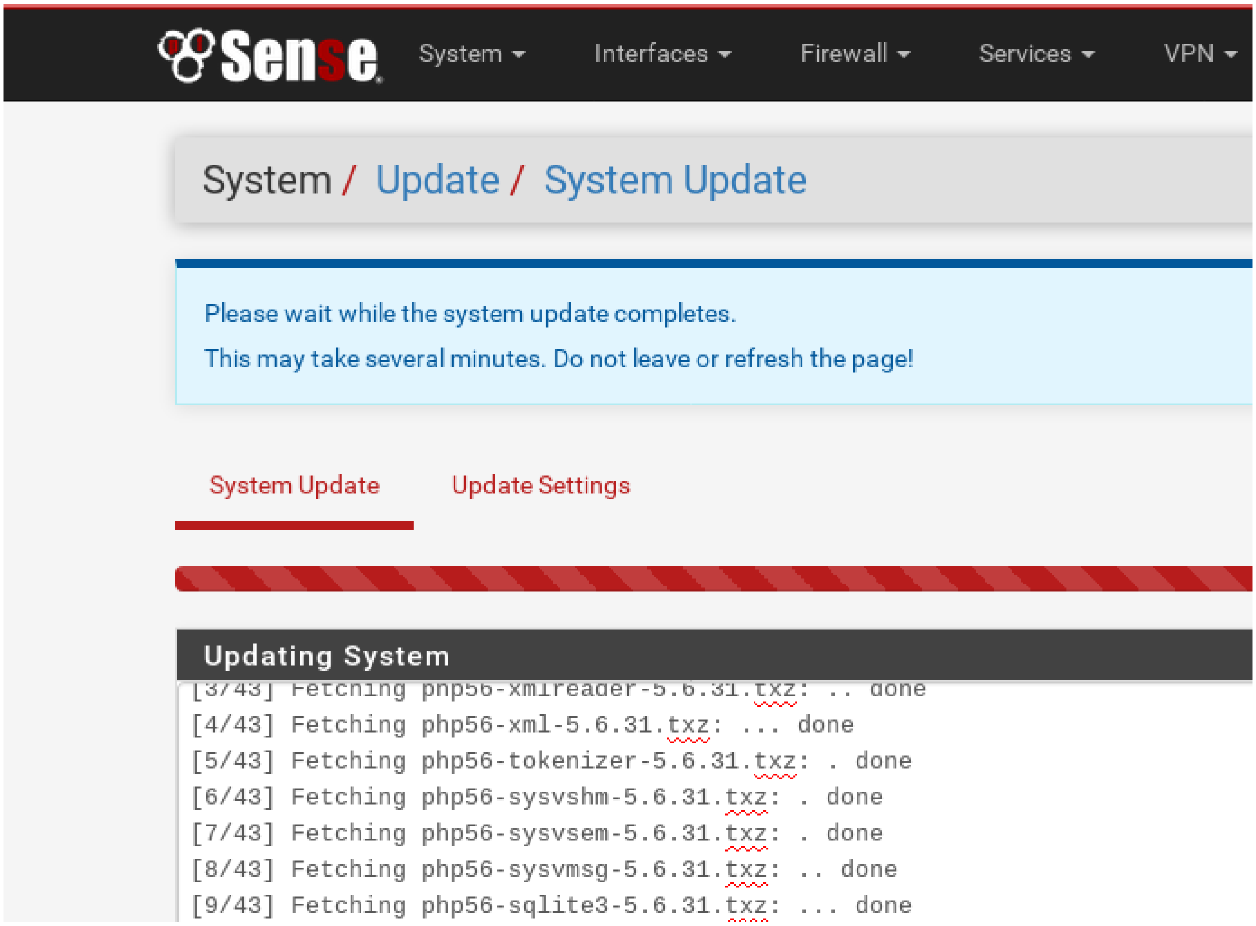
Please select the branch from which to update the system firmware. Use of the development version is at your own risk!

Current Base System: 2.4.4_2

Latest Base System: 2.4.4_3

Confirm Update: Confirm

You will see a page with a progress bar while pfSense performs the upgrade:



Please wait while the system update completes.

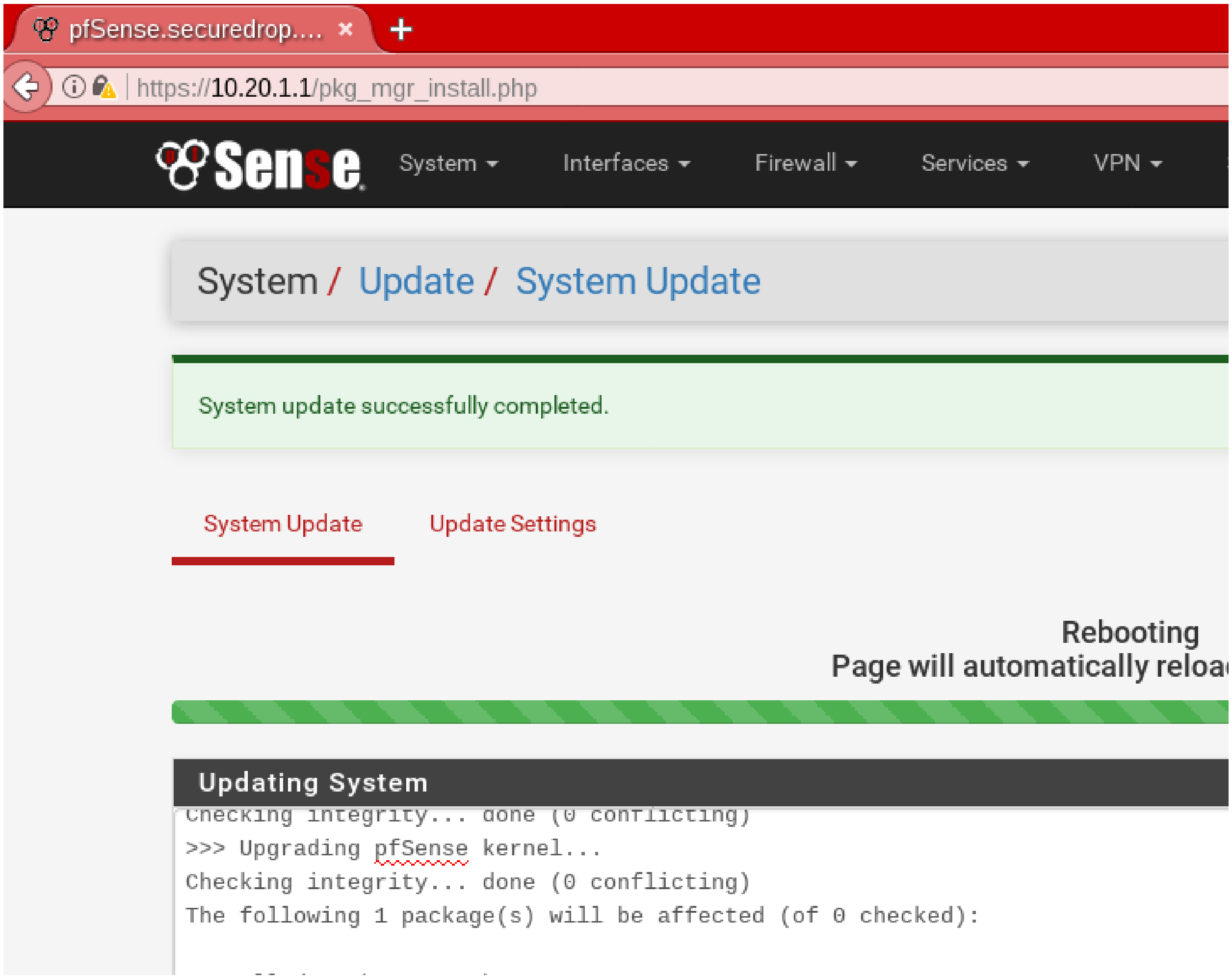
This may take several minutes. Do not leave or refresh the page!

```
[3/43] Fetching php56-xmlreader-5.6.31.txz: .. done
[4/43] Fetching php56-xml-5.6.31.txz: ... done
[5/43] Fetching php56-tokenizer-5.6.31.txz: . done
[6/43] Fetching php56-sysvshm-5.6.31.txz: . done
[7/43] Fetching php56-sysvsem-5.6.31.txz: . done
[8/43] Fetching php56-sysvmsg-5.6.31.txz: .. done
[9/43] Fetching php56-sqlite3-5.6.31.txz: ... done
```

Note

This may take a while, so be patient!

Once it is complete, you will see a notification of successful upgrade:



System / Update / System Update

System update successfully completed.

Rebooting
Page will automatically reloa

Updating System

```
Checking integrity... done (0 conflicting)
>>> Upgrading pfSense kernel...
Checking integrity... done (0 conflicting)
The following 1 package(s) will be affected (of 0 checked):
```

The *Network Firewall* configuration is now complete, allowing you to move to the next step: *setting up the servers.*

1.36 Setting Up An OPNSense Network Firewall

1.36.1 Before You Begin

First, consider how the firewall will be connected to the Internet. You will need to provision several unique subnets, which should not conflict with the network configuration on the WAN interface. If you are unsure, consult your local system administrator.

Many firewalls, including the recommended OPNSense device, automatically set up the LAN interface on `192.168.1.1/24`. This particular private network is also a very common choice for home and office routers. If you are connecting the firewall to a router with the same subnet (common in a small office, home, or testing environment), you will probably be unable to connect to the network at first. However, you will be able to connect from the LAN to the firewall's Web GUI, and from there you will be able to configure the network so it is working correctly.

The recommended TekLager APU4D4 has 4 NICs: WAN, LAN, OPT1, and OPT2. This allows for a dedicated port on the network firewall for each component of SecureDrop (*Application Server*, *Monitor Server*, and *Admin Workstation*).

Depending on your network configuration, you should define the following values before continuing.

- Admin Subnet: `10.20.1.0/24`
- Admin Gateway: `10.20.1.1`

- Admin Workstation: `10.20.1.2`
- Application Subnet: `10.20.2.0/24`
- Application Gateway: `10.20.2.1`
- Application Server (OPT1): `10.20.2.2`
- Monitor Subnet: `10.20.3.0/24`
- Monitor Gateway: `10.20.3.1`
- Monitor Server (OPT2) : `10.20.3.2`

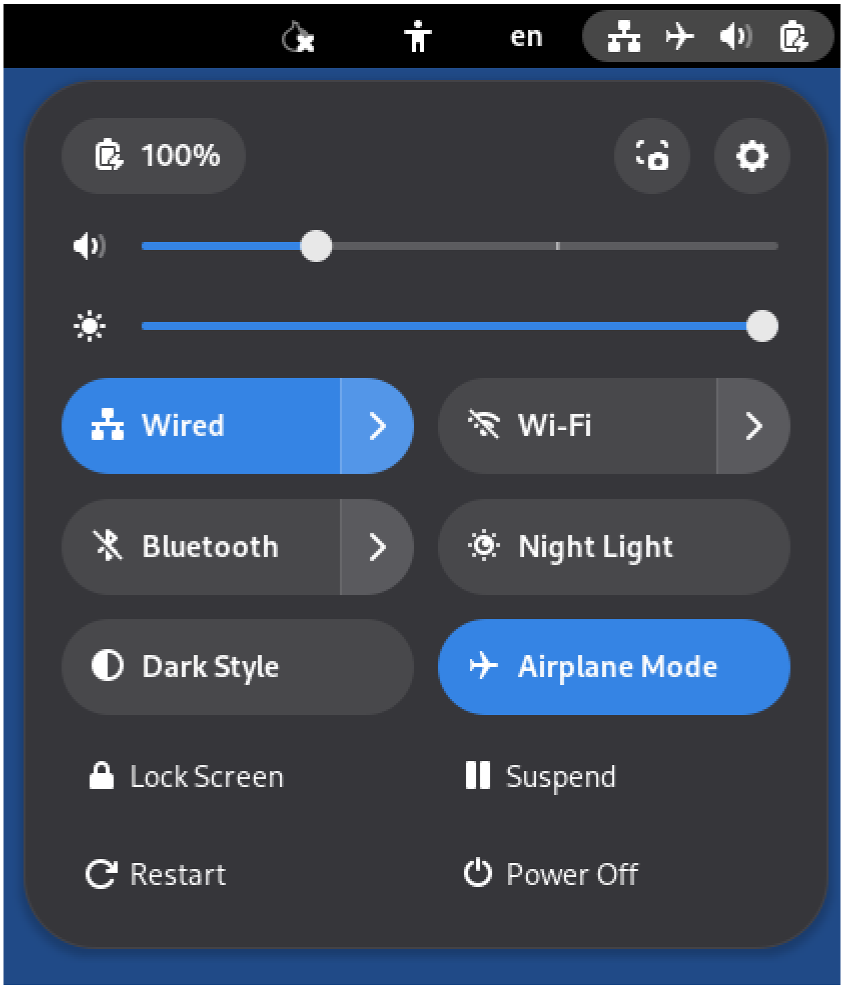
1.36.2 Initial Configuration

Unpack the firewall, connect the power, and power on the device.

We will use the OPNSense Web GUI to do the initial configuration of the network firewall.

Connect to the OPNSense Web GUI

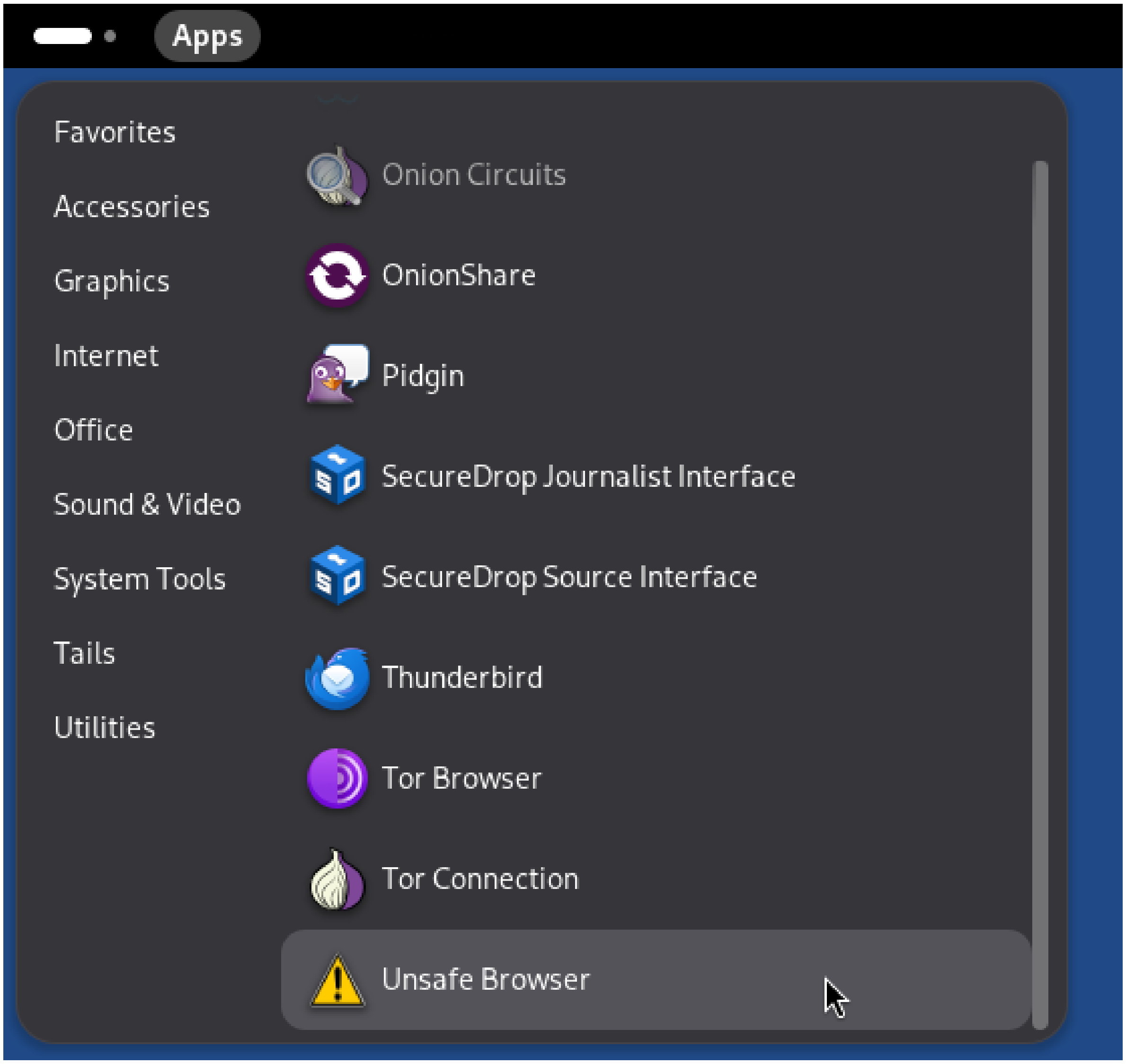
1. If you have not already done so, boot the *Admin Workstation* into Tails using its designated USB drive.
2. Connect the *Admin Workstation* to the LAN interface. You should see a popup notification in Tails that says "Connection Established". If you click on the network icon in the upper right of the Tails Desktop, you should see that the "Wired Connection" is active:



Warning

Make sure your *only* active connection is the one you just established with the network firewall. If you are connected to another network at the same time (e.g. a wireless network), you may encounter problems trying to connect the firewall's Web GUI.

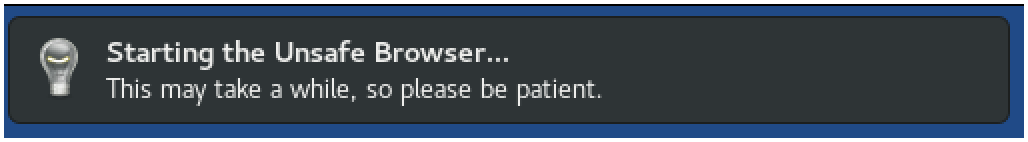
3. Launch the **Unsafe Browser** from the menu bar: **Apps** ▶ **Internet** ▶ **Unsafe Browser**.



Note

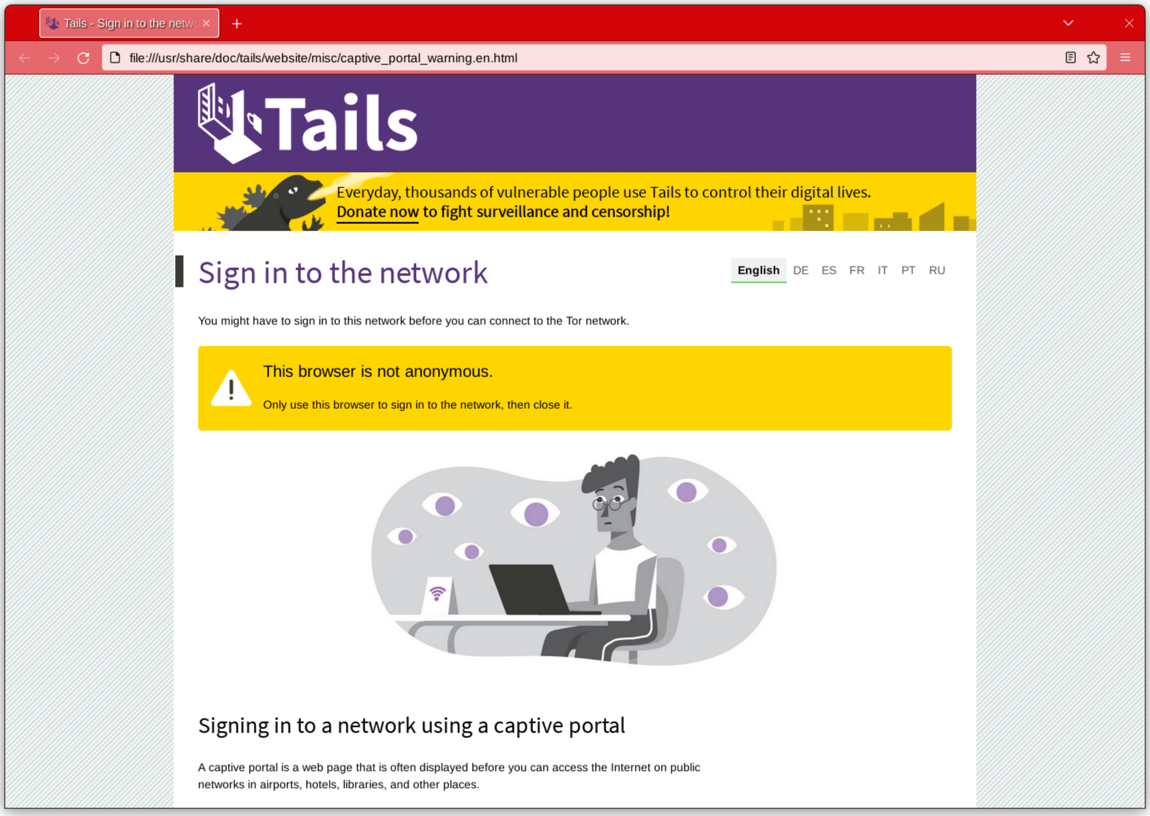
The *Unsafe Browser* is, as the name suggests, **unsafe** (its traffic is not routed through Tor). However, it is the only option because Tails intentionally disables LAN access in the **Tor Browser**.

4. You will see a pop-up notification that says "Starting the Unsafe Browser…"



Starting the Unsafe Browser...
This may take a while, so please be patient.

5. After a few seconds, the Unsafe Browser should launch. The window has a bright red border to remind you to be careful when using it. You should close it once you're done configuring the firewall and use Tor Browser for any other web browsing you might do on the *Admin Workstation*.



Tails - Sign in to the netw
file:///usr/share/doc/tails/website/misc/captive_portal_warning.en.html
Tails
English
DE
ES
FR
IT
PT
RU

Everyday, thousands of vulnerable people use Tails to control their digital lives.
Donate now to fight surveillance and censorship!

Sign in to the network

You might have to sign in to this network before you can connect to the Tor network.

This browser is not anonymous.

Only use this browser to sign in to the network, then close it.

Signing in to a network using a captive portal

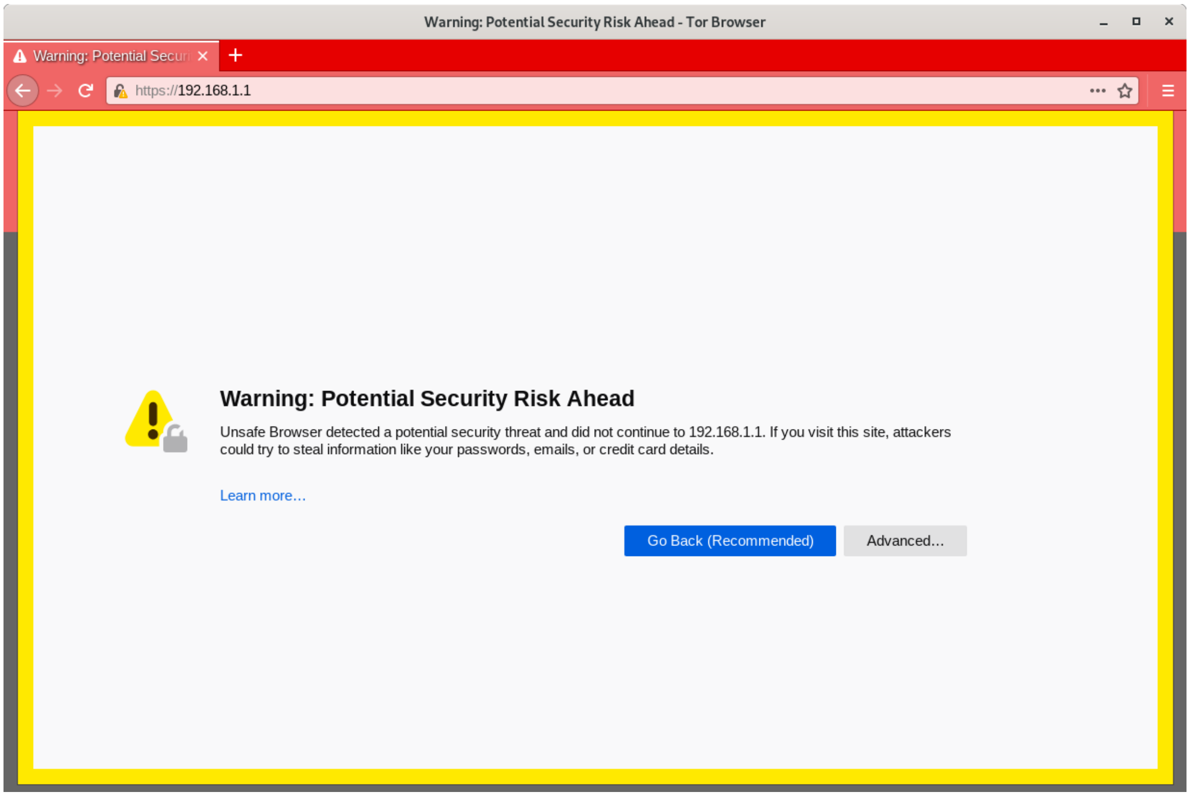
A captive portal is a web page that is often displayed before you can access the Internet on public networks in airports, hotels, libraries, and other places.

6. Navigate to the OPNSense Web GUI in the *Unsafe Browser*: `https://192.168.1.1`

Note

If you have trouble connecting, go to your network settings and make sure that you have an IPv4 address in the `192.168.1.1/24` range. You may need to turn on DHCP, else you can manually configure a static IPv4 address of `192.168.1.x` with a subnet mask of `255.255.255.0`. However, make sure not to configure your Tails device to have the same IP as the firewall (`192.168.1.1`).

7. The firewall uses a self-signed certificate, so you will see a "This Connection Is Untrusted" warning when you connect. This is expected. You can safely continue by clicking **Advanced** and **Accept the Risk and Continue**.



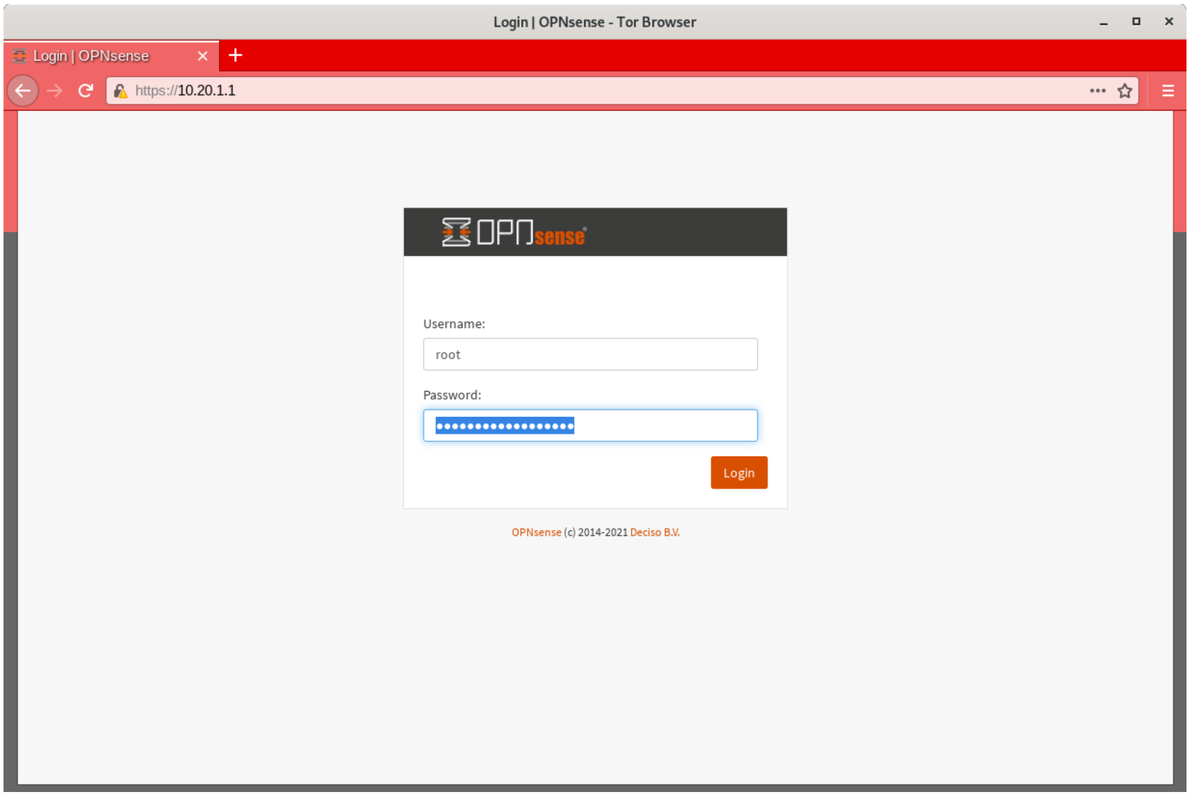
Warning: Potential Security Risk Ahead - Tor Browser

https://192.168.1.1

Warning: Potential Security Risk Ahead

Unsafe Browser detected a potential security threat and did not continue to 192.168.1.1. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

8. You should see the login page for the OPNSense GUI. Log in with the default username and passphrase (`root` / `opnsense`).



Login | OPNsense - Tor Browser

https://10.20.1.1

Username: root

Password: ••••••••••••••••••

OPNsense (c) 2014-2021 Deciso B.V.

If this is your first time logging in to the firewall, the setup wizard will be displayed. You should not step through it at this point, however, as there are other tasks to complete. To exit, click the OPNSense logo in the top left corner of the screen.

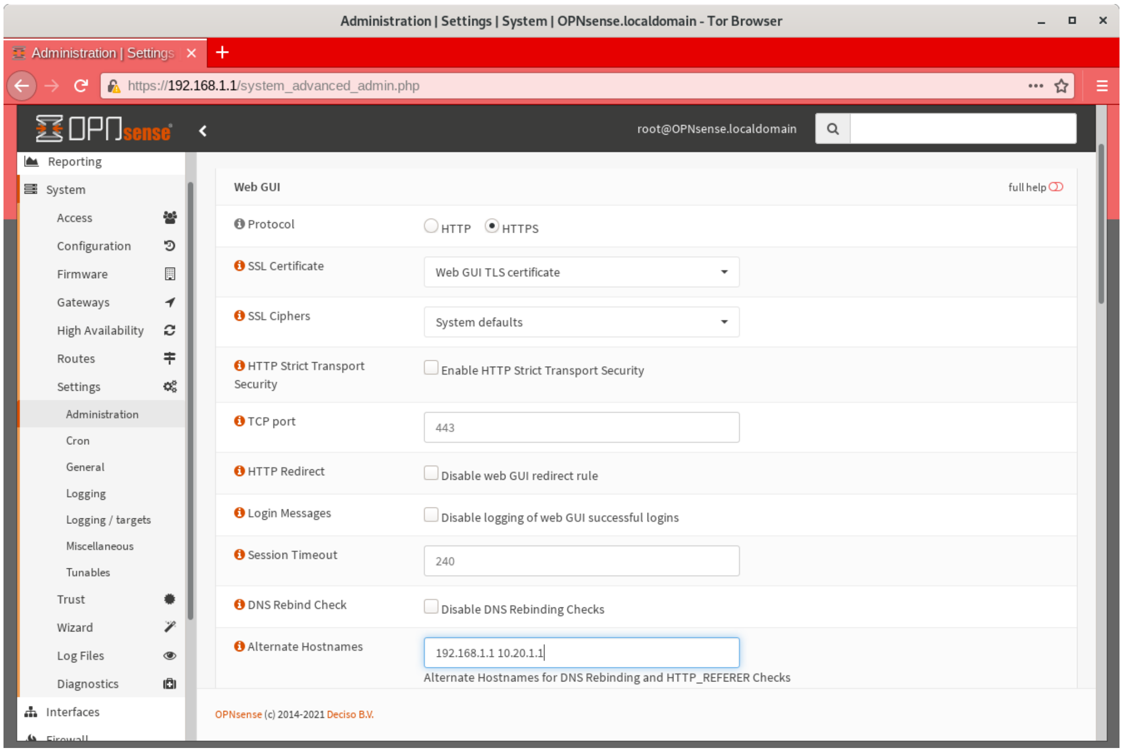
Set a Strong Password

Navigate to **System** ▶ **Access** ▶ **Users** and click the edit button for the `root` user. On the subsequent page, set a strong admin password. We recommend generating a strong passphrase with KeePassXC and saving it in the Tails Persistent folder using the provided KeePassXC database template. Two-factor authentication will be enabled in a later step.

Set Alternate Hostnames

Before you can set up the hardware firewall, you will need to set the **Alternate Hostnames** setting.

First, navigate to **System** ▶ **Settings** ▶ **Administration**. In the **Web GUI** section, update the **Alternate Hostnames** field with the values `192.168.1.1` and the IP address of the *Admin Gateway* (`10.20.1.1` if you are using the recommended default values), separated by a space.



Web GUI

Protocol: ○ HTTP ● HTTPS

SSL Certificate: Web GUI TLS certificate

SSL Ciphers: System defaults

HTTP Strict Transport Security: □ Enable HTTP Strict Transport Security

TCP port: 443

HTTP Redirect: □ Disable web GUI redirect rule

Login Messages: □ Disable logging of web GUI successful logins

Session Timeout: 240

DNS Rebind Check: □ Disable DNS Rebinding Checks

Alternate Hostnames: 192.168.1.1 10.20.1.1

Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks

Finally, scroll to the bottom of the page and click **Save**.

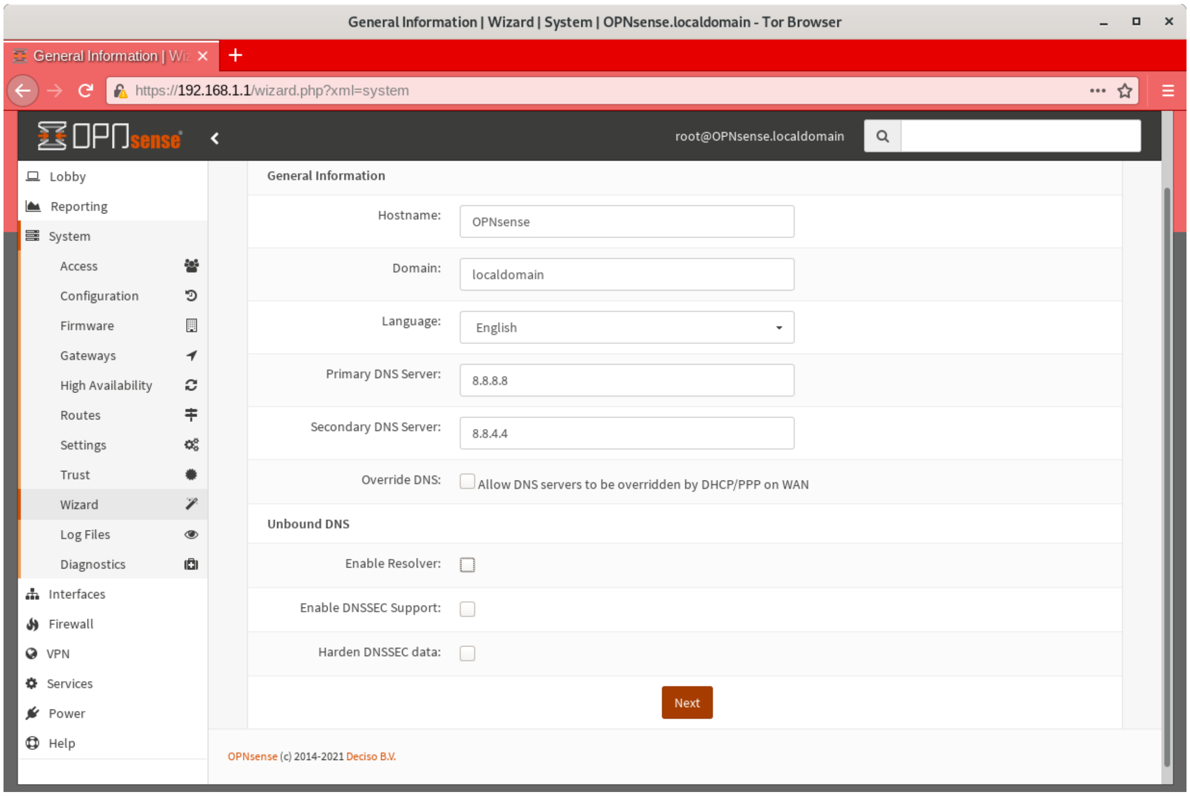
Configure Interfaces Via The Setup Wizard

To start the OPNSense Setup Wizard, navigate to **System** ▶ **Wizard** and click **Next**.

1. **General Information**: Leave your hostname as the default, `OPNsense`. There is no relevant domain for SecureDrop, so we recommend setting this to `securedrop.local` or something similar. Use your preferred DNS servers. If you don't know what DNS servers to use, we recommend using Google's DNS servers: `8.8.8.8` and `8.8.4.4`. Uncheck the **Override DNS** checkbox.

   In the **Unbound DNS** section, uncheck **Enable Resolver**.

   Click **Next**.


General Information | Wizard | System | OPNsense.localdomain - Tor Browser
General Information | Wiz
https://192.168.1.1/wizard.php?xml=system
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Access
Configuration
Firmware
Gateways
High Availability
Routes
Settings
Trust
Wizard
Log Files
Diagnostics
Interfaces
Firewall
VPN
Services
Power
Help
Next
OPNsense (c) 2014-2021 Deciso B.V.

General Information

Hostname: OPNsense

Domain: localdomain

Language: English

Primary DNS Server: 8.8.8.8

Secondary DNS Server: 8.8.4.4

Override DNS: □ Allow DNS servers to be overridden by DHCP/PPP on WAN

Unbound DNS

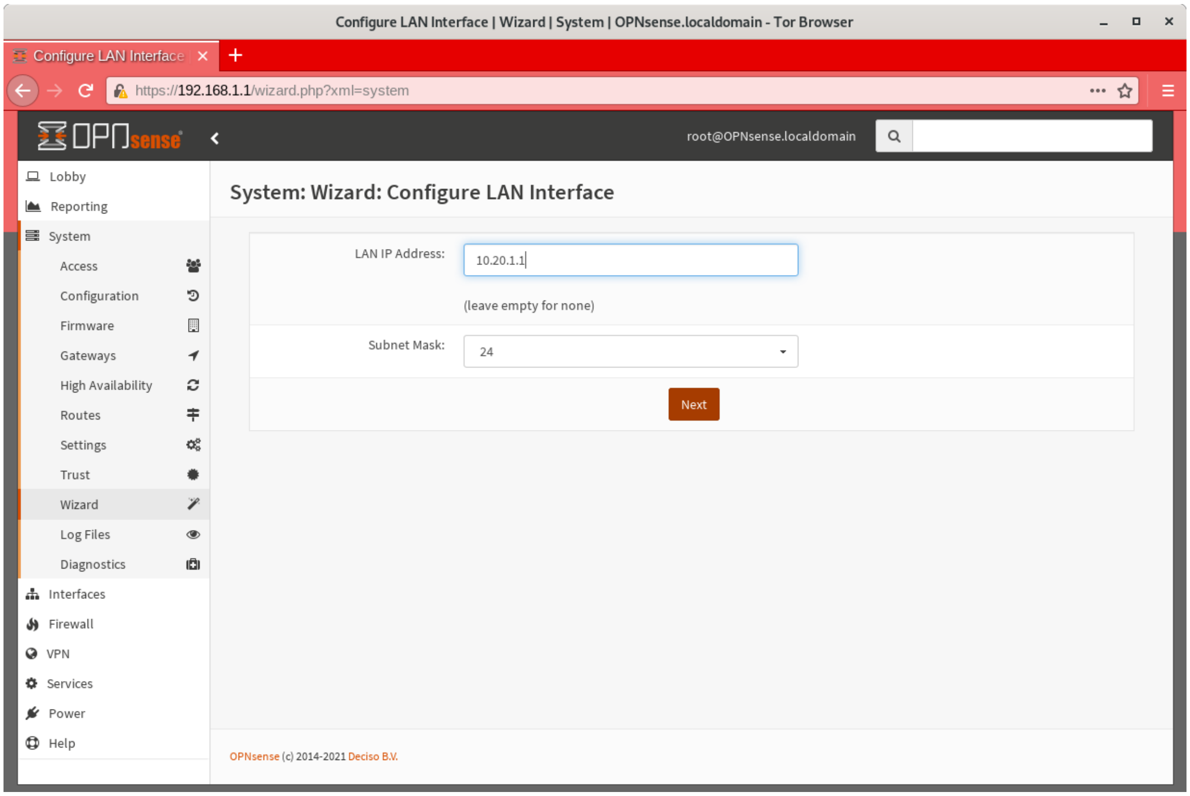
Enable Resolver: □

Enable DNSSEC Support: □

Harden DNSSEC data: □

2. **Time Server Information**: Leave the default settings unchanged and click **Next**.
3. **Configure WAN Interface**: Enter the appropriate configuration for your network. Consult your local sysadmin if you are unsure what to enter here. For many environments, the default of DHCP will work and the rest of the fields can be left at their default values.

   Click **Next** to proceed.
4. **Configure LAN Interface**: Use the IP address of the *Admin Gateway* (`10.20.1.1`) and the subnet mask (`/24`) of the *Admin Subnet*. Click **Next**.



Configure LAN Interface | Wizard | System | OPNsense.localdomain - Tor Browser

https://192.168.1.1/wizard.php?xml=system

System: Wizard: Configure LAN Interface

LAN IP Address: 10.20.1.1

(leave empty for none)

Subnet Mask: 24

Next

OPNsense (c) 2014-2021 Deciso B.V.

5. **Set Root Password**: If the password was already reset during the 2FA setup, you don’t need to set it again. If it was not, then set a strong password now and store it in the *Admin Workstation*’s KeePassXC database. Click **Next** to continue.

6. **Reload Configuration**: Click **Reload** to apply the changes you made in the Setup Wizard.

At this point, since the LAN subnet settings were changed from their defaults, you will no longer be able to connect after reloading the firewall and the reload will time out. This is not an error - the firewall has reloaded and is working correctly.

To connect to the new LAN interface, unplug and reconnect your network cable to get a new network address assigned via DHCP. Note that if you used a subnet with fewer addresses than `/24`, the default DHCP configuration in OPNSense may not work. In this case, you should assign the Admin Workstation a static IP address that is known to be in the subnet to continue.

The Web GUI will now be available on the *Admin Gateway* IP address. Navigate to `https://<Admin Gateway IP>` in the *Unsafe Browser* and log in to the `root` account using an OTP token and the passphrase you just set.

Once you’ve logged in to the Web GUI, you are ready to continue configuring the firewall.

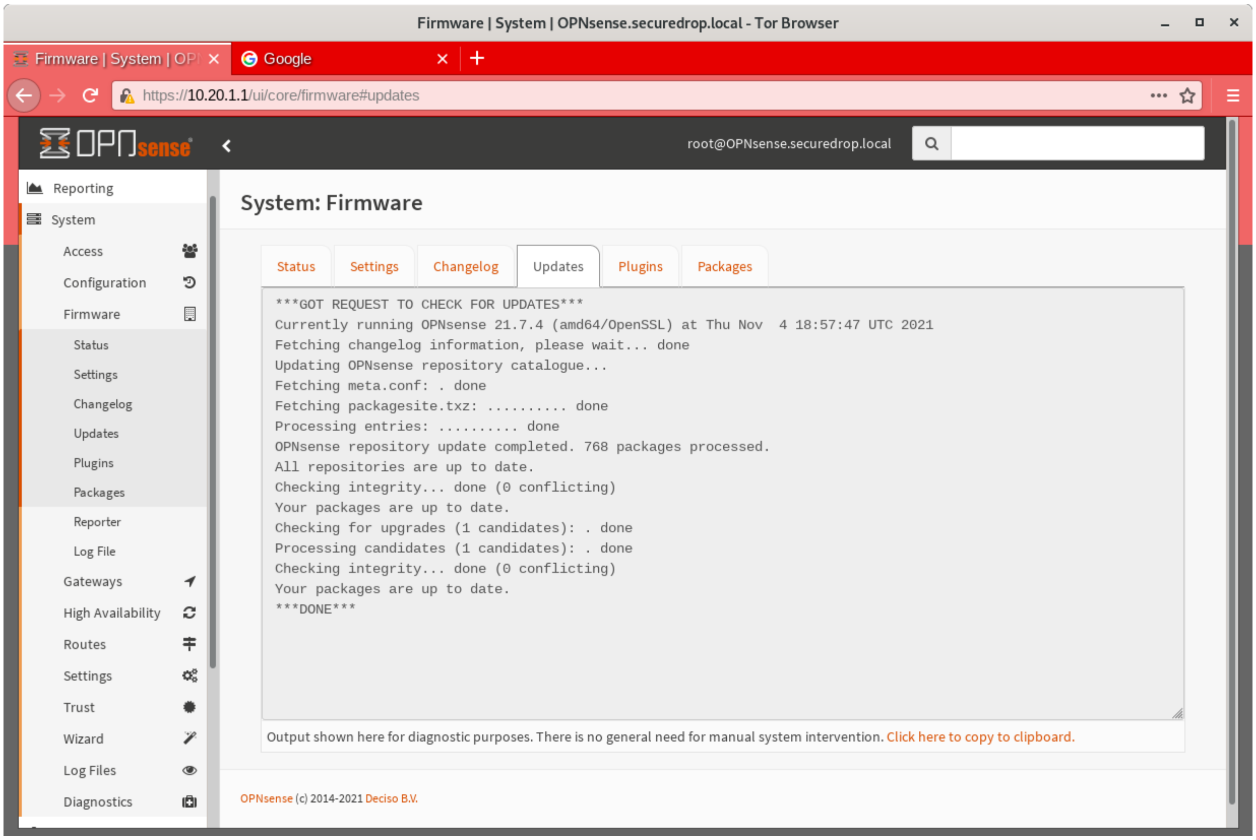
Connect Interfaces and Test

Now that the initial configuration is completed, you can connect the WAN port without potentially conflicting with the default LAN settings (as explained earlier). Connect the WAN port to the external network. You can watch the WAN entry in the Interfaces table on the OPNSense Dashboard homepage to see as it changes from down (red arrow pointing down) to up (green arrow pointing up). This usually takes several seconds. The WAN’s IP address will be shown once it comes up.

Finally, test connectivity to make sure you are able to connect to the Internet through the WAN. The easiest way to do this is to open another tab in the Unsafe Browser and visit a host that you expect to be up (e.g. `google.com`).

Update OPNSense to the latest version

You should update OPNSense to the latest version available before proceeding with the rest of the configuration. Navigate to **Lobby ▶ Dashboard** and click **Click to check for updates** to start the process, and follow any on-screen instructions to complete the update. Note that a reboot may be required, and you may also need to apply several updates in a row to get to the latest version.



```
***GOT REQUEST TO CHECK FOR UPDATES***
Currently running OPNsense 21.7.4 (amd64/OpenSSL) at Thu Nov  4 18:57:47 UTC 2021
Fetching changelog information, please wait... done
Updating OPNsense repository catalogue...
Fetching meta.conf: . done
Fetching packagesite.txz: .......... done
Processing entries: .......... done
OPNsense repository update completed. 768 packages processed.
All repositories are up to date.
Checking integrity... done (0 conflicting)
Your packages are up to date.
Checking for upgrades (1 candidates): . done
Processing candidates (1 candidates): . done
Checking integrity... done (0 conflicting)
Your packages are up to date.
***DONE***
```

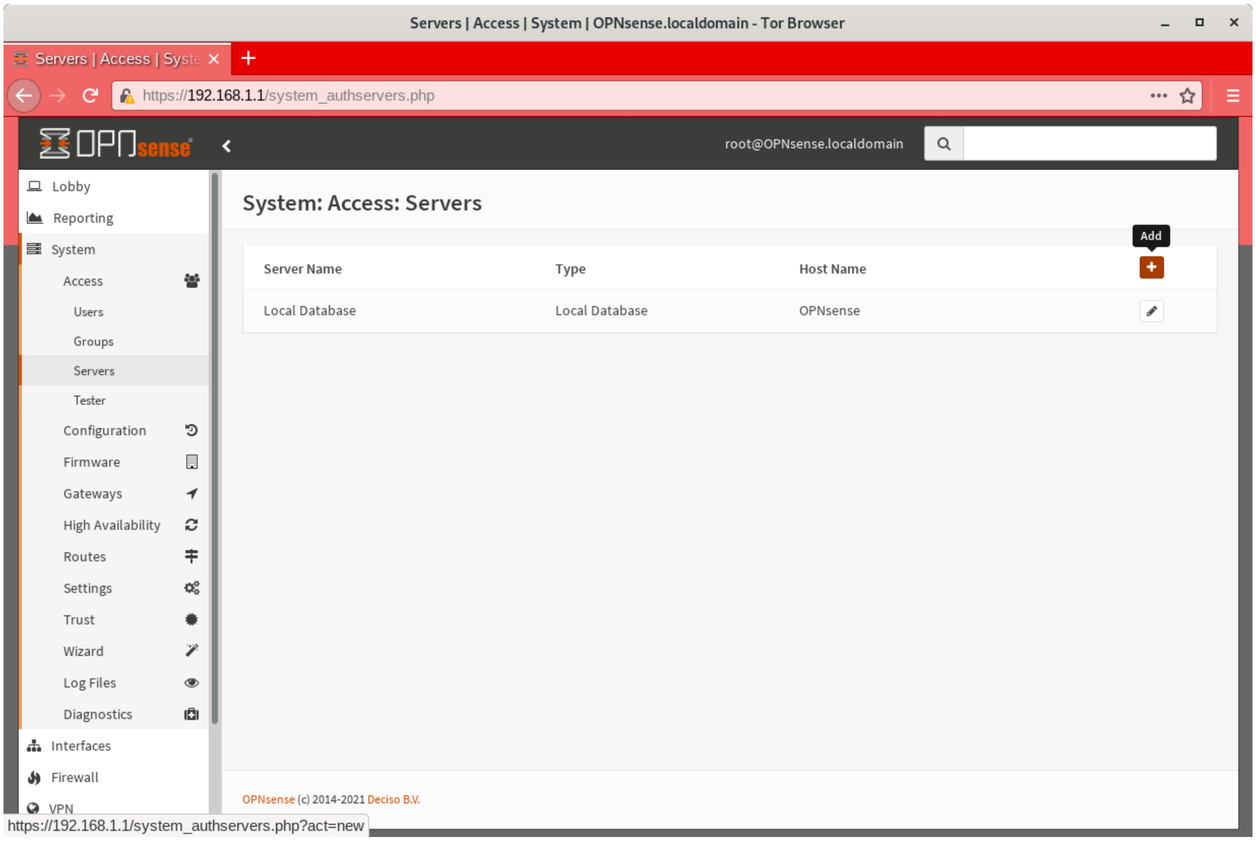
Output shown here for diagnostic purposes. There is no general need for manual system intervention. Click here to copy to clipboard.

OPNsense (c) 2014-2021 Deciso B.V.

Enable Two-Factor Authentication

OPNSense supports two-factor authentication (2FA) via mobile apps such as Google Authenticator or FreeOTP. To set it up, first make sure you have a mobile device available with your choice of 2FA app.

Next, in the OPNSense Web GUI, navigate to **System ▶ Access ▶ Servers** and click **+** to add a new server.


Servers | Access | System | OPNsense.localdomain - Tor Browser
Servers | Access | Syste
https://192.168.1.1/system_authservers.php
root@OPNsense.localdomain
Lobby
Reporting
System
Access
Users
Groups
Servers
Tester
Configuration
Firmware
Gateways
High Availability
Routes
Settings
Trust
Wizard
Log Files
Diagnostics
Interfaces
Firewall
VPN
Add
OPNsense (c) 2014-2021 Deciso B.V.
https://192.168.1.1/system_authservers.php?act=new

System: Access: Servers

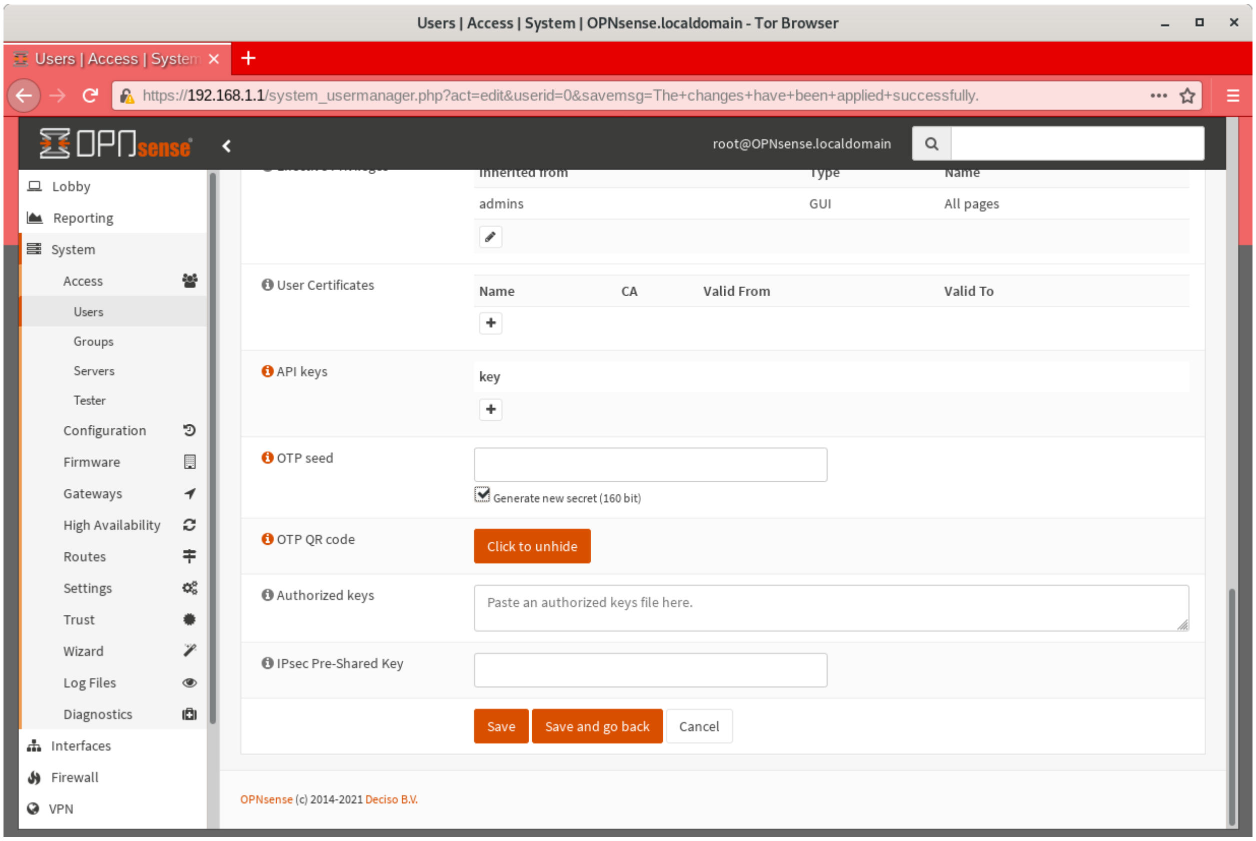
Server Name	Type	Host Name
Local Database	Local Database	OPNsense

Note

The time on your firewall must be set correctly for 2FA to work properly. This should happen automatically once the WAN connection is established.

On the next page, enter `TOTP Local` in the **Descriptive name** field and choose `Local + Timebased One Time Password` from the **Type** dropdown. Leave the other fields at their default values and click **Save**

Next, navigate to **System** ▶ **Access** ▶ **Users** and click the edit button for the `root` user. Scroll down the page to the **OTP seed** section and check the **Generate new secret (160bit)** checkbox. Finally, click **Save**.



Users | Access | System | OPNsense.localdomain - Tor Browser

https://192.168.1.1/system_usermanager.php?act=edit&userid=0&savemsg=The+changes+have+been+applied+successfully.

root@OPNsense.localdomain

Inherited from	Type	Name
admins	GUI	All pages

User Certificates

Name	CA	Valid From	Valid To

API keys

key

OTP seed

☑ Generate new secret (160 bit)

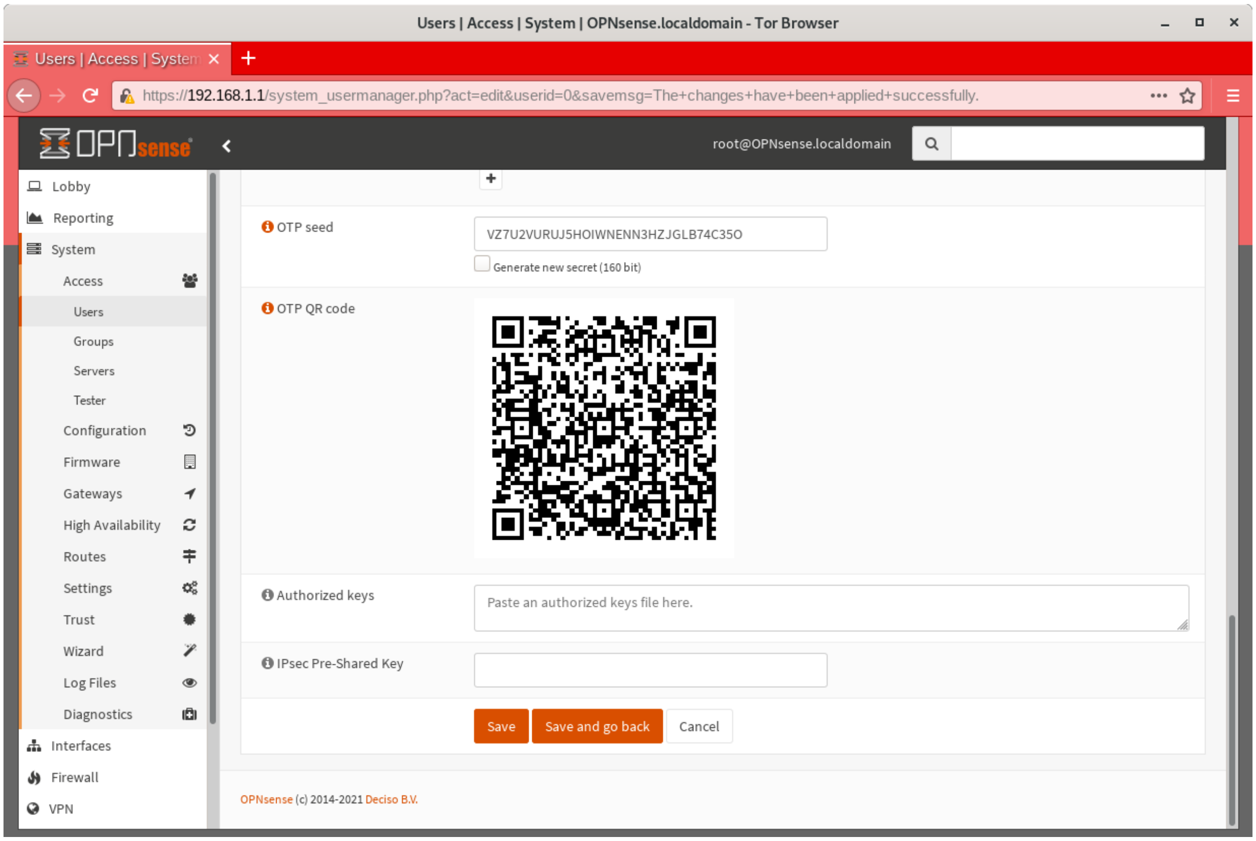
OTP QR code: Click to unhide

Authorized keys: Paste an authorized keys file here.

IPsec Pre-Shared Key

OPNsense (c) 2014-2021 Deciso B.V.

Once the page has reloaded, scroll down to the **OTP QR code** section and click **Click to unhide**, then scan the generated QR code with your mobile auth application of choice.



Users | Access | System | OPNsense.localdomain - Tor Browser
Users | Access | System
https://192.168.1.1/system_usermanager.php?act=edit&userid=0&savemsg=The+changes+have+been+applied+successfully.
OPNsense
root@OPNsense.localdomain
Lobby
Reporting
System
Access
Users
Groups
Servers
Tester
Configuration
Firmware
Gateways
High Availability
Routes
Settings
Trust
Wizard
Log Files
Diagnostics
Interfaces
Firewall
VPN
Save
Save and go back
Cancel
OPNsense (c) 2014-2021 Deciso B.V.

OTP seed: VZ7U2VURUJ5HOIWNENN3HZJGLB74C35O

□ Generate new secret (160 bit)

OTP QR code

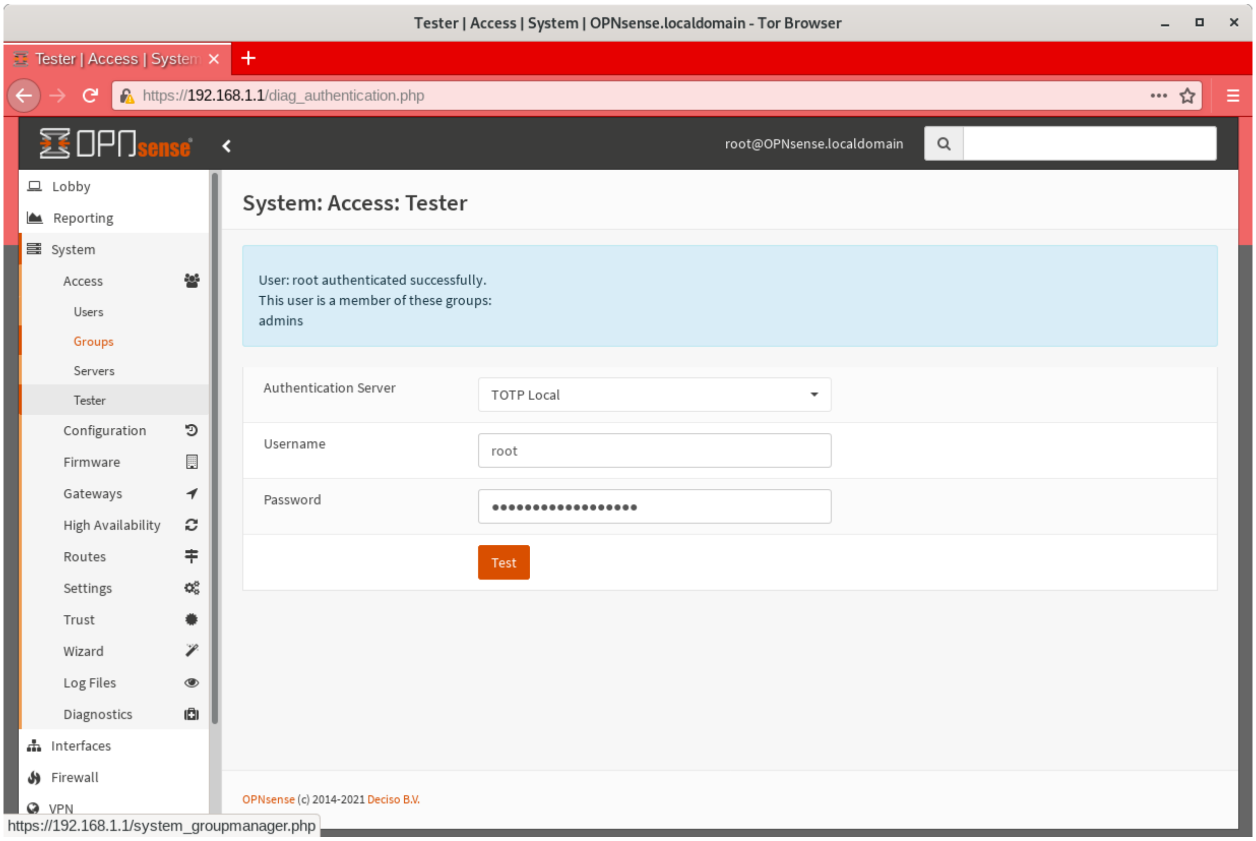
Authorized keys: Paste an authorized keys file here.

IPsec Pre-Shared Key

If you wish, you may also save the OTP seed value displayed above the QR code in your Tails KeePassXC database - this isn't required, but will allow you to set up TOTP on another mobile device if you need to in the future.

Test your new login credentials

To verify that your new password and OTP secret are working, navigate to **System** ▶ **Access** ▶ **Tester**. Select `TOTP Local` from the **Authentication Server** dropdown, enter the `root` username in the **Username** field, and enter your OTP token and password concatenated like `123456PASSWORD` in the **Password** field. Then click **Test**.



Tester | Access | System | OPNsense.localdomain - Tor Browser

https://192.168.1.1/diag_authentication.php

System: Access: Tester

User: root authenticated successfully.
This user is a member of these groups:
admins

Authentication Server	TOTP Local
Username	root
Password	••••••••••••••••••

If the test fails, make sure you have used the correct OTP code and password, and edit the `root` user record as necessary.

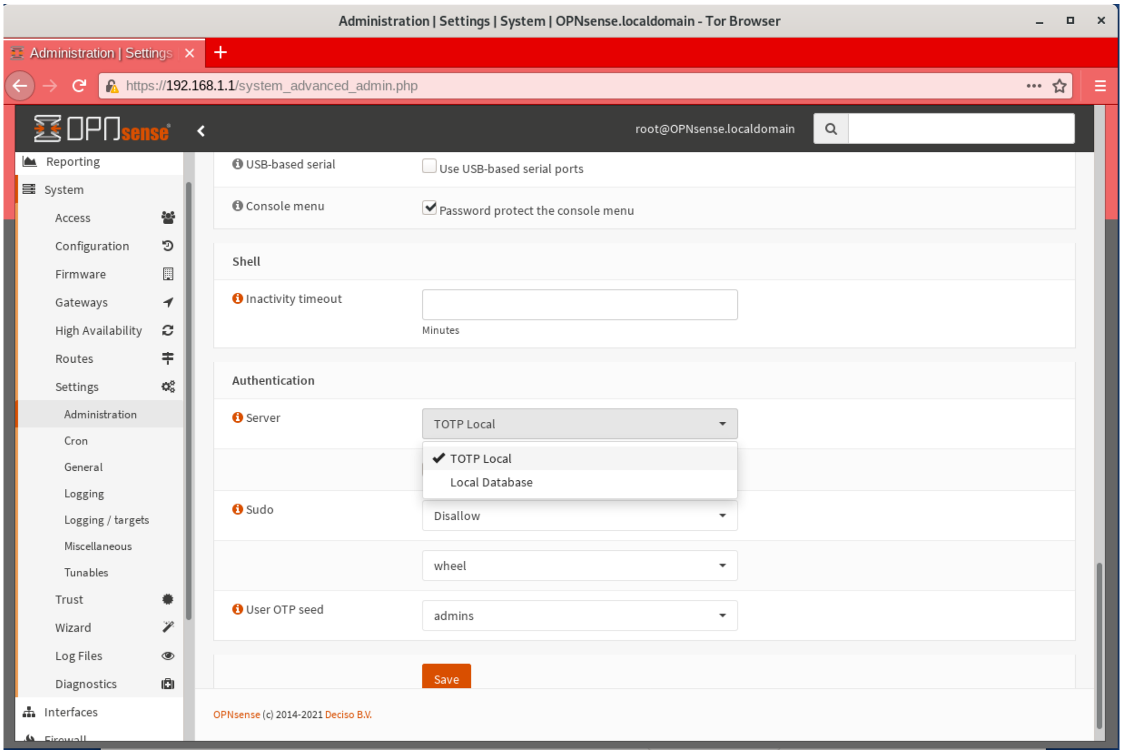
Note

You must enter the OTP token and passphrase concatenated as a single string like `123456PASSWORD` in the **Password** field.

Warning

Do not skip this test, or proceed further until it passes, as you will be locked out of the firewall Web GUI and console if the account is not set up correctly!

Finally, navigate to **System** ▶ **Settings** ▶ **Administration** and scroll down to the **Authentication** section at the bottom of the page. In the **Server** dropdown, select `TOTP Local` and deselect `Local Database.`. Click **Save**.



USB-based serial ☐ Use USB-based serial ports

Console menu ☑ Password protect the console menu

Shell

Inactivity timeout

Minutes

Authentication

Server: TOTP Local

✓ TOTP Local

Local Database

Sudo: Disallow

wheel

User OTP seed: admins

Save

OPNsense (c) 2014-2021 Deciso B.V.

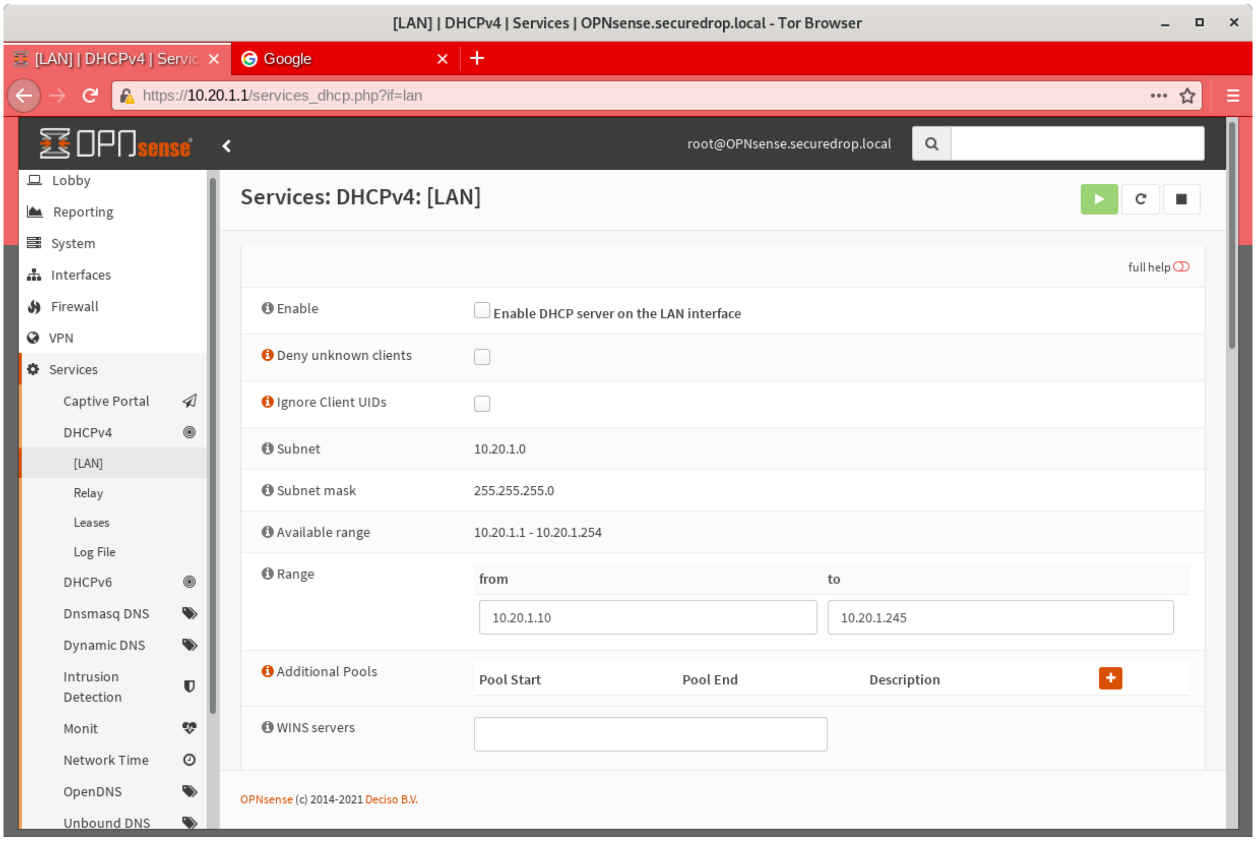
1.36.3 Disable DHCP on the Firewall

OPNSense runs a DHCP server on the LAN interface by default. At this stage in the documentation, the *Admin Workstation* likely has an IP address assigned via that DHCP server.

In order to tighten the firewall rules as much as possible, we recommend disabling the DHCP server and assigning a static IP address to the Admin Workstation instead.

Disable DHCP Server on the LAN Interface

To disable DHCP, navigate to **Services** ▶ **DHCPv4** ▶ **[LAN]** in the Web GUI. Uncheck the **Enable DHCP server on the LAN interface** checkbox, scroll down, and click **Save**.



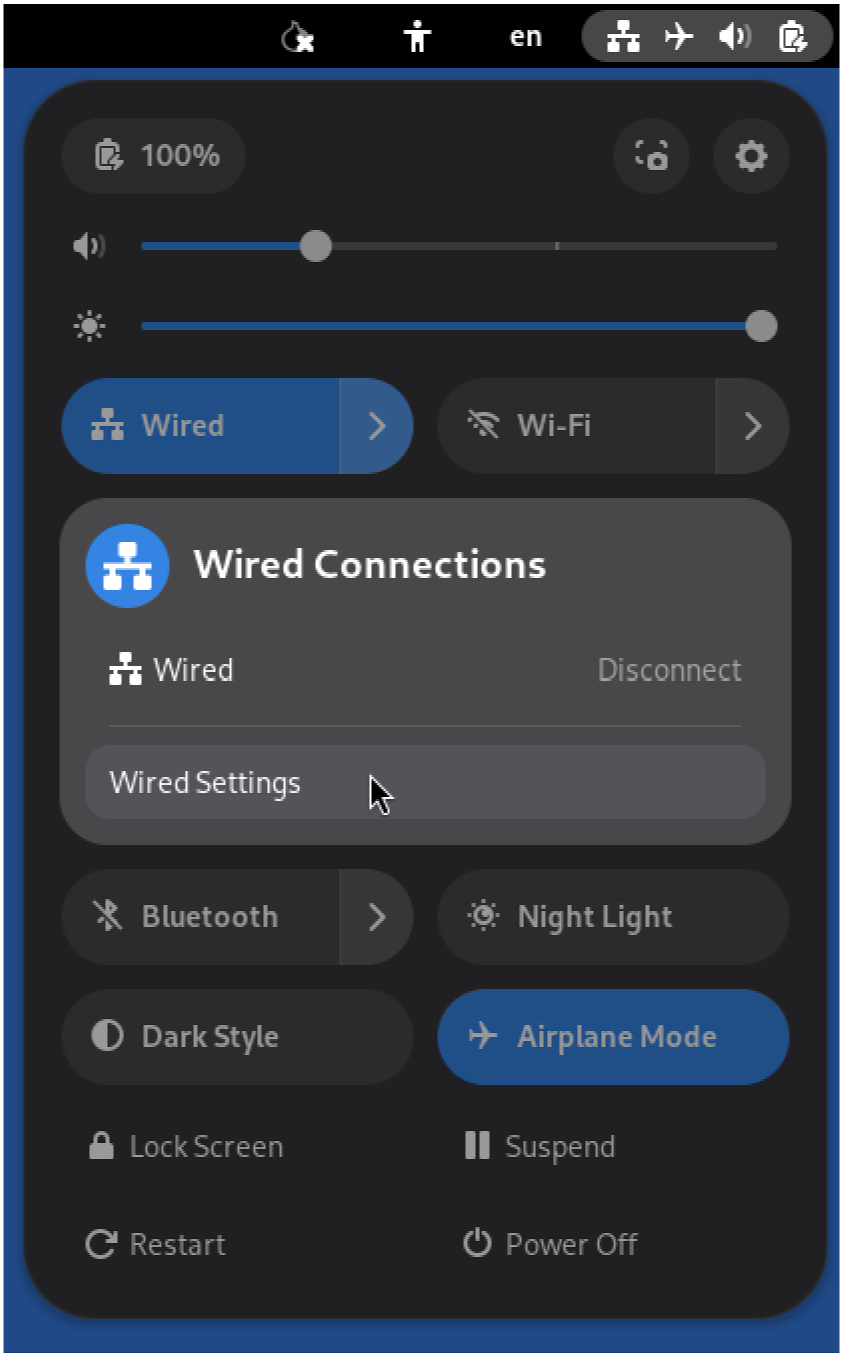
Services: DHCPv4: [LAN]

Enable	☐ Enable DHCP server on the LAN interface
Deny unknown clients	☐
Ignore Client UIDs	☐
Subnet	10.20.1.0
Subnet mask	255.255.255.0
Available range	10.20.1.1 - 10.20.1.254
Range	from: 10.20.1.10 to: 10.20.1.245
Additional Pools	Pool Start / Pool End / Description
WINS servers	

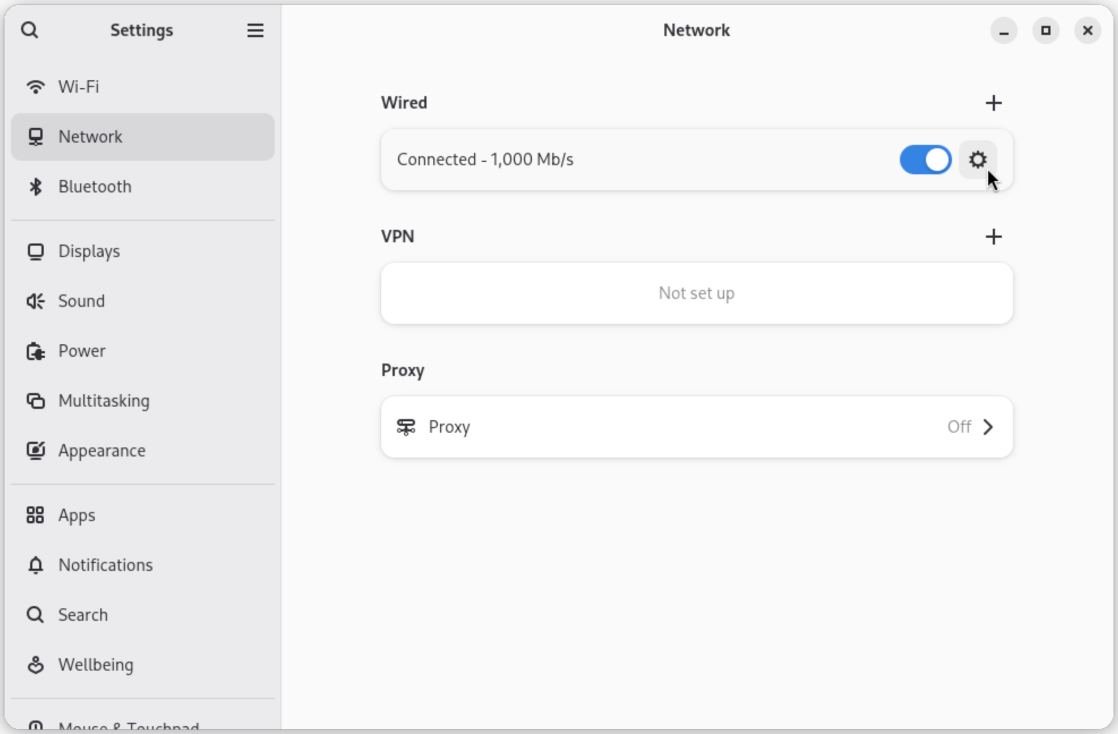
Assign a Static IP Address to the *Admin Workstation*

Now you will need to assign a static IP to the *Admin Workstation*.

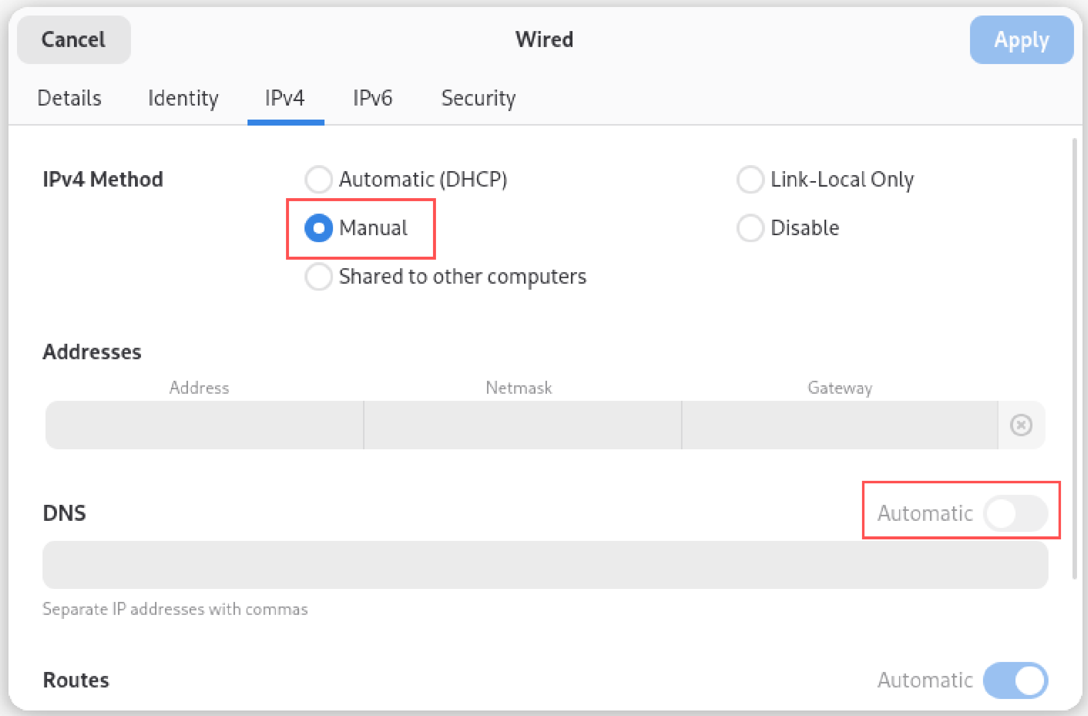
You can easily check your current IP address by *clicking* the top right of the menu bar, clicking on the **Wired Connection** and then clicking **Wired Settings**.



From here you can click on the cog beside the wired network connection:



This will take you to the network settings. Change to the **IPv4** tab. Ensure that **IPv4 Method** is set to **Manual**, and that the **Automatic** switch for **DNS** is in the "off" position, as highlighted in the screenshot below:



IPv4 Method: ○ Automatic (DHCP) ○ Link-Local Only ● Manual ○ Disable ○ Shared to other computers

Addresses

Address	Netmask	Gateway

DNS: Automatic (off)

Separate IP addresses with commas

Routes: Automatic (on)

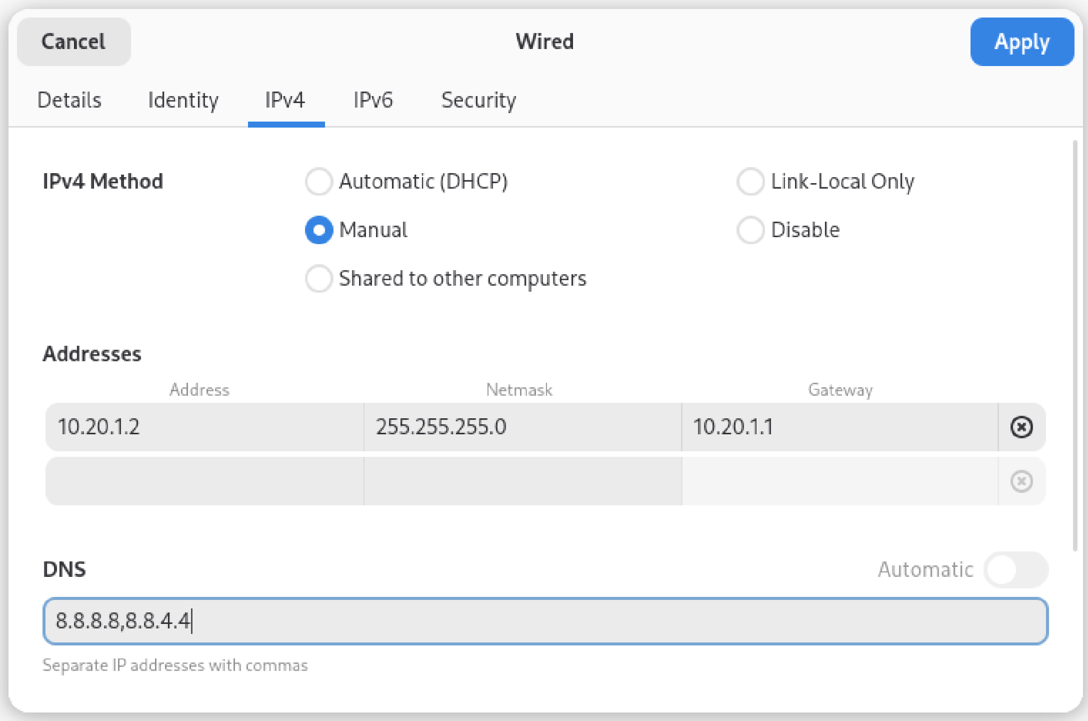
Note

The Unsafe Browser will not launch when using a manual network configuration if it does not have DNS servers configured. This is technically unnecessary for our use case because we are only using it to access IP addresses on the LAN, and do not need to resolve anything with DNS. Nonetheless, you should configure some DNS servers here so you can continue to use the Unsafe Browser to access the WebGUI in future sessions.

We recommend keeping it simple and using the same DNS servers that you used for the network firewall in the setup wizard.

Fill in the static networking information for the *Admin Workstation*:

- Address: `10.20.1.2`
- Netmask: `255.255.255.0`
- Gateway : `10.20.1.1`



IPv4 Method

○ Automatic (DHCP)   ○ Link-Local Only
● Manual   ○ Disable
○ Shared to other computers

Addresses

Address	Netmask	Gateway
10.20.1.2	255.255.255.0	10.20.1.1

DNS   Automatic ○

8.8.8.8,8.8.4.4

Separate IP addresses with commas

Click **Apply**. If the network does not come up within 15 seconds or so, try disconnecting and reconnecting your network cable to trigger the change. You will need you have succeeded in connecting with your new static IP when you are able to connect using the Tor Connection assistant, and you see the message “Connected to Tor successfully”.

Troubleshooting: DNS Servers and the Unsafe Browser

After saving the new network configuration, you may still encounter the “No DNS servers configured” error when trying to launch the Unsafe Browser. If you encounter this issue, you can resolve it by disconnecting from the network and then reconnecting, which causes the network configuration to be reloaded.

To do this, click the network icon in the system toolbar, and click **Disconnect** under the name of the currently active network connection, which is displayed in bold. After it disconnects, click the network icon again and click the name of the connection to reconnect. You should see a popup notification that says “Connection Established”, and the Tor Connection assistant should show the message “Connected to Tor successfully”.

For the next step, SecureDrop Configuration, you will manually configure the firewall for SecureDrop, using screenshots as a reference.

1.36.4 SecureDrop Configuration

SecureDrop uses the firewall to achieve two primary goals:

1. Isolating SecureDrop from the existing network, which may be compromised (especially if it is a venerable network in a large organization like a newsroom).
2. Isolating the *Application Server* and the *Monitor Server* from each other as much as possible, to reduce attack surface.

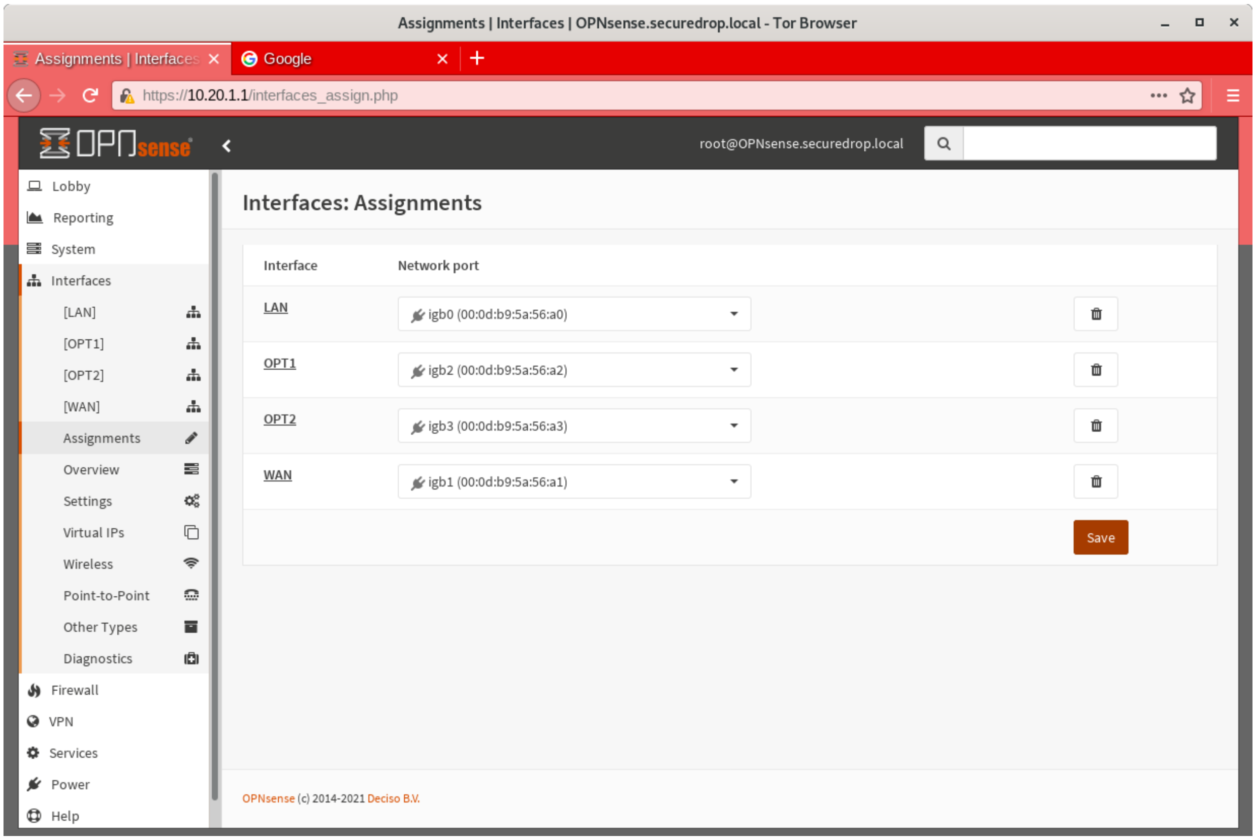
In order to use the firewall to isolate the *Application Server* and the *Monitor Server* from each other, we need to connect them to separate interfaces, and then set up firewall rules that allow them to communicate.

Enable The OPT1 And OPT2 Interfaces

The OPT1 and OPT2 interfaces will be used for the *Application Server* and *Monitor Server* respectively. To enable them, first connect the *Application Server* to the physical OPT1 port and the *Monitor Server* to the OPT2 port.

Next, navigate to **Interfaces ▶ Assignments**. LAN and WAN will already be enabled. Click the **+** button in the **New Interface** section to enable the OPT1 interface on the next available NIC (`igb2` in the screenshot below). Once OPT1 has been added, click **+** again to add OPT2 (on `igb3` in the screenshot below)

Finally, click **Save**.



Interfaces: Assignments

Interface	Network port
LAN	igb0 (00:0d:b9:5a:56:a0)
OPT1	igb2 (00:0d:b9:5a:56:a2)
OPT2	igb3 (00:0d:b9:5a:56:a3)
WAN	igb1 (00:0d:b9:5a:56:a1)

Configure the LAN, WAN, OPT1, and OPT2 interfaces

OPT1 and OPT2 need to be configured to use the subnets defined for the *Application* and *Monitor Servers*, and some additional configuration is required for the LAN and WAN interfaces, that is not covered by the Setup Wizard.

Configure the WAN interface

First, navigate to **Interfaces ▶ [WAN]**. In the **Basic configuration** section, check the checkbox labeled **Prevent interface removal**.

In the **Generic configuration** section, make sure that the **Block private networks** and **Block bogon networks** checkboxes are checked.

Scroll down and click **Save**, then click **Apply changes** when prompted.

Configure the LAN interface

Next, navigate to **Interfaces ▶ [LAN]**. In the **Basic configuration** section, check the checkbox labeled **Prevent interface removal**.

In the **Generic configuration** section, select `Static IPv4` in the **IPv4 Configuration Type** dropdown, and `None` in the **IPV6 Configuration Type** dropdown.

Scroll down and click **Save**, then click **Apply changes** when prompted.

Configure the OPT1 interface

Next, navigate to **Interfaces ▶ [OPT1]**. In the **Basic configuration** section, check the checkboxes labeled **Enable interface** and **Prevent interface removal**.

In the **Generic configuration** section, select `Static IPv4` in the **IPv4 Configuration Type** dropdown, and `None` in the **IPV6 Configuration Type** dropdown.

Scroll down. In the **Static IPv4 Configuration** section, enter the *Application Gateway* IP address and routing prefix (`10.20.2.1` and `24` if you are using the recommended values).

Click **Save**, then click **Apply changes** when prompted.

Configure the OPT2 interface

Finally, navigate to **Interfaces ▶ [OPT2]**. In the **Basic configuration** section, check the checkboxes labeled **Enable interface** and **Prevent interface removal**.

In the **Generic configuration** section, select `Static IPv4` in the **IPv4 Configuration Type** dropdown, and `None` in the **IPV6 Configuration Type** dropdown.

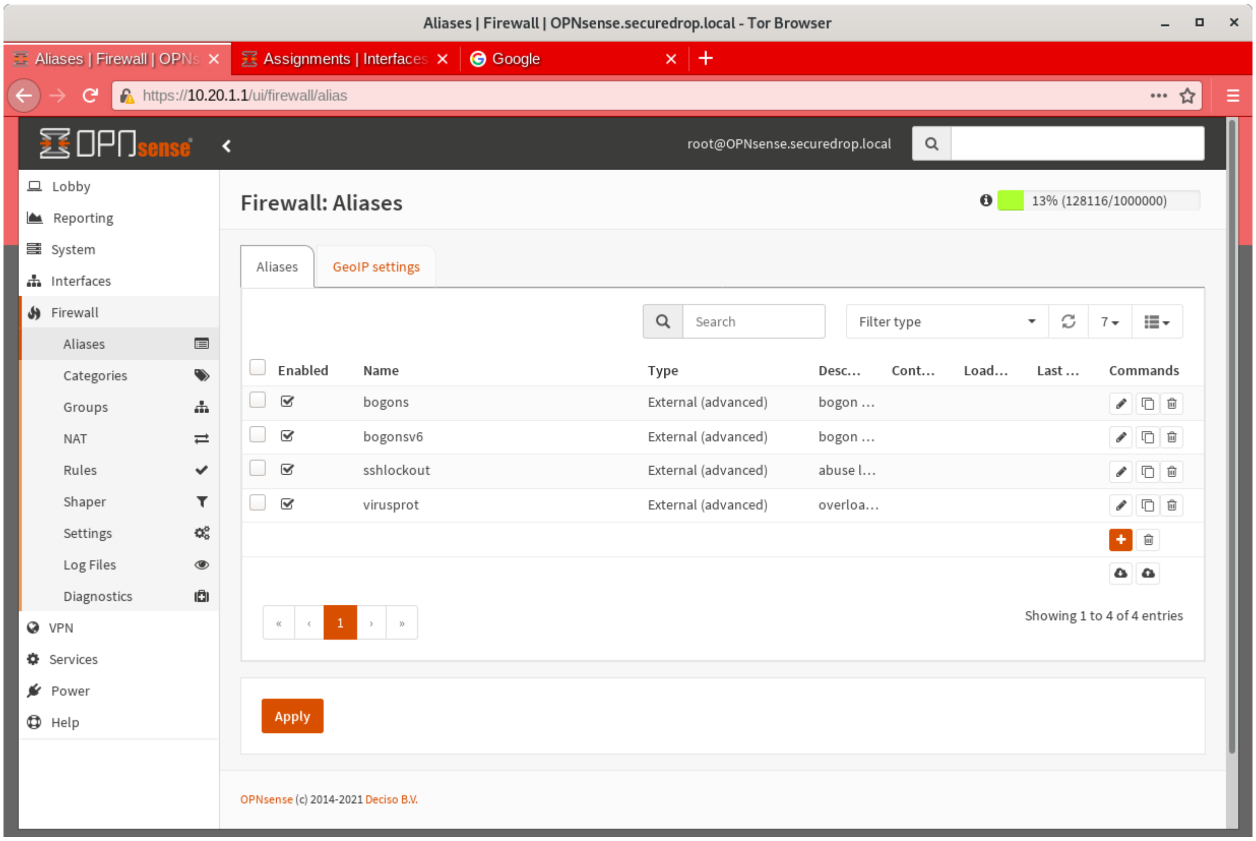
Scroll down. In the **Static IPv4 Configuration** section, enter the *Monitor Gateway* IP address and routing prefix (`10.20.3.1` and `24` if you are using the recommended values).

Click **Save**, then click **Apply changes** when prompted.

Configure Firewall Aliases

In order to simplify firewall rule setup, the next step is to configure aliases for hosts and ports referred to in the rules.

To start, first navigate to **Firewall ▶ Aliases**. You should see some system-defined aliases as shown below:



Firewall: Aliases

13% (128116/1000000)

	Enabled	Name	Type	Desc…	Cont…	Load…	Last …	Commands
□	☑	bogons	External (advanced)	bogon …				
□	☑	bogonsv6	External (advanced)	bogon …				
□	☑	sshlockout	External (advanced)	abuse l…				
□	☑	virusprot	External (advanced)	overloa…				

« ‹ 1 › »

Showing 1 to 4 of 4 entries

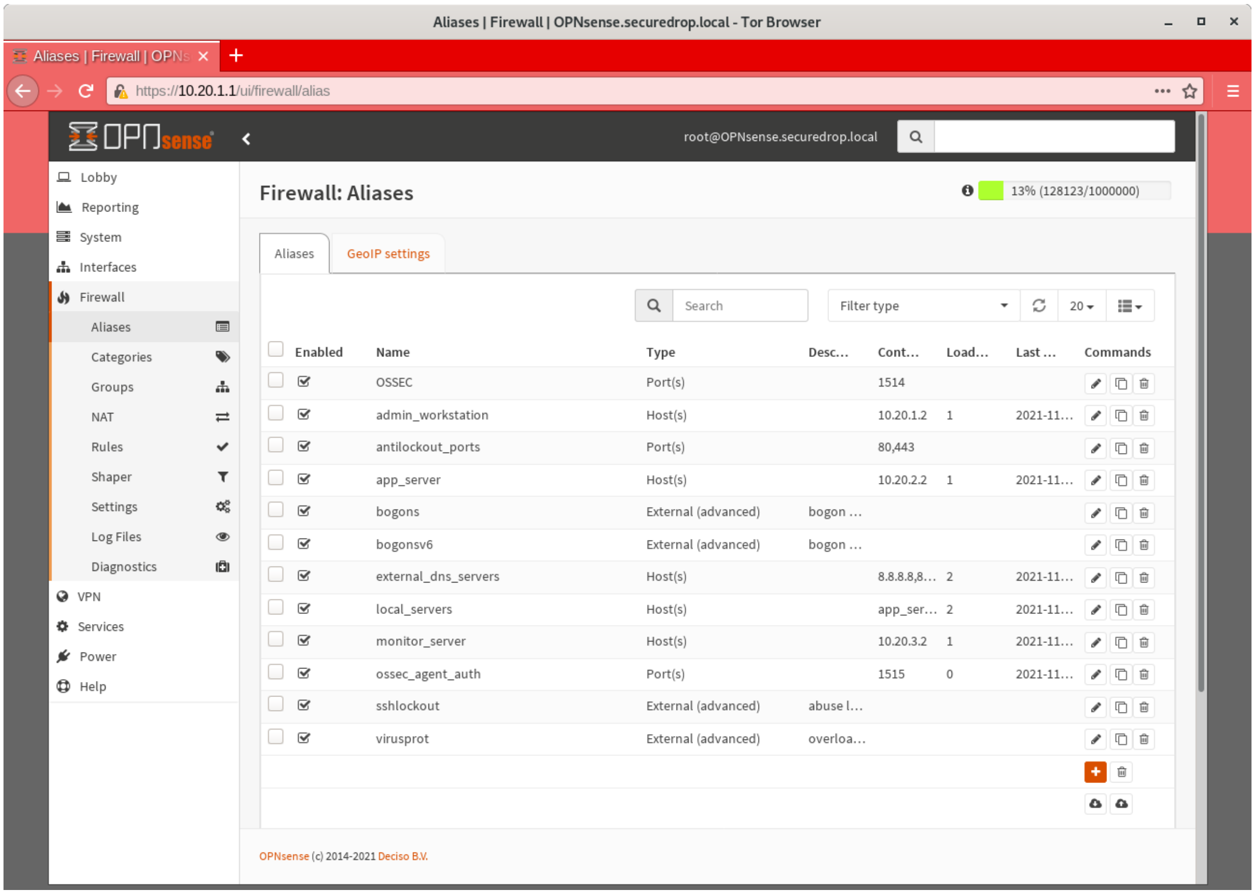
OPNsense (c) 2014-2021 Deciso B.V.

Click the **+** button to add new aliases. You should add the aliases defined in the table below (assuming recommended values for IP addresses):

Table 1: Firewall Aliases

Name	Type	Content
admin_workstation	Host(s)	`10.20.1.2`
app_server	Host(s)	`10.20.2.2`
external_dns_servers	Host(s)	`8.8.8.8`, `8.8.4.4`
monitor_server	Host(s)	`10.20.3.2`
local_servers	Host(s)	`app_server`, `monitor_server`
OSSEC	Port(s)	`1514`
ossec_agent_auth	Port(s)	`1515`
antilockout_ports	Port(s)	`80`, `443`

When complete, the **Aliases** page should look like this:



Aliases | Firewall | OPNsense.securedrop.local - Tor Browser
Aliases | Firewall | OPNs
https://10.20.1.1/ui/firewall/alias
OPNsense
root@OPNsense.securedrop.local
Lobby
Reporting
System
Interfaces
Firewall
Aliases
Categories
Groups
NAT
Rules
Shaper
Settings
Log Files
Diagnostics
VPN
Services
Power
Help
Aliases
GeoIP settings
Search
Filter type
20
OPNsense (c) 2014-2021 Deciso B.V.

Firewall: Aliases

13% (128123/1000000)

Enabled	Name	Type	Desc...	Cont...	Load...	Last ...	Commands
☑	OSSEC	Port(s)		1514			
☑	admin_workstation	Host(s)		10.20.1.2	1	2021-11...	
☑	antilockout_ports	Port(s)		80,443			
☑	app_server	Host(s)		10.20.2.2	1	2021-11...	
☑	bogons	External (advanced)	bogon ...				
☑	bogonsv6	External (advanced)	bogon ...				
☑	external_dns_servers	Host(s)		8.8.8.8,8...	2	2021-11...	
☑	local_servers	Host(s)		app_ser...	2	2021-11...	
☑	monitor_server	Host(s)		10.20.3.2	1	2021-11...	
☑	ossec_agent_auth	Port(s)		1515	0	2021-11...	
☑	sshlockout	External (advanced)	abuse l...				
☑	virusprot	External (advanced)	overloa...				

Scroll down and click **Apply** to save and apply your new aliases.

Configure Firewall Rules

Next, configure firewall rules for each interface.

Configure Firewall Rules on LAN

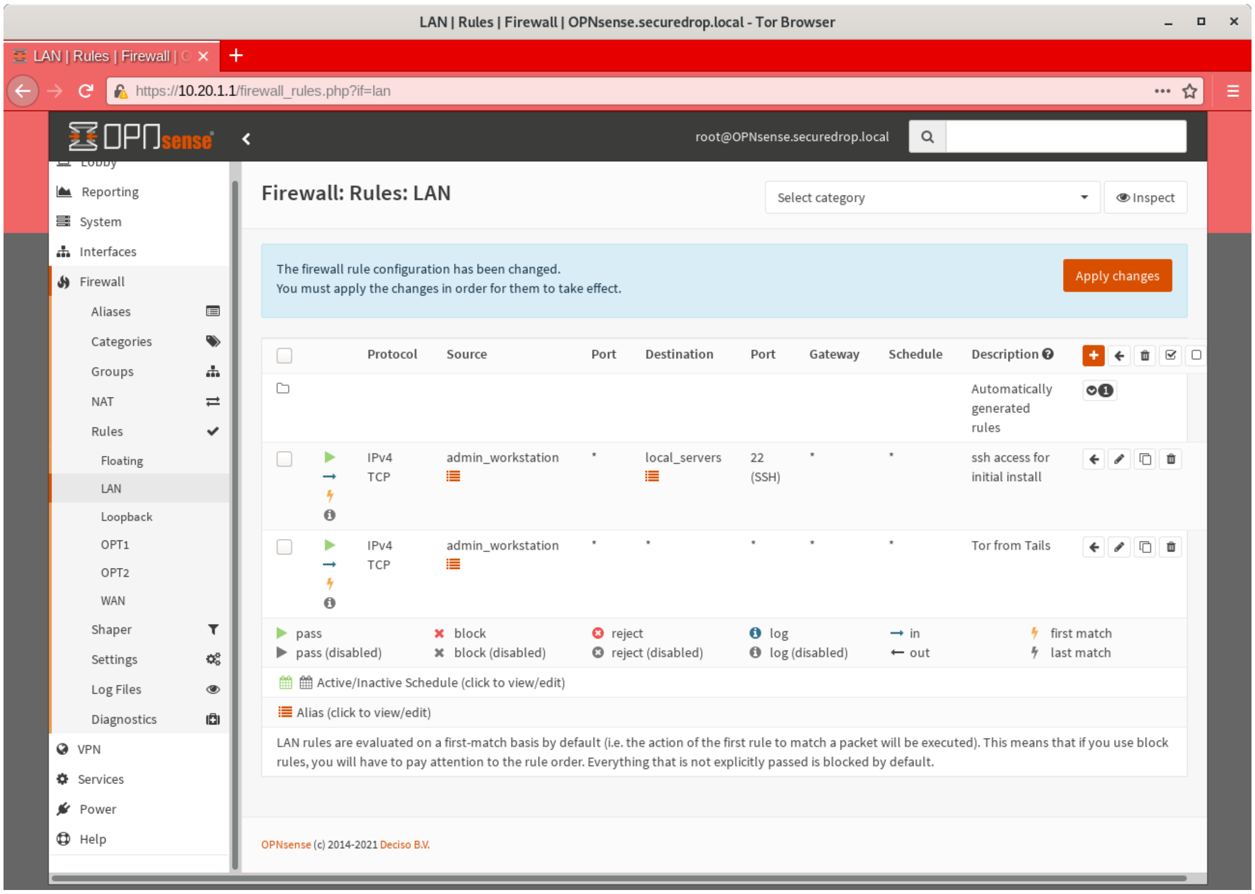
First, navigate to **Firewall** ▶ **Rules** ▶ **LAN**. The LAN interface should have one automatically-generated anti-lockout rule in place, in addition to two default-allow rules. The default-allow rules should be removed once the SecureDrop-specific rules below have been added. The anti-lockout feature should be disabled as a last step.

The rules needed are described in this table:

Table 2: Firewall Rules - LAN

Action	TCP/IP Version	Protocol	Src	Src port	Dest	Dest port	Description
Pass	IPv4	TCP	admin_workstat	•	local_servers	22 (SSH)	SSH access for initial install
Pass	IPv4	TCP	admin_workstat	•	•	•	Tor from Tails

Add or remove rules until they match the following screenshot including ordering. Click the **+** button to add a rule.



Firewall: Rules: LAN

The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
								Automatically generated rules
□	IPv4 TCP	admin_workstation	*	local_servers	22 (SSH)	*	*	ssh access for initial install
□	IPv4 TCP	admin_workstation	*	*	*	*	*	Tor from Tails

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

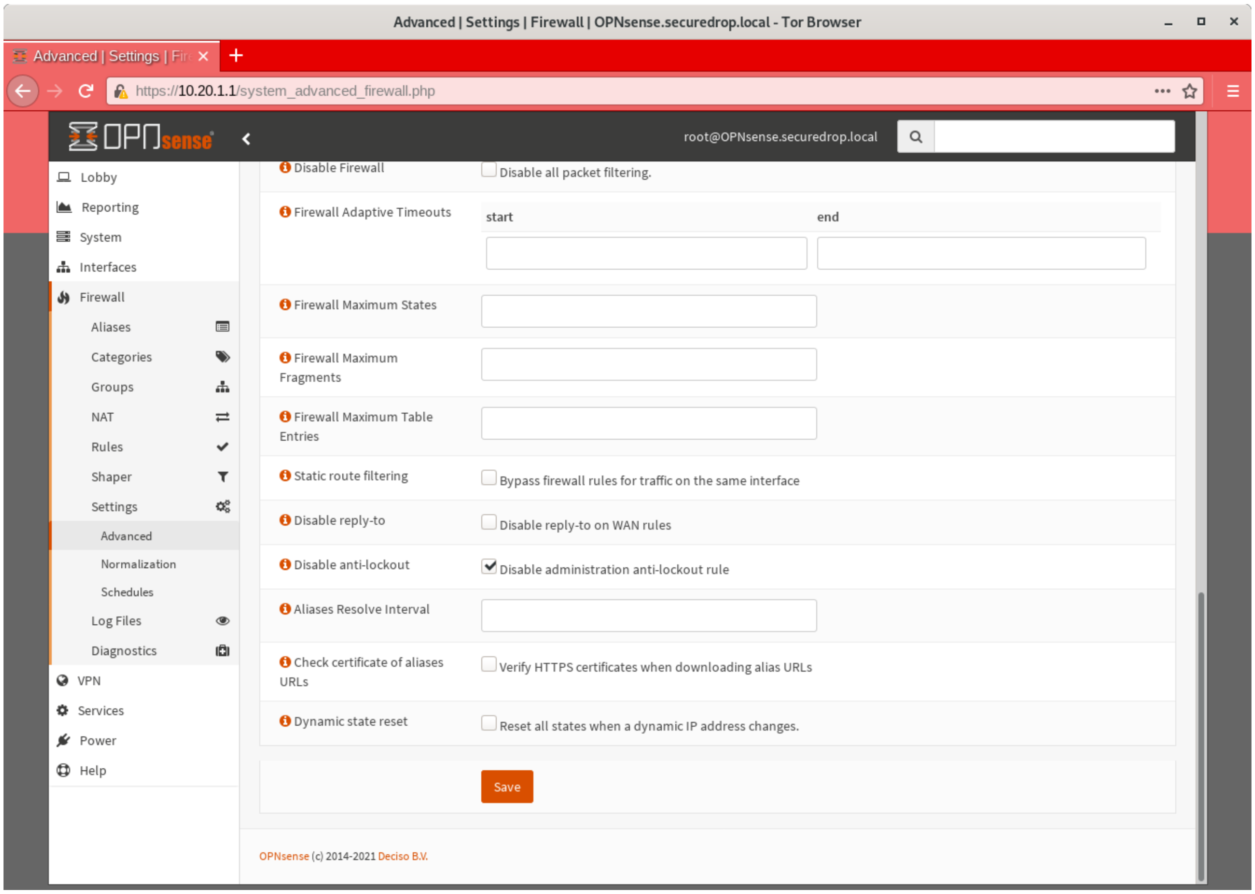
Alias (click to view/edit)

LAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

OPNsense (c) 2014-2021 Deciso B.V.

Once the rules match, click **Apply Changes.**

Finally, remove the default anti-lockout rule. First, navigate to **Firewall** ▶ **Settings** ▶ **Advanced**. Scroll down to the **Miscellaneous** section and check the **Disable anti-lockout** checkbox. Then, click **Save**.


Advanced | Settings | Firewall | OPNsense.securedrop.local - Tor Browser
Advanced | Settings | Fir
https://10.20.1.1/system_advanced_firewall.php
OPNsense
root@OPNsense.securedrop.local
Lobby
Reporting
System
Interfaces
Firewall
Aliases
Categories
Groups
NAT
Rules
Shaper
Settings
Advanced
Normalization
Schedules
Log Files
Diagnostics
VPN
Services
Power
Help
Save
OPNsense (c) 2014-2021 Deciso B.V.

Disable Firewall ☐ Disable all packet filtering.

Firewall Adaptive Timeouts start end

Firewall Maximum States

Firewall Maximum Fragments

Firewall Maximum Table Entries

Static route filtering ☐ Bypass firewall rules for traffic on the same interface

Disable reply-to ☐ Disable reply-to on WAN rules

Disable anti-lockout ☑ Disable administration anti-lockout rule

Aliases Resolve Interval

Check certificate of aliases URLs ☐ Verify HTTPS certificates when downloading alias URLs

Dynamic state reset ☐ Reset all states when a dynamic IP address changes.

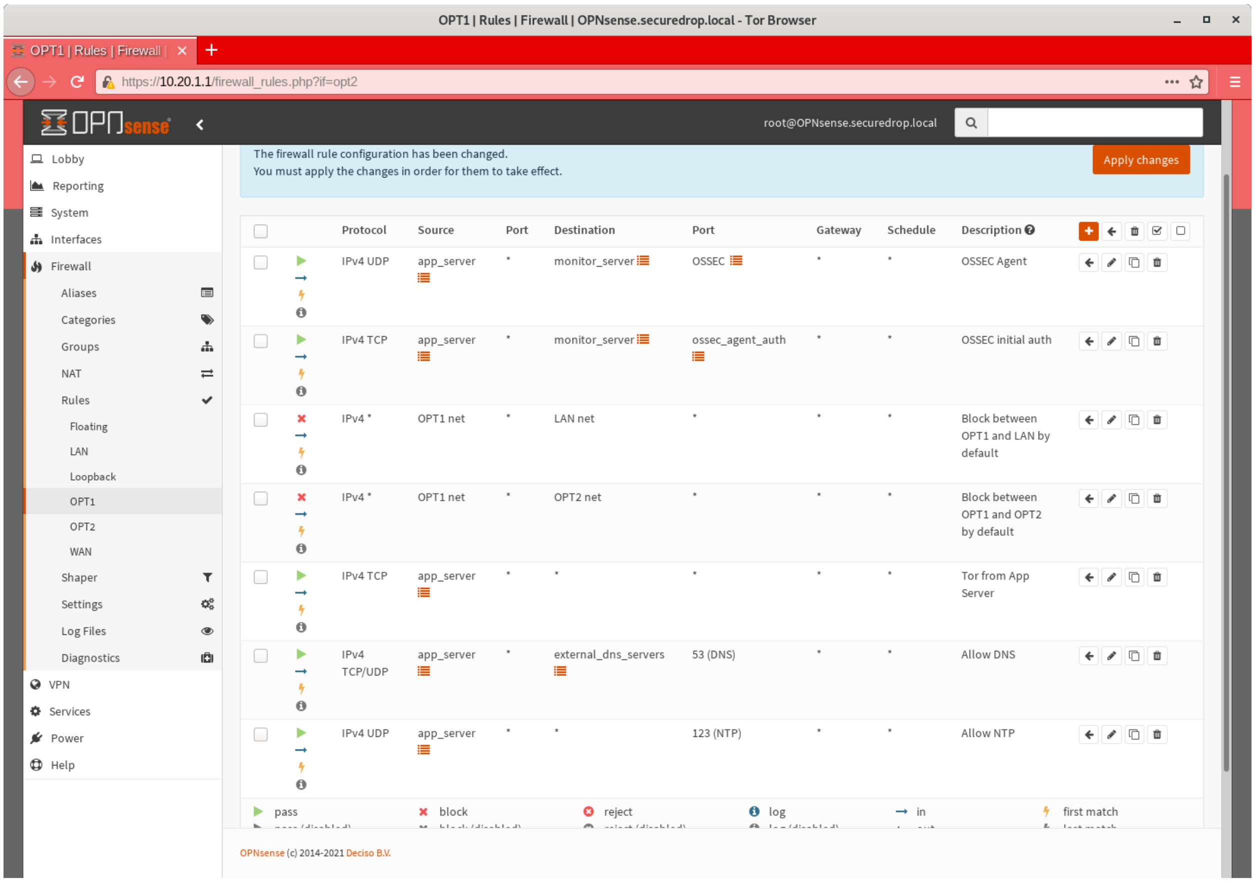
Configure Firewall Rules On OPT1

Next, navigate to **Firewall** ▶ **Rules** ▶ **OPT1**. There should be no rules defined on this interface. Add the rules below:

Table 3: Firewall Rules - OPT1

Action	TCP/IP Version	Protocol	Src	Src port	Dest	Dest port	Description
Pass	IPv4	UDP	app_server	•	monitor_server	OSSEC	OSSEC Agent
Pass	IPv4	TCP	app_server	•	monitor_server	ossec_agent_au	OSSEC initial auth
Block	IPv4	any	OPT1 net	•	LAN net	•	Block between OPT1 and LAN by default
Block	IPv4	any	OPT1 net	•	OPT2 net	•	Block between OPT1 and OPT2 by default
Pass	IPv4	TCP	app_server	•	•	•	Tor from App Server
Pass	IPv4	TCP/UDP	app_server	•	external_dns_serv	53 (DNS)	Allow DNS
Pass	IPv4	UDP	app_server	•	•	123 (NTP)	Allow NTP

Once they match the screenshot below, click **Apply Changes**.



The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

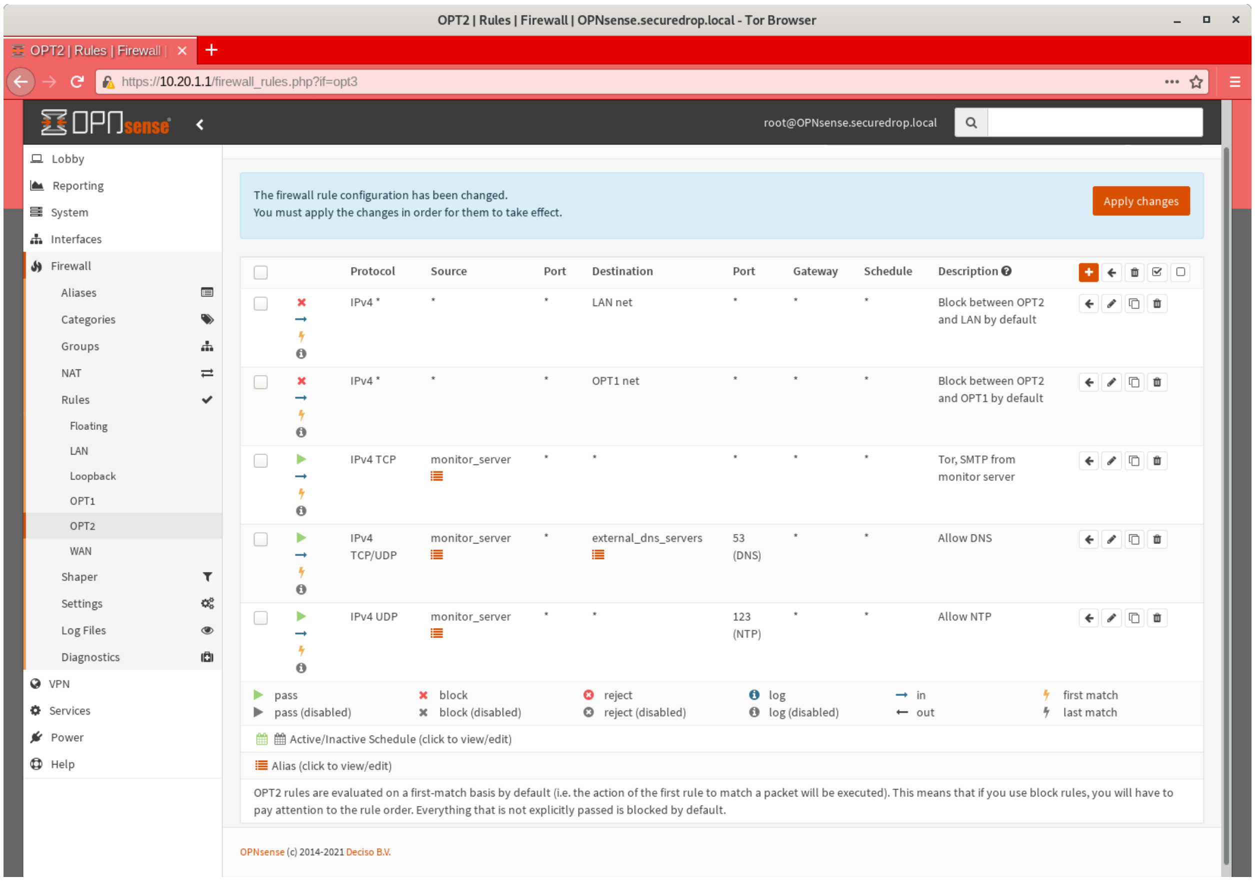
	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
▶ → ϟ ℹ	IPv4 UDP	app_server	*	monitor_server	OSSEC	*	*	OSSEC Agent
▶ → ϟ ℹ	IPv4 TCP	app_server	*	monitor_server	ossec_agent_auth	*	*	OSSEC initial auth
✖ → ϟ ℹ	IPv4 *	OPT1 net	*	LAN net	*	*	*	Block between OPT1 and LAN by default
✖ → ϟ ℹ	IPv4 *	OPT1 net	*	OPT2 net	*	*	*	Block between OPT1 and OPT2 by default
▶ → ϟ ℹ	IPv4 TCP	app_server	*	*	*	*	*	Tor from App Server
▶ → ϟ ℹ	IPv4 TCP/UDP	app_server	*	external_dns_servers	53 (DNS)	*	*	Allow DNS
▶ → ϟ ℹ	IPv4 UDP	app_server	*	*	123 (NTP)	*	*	Allow NTP

Configure Firewall Rules On OPT2

Next, navigate to **Firewall ▶ Rules ▶ OPT2**. Similarly to OPT1, there should be no rules defined on this interface. Add the rules below until the rules in the Web GUI match those in the screenshot:

Table 4: Firewall Rules - OPT2

Action	TCP/IP Version	Protocol	Src	Src port	Dest	Dest port	Description
Block	IPv4	any	OPT2 net	•	LAN net	•	Block between OPT2 and LAN by default
Block	IPv4	any	OPT2 net	•	OPT1 net	•	Block between OPT2 and OPT1 by default
Pass	IPv4	TCP	monitor_server	•	•	•	Tor, SMTP from Monitor Server
Pass	IPv4	TCP/UDP	monitor_server	•	external_dns_serv	53 (DNS)	Allow DNS
Pass	IPv4	UDP	monitor_server	•	•	123 (NTP)	Allow NTP



The firewall rule configuration has been changed.
You must apply the changes in order for them to take effect.

	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description
✖ → ϟ ℹ	IPv4 *	*	*	LAN net	*	*	*	Block between OPT2 and LAN by default
✖ → ϟ ℹ	IPv4 *	*	*	OPT1 net	*	*	*	Block between OPT2 and OPT1 by default
▶ → ϟ ℹ	IPv4 TCP	monitor_server ☰	*	*	*	*	*	Tor, SMTP from monitor server
▶ → ϟ ℹ	IPv4 TCP/UDP	monitor_server ☰	*	external_dns_servers ☰	53 (DNS)	*	*	Allow DNS
▶ → ϟ ℹ	IPv4 UDP	monitor_server ☰	*	*	123 (NTP)	*	*	Allow NTP

▶ pass ✖ block ⊗ reject ℹ log → in ϟ first match
▶ pass (disabled) ✖ block (disabled) ⊗ reject (disabled) ℹ log (disabled) ← out ϟ last match

Active/Inactive Schedule (click to view/edit)

☰ Alias (click to view/edit)

OPT2 rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

OPNsense (c) 2014-2021 Deciso B.V.

Finally, click **Apply Changes**.

The *Network Firewall* configuration is now complete, allowing you to move to the next step: *setting up the servers*.

1.36.5 Troubleshooting Tips

Here are some general tips for setting up OPNSense firewall rules:

1. Create aliases for the repeated values (IPs and ports).
2. OPNSense is a stateful firewall, which means that you don't need corresponding rules to allow incoming traffic in response to outgoing traffic (like you would in, e.g. iptables with `--state ESTABLISHED,RELATED`).
3. You should create the rules *on the interface where the traffic originates*.
4. Make sure you delete the default "allow all" rule on the LAN interface.
5. If you are troubleshooting connectivity, the firewall logs can be very helpful. You can find them in the Web GUI in **Firewall ▶ Log Files**

1.36.6 Keeping OPNSense up to Date

Periodically, the OPNSense project maintainers release an update to the OPNSense software running on your firewall. You can check for updates using the link on the OPNSense dashboard.

If you see that an update is available, we recommend installing it. Most of these updates are for minor bugfixes, but occasionally they can contain important security fixes. You should keep apprised of updates yourself by checking the OPNSense Blog or subscribing to the OPNSense Blog RSS feed.

1.37 Set Up the Servers

1.37.1 Pre-Install Steps

Upgrade the Server BIOS

Before beginning the installation process, you should upgrade your servers' BIOS to the most recent stable version available. This process will differ for each server make/model - if you are using one of the recommended NUC models, you can find instructions in *BIOS Updates on the Servers*.

Update BIOS Settings

Once the BIOS has been updated, you should boot into it again to disable any unused hardware, including:

- wireless LAN and Bluetooth
- Thunderbolt support
- audio support (output, speakers, microphones)
- other features supported by the hardware but not used by SecureDrop.

In most cases, you should enable support for LAN and USB ports only.

You should also check the servers' boot settings. Ubuntu 24.04 supports both Legacy and UEFI boot modes, with UEFI preferred. You should also disable Secure Boot. SecureDrop uses a custom kernel with security patches, which is unsigned and will not boot if Secure Boot is enabled.

Our *specific hardware recommendations* enumerate recommended BIOS settings for hardware that we have tested.

1.37.2 Install Ubuntu

The SecureDrop *Application Server* and *Monitor Server* run **Ubuntu 24.04.3 LTS (Noble Numbat)**. To install Ubuntu on the servers, you must first download and verify the Ubuntu installation media.

You should have already performed this step while setting up the Tails USB Disks, but if not, or if you would like a refresher, please review the *Create USB Boot Disk documentation.*

With the Ubuntu Server install USB ready, you may now proceed to the installation.

Perform the Installation

The steps below are the same for both the *Application Server* and the *Monitor Server*.

Start by inserting the Ubuntu installation media into the server. Boot or reboot the server with the installation media inserted, and enter the boot menu. To enter the boot menu, you need to press a key as soon as you turn the server on. This key varies depending on server model, but common choices are Esc, F2, F10, and F12. Often, the server will briefly display a message on boot that shows which key should be pressed to enter the boot menu. Once you've entered the boot menu, select the installation media (USB or CD) and press Enter to boot it.

On newer hardware, such as the NUC12s, you may need to use a newer Linux kernel than the one that ships by default in **Ubuntu Server 24.04.3** in order to have more up-to-date hardware drivers. To use a newer Linux kernel, select **Ubuntu Server with the HWE kernel** in the initial OS boot menu that appears prior to booting the Ubuntu image.

After booting the Ubuntu image, select **Install Ubuntu Server**.

Follow the steps to select your language, country and keyboard settings. Once that's done, let the installation process continue.

Configure the Network

On the **Network connections** screen, the installer will ask you to configure at least one interface for use by the server. Your server should only have one available, corresponding to its Ethernet, usually named `eno1`. Select its list entry using the arrow keys and press **Enter**, then select **Edit IPv4** and press **Enter** again.

The **Edit eno1 IPv4 configuration** dialog will be displayed. In the **IPv4 Method** menu, select **Manual**, then add your server-specific settings.

Note

For a production install with a pfSense network firewall in place, the *Application Server* and the *Monitor Server* are on separate networks. You may choose your own network settings at this point, but make sure the settings you choose are unique on the firewall's network and remember to propagate your choices through the rest of the installation process.

Below are the configurations you should enter, assuming you used the default network settings from the network firewall guide. If you did not, adjust these settings accordingly.

- *Application Server*:
- **Subnet:** 10.20.2.0/24
- **Address:** 10.20.2.2
- **Gateway:** 10.20.2.1
- **Name servers:** 8.8.8.8, 8.8.4.4
- **Search domains:** *should be left blank*
- *Monitor Server*:
- **Subnet:** 10.20.3.0/24
- **Address:** 10.20.3.2
- **Gateway:** 10.20.3.1
- **Name servers:** 8.8.8.8, 8.8.4.4

- **Search domains:** *should be left blank*

Select **Save** and press **Enter** to apply your settings. Then select **Done** and press **Enter**.

The default values on the **Configure Proxy** and **Configure Ubuntu archive mirror** screens should not need to be changed. Select **Done** for both.

Continue Without Updating the Installer

With the network connection now active, the installer may alert you that a newer version of Ubuntu Sever is now available.

It is critical that you use the version of Ubuntu Server you downloaded and verified in the previous steps, rather than upgrading to the latest available version.

Select the **Continue without updating** option when prompted.

Full Disk Encryption - pros and cons

The use of Full Disk Encryption (FDE) with SecureDrop is **not recommended**. While FDE does offer data protection for devices that are powered down, SecureDrop's servers are designed to be always-on, with the exception of a nightly reboot after automatic upgrades are applied. Given this update schedule, with FDE enabled, the servers would become unreachable once every 24 hours until an administrator entered the full-disk encryption passphrase via the console, and during that time, sources and journalists would be unable to access your instance.

The increased responsibility for administrators, as well as the daily downtime and limited scenarios in which FDE would be a net security benefit, inform this recommendation, but you may make a decision based on your own requirements. (See this GitHub issue for more information.)

Setting up storage

On the **Guided storage configuration** screen, verify that **Use an entire disk** is checked, and that the server's local disk is selected. Also verify that **Set up this disk as an LVM group** is selected.

If you decided to set up FDE, despite the implications for administration overhead, select **Encrypt the LVM group with LUKS**, and enter and confirm the disk passphrase. Store this passphrase securely, as it will be required to unlock storage on every reboot.

Select **Done** and press **Enter** to move to the **Storage Configuration** screen. Review the configuration and select **Done** and press **Enter** to continue. Then, choose **Continue** on the **Confirm destructive action** dialog.

Configure account and hostname

On the **Profile setup** screen, configure the server's hostname and the administration account. The administrator account username and password should be the same for both servers:

- **Your name:** Specify the administrator account name, e.g. `SecureDrop Admin`
- **Your server's name:** Use `app` for the *Application Server*, and `mon` for the *Monitor Server*
- **Pick a username:** Specify the administrator account username, e.g. `sdadmin`
- **Choose a password:** Specify a strong password for the administrator account. A Diceware-generated passphrase is recommended.
- **Confirm your password:** Enter the password chosen above.

Select **Done** and press **Enter** to proceed.

Warning

The username and password you choose must be the same on both the *Application Server* and the *Monitor Server*. When you deploy SecureDrop from your *Admin Workstation* in a later step, you will only be allowed to enter one password, so it must be identical on both servers.

Decline upgrade to Ubuntu Pro

The SecureDrop servers should not be registered with Ubuntu Advantage. On the **Upgrade to Ubuntu Pro** screen, make sure **Skip for now** is selected, then choose **Continue**.

Set up SSH access

On the **SSH Setup** screen, enable **Install OpenSSH server**. Verify that **No** is selected for the **Import SSH Identity** option, as a custom SSH key will be created for the administration account later in the installation process.

Verify that **Allow password authentication over SSH** is selected, and choose **Done** to proceed.

Finish the Installation

On the **Featured server snaps** screen, ensure that no snaps are selected and choose **Done** to start the server installation process.

Once the server installation is complete, choose **Reboot Now** to reboot the system.

Save the Configurations

When you are done, make sure you save the following information:

- The IP address of the *Application Server*
- The IP address of the *Monitor Server*
- The non-root user's name and passphrase for the servers.

1.37.3 Test Connectivity

Now that the firewall is set up, you can plug the *Application Server* and the *Monitor Server* into the firewall. If you are using a setup where there is a switch on the LAN port, plug the *Application Server* into the switch and plug the *Monitor Server* into the OPT1 port.

You should make sure you can connect from the Admin Workstation to both of the servers before continuing with the installation.

In a terminal, verify that you can SSH into both servers, authenticating with your passphrase:

```
$ ssh <username>@<App IP address> hostname
app
$ ssh <username>@<Monitor IP address> hostname
mon
```

Tip

If you cannot connect, check the network firewall logs for clues.

1.37.4 Set Up SSH Keys

Ubuntu's default SSH configuration authenticates users with their passphrases; however, public key authentication is more secure, and once it's set up it is also easier to use. In this section, you will create a new SSH key for authenticating to both servers. Since the *Admin Workstation* was set up with SSH Client Persistence, this key will be saved on the *Admin Workstation* and can be used in the future to authenticate to the servers in order to perform administrative tasks.

First, generate the new SSH keypair:

```
ssh-keygen -t rsa -b 4096
```

You'll be asked to "Enter file in which to save the key" Type **Enter** to use the default location.

Given that this key is on the encrypted persistence of a Tails USB, you do not need to add an additional passphrase to protect the key. If you do elect to use a passphrase, note that you will need to manually type it (Tails' pinentry will not allow you to copy and paste a passphrase).

Once the key has finished generating, you need to copy the public key to both servers. Use `ssh-copy-id` to copy the public key to each server, authenticating with your passphrase:

```
ssh-copy-id <username>@<App IP address>
ssh-copy-id <username>@<Mon IP address>
```

Verify that you are able to authenticate to both servers by running the below commands. You should not be prompted for a passphrase (unless you chose to passphrase-protect the key you just created).

```
$ ssh <username>@<App IP address> hostname
app
$ ssh <username>@<Monitor IP address> hostname
mon
```

If you have successfully connected to the server via SSH, the terminal output will be name of the server to which you have connected ('app' or 'mon') as shown above.

1.38 Install SecureDrop

1.38.1 Localization of the *Source Interface* and *Journalist Interface*

The *Source Interface* and *Journalist Interface* are translated in the following languages:

https://github.com/freedomofpress/securedrop/blob/develop/securedrop/i18n.rst

During the installation you will be given the opportunity to choose from a list of supported languages to display using the codes shown in parentheses.

> **Note**
>
> With a *Source Interface* displayed in French (for example), sources submitting documents are likely to expect a journalist fluent in French to be available to read the documents and follow up in that language.

1.38.2 Configure the Installation

Make sure you have the following information and files ready before continuing:

- the *Application Server* local IP address
- the *Monitor Server* local IP address

- the *Submission Public Key* (from the *Transfer Device*)
- the *Submission Key* fingerprint
- the email address that will receive alerts from OSSEC
- the GPG public key and fingerprint for the email address that will receive the alerts
- connection information for the SMTP relay that handles OSSEC alerts (see the *OSSEC Alerts Guide*)
- the username of a journalist who will be using SecureDrop (you can add more later)
- the username of the system admin

Optionally, you can configure *daily email notifications* of submission activity for journalists. These help journalists avoid spending time checking the *Journalist Interface* when there are no submissions. For this you will need:

- the *Journalist Alert Public Key*
- the *Journalist Alert Public Key* fingerprint
- the email address that will receive the journalist alerts

Note

It is not possible to specify multiple email addresses for email notifications. If there are multiple intended recipients, use an alias or mailing list. However, all subscribers must share the GPG private key, as it is not possible to specify multiple keys.

Note

The journalist notification is sent after the daily reboot of the *Application Server*.

Before proceeding, you will need to copy the following files to `~/.config/securedrop-admin`:

- the *Submission Public Key* file
- the *OSSEC Alert Public Key*

The *Submission Public Key* should be located on your *Transfer Device* from earlier. Its exact path will depend on the location where the USB stick is mounted. From the root of the SecureDrop repository, run:

```
cp /media/[USB folder]/SecureDrop.asc ~/.config/securedrop-admin/
```

where `/media/[USB folder]/` corresponds to the *Transfer Device*. (You can also use the copy and paste capabilities of the file manager.)

Next, copy the *OSSEC Alert Public Key* into `~/.config/securedrop-admin` as well.

Next, run the configuration playbook and answer the prompts with values that match your environment:

```
securedrop-admin sdconfig
```

The script will automatically validate the answers you provided and display error messages if any problems are detected. The answers will be written to the file `~/.config/securedrop-admin/site-specific`.

When you’re done, save the file and quit the editor.

1.38.3 Install SecureDrop Servers

Now you are ready to install! This process will configure the servers and install SecureDrop and all of its dependencies on the remote servers.

```
securedrop-admin install
```

You will be prompted to enter the sudo passphrase for the *Application Server* and *Monitor Server* (which should be the same).

The installation process will take some time. It will return you to the terminal prompt when complete.

If any errors occur while running the install, carefully inspect the error output. Considering saving any error messages for reference and troubleshooting.

Note

If you see an error running `securedrop-admin install`, and believe it may be an intermittent issue (for example, due to losing network connectivity to the servers), it is safe to run the `securedrop-admin install` command again. If you see the same issue consistently, then you will need to troubleshoot it.

If you see the error message "timeout (62s) waiting for privilege escalation prompt", try deleting the Ansible control path directory on your *Admin Workstation* (`rm -rf ~/.ansible/cp`) to reset the connection to the servers, then re-run the `securedrop-admin install`.

If you encounter other errors, we encourage you to submit a bug report, or to contact us at securedrop@freedom.press (GPG encrypted).

If needed, make edits to the file located at `~/.config/securedrop-admin/site-specific` as described *above*. If you continue to have issues, please submit a detailed issue notice on GitHub or send an email to securedrop@freedom.press.

Note

The SecureDrop install process configures a custom Linux kernel hardened with the grsecurity patch set. Only binary images are hosted in the apt repo. For source packages, see the Source Offer.

Once the installation is complete, addresses and credentials for each onion service will be available in the following files under `~/.config/securedrop-admin`:

V3 onion services

- `app-sourcev3-ths` contains the v3 `.onion` address of the *Source Interface*.
- `app-journalist.auth_private` contains the `onion` address and private key providing access to the *Journalist Interface*.
- `app-ssh.auth_private` contains the `onion` address and private key providing SSH access to the *Application Server*.
- `mon-ssh.auth_private` contains the `onion` address and private key providing SSH access to the *Monitor Server*.
- `tor_v3_keys.json` contains the keypairs required for access to the *Journalist Interface* and SSH access to the servers - it is required for future runs of `securedrop-admin install`.

Warning

The three `.auth_private` files and the `tor_v3_keys.json` file contain secret keys that should not be shared with third parties, or copied from the *Admin Workstation* for any purpose other than tasks such as performing backups or onboarding new users.

The dynamic inventory file will automatically read the `onion` addresses from the `app-ssh.auth_private` and `mon-ssh.auth_private` files and use them to connect to the servers over SSH during subsequent playbook runs.

1.39 Configure the Admin Workstation Post-Install and Create Backups

1.39.1 Auto-connect to the Authenticated Onion Services

The SecureDrop installation process adds multiple layers of authentication to protect access to the most sensitive assets in the SecureDrop system:

1. The *Journalist Interface*, because it provides access to submissions (although they are encrypted to an offline key), and some metadata about sources and submissions.
2. SSH on the *Application Server*
3. SSH on the *Monitor Server*

The installation process blocks direct access to each of these assets, and sets up authenticated onion services to provide authenticated access instead. Authenticated onion services share the benefits of regular onion services, but are only accessible to users who possess a shared secret (`auth-cookie` in the Tor documentation) that is generated during the onion service setup process.

In order to access an authenticated onion service, you require its authentication secret. SecureDrop includes a set of scripts to configure Tails access to the authenticated onion services. In order to persist these changes across reboots, persistence must be enabled in Tails.

To install the auto-connect configuration, run:

```
securedrop-admin localconfig
```

Type the Administration Password that you selected when starting Tails and hit **Enter**. This script installs a persistent script that runs every time you connect to a network in Tails, and automatically configures access to the *Journalist Interface* and to the servers via SSH. The HidServAuth info is collected from files in `~/usr/share/securedrop-admin/ansible-base` and stored in `~/.config/securedrop-admin/torrc_additions` thereafter.

In addition, the script creates the *SecureDrop Menu*, directs Tails to install Ansible at the beginning of every session, and sets up SSH host aliases for the servers.

The only thing you need to remember to do is enable persistence when you boot the *Admin Workstation*. If you are using the *Admin Workstation* and are unable to connect to any of the authenticated onion services, restart Tails and make sure to enable persistence.

1.39.2 Back Up the Workstations

USB drives can wear out, get lost, or otherwise become corrupted, making it very important to be sure to keep current backups. Follow the *Backup the Workstations* document to create a backup of your *Secure Viewing Station*, *Admin Workstation*, and *Journalist Workstations* after you've completed the installation and post-installation steps.

1.40 Create an Admin Account on the *Journalist Interface*

In order for any user (admin or journalist) to access the *Journalist Interface*, they need:

1. The `auth-cookie` for the *Journalist Interface*'s ATHS
2. An account on the *Journalist Interface*, which requires the following credentials to log in:
    - Username
    - Passphrase
    - Two-factor authentication code

You should create a separate account on the *Journalist Interface* for each user who needs access. This makes it easy to enable or disable access to the *Journalist Interface* on an individual basis, so you can grant access to new users or revoke access for users who have left the organization or should no longer be allowed to access the Journalist Interface.

There are two types of accounts on the *Journalist Interface*: admin accounts and normal accounts. Admins accounts are like normal accounts, but they are additionally allowed to manage (add, change, delete) other user accounts through the web interface.

You must create the first admin account on the *Journalist Interface* by running a command on the *Application Server*. After that, the Journalist Interface admin can create additional accounts through the web interface.

To create an admin account via the command line, *SSH to the Application Server*, then:

```
sudo -u www-data bash
cd /var/www/securedrop
./manage.py add-admin
```

Follow the prompts.

A secure diceware passphrase will be generated by *manage.py*. You will see output like this:

```
This journalist's passphrase is: delivery propose requisite stunner dragonfly unstamped␣
↪stowaway
```

Passphrases include the spaces between the words, but not leading or trailing whitespace. Be sure to save this passphrase in the appropriate KeePassXC database.

Once that's done, you should open Tor Browser and navigate to the *Journalist Interface*'s .onion address. Verify that you can log in to the *Journalist Interface* with the admin account you just created.

For adding more user accounts, please refer now to our *Admin Interface Guide*.

Note

You can now set a custom logo image on your web interfaces by following the *Updating the Logo Image* documentation.

1.41 Test the Installation

1.41.1 Test Connectivity

SSH to Both Servers Over Tor

Assuming you haven't disabled SSH over Tor, SSH access will be restricted to the Tor network.

On the *Admin Workstation*, you should be able to SSH to the *Application Server* and the *Monitor Server*.

```
ssh app
ssh mon
```

The SSH aliases should have been configured automatically by running the `securedrop-admin localconfig` command. If you're unable to connect via aliases, try using the verbose command format to troubleshoot:

```
ssh <username>@<app .onion>
ssh <username>@<mon .onion>
```

Tip

Check the `app-ssh.auth_private` and `mon-ssh.auth_private` files in the `~/.config/securedrop-admin` directory to find the ssh onion service addresses. The files contain one line with 4 colon-delimited fields. The address is the first 56-character field, just add a `.onion` at the end.

Log in to Both Servers via TTY

All access to the SecureDrop servers should be performed over SSH from the *Admin Workstation*. To aid in troubleshooting, login via a physical keyboard attached to the server is also supported.

1.41.2 Sanity-Check the Installation

On each server:

1. Check that you can execute privileged commands by running `sudo su`.
2. Verify that you are booted into a grsec kernel: run `uname -r` and verify that the name of the running kernel ends with `-grsec`.
3. Check the current applied iptables rules with `iptables-save`. It should output *approximately* 50 lines.
4. You should have received an email alert from OSSEC when it first started. If not, review our *OSSEC Alerts Guide*.

On the *Application Server*:

1. Check the AppArmor status with `sudo aa-status`. On a production instance all profiles should be in `enforce` mode.

1.41.3 Test the Web Interfaces

1. Make sure the *Source Interface* is available, and that you can make a submission.
   - Open the *Source Interface* in Tor Browser by clicking on its desktop shortcut. Proceed through the codename generation (copy this down somewhere) and submit a test message or file.
   - Usage of the Source Interface is covered by our *Source User Manual*.
2. Test that you can access the *Journalist Interface*, and that you can log in as the admin user you just created.
   - Open the *Journalist Interface* in Tor Browser by clicking on its desktop shortcut. Enter your passphrase and two-factor code to log in.
   - If you have problems logging in to the *Admin/Journalist Interface*, SSH to the *Application Server* and restart the time synchronization daemon to synchronize the time: `sudo systemctl restart systemd-timesyncd`. Also check that your smartphone's time is accurate and set to network time in its device settings.
3. Test replying to the test submission.

- While logged in as an admin, you can send a reply to the test source submission you made earlier.
- Usage of the *Journalist Interface* is covered by our *Journalist User Manual*.

4. Test that the source received the reply.
   - Within Tor Browser, navigate back to the *Source Interface* and use your previous test source codename to log in (or reload the page if it's still open) and check that the reply you just made is present.
5. Remove the test submissions you made prior to putting SecureDrop to real use. On the main *Journalist Interface* page, select all sources and click **Delete selected**.

Once you've tested the installation and verified that everything is working, see *How to Use SecureDrop*.

1.42 Deployment Overview

Once SecureDrop is installed on a news organization's servers, it's important for the administrator to configure it in a way that provides the greatest protection for sources and journalists, given the unique needs and constraints of the organization.

The deployment section here covers a variety of tasks an administrator might need to perform to successfully deploy SecureDrop, depending on organizational needs and requirements.

Certain topics, such as creating a landing page and onboarding journalists, are universal to all SecureDrop instances. Other topics are optional, and are only needed if they fit in with the organization's security policies and newsroom workflows.

The deployment tasks generally only need to be performed once. For tasks related to the upkeep and troubleshooting of your SecureDrop instance, we recommend reviewing *the maintenance documentation.*

1.43 Protecting the Security of the System

SecureDrop is only as secure as the environment that surrounds it. To keep sources safe, the news organization's website, physical space, and dedicated SecureDrop hardware must employ a set of basic security best practices or risk losing any source protection provided by SecureDrop.

Freedom of the Press Foundation eventually plans to list all of those SecureDrop onion URLs that meet the minimum requirements for deployment best practices as "verified" on its website. If your organization cannot follow the minimum guidelines, we cannot recommend your SecureDrop instance as safe to use.

In addition to implementing the following best practices, we strongly recommend that you have a reputable security firm perform a review of your organization's public website prior to launching an instance of SecureDrop. Upon request, we can help put you in touch with a few security firms if you need more assistance.

1.44 *Landing Page*

SecureDrop itself runs as a Tor Onion Service. Organizations also need to create a SecureDrop *Landing Page* that will:

- explain how SecureDrop works
- give sources instructions on how to access the Tor Onion Service
- disclose the risks of accessing the SecureDrop instance or submitting documents

We also recommend including a privacy policy (see our *Sample SecureDrop Privacy Policy*) describing what data is collected and how it will be used by your organization.

Note

SecureDrop will bring more attention to your organization from security researchers and others. A *Landing Page* that fails to implement minimum security requirements is sure to be noticed, and could undermine trust, discouraging possible sources.

1.44.1 *Landing Page* Content Suggestions

The content below presents sample text for the SecureDrop component of a news organization's tips page. It does not account for any specific legal or organizational needs, but should provide guidance for any outlet getting started on crafting *Landing Page* language. Any tweaks to the sample content should be left to the legal and editorial discretion of the individual outlet, and should be viewed as essential to upholding source protection and transparency.

What is SecureDrop?

SecureDrop is an anonymity tool for journalists and whistleblowers. As a source, you can use our SecureDrop installation to anonymously submit documents to our organization. Our journalists use SecureDrop to receive source materials and securely communicate with anonymous contacts.

What should I know before submitting material through SecureDrop?

To protect your anonymity when using SecureDrop, it is essential that you do not use a network or device that can easily be traced back to your real identity. Instead, use public wifi networks and devices you control.

- Do NOT access SecureDrop on your employer's network.
- Do NOT access SecureDrop using your employer's hardware.
- Do NOT access SecureDrop on your home network.
- DO access SecureDrop on a network not associated with you, like the wifi at a library or cafe.

Got it. How can I submit files and messages through SecureDrop?

Once you are connected to a public network at a cafe or library, download and install the desktop version of Tor Browser.

Launch Tor Browser. Visit our organization's unique SecureDrop URL at **http://our-unique-URL.onion/**. Follow the instructions you find on our source page to send us materials and messages.

When you make your first submission, you will receive a unique codename. Memorize it. If you write it down, be sure to destroy the copy as soon as you've committed it to memory. Use your codename to sign back in to our source page, check for responses from our journalists, and upload additional materials.

As a source, what else should I know?

No tool can absolutely guarantee your security or anonymity. The best way to protect your privacy and anonymity as a source is to adhere to best practices.

You can use a separate computer you've designated specifically to handle the submission process. Or, you can use an alternate operating system like Tails, which boots from a USB stick and erases your activity at the end of every session.

A file contains valuable metadata about its source — when it was created and downloaded, what machine was involved, the machine's owner, etc. You can scrub metadata from some files prior to submission using the Metadata Anonymization Toolkit featured in Tails.

Your online behavior can be extremely revealing. Regularly monitoring our publication's social media or website can potentially flag you as a source. Take great care to think about what your online behavior might reveal, and consider using Tor Browser to mitigate such monitoring.

Our organization retains strict access control over our SecureDrop project. A select few journalists within our organization will have access to SecureDrop submissions. We control the servers that store your submissions, so no third party has direct access to the metadata or content of what you send us.

Do not discuss leaking or whistleblowing, even with trusted contacts.

1.44.2 The SecureDrop Directory

SecureDrop maintains a directory of instances that meet our strict guidelines. If you would like to be considered for inclusion in this directory, make sure your landing page features the necessary items from the sample above, and is in compliance with the technical requirements below, then send us a request using this form.

There are several benefits to being included in the SecureDrop directory. The most significant benefit is that it will be easier for potential sources to find your SecureDrop instance. Additionally, being included in the directory makes you eligible for *an onion name*. This improves the experience by turning a lengthy, non-descriptive address into one that is short and memorable. For example, a long .onion address might look like:

```
sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion
```

whereas the shorter onion name might look like:

```
nyworld.securedrop.tor.onion
```

If you wish to receive an onion name, one can be provided during the instance verification process. The format for short onion addresses is:

```
organization.securedrop.tor.onion
```

where `organization` can be any name you request, within reason.

Being included in the SecureDrop directory may make your instance more visible, which could result in an uptick of illegitimate (spam) submissions. If you notice an increase in spam after being included in the directory, please let us know and we can remove your instance from the directory.

1.44.3 URL and Location

Your *Landing Page* must be a path at your top-level domain, e.g. organization.com/securedrop, rather than a subdomain (e.g., securedrop.organization.com). This is because DNS and TLS do not always encrypt the hostname, so a SecureDrop user whose connection is being monitored would be trivially discovered if you were to use a subdomain.

If the *Landing Page* is deployed on the same domain as another site, you might consider having some specific configuration (such as the security headers below) apply only to the /securedrop request URI. This can be done in Apache by the encapsulating these settings within a <Location> block, which can be defined similarly in nginx by using the location { } directive.

Warning

Except for rare extenuating circumstances, this is a requirement for inclusion in the SecureDrop Directory

1.44.4 HTTPS Only (No Mixed Content)

HTTPS encryption is the number-one security requirement for your site's SecureDrop *Landing Page*. Without HTTPS, a source can easily be exposed as a visitor to your site.

This may be difficult if your website serves advertisements or utilizes a legacy content delivery network. You should make sure the SecureDrop *Landing Page* does not serve ads of any kind, even if the rest of your site does.

If you do not serve ads on any of your site, you should also consider switching your whole site over to HTTPS by default immediately. If you do serve ads, consider pressuring your ad networks to enable you to switch to HTTPS for your entire website in the future.

If your website needs to operate in both HTTPS and HTTP mode, use protocol-relative URLs for resources such as images, CSS and JavaScript in common templates to ensure your page does not end up in a mixed HTTPS/HTTP state.

Consider submitting your domain to be included in the Chrome HSTS preload list if you can meet all of the requirements. This will tell web browsers that the site is only ever to be reached over HTTPS.

Warning

This is a strict requirement for inclusion in the SecureDrop Directory

1.44.5 Perfect Forward Secrecy

Perfect Forward Secrecy (PFS) is a property of encryption protocols that ensures each SSL session has a unique key, meaning that if the key is compromised in the future it can't be used to decrypt previously recorded SSL sessions. You may need to talk to your CA (certificate authority) and CDN (content delivery network) for this, although our recommended configuration below provides forward secrecy.

1.44.6 SSL Certificate Recommendations

Regardless of where you choose to purchase your SSL cert and which CA issues it, you'll often be asked to generate the private key and a CSR (certificate signing request).

When you do this, it's imperative that you use SHA-2 as the hashing algorithm instead of SHA-1, which is being phased out. You should also choose a key size of *at least* 2048 bits. These parameters will help ensure that the encryption used on your *Landing Page* is sufficiently strong. The following example OpenSSL command will create a private key and CSR with a 4096-bit key length and a SHA-256 signature:

```
openssl req -new -newkey rsa:4096 -nodes -sha256 -keyout domain.com.key -out domain.com.
↪csr
```

Don't load any resources (scripts, web fonts, etc.) from third parties (e.g. Google Web Fonts)

This will potentially leak information about sources to third parties, which can more easily be accessed by law enforcement agencies. Simply copy them to your server and serve them yourself to avoid this problem.

1.44.7 Do Not Use Third-Party Analytics, Tracking, or Advertising

Most news websites, even those that are non-profits, use third-party analytics tools or tracking bugs on their websites. It is vital that these are disabled for the SecureDrop *Landing Page*.

In the past, some news organizations were heavily criticized when launching their SecureDrop instances because their *Landing Page* contained trackers. They claimed they were going to great lengths to protect sources' anonymity, but by having trackers on their *Landing Page*, this also opened up multiple avenues for third parties to collect information on those sources. This information can potentially be accessed by law enforcement or intelligence agencies and could unduly expose a source.

Similarly, consider avoiding Cloudflare (and other CDNs like Akamai, StackPath, Incapsula, Amazon CloudFront, etc.) for the SecureDrop *Landing Page*. These services intercept requests between a potential source and the SecureDrop *Landing Page* and can be used to track or collect information on sources.

Warning

This is a strict requirement for inclusion in the SecureDrop Directory

1.44.8 Do Not Hyperlink .onion Addresses

Because a visitor to your *Landing Page* may not be using Tor Browser yet, clicking a link to your SecureDrop instance or to any other .onion address may result in an error message. Worse, depending on the browser and network configuration, it may cause lookups that an adversary can use to identify SecureDrop-related behavior.

Instead, we recommend including .onion addresses in plain text, without a hyperlink.

If you have been provided a short onion name for your instance, this address will also need to be plain text, without a hyperlink. We recommend using the text below to provide maximum clarity:

```
The SecureDrop instance can be found by entering the following address in
the desktop version of Tor Browser: <short onion name>

Alternately, you can access the instance by entering: <long onion address>
```

Warning

This is a strict requirement for inclusion in the SecureDrop Directory

1.44.9 Avoid Direct Links to SecureDrop.org

We appreciate that you may want to link to the SecureDrop website to give *Landing Page* visitors more information about the system. Unfortunately, if a visitor visits these links without using Tor Browser, this generates traffic that an adversary may be able to use to identify SecureDrop-related behavior, regardless of the use of HTTPS.

We suggest offering a reference to the SecureDrop Onion Service in plain text, without a hyperlink (as per the preceding section):

sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion

Warning

This is a strict requirement for inclusion in the SecureDrop Directory

1.44.10 Apply Security Headers

Security headers give instructions to the web browser on how to handle requests from the web application. These headers set strict rules for the browser and help mitigate against potential attacks. Given the browser is a main avenue for attack, it is important these headers are as strict as possible.

You can use the site securityheaders.com to easily test your website's security headers.

If you use Apache, you can use these:

```
Header set Cache-Control "max-age=0, no-cache, no-store, must-revalidate"
Header edit Set-Cookie ^(.*)$ $;HttpOnly
Header set Pragma "no-cache"
Header set Expires "-1"
```

(continues on next page)

(continued from previous page)

```
Header always append X-Frame-Options: DENY
Header set X-XSS-Protection: "1; mode=block"
Header set X-Content-Type-Options: nosniff
Header set X-Download-Options: noopen
Header set X-Permitted-Cross-Domain-Policies: master-only
Header set Content-Security-Policy: "default-src 'none'; script-src 'self'; style-src
↪'self'; img-src 'self'; font-src 'self';"
Header set Referrer-Policy "no-referrer"
Header set Permissions-Policy "camera 'none'; display-capture 'none'; geolocation 'none';
↪ microphone 'none'; payment 'none'; usb 'none';"
```

If you intend to run nginx as your webserver instead, this will work:

```
add_header Cache-Control "max-age=0, no-cache, no-store, must-revalidate";
add_header Pragma no-cache;
add_header Expires -1;
add_header X-Frame-Options DENY;
add_header X-XSS-Protection "1; mode=block";
add_header X-Content-Type-Options nosniff;
add_header X-Download-Options noopen;
add_header X-Permitted-Cross-Domain-Policies master-only;
add_header Content-Security-Policy "default-src 'none'; script-src 'self'; style-src
↪'self'; img-src 'self'; font-src 'self';";
add_header Referrer-Policy "no-referrer";
add_header Permissions-Policy "camera 'none'; display-capture 'none'; geolocation 'none';
↪ microphone 'none'; payment 'none'; usb 'none';";
```

1.44.11 Additional Apache Configuration

To enforce HTTPS/SSL always, you need to set up redirection within the HTTP (port 80) virtual host:

```
RewriteEngine On
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
```

The same thing can be achieved in nginx with a single line:

```
return 301 https://$server_name$request_uri;
```

In your SSL (port 443) virtual host, set up HSTS and use these settings to give preference to the most secure cipher suites:

```
Header set Strict-Transport-Security "max-age=16070400;"
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder on
SSLCompression off
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
```

Here's a similar example for nginx:

```
add_header Strict-Transport-Security max-age=16070400;
ssl_protocols TLSv1.2;
```

(continues on next page)

(continued from previous page)

```
ssl_prefer_server_ciphers on;
ssl_ciphers "EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";
```

Here's a similar example for nginx if the system supports TLS 1.3:

```
add_header Strict-Transport-Security max-age=16070400;
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers on;
ssl_ciphers "TLS-CHACHA20-POLY1305-SHA256:TLS-AES-256-GCM-SHA384:TLS-AES-128-GCM-
↪SHA256:EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH";
```

Note

We have prioritized security in selecting these cipher suites, so if you choose to use them then your site might not be compatible with legacy or outdated browsers and operating systems. For a good reference check out Mozilla's recommendations.

You'll need to run `a2enmod headers ssl rewrite` for all these to work. You should also set `ServerSignature Off` and `ServerTokens Prod`, typically in /etc/apache2/conf.d/security. For nginx, use `server_tokens off;` so that the webserver doesn't leak extra information.

If you use nginx, you can follow this link and use the configuration example provided by ProPublica.

Warning

Setting the `Referrer-policy` header to `no-referrer` is a strict requirement for inclusion in the SecureDrop directory. Setting the remaining headers as described is strongly recommended, but will be reviewed on a case-by-case basis for inclusion in the directory and does not necessarily prevent the instance from being included.

Set up change detection monitoring for the web application configuration and *Landing Page* content

If possible, you should set up monitoring to detect changes to the *Landing Page* and the configuration files of the web server hosting the page. If you do not have an existing monitoring system for your site, OSSEC is a free and open source host-based intrusion detection suite that includes a file integrity monitor. More information can be found here.

Note

We do not recommmend using the *Monitor Server* to monitor your landing page. It should be used for the *Application Server* only.

Don't log access to the *Landing Page* in the webserver

Here's an Apache example that would exclude the *Landing Page* from logging. However you still need to make sure no other assets get logged!

```
SetEnvIf Request_URI "^/securedrop($|(\/.*))" dontlog
CustomLog logs/access_log common env=!dontlog
```

In nginx, logging can be disabled by adding the following directives within the *Landing Page* `location {}` block:

```
access_log off;
error_log /dev/null;
```

1.44.12 Further Security Considerations

To guard your *Landing Page* against being modified by an attacker and directing sources to a rogue SecureDrop instance, you will need good security practices applying to the machine where it is hosted. Whether it's a VPS in the cloud or dedicated server in your office, you should consider the following:

- Brute force login protection (see fail2ban or sshguard)
- Disable root SSH login
- Use SSH keys instead of passwords
- Use long, random and complex passwords
- Firewall rules to restrict accessible ports (see iptables or ufw)
- AppArmor, grsecurity, SELINUX, modsecurity
- Intrusion and/or integrity monitoring (see Logwatch, OSSEC, Snort, rkhunter, chkrootkit)
- Downtime alerts (Nagios or Pingdom)
- Two-factor authentication (see libpam-google-authenticator, libpam-yubico)

It's preferable for the *Landing Page* to have its own segmented environment instead of hosting it alongside other sites running potentially vulnerable software or content management systems. Check that user and group file permissions are locked down and that modules or gateway interfaces for dynamic scripting languages are not enabled. You don't want any unnecessary code or services running as this increases the attack surface.

1.44.13 How to test your *Landing Page* using Tor Browser

Sources may visit your *Landing Page* using Tor.

Many websites are configured with security measures that only apply when Tor is in use. For example, Tor visitors may be requested to solve a CAPTCHA, may trigger warnings that are specific to some Tor exit nodes, or may be unable to load the page altogether because of Tor-specific DDoS protections.

The effect of such measures cannot be tested without using Tor, and it is a very bad experience for a *source* if visiting a *Landing Page* doesn't work as expected. Because of that, we **recommended strongly** that you test your organization's *Landing Page* using Tor *before* you start advertising it.

You can do so using Tor Browser:

1. Download Tor Browser from the Tor Project website.
2. Ensure the Tor Browser security level is set to “Safest” by clicking on the shield icon. If not, click “Settings…”, then “Change…”, then select “Safest”. Finally, click “Save and restart” to re-launch the browser and apply the new settings.
3. Visit your *Landing Page*.
4. Verify that everything works as expected.
5. Reload the page using a different Tor circuit by clicking on “New Tor Circuit for this Site” in the site information menu (padlock icon in the URL bar) or in the hamburger menu.
6. Verify that everything still works as expected.
7. Repeat the previous two steps several times to test with exit nodes in different countries and regions.

1.45 Getting An Onion Name for Your SecureDrop

1.45.1 What Are Onion Names?

Onion names are short, memorable addresses that visitors can use to access an onion service (e.g., a news organization's SecureDrop) using Tor Browser.

Imagine a SecureDrop instance for a new organization called *The New York World* with a .onion address like this:

sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion

An onion name for this SecureDrop instance could be:

nyworld.securedrop.tor.onion

The general format for a SecureDrop onion name is:

`<organization>.securedrop.tor.onion`

1.45.2 How They Work

Onion names are supported in the desktop version of Tor Browser (introduced in version 9.5). The mapping between onion names and the full-length .onion addresses is done using a custom, signed ruleset for SecureDrop instances maintained by Freedom of the Press Foundation. The ruleset is updated automatically by Tor Browser, and no information is sent to third party servers when contacting a SecureDrop using an onion name.

Onion names are currently not supported by the mobile version of Tor Browser, or by any other browser. (SecureDrop strongly recommends the use of the desktop version of Tor browser.)

The Tor project has committed to continued support of the onion name feature in some form. The underlying implementation and the address format may change in future iterations of this feature. To the extent that any changes are required, we will reach out to coordinate them with you.

1.45.3 Getting An Onion Name

Freedom of the Press Foundation maintains onion names for SecureDrop instances which:

- are using v3 onion services
- are part of the SecureDrop Directory

We will generally approve onion names that meaningfully correspond to your name or that of your organization. Please note that, to disambiguate organizations in different countries with the same name, we may request the addition of a country code (e.g. `<organization>.<country code>.securedrop.tor.onion`).

If your SecureDrop instance is not part of the directory yet, you can *begin the process here*. In order to be eligible for inclusion, your SecureDrop and its associated clearnet landing page must be set up consistent with the best practices recommended in our documentation.

If you are already part of the SecureDrop directory and would like an Onion Name, *please contact us.*

1.45.4 Does This Replace the Original Address?

No, the onion name is only a human-friendly name for the full-length address. The original v3 address can continue to be used like normal, this just gives sources an easier to remember option for accessing your SecureDrop.

We recommend that you list both the onion name and the full v3 address on your landing page. This allows sources to verify both addresses against the information included in our directory, and also provides a fallback should the onion name fail to load for any reason.

Please note that the desktop version of Tor Browser is needed to access onion names, which is also generally our security recommendation.

1.45.5 Updating an Onion Name

If you wish to change or retire your Onion Name, please reach out to the SecureDrop Team. In the event that you wish to completely retire your SecureDrop instance, we recommend that you contact us ahead of time if possible, so we can schedule the Onion Name update on the same day.

In any event, we will attempt to respond to any update request within 2 business days.

1.45.6 Revoking Onion Names

Onion names are tied to inclusion in the SecureDrop Directory. We may remove SecureDrop instances from the directory at our discretion for reasons including but not limited to:

- an instance is stuck on an old software version, and can no longer be considered secure;
- an instance is unreachable for extended periods of time;
- the configuration of an instance or the associated landing page differs substantially from our security recommendations in a manner that may put sources at risk.

Unless the removal is an emergency, we will attempt to offer a substantial grace period prior to the revocation of an onion name, to ensure you can inform your sources about the change to your .onion address.

1.46 Whole Site Changes

Ideally, some or all of the following changes are made to improve the overall security of the path to the *Landing Page* and obfuscate traffic analysis.

1. Make your entire site available through HTTPS.
   - That way, visits to your *Landing Page* won’t stand out as the only encrypted traffic to your site.
2. Include an iframe for all (or a random subset of) visitors, loading this particular URL (hidden).
   - By artificially generating traffic to the endpoint it will be harder to distinguish these from other, ‘real’ requests.
   - Use a random delay for adding the iframe (otherwise the ‘pairing’ with the initial HTTP request may distinguish this traffic).
3. Print the link, URL and info block on the dead trees (the paper), as others have suggested.
4. Add HSTS headers.

1.46.1 Suggested

- For publicly advertised SecureDrop instances display the Source Interface’s Onion Service onion address on all of the organization public pages.
- Mirror Tor Browser and Tails so sources do not have to visit torproject.org to download it.

1.47 Sample SecureDrop Privacy Policy

[DATE]

SecureDrop strives to create a more secure environment for whistleblowers to give information to journalists. It was installed at **[MEDIA ORG]** with the help of Freedom of the Press Foundation.

Please read this privacy policy carefully. It explains what information what type of information SecureDrop does and does not collect, and why.

1.47.1 Collection of Information From Sources

- We don't ask or require you to provide any personally identifying information when you submit materials through SecureDrop.
- The system does not record your IP address, information about your browser, computer, or operating system. Furthermore, the SecureDrop pages do not embed third-party content or deliver persistent cookies to your browser.
- The server will only store the date and time of the newest message sent from each source. Once you send a new message, the time and date of your previous message is automatically deleted.
- Journalists decrypt and read each message offline. They are encouraged to delete messages from the server on a regular basis.
- Please keep in mind that the actual messages you send and receive through SecureDrop may include personally identifying information. For this reason, once you read a journalist's message, we recommend you delete it.

Also please note that when you submit certain types of files through SecureDrop, you may be sending us metadata associated with that file.

For example, if you submit a photo through SecureDrop in JPEG format, the file may include information about the date, time, and the GPS location of where it was taken, and the type of device used to take the photo. Similarly, if you submit a Word file (.doc or .docx) through SecureDrop, it may include the identity of the document's author, the author's operating system, GPS data about the author's location, and the date and time when the document was created.

Our policy is to scrub metadata from the files we receive through SecureDrop before publication. If you don't want to send us metadata, please use the Metadata Anonymization Toolkit to scrub the file before you submit it.

1.47.2 Collection of Information About Journalists' Use of SecureDrop

[MEDIA ORG] collects information about journalists' use of SecureDrop for security monitoring and to make sure the system works properly.

This information we collect about journalists includes details about the device, browser, and operating system journalists use when accessing the system, and the date and time of each session.

We retain these access logs for **[___]** days, and then delete them.

1.47.3 Data Security

[MEDIA ORG] works diligently to protect the identities of our sources and keep the information they give us confidential.

SecureDrop servers are under the physical control of **[MEDIA ORG]** and do not share common elements of the **[MEDIA ORG'S]** other infrastructure.

However, no one can truly guarantee 100% security of any system. Like all software, SecureDrop may contain bugs. Ultimately, you use the SecureDrop service at your own risk.

1.47.4 Children Under 13

The Children's Online Privacy Protection Act restricts our ability to collect personal information from children under 13. This site is not directed to children 12 or younger.

1.47.5 Changes to This Policy

We may revise this Privacy Policy from time to time. The most current version of the policy will govern our collection and use of personal information and will always be at **[LINK]**. If we make changes that we believe are material, we will prominently display a notice on our site **[___]** days before we make those changes.

1.47.6 Contact

[MEDIA ORG] welcomes questions, concerns, and feedback about this policy. If you have suggestions for us, feel free to let us know at **[EMAIL ADDRESS]**.

1.48 Promoting Your SecureDrop Instance

At Freedom of the Press Foundation, we've found news organizations that get the most out of SecureDrop are those who promote it regularly and effectively. SecureDrop will only be used by sources if they know it exists, so it's best to promote its use in a variety of ways so that a wide swath of people will see it.

So here are a few tips used by some of the news outlets that have seen the most success with SecureDrop.

1.48.1 Make a High Profile Announcement

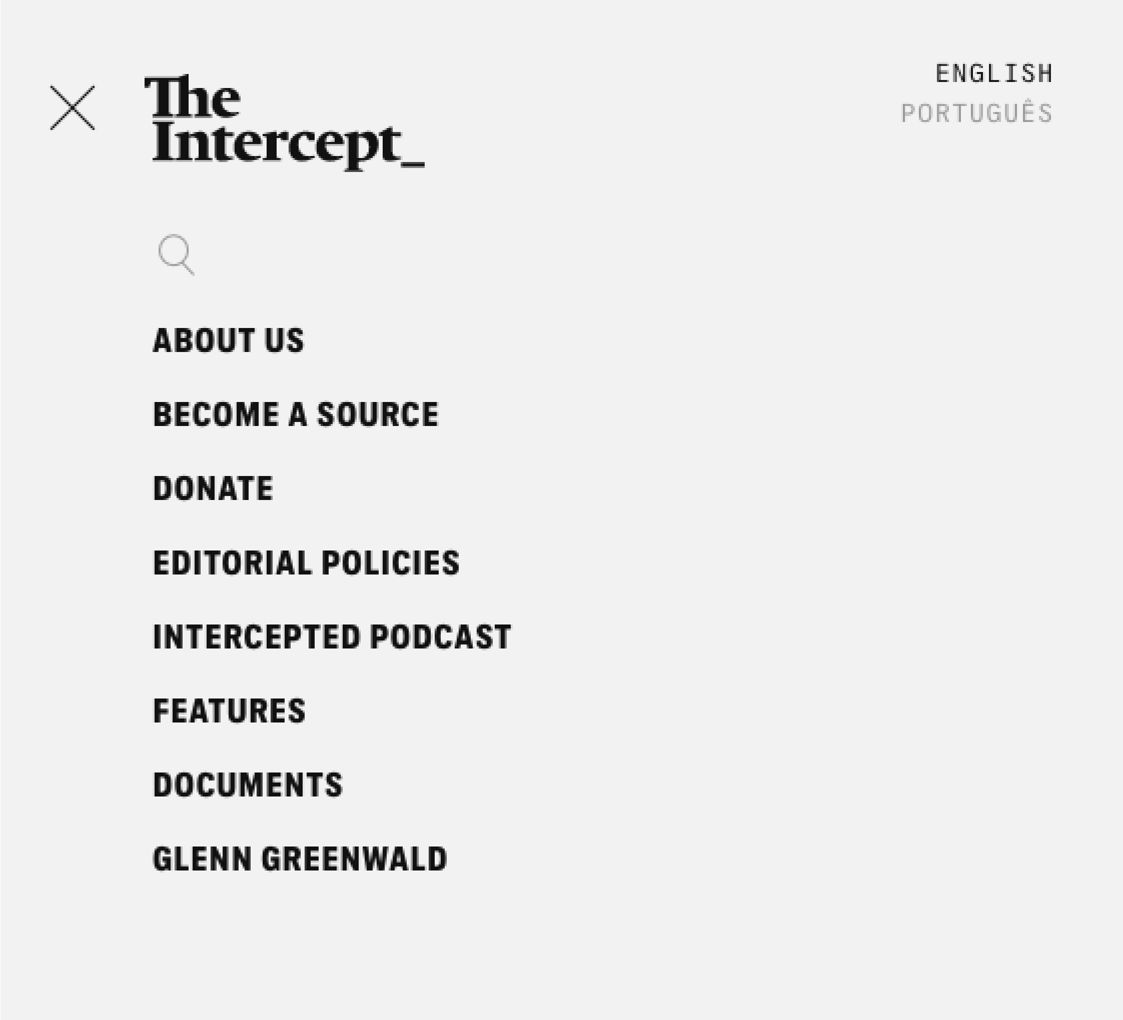
Anytime you launch a SecureDrop, you'll want to write an accompanying news story along with it to alert your readers and potential sources where to submit information. Almost every news organization already does this, but some good recent examples come from USA Today, The Guardian, and Wired. You can also write a companion Q & A like the Washington Post did.

However, a launch announcement is really just a small piece of the puzzle. It's important to regularly remind readers and potential sources that your SecureDrop exists, because only a tiny fraction will likely see the launch announcement and it will quickly be buried in other news after a couple of days.

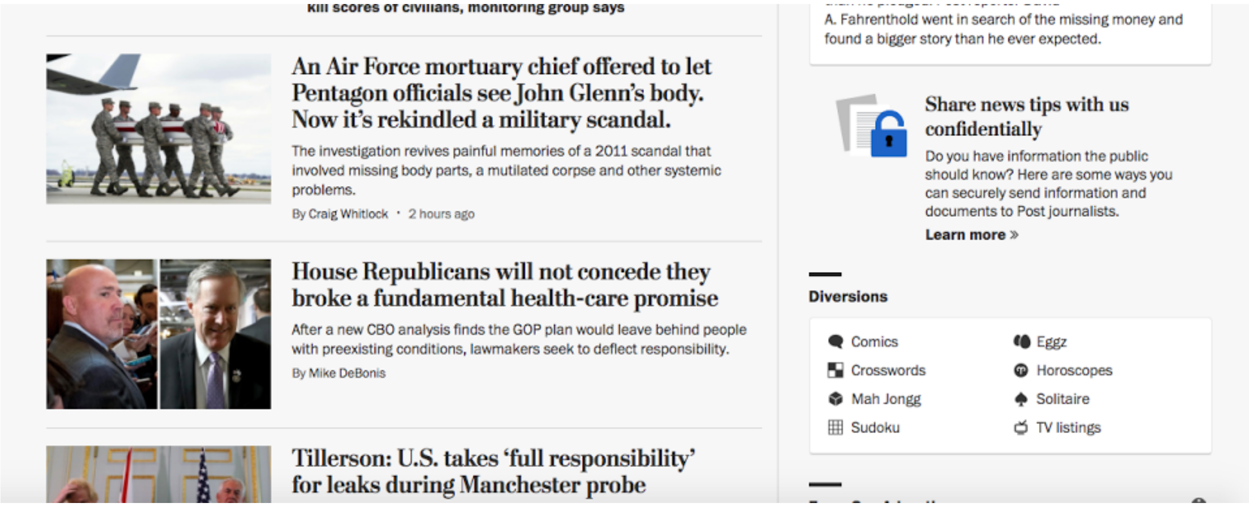
1.48.2 Provide a Clear Link on Your Homepage

Making your SecureDrop or secure tips page easy to find is one of the most important things you can do to ensure that potential sources use it. The best way you can do this is providing a clear link on your home page, so that every time a user goes to your website, they can quickly see where they need to go.

For example, the Intercept has a "become a source" link in its main menu:



The Washington Post has a link on their front page for "how to share a tip securely":


kill scores of civilians, monitoring group says

A. Fahrenthold went in search of the missing money and found a bigger story than he ever expected.

An Air Force mortuary chief offered to let Pentagon officials see John Glenn's body. Now it's rekindled a military scandal.

The investigation revives painful memories of a 2011 scandal that involved missing body parts, a mutilated corpse and other systemic problems.

By Craig Whitlock · 2 hours ago

Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

Learn more »

House Republicans will not concede they broke a fundamental health-care promise

After a new CBO analysis finds the GOP plan would leave behind people with preexisting conditions, lawmakers seek to deflect responsibility.

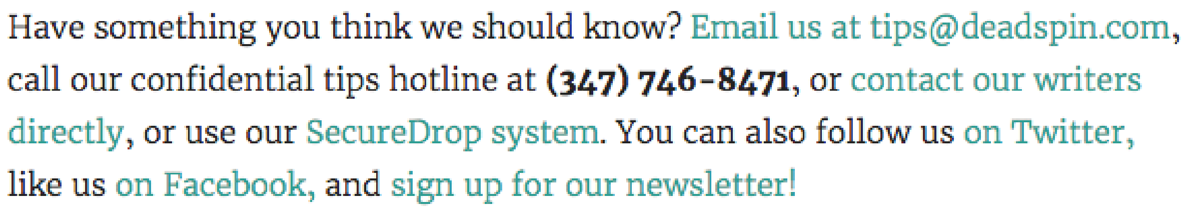
By Mike DeBonis

Tillerson: U.S. takes 'full responsibility' for leaks during Manchester probe

Other news organizations put a little link in their footer, however, we've found that this is not as effective as putting it in a more prominent on your front page.

1.48.3 Provide Links at the Bottom of Your Articles

Another great way to remind potential sources know that they can use SecureDrop is to put a link at the bottom of each article. For example, Gizmodo Media Group, uses a message like this:



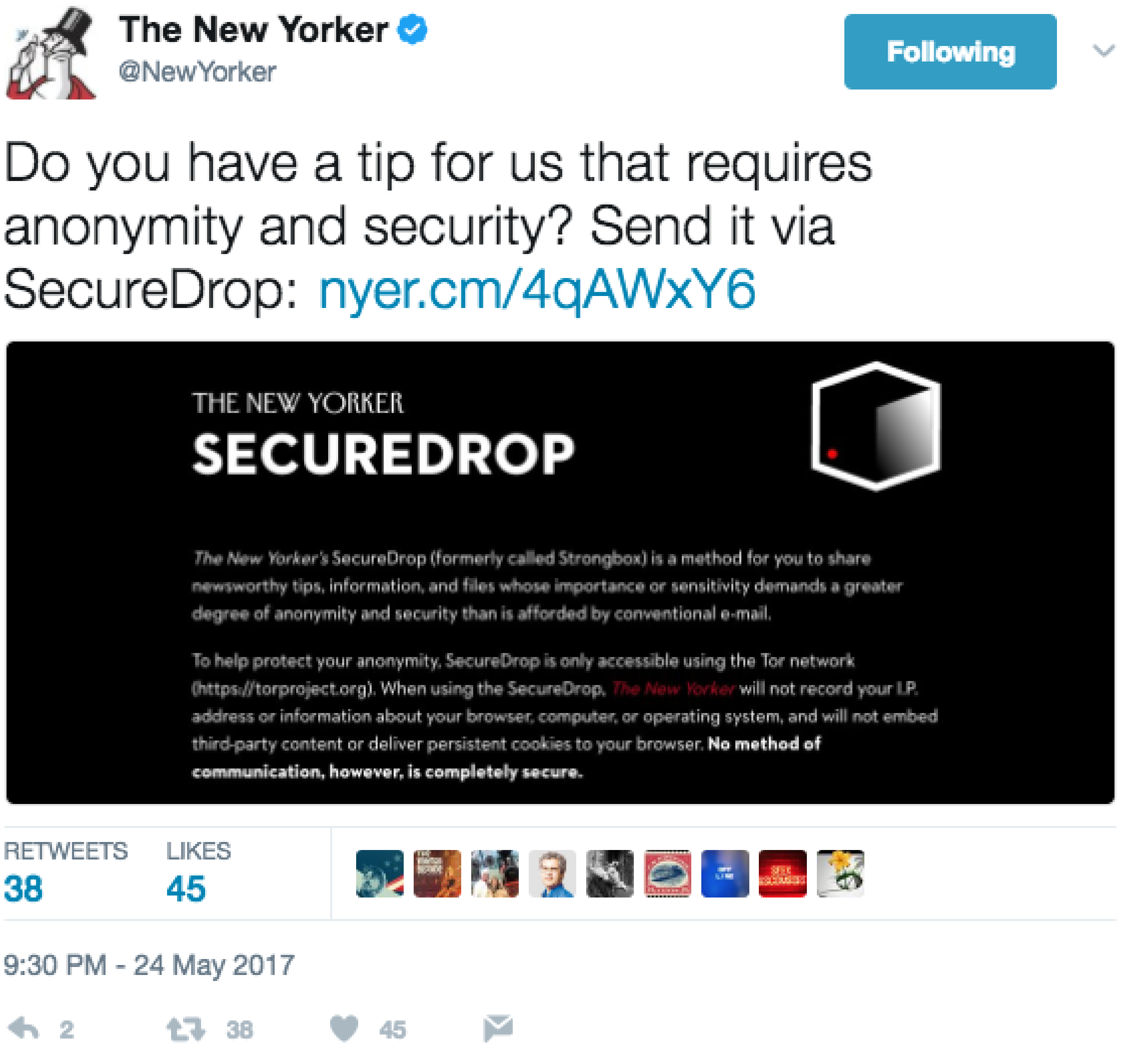
Have something you think we should know? Email us at tips@deadspin.com, call our confidential tips hotline at **(347) 746-8471**, or contact our writers directly, or use our SecureDrop system. You can also follow us on Twitter, like us on Facebook, and sign up for our newsletter!

1.48.4 Create an Instructional Video on How to Access and Use Your SecureDrop

To better help potential sources visualize how SecureDrop works, several organizations have made short instructional videos walking through all the steps. Some good examples include the Toronto Globe and Mail, The Intercept, and Lucy Parsons Labs.

1.48.5 Regularly Share Your SecureDrop *Landing Page* on Social Media

The majority of adults in the United States now get their news from Facebook or other social media sites like Twitter, so it's important to regularly remind people via social media posts that SecureDrop is the safest way they can contact your journalists if they have a sensitive tip to share. If there's specific stories you are looking for tips on that may already be in the news, this is a great way of getting added attention to your SecureDrop.



The New Yorker
@NewYorker

Do you have a tip for us that requires anonymity and security? Send it via SecureDrop: nyer.cm/4qAWxY6

THE NEW YORKER
SECUREDROP

The New Yorker's SecureDrop (formerly called Strongbox) is a method for you to share newsworthy tips, information, and files whose importance or sensitivity demands a greater degree of anonymity and security than is afforded by conventional e-mail.

To help protect your anonymity, SecureDrop is only accessible using the Tor network (https://torproject.org). When using the SecureDrop, *The New Yorker* will not record your I.P. address or information about your browser, computer, or operating system, and will not embed third-party content or deliver persistent cookies to your browser. **No method of communication, however, is completely secure.**

RETWEETS 38 LIKES 45

9:30 PM - 24 May 2017

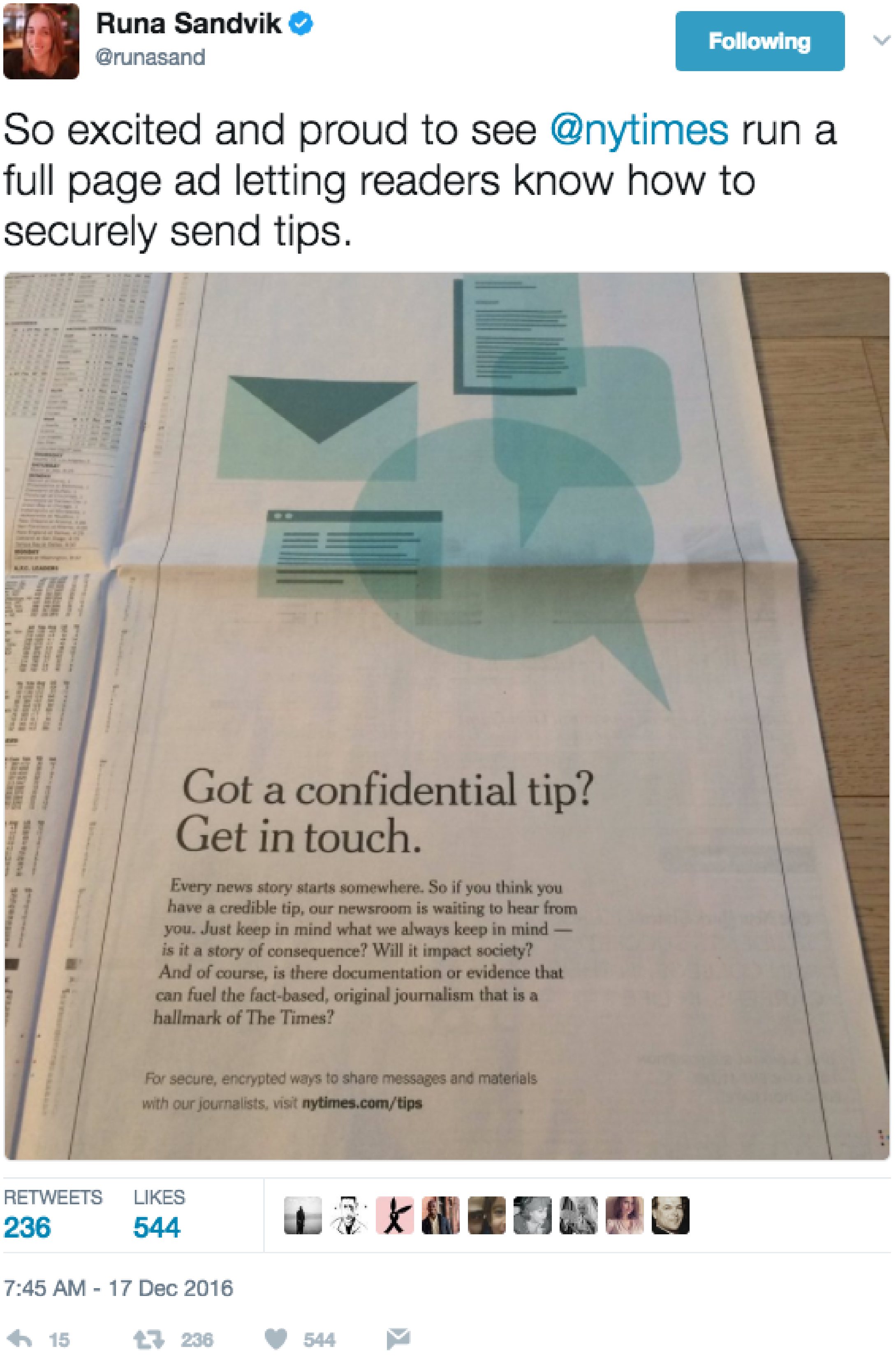
1.48.6 Target Potential Whistleblowers with Advertising

Facebook and Twitter also allow for targeted advertising to users in specific locations, attributes, and sometimes even specific users. For example, Gizmodo Media Group targeted online advertisements for their secure tips page at DC residents imploring them to tell on trump. At Freedom of the Press Foundation, we ran a proof of concept Twitter advertisement aimed at EPA and NOAA employees to show how it can be done. You can read about how you can do the same thing here.

1.48.7 Put an Advertisement in Your Physical Paper

Obviously this tip only applies to news outlets that also print a physical newspaper, but putting an ad or in the paper to tell readers where to go to access SecureDrop can be extremely effective.

The New York Times took out a full page ad in their own paper when they launched SecureDrop and other secure communications tools for their tips line:



Runa Sandvik
@runasand

So excited and proud to see @nytimes run a full page ad letting readers know how to securely send tips.

Got a confidential tip? Get in touch.

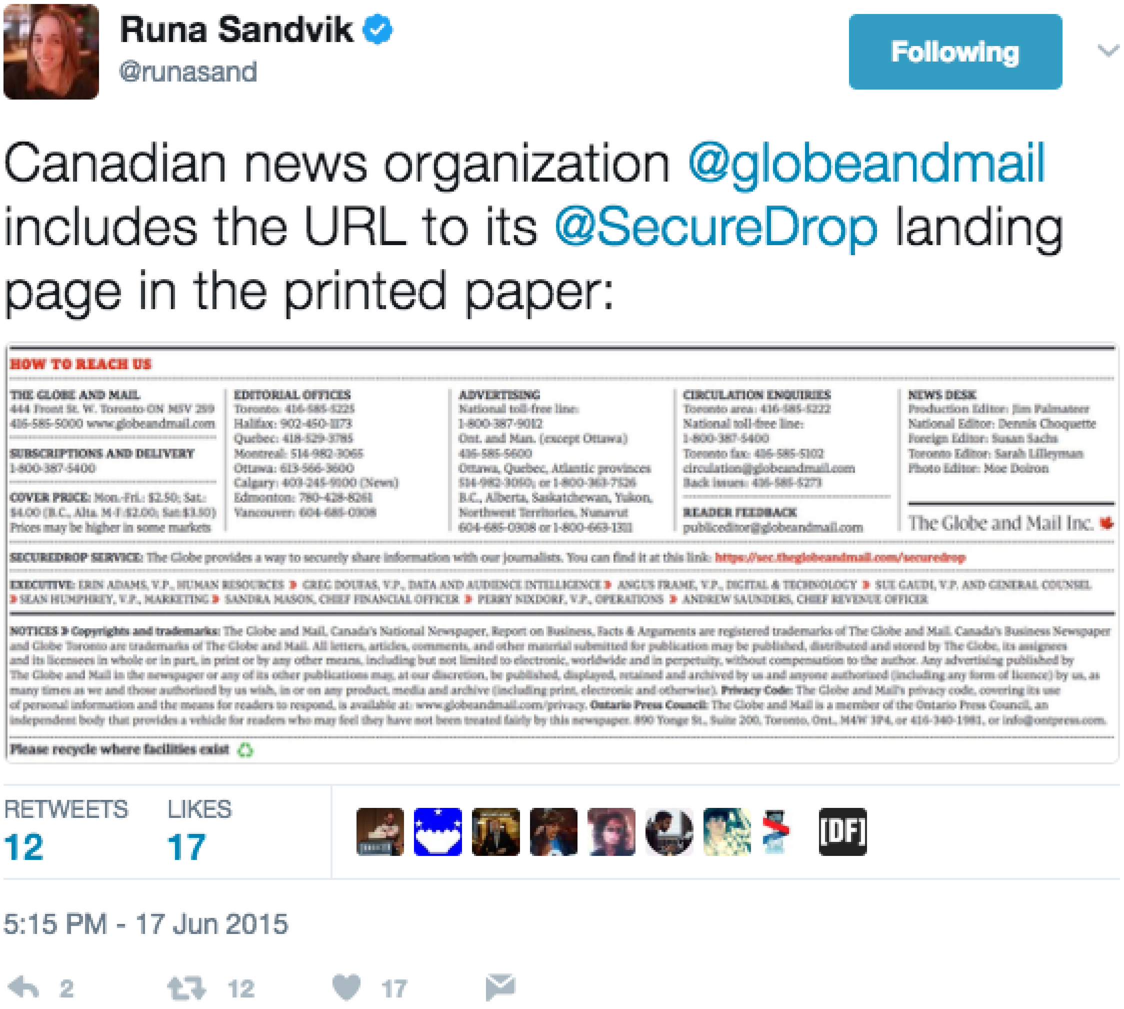
Every news story starts somewhere. So if you think you have a credible tip, our newsroom is waiting to hear from you. Just keep in mind what we always keep in mind — is it a story of consequence? Will it impact society? And of course, is there documentation or evidence that can fuel the fact-based, original journalism that is a hallmark of The Times?

For secure, encrypted ways to share messages and materials with our journalists, visit **nytimes.com/tips**

RETWEETS 236 LIKES 544

7:45 AM - 17 Dec 2016

And the Toronto Globe and Mail regularly puts a note in their physical paper reminding potential sources where they can go:



Runa Sandvik
@runasand

Canadian news organization @globeandmail includes the URL to its @SecureDrop landing page in the printed paper:

HOW TO REACH US

THE GLOBE AND MAIL
444 Front St. W. Toronto ON M5V 2S9
416-585-5000 www.globeandmail.com

SUBSCRIPTIONS AND DELIVERY
1-800-387-5400

COVER PRICE: Mon.-Fri.: $2.50; Sat.: $4.00 (B.C., Alta. M-F:$2.00; Sat:$3.50) Prices may be higher in some markets

EDITORIAL OFFICES
Toronto: 416-585-5225
Halifax: 902-450-1173
Quebec: 418-529-3785
Montreal: 514-982-3065
Ottawa: 613-566-3600
Calgary: 403-245-9100 (News)
Edmonton: 780-428-8261
Vancouver: 604-685-0308

ADVERTISING
National toll-free line:
1-800-387-9012
Ont. and Man. (except Ottawa)
416-585-5600
Ottawa, Quebec, Atlantic provinces
514-982-3050; or 1-800-363-7526
B.C., Alberta, Saskatchewan, Yukon, Northwest Territories, Nunavut
604-685-0308 or 1-800-663-1311

CIRCULATION ENQUIRIES
Toronto area: 416-585-5222
National toll-free line:
1-800-387-5400
Toronto fax: 416-585-5102
circulation@globeandmail.com
Back issues: 416-585-5273

READER FEEDBACK
publiceditor@globeandmail.com

NEWS DESK
Production Editor: Jim Palmateer
National Editor: Dennis Choquette
Foreign Editor: Susan Sachs
Toronto Editor: Sarah Lilleyman
Photo Editor: Moe Doiron

The Globe and Mail Inc.

SECUREDROP SERVICE: The Globe provides a way to securely share information with our journalists. You can find it at this link: https://sec.theglobeandmail.com/securedrop

EXECUTIVE: ERIN ADAMS, V.P., HUMAN RESOURCES ❯ GREG DOUFAS, V.P., DATA AND AUDIENCE INTELLIGENCE ❯ ANGUS FRAME, V.P., DIGITAL & TECHNOLOGY ❯ SUE GAUDI, V.P. AND GENERAL COUNSEL ❯ SEAN HUMPHREY, V.P., MARKETING ❯ SANDRA MASON, CHIEF FINANCIAL OFFICER ❯ PERRY NIXDORF, V.P., OPERATIONS ❯ ANDREW SAUNDERS, CHIEF REVENUE OFFICER

NOTICES ❯ Copyrights and trademarks: The Globe and Mail, Canada's National Newspaper, Report on Business, Facts & Arguments are registered trademarks of The Globe and Mail. Canada's Business Newspaper and Globe Toronto are trademarks of The Globe and Mail. All letters, articles, comments, and other material submitted for publication may be published, distributed and stored by The Globe, its assignees and its licensees in whole or in part, in print or by any other means, including but not limited to electronic, worldwide and in perpetuity, without compensation to the author. Any advertising published by The Globe and Mail in the newspaper or any of its other publications may, at our discretion, be published, displayed, retained and archived by us and anyone authorized (including any form of licence) by us, as many times as we and those authorized by us wish, in or on any product, media and archive (including print, electronic and otherwise). **Privacy Code:** The Globe and Mail's privacy code, covering its use of personal information and the means for readers to respond, is available at: www.globeandmail.com/privacy. **Ontario Press Council:** The Globe and Mail is a member of the Ontario Press Council, an independent body that provides a vehicle for readers who may feel they have not been treated fairly by this newspaper. 890 Yonge St., Suite 200, Toronto, Ont., M4W 3P4, or 416-340-1981, or info@ontpress.com.

Please recycle where facilities exist

RETWEETS 12 LIKES 17

5:15 PM - 17 Jun 2015

1.49 Onboard Journalists

Congratulations! You've successfully installed SecureDrop.

At this point, the only person who has access to the system is the admin. In order to grant access to journalists, you will need to do some additional setup for each individual journalist.

In order to use SecureDrop, each journalist needs two things:

1. A *Journalist Tails USB*.

   The *Journalist Interface* is only accessible as an authenticated onion service. For ease of configuration and security, we require journalists to set up a Tails USB with persistence that they are required to use to access the *Journalist Interface*.

2. Access to the *Secure Viewing Station*.

   The *Journalist Interface* allows journalists to download submissions from sources, but they are encrypted to the offline private key that is stored on the *Secure Viewing Station* Tails USB. In order for the journalist to decrypt and view submissions, they need access to a *Secure Viewing Station*.

1.49.1 Determine Access Protocol for the *Secure Viewing Station*

Currently, SecureDrop only supports encrypting submissions to a single public/private key pair - the *Submission Key*. As a result, each journalist needs a way to access the *Secure Viewing Station* with a Tails USB that includes the *Submission Private Key*.

The access protocol for the *Secure Viewing Station* depends on the structure and distribution of your organization. If your organization is centralized and there are only a few journalists with access to SecureDrop, they should be fine with sharing a single Secure Viewing Station. On the other hand, if your organization is distributed, or if you have a lot of journalists who wish to access SecureDrop concurrently, you will need to provision multiple *Secure Viewing Stations*.

1.49.2 Create a Journalist Tails USB

Each journalist will need a Journalist Tails USB and a *Journalist Workstation*, which is the computer they use to boot their Tails USB.

To create a *Journalist Interface* Tails USB, just follow the same procedure you used to create a Tails USB with persistence for the *Admin Workstation*, as documented in the *Tails Setup Guide*.

Note

As with your *Admin Workstation*, you can use a fresh copy of the blank KeePassXC template in the repository to initialize the password database on the *Journalist Workstation*. You can safely edit this copy to remove sections or fields that are not relevant for the journalist you are onboarding. For example, the admin section of the password database should never be filled in on a *Journalist Workstation*.

Once you're done, boot into the new Journalist Tails USB on the *Journalist Workstation*. Enable persistence and set an admin passphrase before continuing with the next section.

1.49.3 Set Up Automatic Access to the *Journalist Interface*

Since the *Journalist Interface* is an authenticated onion service, you must set up the *Journalist Workstation* to autoconfigure Tor, similarly to the *Admin Workstation*. The procedure is essentially identical, except the SSH configuration will be skipped, since only admins need to access the servers over SSH.

- First, boot into the *Admin Workstation* and copy the following v3 service files to a *Transfer Device*:

  ```
  ~/.config/securedrop-admin/app-sourcev3-ths
  ~/.config/securedrop-admin/app-journalist.auth_private
  ```

  Then, boot into the new *Journalist Workstation* USB.

Warning

Do **not** copy the `app-ssh.auth_private`, `mon-ssh.auth_private`, or `tor_v3_keys.json` files to the *Journalist Workstation*. Those files contain private keys and authentication information for SSH server access. Only the *Admin Workstation* should have shell access to the servers.

- Install the SecureDrop package on the *Journalist Workstation*'s persistent volume, following the documentation to *Download the SecureDrop Repository* and *Install the SecureDrop Package and Dependencies*.
- Copy the files from the *Transfer Device* to `~/.config/securedrop-admin`
- Open a terminal and run the following commands:

```
sudo apt update
securedrop-admin localconfig
```

- Once the `localconfig` command is complete, verify that the *Source* and *Journalist Interfaces* are accessible at their v3 addresses via the SecureDrop Menu.
- Delete the files on the *Transfer Device* by right-clicking them in the file manager, selecting **Move to Trash**, then navigating to **Trash** in the sidebar and selecting **Empty Trash**.

Warning

The `app-journalist.auth_private` file contains secret authentication information for the authenticated onion service used by the *Journalist Interface*, and should not be shared except through the onboarding process.

1.49.4 Add an account on the *Journalist Interface*

Finally, you need to add an account on the *Journalist Interface* so the journalist can log in and access submissions. See the section on *Adding Users* in the admin Guide.

1.49.5 Provision a personal *Transfer Device* and *Export Device*

In small organizations, a team of journalists may want to share a single *Transfer Device* and a single *Export Device*. In larger organizations, you may want to provision a personal *Transfer Device* and *Export Device* for each journalist who may need to copy files off the *Secure Viewing Station*. Please see the *setup guide* for more information.

1.49.6 Verify Journalist Setup

Once the journalist device and account have been provisioned, then the admin should run through the following steps with *each journalist* to verify the journalist is set up for SecureDrop.

The journalist should verify that they:

1. Have their own *Journalist Workstation* USB drive that they are able to boot on the computer designated for this purpose (which can be their everyday laptop).

Note

It is important that they test exactly on the computer they will be using as the *Journalist Workstation*, as there can be differences in Tails compatibility between different laptop models.

2. Verify they are able to decrypt the persistent volume on the *Journalist Workstation*.
3. Ensure that they can connect to and login to the *Journalist Interface*.
4. Ensure that they have a *Transfer Device*, and access to its passphrase.
5. Verify they have access to the *Secure Viewing Station* by plugging in the *Secure Viewing Station* USB drive into the air-gapped computer designated for this purpose, booting, and verifying they can decrypt the persistent volume.

Note

It is especially important to only boot the *Secure Viewing Station* USB drive on the air-gapped computer designated for this purpose.

6. Verify the *Submission Private Key* is present in the *Secure Viewing Station* persistent volume by clicking the clipboard icon 📋 in the top right corner of the Tails desktop and selecting "Manage Keys". When clicking "GnuPG keys" the key should be present.

Tip

The journalist should have all the credentials used in this checklist saved in the KeePassXC database stored in the persistent volume of the *Journalist Workstation*.

7. If you are using a printer, verify that they are able to print a document from the *Secure Viewing Station*. If you are using an *Export Device*, verify that they are able to unlock the encrypted volume.

At this point, the journalist has verified they have the devices and credentials they need and can proceed to a walkthrough of the entire SecureDrop workflow.

1.50 Onboard Additional Admins

If you are the only admin for your SecureDrop, you can skip this chapter. It instructs you how to create additional *Admin Workstation* USB drives. Each *Admin Workstation* will have its own SSH keypair.

This chapter assumes that you have one working *Admin Workstation*. If you've not completed that part of the setup yet, see *Set Up the Admin Workstation*. If your *Admin Workstation* is corrupted or lost, and you don't have a *backup*, see *Rebuilding an Admin Workstation USB*.

Important

If you make configuration changes on your servers using one *Admin Workstation*, they may be overwritten by another *Admin Workstation* if its local copy of the configuration is not identical. When working with multiple admins, it is therefore important to establish protocols for coordinating configuration changes. See *Managing Configuration Updates with Multiple Admins*.

To onboard an additional administrator, you will need:

- your existing *Admin Workstation* USB drive (referred to as **AW1** below)
- an additional empty USB drive (referred to as **AW2** below)

To set up AW2, follow these steps:

1. Boot AW1, unlock its persistent volume, and set an admin password on the welcome screen
2. Ensure that Tails and the SecureDrop version on AW1 are up-to-date. If not, update now by following the *most recent upgrade guide*.
3. **Log into the *Journalist Interface* using your admin credentials, and create**

   a new user account with admin rights. Record its passphrase securely; you will add it to the password manager on AW2 in step 11.

   (You will need to on-board the new admin's 2FA device to complete this step. If this is not possible yet, you can defer it until later.)
4. Insert the empty AW2 USB drive.
5. Launch the Tails Cloner (**Apps** ▶ **Tails** ▶ **Tails Cloner**). Select the option to **Clone the current Tails.** This will delete all data on the AW2 USB drive.
6. Check the box marked **Clone the current Persistent Storage.**

7. Click **Install**.
8. Choose a unique passphrase for the new Persistent Storage Volume on AW2 (a 6-word Diceware passphrase is recommended) and record it securely.
9. Shut down AW1.
10. Boot AW2 and unlock the Persistent Storage.
11. Open the KeePassXC database, delete unneeded credentials from AW1, right-click the **Recycle Bin** item under **Root** in the KeePassXC sidebar, and select **Empty recycle bin**. Then, store the new account credentials you created in step 3.
12. Generate a new keypair on AW2 using the following command:

    `ssh-keygen -t rsa -b 4096`

    When prompted, store the keypair in the default location.
13. Run the command `securedrop-admin localconfig`.

    This will set up the *SecureDrop Menu* and SSH access.
14.
    a. Insert AW1. It should show up in the list of storage devices in the file manager under a label like “7.0 GB Encrypted”. Click the label and enter the drive password when prompted to unlock it.

    b. In a terminal, type the following commands to authorize the newly created SSH keypair on your servers:

    - `ssh-add`
    - `ssh-add /media/amnesia/TailsData/openssh-client/id_rsa`
    - `ssh-copy-id app`
    - `ssh-copy-id mon`
    - `ssh-add -D`

    c. From the file manager (**Apps ▸ Accessories ▸ Files**), eject AW1.
15. Confirm that you are able to access `mon` and `app` via SSH. The following commands should produce the following output:

```
amnesia@amnesia:~$ ssh app hostname
app
amnesia@amnesia:~$ ssh mon hostname
mon
```

16. Confirm that you are able to access the *Source Interface* and the *Journalist Interface* using the *SecureDrop Menu*.
17. *Initialize a passphrase database* on AW2. Store the admin account details using KeePassXC, and other account information this admin will need in the course of administering this system.
18. Shut down AW2.
19. *Back up AW2*.

You can now provide AW2 to the new administrator. Ensure that they store the disk encryption passphrase in a secure manner: in most configurations, it is the only passphrase that is required to SSH into your servers for anyone who obtains access to the USB drive.

The SSH keypair on AW2 is unique to that workstation. When offboarding the administrator, you can manually remove the SSH public key from your admin user’s `~/.ssh/authorized_keys` on `app` and `mon`. Alternatively, if only a single *Admin Workstation* is in active use, you can use the `securedrop-admin reset_admin_access` command to revoke access to all other SSH keys. See our *offboarding guide* for more information.

1.51 Using a YubiKey with the *Journalist Interface*

This guide describes in detail how to set up a YubiKey for two-factor authentication on the *Journalist Interface*. This setup is performed once per journalist to create a secure log-in method. The process requires some configuration steps using a separate software tool.

Note

You will do all of these steps from within the Tails operating system.

1.51.1 What is a YubiKey?

A YubiKey is a physical token used for two-factor authentication. They are made by a company called Yubico and are commercially available. Note that not all physical tokens are compatible with the YubiKey Personalization Tool; for this, you require a key that can support OATH-HOTP.

1.51.2 Download and Launch the YubiKey Personalization Tool

1. Start Tails. At the log in-screen, choose the option to allow an administrator passphrase.
2. Open a terminal and enter

```
sudo apt-get update;
sudo apt-get install yubikey-personalization-gui
```

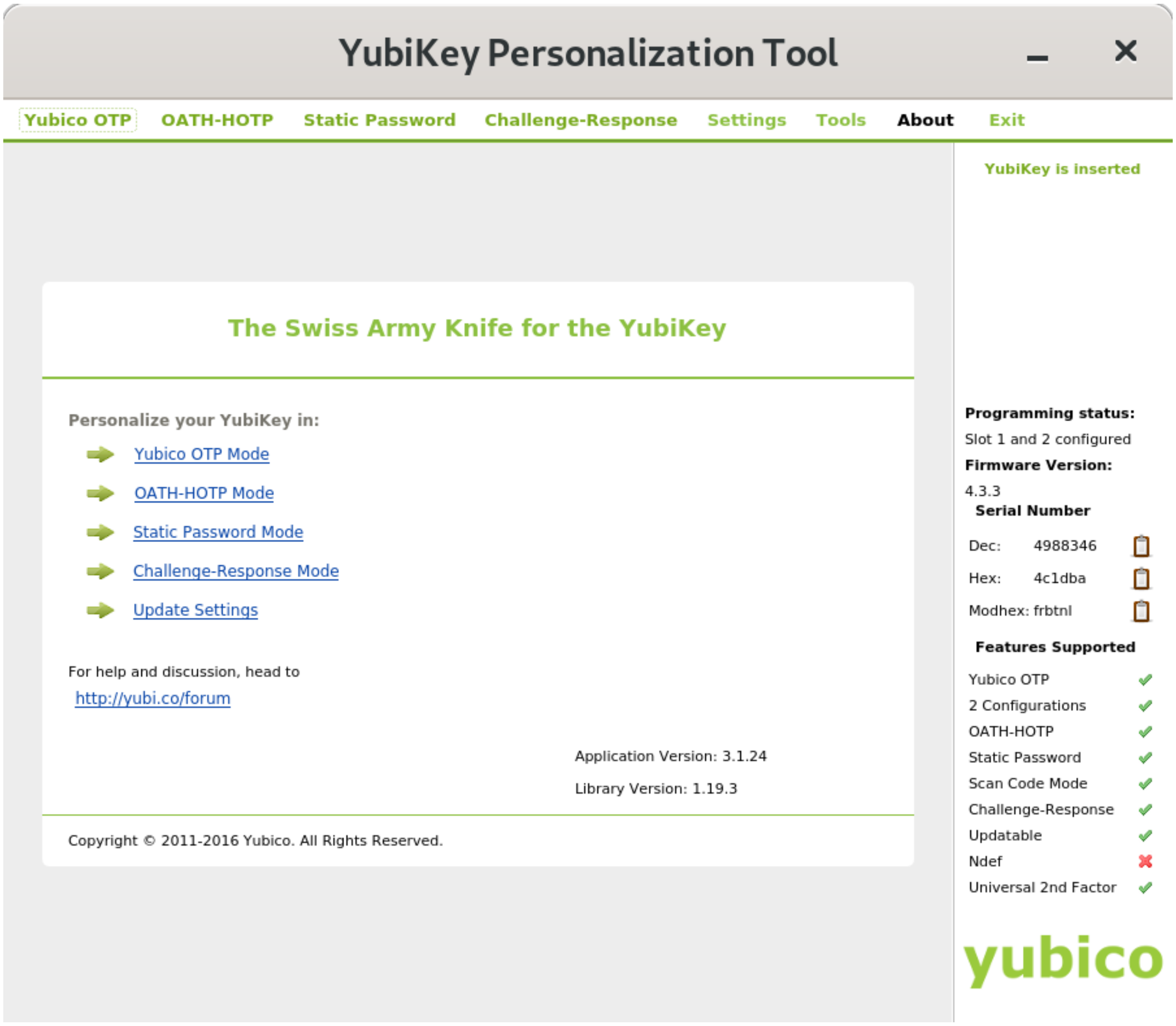
1. Once you have downloaded and installed the personalization program, open a **Root Console** by choosing **Apps ► System Tools ► Root Console**.
2. Open the YubiKey personalization tool by entering

```
yubikey-personalization-gui
```

1.51.3 Setting Up Hardware-Based Codes

After opening the personalization tool, click the heading **OATH-HOTP**. This will bring you to a window called **Program in OATH-HOTP mode**.

Click on the **Quick** button.



The Swiss Army Knife for the YubiKey

Personalize your YubiKey in:

- Yubico OTP Mode
- OATH-HOTP Mode
- Static Password Mode
- Challenge-Response Mode
- Update Settings

For help and discussion, head to http://yubi.co/forum

Application Version: 3.1.24

Library Version: 1.19.3

Copyright © 2011-2016 Yubico. All Rights Reserved.

Programming status:
Slot 1 and 2 configured
Firmware Version:
4.3.3

Serial Number

Dec:	4988346
Hex:	4c1dba
Modhex:	frbtnl

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

Under **Configuration Slot**, click **Configuration Slot 1**.

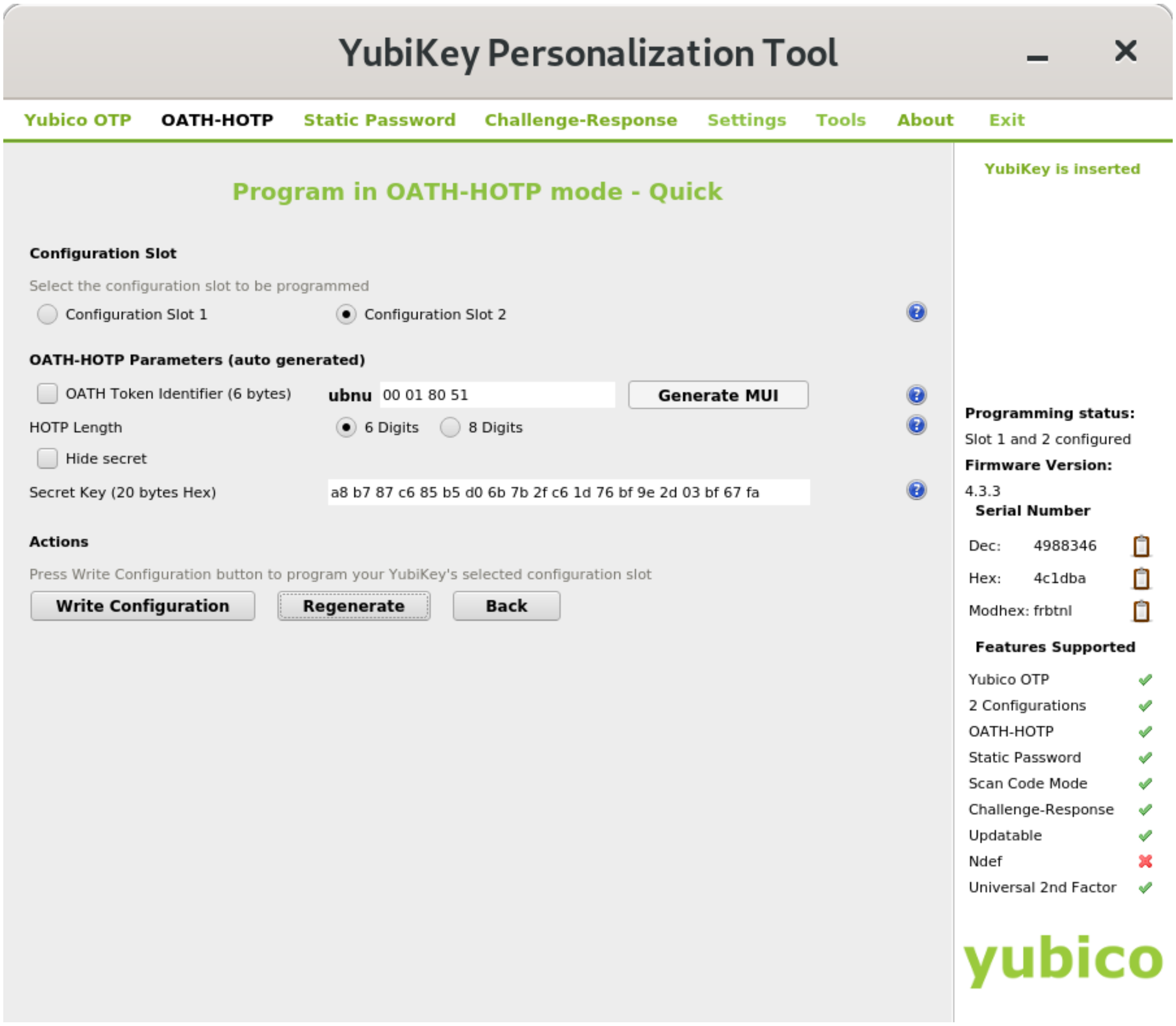
Note

If you are already using this YubiKey for something else, you should choose **Configuration Slot 2**. You will have to press and hold for several seconds to use the token from **Slot 2** instead of the one in **Slot 1**. See the YubiKey manual for more information.

In the section titled **OATH-HOTP parameters**, uncheck the box for **OATH Token Identifier (6 bytes)**. Leave the HOTP length at 6 digits. Next, uncheck the box for **Hide secret**. This will display the **Secret Key (20 bytes Hex)** field.

Important

Make a note somewhere safe of the **Secret Key (20 bytes Hex)** value.



Program in OATH-HOTP mode - Quick

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ● Configuration Slot 2

OATH-HOTP Parameters (auto generated)

□ OATH Token Identifier (6 bytes) **ubnu** 00 01 80 51

HOTP Length ● 6 Digits ○ 8 Digits

□ Hide secret

Secret Key (20 bytes Hex) a8 b7 87 c6 85 b5 d0 6b 7b 2f c6 1d 76 bf 9e 2d 03 bf 67 fa

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

YubiKey is inserted

Programming status:

Slot 1 and 2 configured

Firmware Version:

4.3.3

Serial Number

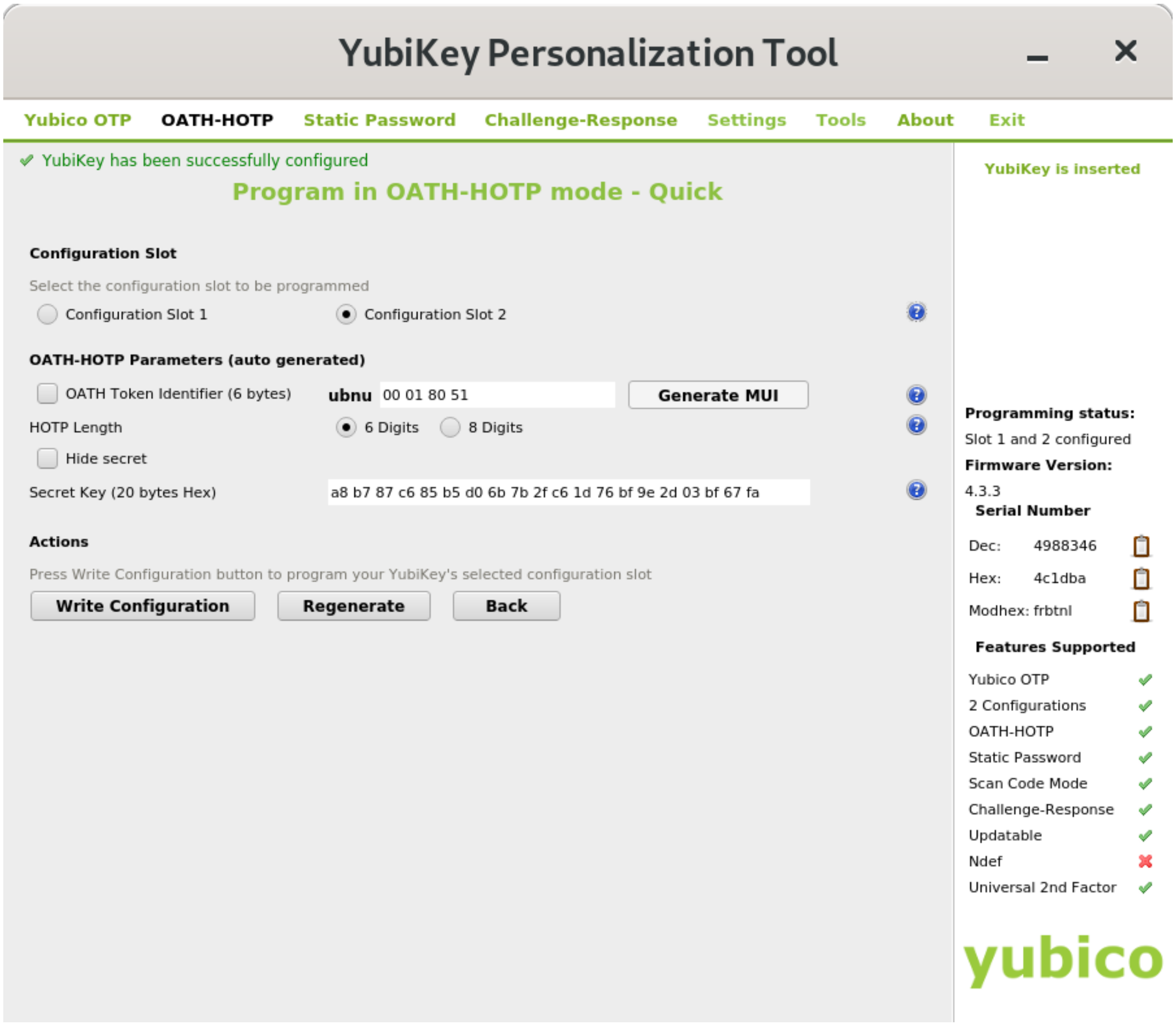
Dec:	4988346
Hex:	4c1dba
Modhex:	frbtnl

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

When ready, click the **Write Configuration** button.

Click through the warning about overwriting the configuration slot and choose a location to save the log file. When the configuration is done, you should see green text saying **YubiKey configured** at the top of the window.



✓ YubiKey has been successfully configured

Program in OATH-HOTP mode - Quick

Configuration Slot

Select the configuration slot to be programmed

○ Configuration Slot 1 ● Configuration Slot 2

OATH-HOTP Parameters (auto generated)

□ OATH Token Identifier (6 bytes) **ubnu** 00 01 80 51

HOTP Length ● 6 Digits ○ 8 Digits

□ Hide secret

Secret Key (20 bytes Hex) a8 b7 87 c6 85 b5 d0 6b 7b 2f c6 1d 76 bf 9e 2d 03 bf 67 fa

Actions

Press Write Configuration button to program your YubiKey's selected configuration slot

YubiKey is inserted

Programming status:
Slot 1 and 2 configured

Firmware Version:
4.3.3

Serial Number

Dec:	4988346
Hex:	4c1dba
Modhex:	frbtnl

Features Supported

Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✓

1.51.4 Adding Users

When adding new users, a SecureDrop admin will need the **Secret Key** value described above. She will enter it after selecting the **I'm Using a YubiKey** option while *adding users*. The new user will then have to verify their YubiKey before being added to the system. This means that the new user and the admin should be physically present for this process.

1.51.5 Using Your YubiKey

When using a Yubikey to log-in to the *Journalist Interface*, insert the Yubikey into the USB port and enter your username and passphrase. Then click the **Two-factor Code** field to focus the cursor there. Quickly press the lighted button on your YubiKey. This will insert the 6-digit code that you will need to log in.

> **Note**
>
> When using **Configuration Slot 2**, be sure to press and hold the YubiKey button for approximately 3 seconds. This can be somewhat finicky.

1.52 Tor Proof-of-Work Defense on the *Source Interface*

The SecureDrop *Source Interface* is served as an onion service with an `.onion` URL, requiring Tor Browser to access it over the Tor network. Tor is sometimes targeted for denial-of-service (DoS) attacks that can slow down the Tor network as a whole as well as burden individual onion services, including SecureDrops.

Tor now includes a proof-of-work (PoW) defense against denial-of-service attacks that can be turned on for individual onion services. As of SecureDrop 2.9.0, new SecureDrops have this feature enabled by default, and we encourage all SecureDrop administrators to turn it on for their instances. While this measure can't speed up the Tor network as a whole if it's slow, it can protect your SecureDrop from being attacked specifically; and more onion services running with this feature helps improve the resilience of the Tor network.

1.52.1 Enabling the proof-of-work defense

If you're *installing SecureDrop for the first time*, the proof-of-work defense will be enabled by default, unless you *explicitly disable it*.

To enable it on an existing SecureDrop instance, on the *Admin Workstation*:

```
securedrop-admin sdconfig
```

The prompts will include:

```
Enable Tor's proof-of-work defense against denial-of-service attacks for the Source␣
↪Interface?: yes
```

Type <Enter> to accept the new default `yes` value. When you finish the prompts, rerun the installation script:

```
securedrop-admin install
```

The Tor configuration will be updated to enable the proof-of-work defense. When the script finishes, confirm that you can access the Source Interface.

1.52.2 Disabling the proof-of-work-defense

Follow the instructions above for *enabling the proof-of-work defense*, but answer `no` at the prompt:

```
Enable Tor's proof-of-work defense against denial-of-service attacks for the Source␣
↪Interface?: no
```

1.53 HTTPS on the *Source Interface*

The SecureDrop *Source Interface* is served as an onion service with an `.onion` URL, requiring Tor Browser to access it. While onion services provide end-to-end encryption by default, as well as strong anonymity, there are several reasons why you might want to consider deploying an additional layer of encryption and authentication via HTTPS:

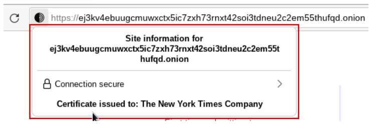
- Extended Validation (EV) certificates, which are currently the only type of certificates that may be issued for `*.onion` addresses, are intended to attest to the identity of the organization running a service. This provides an additional measure of authenticity (in addition to the organization's *Landing Page* and the SecureDrop Directory) to help assure sources that they are communicating with the intended organization when they access a given Source Interface.
- SecureDrop supports v3 onion services, which use updated cryptographic primitives that provide better transport-layer encryption than those used by v2 onion services. Using HTTPS on the source interface will provide an extra layer of encryption for data in transit.

1.53.1 Obtaining an HTTPS certificate for Onion URLs

Digicert

DigiCert is one of only two Certificate Authorities (CA) that issue HTTPS certificates for `.onion` sites. DigiCert requires organizations to follow the Extended Validation (EV) process in order to obtain a certificate for an Onion URL, so you should start by reviewing DigiCert's documentation for obtaining a `.onion` certificate.

The EV certificates display information about an organization under the certificate icon beside the URL bar:



https://ej3kv4ebuugcmuwxctx5ic7zxh73rnxt42soi3tdneu2c2em55thufqd.onion

Site information for
ej3kv4ebuugcmuwxctx5ic7zxh73rnxt42soi3tdneu2c2em55t
hufqd.onion

Connection secure

Certificate issued to: The New York Times Company

Additional information about the organization, such as name and geographic location, are checked by the CA during the EV process. A Source can use this information to confirm the authenticity of a SecureDrop instance, beyond the verification already available in the SecureDrop Directory.

In order to obtain an HTTPS certificate for your SecureDrop instance, contact DigiCert directly. As part of the Extended Validation, you will be required both to confirm your affiliation with the organization, and to demonstrate control over the Onion URL for your Source Interface.

In order for you to demonstrate control over the Onion URL for your Source Interface, you will need to perform a signing operation leveraging the private key of the Onion service used on the Source Interface. DigiCert will provide you with some text and request that you use that text in a signing operation. At a high level, obtaining a certificate from DigiCert involves:

1. Generating an HTTPS keypair and CSR via `openssl`.
2. Submitting the CSR to DigiCert. (This CSR demonstrates control over the private key used for HTTPS.)
3. Scheduling a phone call and verifying your relationship to the organization.
4. Generating another CSR, using a custom tool, leveraging the Onion service private key.
5. Submitting the second CSR to DigiCert. (This CSR demonstrates control over the private key for the onion service.)
6. Downloading the certificate from the DigiCert panel.
7. Installing the cert on the SecureDrop Application Server, via `securedrop-admin`.

For SecureDrop, you should perform these steps on the Admin Workstation. Below are detailed steps for use on Tails:

```
# On the Admin Workstation, generate the first CSR
$ mkdir ~/Persistent/sd-https-key-generation
$ cd ~/Persistent/sd-https-key-generation
$ openssl req -new -newkey rsa:4096 -nodes -keyout sd.key -out sd.csr
```

That command will generate two files: `sd.key`, the private key that will be used by the SecureDrop Application Server; and `sd.csr`, the certificate signing request (CSR), that will be sent to certificate authority in order to receive a certificate. Upload that CSR to the DigiCert website, to begin the request. After passing the EV organization verification, you'll receive an email with a nonce. Use that value to generate the second CSR:

```
# On the Admin Workstation, generate the second CSR
$ source /usr/share/securedrop-admin/venv/bin/activate
$ torify pip install onionmaker
# Copy the Onion service key material to the Admin Workstation:
$ mkdir hsdir
$ ssh app sudo cat /var/lib/tor/services/sourcev3/hostname > hsdir/hostname
```

(continues on next page)

(continued from previous page)

```
$ ssh app sudo cat /var/lib/tor/services/sourcev3/hs_ed25519_public_key > hsdir/hs_
↪ed25519_public_key
$ ssh app sudo cat /var/lib/tor/services/sourcev3/hs_ed25519_secret_key > hsdir/hs_
↪ed25519_secret_key
# Generate (second) CSR
$ onionmaker <nonce> hsdir
```

The CSR will be printed to stdout, starting with `BEGIN CERTIFICATE REQUEST`. Save that CSR, and send it via email reply to DigiCert. After you receive your final certificate, see instructions below for installing the certificate on the SecureDrop Application Server.

Harica

The Greek CA Harica is now providing Domain Validation (DV) certificates for `.onion` addresses. DV certificates are less useful for authentication purposes, but may still be used to provide another layer of encryption for source traffic. The commands provide detail on how to obtain a DV certificate from Harica on the Admin Workstation:

```
# On the Admin Workstation
$ cd ~/
$ git clone --recurse-submodules https://github.com/HARICA-official/onion-csr.git
$ cd onion-csr
$ sudo apt-get update && sudo apt-get install -y ruby-dev rubygems build-essential
# If prompted, choose to install the packages "Only once"
$ torify gem install --user-install ffi
$ gcc -shared -o libed25519.so -fPIC ed25519/src/*.c
# Confirm the binary works by checking that "help" info is displayed:
$ ./onion-csr.rb -h

# Copy the Onion service key material to the Admin Workstation:
$ mkdir hsdir
$ ssh app sudo cat /var/lib/tor/services/sourcev3/hostname > hsdir/hostname
$ ssh app sudo cat /var/lib/tor/services/sourcev3/hs_ed25519_public_key > hsdir/hs_
↪ed25519_public_key
$ ssh app sudo cat /var/lib/tor/services/sourcev3/hs_ed25519_secret_key > hsdir/hs_
↪ed25519_secret_key

# Generate CSR
$ ./onion-csr.rb -n <nonce> -d ./hsdir
```

1.53.2 Activating HTTPS in SecureDrop

Make sure you have *installed SecureDrop already*.

Make note of the Source Interface Onion URL. Now from a Terminal on your *Admin Workstation*:

```
securedrop-admin sdconfig
```

This command will prompt you for the following information:

```
Whether HTTPS should be enabled on Source Interface (requires EV cert): yes
Local filepath to HTTPS certificate (optional, only if using HTTPS on source interface):␣
↪sd.crt
Local filepath to HTTPS certificate key (optional, only if using HTTPS on source␣
```

(continues on next page)

(continued from previous page)

```
↪interface): sd.key
Local filepath to HTTPS certificate chain file (optional, only if using HTTPS on source␣
↪interface): ca.crt
```

The filenames should match the names of the files provided to you by DigiCert, and should be saved inside the `~/.config/securedrop-admin` directory. You'll rerun the configuration scripts:

```
securedrop-admin install
```

The webserver configuration will be updated to apply the HTTPS settings. Confirm that you can access the Source Interface at `https://<onion_url>`, and also that the HTTP URL `http://<onion_url>` redirects automatically to HTTPS.

Note

By default, Tor Browser will send an OCSP request to a Certificate Authority (CA) to check if the Source Interface certificate has been revoked. Fortunately, this occurs through Tor. However, this means that a CA or anyone along the path can learn the time that a Tor user visited the SecureDrop Source Interface. Future versions of SecureDrop will add OCSP stapling support to remove this request. See OCSP discussion for the full discussion.

1.54 SSH Over Local Network

Under a production installation post-install, the default way to gain SSH administrative access is over the Tor network. This provides a number of benefits:

- Allows remote administration outside of the local network.
- Provides anonymity to an administrator while logging into the SecureDrop servers.
- Can mitigate against an attacker on your local network attempting to exploit vulnerabilities against the SSH daemon.

Most administrators will need SSH access during the course of running a SecureDrop instance and a few times a year for maintenance. So the potential shortfalls of having SSH over Tor are not usually a major issue. The cons of having SSH over Tor can include:

- Slow and delayed remote terminal performance
- Allowing SSH access from outside of your local network can be seen as a potential larger security hole for some organizations, particularly those with tight network security controls.

That being said, the default setting of only allowing SSH over Tor is a good fit for most organizations. If you happen to require SSH restricted to the local network instead please continue to read.

1.54.1 Configuring SSH for Local Access

Warning

It is important that your firewall is configured adequately if you decide you need SSH over the local network. The install process locks down access as much as possible with net restrictions, SSH keys, and two-factor authentication. However, you could still leave the interface exposed to unintended users if you did not properly follow our network firewall guide.

Warning

This setting will lock you out of SSH access to your instance if your *Admin Workstation* passes through a NAT in order to get to the SecureDrop servers. If you are unsure whether this is the case, please consult your firewall configuration or network administrator.

Note

Whichever network you install from will be the one that SSH is restricted to post-install. This will come into play particularly if you have multiple network interfaces.

First, make sure your local SecureDrop environment is up-to-date and on the latest production release.

```
sudo apt update
securedrop-admin check_for_update
```

The setting that controls SSH over LAN access is set during the `sdconfig` step of the install. Below is an example of what the prompt will look like. You can answer either ‘no’ or ‘false’ when you are prompted for `Enable SSH over Tor`:

```
securedrop-admin sdconfig

Username for SSH access to the servers: vagrant
Local IPv4 address for the Application Server: 10.0.1.4
Local IPv4 address for the Monitor Server: 10.0.1.5
Hostname for Application Server: app
Hostname for Monitor Server: mon
[...]
Enable SSH over Tor (recommended, disables SSH over LAN). If you respond no, SSH will be␣
↪available over LAN only: no
```

Then you’ll have to run the installation script:

```
securedrop-admin install
```

Note

If you are migrating from a production install previously configured with SSH over Tor, you will be prompted to re-run the `install` portion twice. This is due to the behind the scenes configuration changes being done to switch between Tor and the local network.

Finally, re-configure your *Admin Workstation* as follows:

```
securedrop-admin localconfig
```

Assuming everything is working you should be able to gain SSH access as follows:

```
ssh app
ssh mon
```

1.55 Accessing SecureDrop Remotely

While it's necessary for SecureDrop servers to be hosted on-premise within your organization, and for administrators to retain direct physical access to troubleshoot any potential network-related issues that might arise, there are methods available for both admins and journalists to access the system remotely.

1.55.1 SSH Over Tor

By default, SSH access to SecureDrop servers is routed through the Tor network, allowing you to access the servers using an *Admin Workstation* from anywhere in the world where you have a stable internet connection and are able to access the Tor network.

To do so, simply select the "SSH into the App Server" or "SSH into the Monitor Server" option in the *SecureDrop Menu* from your *Admin Workstation*. Alternately, you can open a Terminal and run either the `ssh app` or `ssh mon` command, depending on which server you are intending to access.

This is useful for routine maintenance and log investigation tasks, although direct physical access will still be necessary for network-related issues, in situations where SSH access is not available.

For more details about the types of tasks that can be completed via SSH, you can *review the SSH portion of our Admin Guide*.

If you'd like to make adjustments to the SSH configuration, or disable SSH access over Tor, you can do so by *following the steps here*.

In addition to remote SSH access, the web-based *Admin Interface* is also available from an *Admin Workstation* from any location with a network connection and access to the Tor network.

1.55.2 Remote *Secure Viewing Station*

Risk Mitigation for Remote *Secure Viewing Stations*

To allow uninterrupted access to SecureDrop for individual journalists, it may be worthwhile to set up a Remote *Secure Viewing Station*.

This may be a good option for organizations with a distributed staff or a strong work-from-home culture, although it's important to weigh the risks and benefits of setting up remote access by adding additional *Secure Viewing Stations* (SVS).

Warning

This increases the risk of the SVS—and its *Submission Key*—being compromised.

If you're considering the use of a remote SVS, here are some steps you can follow to minimize the associated risks:

1. Provide access to the smallest number of people that is reasonable to ensure sufficient coverage. Individuals with access to a *Secure Viewing Station* can triage submissions on behalf of other members of your team. This minimizes the risk that the *Submission Key* falls into the wrong hands.

2. Ensure that journalists have the necessary hardware off-site to access the Journalist Interface and to work with sensitive data. Discourage the use of personal hardware. Provide assistance to journalists to ensure the physical and digital security of sensitive devices and documents.

3. Provision a new *Secure Viewing Station* USB drive. This USB should be on the latest version of Tails, and should contain only the *Submission Key*. Keep an inventory of any provisioned SVS USBs for later decommissioning purposes. Please see below for a step-by-step guide.

4. Provide a secure communications method for SecureDrop users and administrators. The chosen procedure should provide end-to-end encryption and ideally guard against the threat of malware. Please see below for some considerations for sharing files securely.

5. Ensure the physical security of the SecureDrop servers and original SVS while your team works remotely. If the office will be completely unattended, consider storing the original SVS USB with senior staff or legal counsel.

6. Prepare to respond to the loss or compromise of the remote SVS. At a minimum, this would involve *rotating the Submission Key*, which would prevent an adversary from decrypting future submissions using the compromised key.

Necessary Equipment

In order to create a new SVS for remote use, you will need the following:

- An air-gapped computer similar to the computer being used for your current *Secure Viewing Station*. This workstation will be used for provisioning the new SVS USB, and will also be used as part of the remote SVS system.

> **Warning**
>
> Any computer used as an SVS must be air-gapped by removing or physically disabling all networking hardware (including Bluetooth), and by removing or physically disabling speakers and microphones. A computer used as an SVS should never be used for any other purpose.

- The current SVS USB, and its persistent volume's passphrase
- A USB key to act as the new SVS USB

Creating New SVS USB Drives

To create the new SVS USB:

1. Boot into Tails using the primary Tails USB on the air-gapped workstation. When you see the welcome dialog, you can proceed without enabling persistence or setting an admin password.

2. Install Tails on the new SVS USB, following the instructions here.

3. Boot into the new SVS USB and enable persistence with a strong passphrase (a 6-word Diceware passphrase is recommended). In the Persistent volume configuration wizard, be sure to enable persistence for "GnuPG - GnuPG Keyrings and configuration".

4. Temporarily store the persistent volume passphrase in your password manager. You should delete it once you have given the USB and passphrase to the journalist who will be using them.

5. Reboot the new SVS USB with persistence enabled and an administration password set.

6. Plug the current SVS USB into a free port on the workstation.

7. Mount its persistent volume by opening **Apps** ▸ **Accessories** ▸ **Files**, and clicking the USB disk in the left-hand column, and entering its persistent volume's passphrase.

8. Open a terminal via **Apps** ▸ **System Tools** ▸ **Console**

9. Copy the current SVS's GPG keychain (which includes the *Submission Key*) to the new SVS USB using the following command (without linebreaks):

```
sudo bash -c "rsync -a --no-specials --no-devices \
/media/amnesia/TailsData/gnupg/ \
/live/persistence/TailsData_unlocked/gnupg/"
```

10. Eject and remove the current SVS USB.

11. Verify that the *Submission Key* is present with the correct fingerprint on the new SVS USB via **Apps ▶ Accessories ▶ Kleopatra**.

The new SVS should now be ready for use. The journalist that will be checking submissions will need the new SVS USB, its Persistent Volume passphrase, and the air-gapped computer—they should be handed over in a secure manner. They should test the regular decryption workflow using the new SVS as part of the handover process.

Sharing Files and Messages with Other Journalists

If you receive documents via SecureDrop, if possible, avoid sharing or opening these files electronically outside of the *Secure Viewing Station*. Opening documents on your daily-use computer exposes you to the risk that embedded malware and tracking code could exfiltrate information or de-anonymize your sources.

If printing is an option, printing and re-scanning a document is the most effective mitigation against many of these risks.

If you want to transfer files electronically, you can take steps on the *Secure Viewing Station* to mitigate against these risks (e.g., *stripping metadata from files* and converting them to other formats). If you decide to copy files off the *Secure Viewing Station*, we recommend using an encrypted Export Device, as *described here*.

If you want to transfer files to another journalist using your day-to-day work computer, we strongly recommend using end-to-end encrypted communication tools like Signal and Wire, both of which have desktop apps, instead of more common tools like Slack or unencrypted email.

For security reasons, we advise against taking photos of documents using your phone, but if you decide to do so, please see our guide to taking private photos with Signal.

Protecting, Moving, or Taking Down Your SecureDrop Instance

If the location hosting your SecureDrop servers is going to be empty for extended periods of time, you should take steps to ensure the security of your servers and associated hardware:

1. Ensure that the room where the servers are installed is locked by default, and that only authorized personnel have access. If possible, have access logged.
2. If the server room is covered by CCTV, verify that the footage will be monitored or reviewed periodically.
3. Ask to have adjacent corridors included in any regular security patrols.
4. Ask journalists to purge old submissions, to reduce the impact if the servers are compromised (this is good general practice in any case).
5. If your SecureDrop instance is set up to allow SSH-over-LAN admin access, consider switching it to SSH-over-Tor access instead. To do so, you will need to *update the server configuration using the Admin Workstation*.

In some cases, if you are not able to ensure the security of your instance during periods of prolonged absence, it may be better to relocate it, or in extreme circumstances, temporarily take it down. If you decide to take down your SecureDrop instance, we recommend the following steps:

1. Consult with journalists using the system, to ensure that any active sources are aware of the situation, and that source conversations can either be paused or continued via other means.
2. Update your SecureDrop landing page (typically a "send us tips" page, or a page linked from there) to let prospective sources know that the outage is coming, and optionally to redirect them to other contact methods, such as a shared Signal tipline.
3. *Back up your servers* and *your workstation USBs*.
4. Power down the servers, and remove them and the network firewall from the server room. Store the equipment securely offsite.

Warning

By default the SecureDrop servers are not set up with full disk encryption enabled, to allow for hands-off reboots. This means that it is crucial that they be kept secure. If the servers are lost or stolen, an adversary would gain access to all encrypted submissions and messages. While they would not be able to decrypt them, this would still provide valuable metadata about source conversations.

In most cases, restoring the instance, whether in their original hosting location or elsewhere, is a matter of reconnecting the servers to the firewall, attaching a WAN connection that allows unfiltered access to Tor to the firewall WAN port, and powering everything on.

1.56 Setting Up a Printer in Tails

Because Tails is supposed to be as **amnesiac** as possible, you want to shield your Tails stick from any extra inputs from, and outputs to, a potentially untrusted network. This is why **we strongly recommend using a printer that does not have WiFi or Bluetooth**, and connecting to it using a regular USB cable to print.

Finding a printer that works with Tails can be challenging because Tails is based on the Linux operating system, which often has second-class hardware support in comparison to operating systems such as Windows or macOS.

We *maintain a list of printers* that we have personally tested and gotten to work with Tails, in the Hardware guide; if possible, we recommend using one of those printers. The Linux Foundation also maintains the OpenPrinting database, which documents the compatibility, or lack thereof, of numerous printers from almost every manufacturer.

Note

The latest generations of printers might or might not be represented by the OpenPrinting database; also, the database does not document whether or not a printer is wireless, so this will involve manually checking models of interest, if you wish to use this resource as a guide for purchasing a non-wireless printer suitable for use with SecureDrop.

With that in mind, this database is arguably the best resource for researching the compatibility of printers with Linux. As a tip for narrowing down your search, look for printers that are compatible with Debian, or Debian-based distributions like Ubuntu, since Tails itself is also Debian-based. This might increase the chances for a seamless installation experience in Tails.

In any case, this document outlines the usual set of steps that we follow when attempting to use a new printer with Tails.

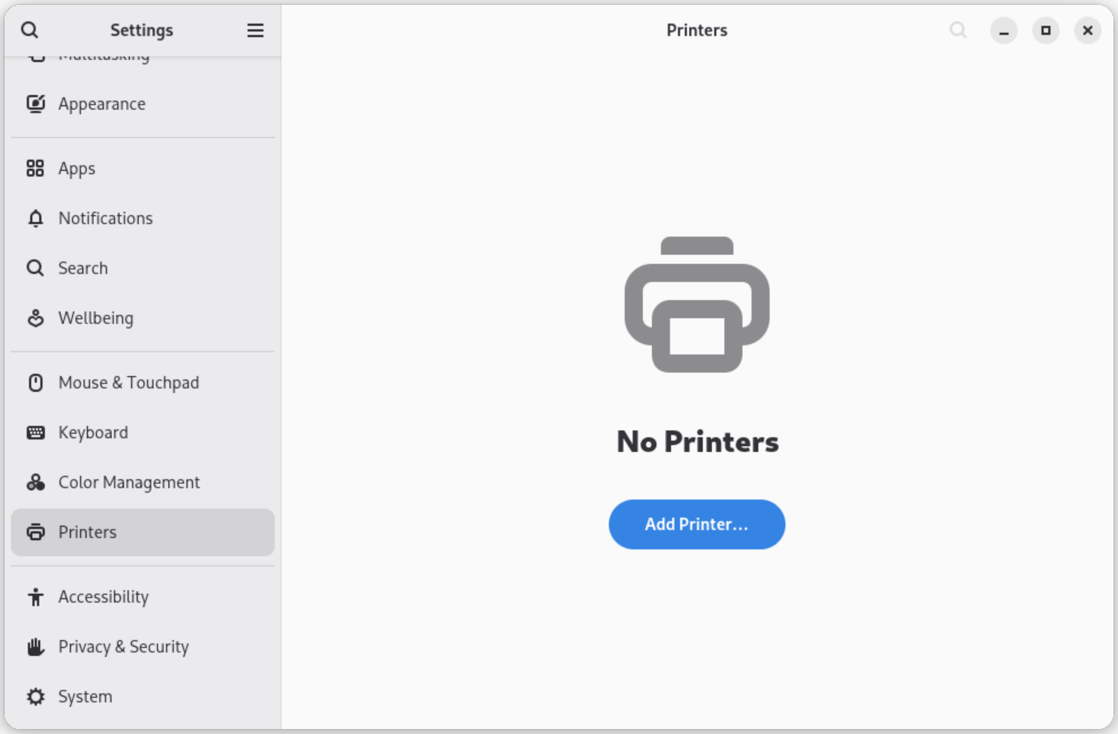
1.56.1 Installing and Printing via the Tails GUI

Let’s look at the flow in Tails 4 for installing a USB-connected printer. On the Tails welcome screen, unlock your persistent volume, and set an admin password. This ensures that you won’t have to reinstall the printer each time you start Tails.

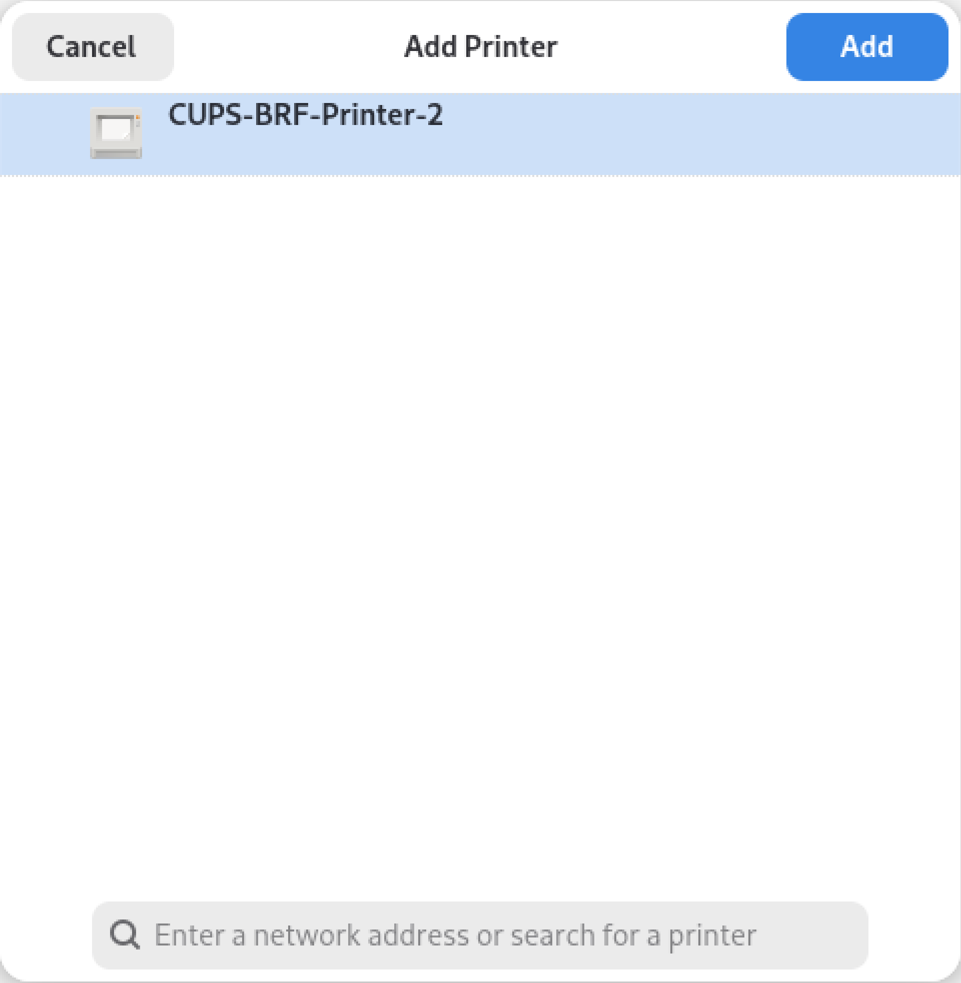
Connect the printer to your Tails-booted computer via USB, then turn the printer on.

Now, you’ll want to single-click your way through **Apps** ► **System Tools** ► **Settings**, then select **Printers**.

If this is the first time you’ve tried to install a printer, the “Printers” section will look like this:

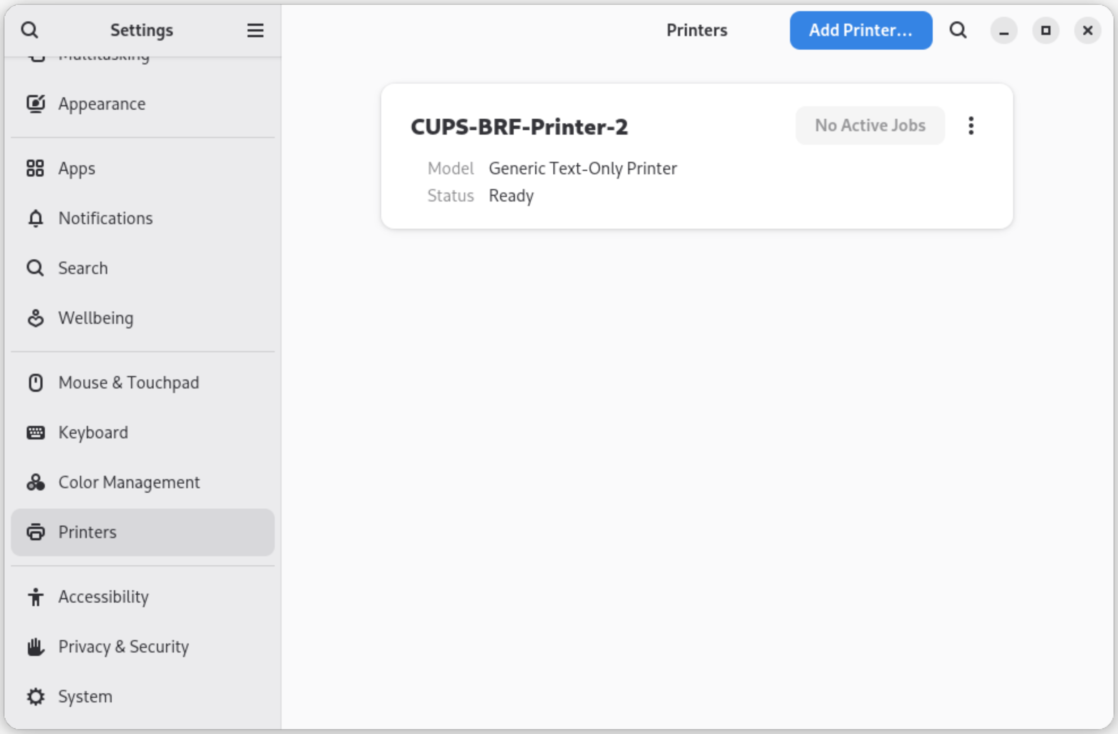


Click **Add a Printer**. After a brief period during which Tails searches for printers, you should see a list of printers that Tails has auto-detected:



In this example we've connected a virtual printer, but the process for adding a real printer is identical. Clicking on the name of your printer in the list will select it for installation. The installation can take a few seconds, during which it looks like nothing is happening.

Assuming you receive no errors in this process, you will then see a screen like the following one, which indicates that the printer is ready for printing.



CUPS-BRF-Printer-2

Model Generic Text-Only Printer

Status Ready

1.56.2 Printing from the Command Line

After you have configured your printer, you can also easily print from the command line using the `lp` command. If you haven't already set your installed printer as default in the GUI, you can quickly do so by adding this line to your `~/.bashrc` file, or entering this directly into the terminal:

```
export PRINTER=Printer-Name-Here
```

If you need to find the name of the printer, you can use `lpstat` to get a list of installed printers, as such:

```
lpstat -a
```

Once you've set your default printer, you can easily print from the terminal by using the following syntax:

```
lp filename.extension
```

While printing from the GUI is much easier, once you've got everything set up, it's equally straightforward from the command line, if you prefer that environment.

1.57 Off-board Administrators and Journalists

When journalists and SecureDrop administrators leave your organization, it is important to off-board them from SecureDrop.

What you need:

- An *Admin Workstation*. *Contact SecureDrop Support* or follow our *guide to rebuilding an Admin Workstation* if you do not have one.
- An admin account on the Journalist Interface

Important

Additional measures may need to be taken if the user's departure is on unfriendly terms. These measures will vary depending on the circumstances and your own internal incident response procedures, and may include doing a full reinstall of SecureDrop. If you are in such a situation, feel free to *contact us* for further assistance.

1.57.1 Off-boarding checklist

- *Inform the SecureDrop Support* team that the user should be removed from any support Signal groups, and indicate if any new staff members should be added.
- Delete the user's account on the *Journalist Interface*.
- Retrieve *Admin Workstation* or *Journalist Workstation* USB drive(s), *Transfer*, *Export*, and *Backup* drive(s), and any other SecureDrop hardware or materials.
- If the user receives email alerts (OSSEC alerts or daily submission notifications), either directly or as a member of an email alias, remove them from those alerts and *set up someone new* to *receive those alerts*.
- (Circumstance-dependent) If you have specific concerns that the *Submission Key* has been compromised, you should consider a full reinstall of SecureDrop. At minimum, you should *rotate the Submission Key*.

1.57.2 Additional steps for off-boarding administrators

- If the departing user was your primary SecureDrop admin, designate the next person who will take over their function. Ideally, your outgoing administrator will be able to provide as much training as possible on the use and maintenance of the system, as well as on your organizational policies (such as backup strategies, and so on) before they leave; if this is not the case, *contact the SecureDrop Support team*.
- We do not recommend enabling remote management for SecureDrop's network firewall. However, if your SecureDrop firewall can be accessed remotely, even if only from within your organization's network, you may want to rotate its login credentials.
- Back up and *rotate the Admin Workstation SSH key* to prevent unauthorized SSH access to the *Application* and *Monitor Servers* in the event that this user has retained their Admin SSH credentials.

Rotate SSH keys on the SecureDrop Servers

If you are concerned that the user may have a copy of the *Admin Workstation* USB or that they may have kept a copy of the *Admin Workstation* SSH key, you should rotate the key in the following manner.

1. Create a new SSH keypair. From an *Admin Workstation*, run

   ```
   ssh-keygen -t rsa -b 4096
   ```

   and make sure to change the key name. This is the only parameter you need to change. For example, instead of `/home/amnesia/.ssh/id_rsa`, call the key `/home/amnesia/.ssh/newkey`. You don't need a passphrase for the key.

2. Copy new public key to the SecureDrop Servers. Copy the public portion of the key to the *Application* and *Monitor Servers* by running

```
scp -O /home/amnesia/.ssh/newkey.pub scp://app
```

and

```
scp -O /home/amnesia/.ssh/newkey.pub scp://mon
```

3. Add this key to the list of authorized keys. SSH to the *Application Server* and append this new key to the list of authorized keys by using

   ```
   cat newkey.pub >> ~/.ssh/authorized_keys
   ```

   Be sure to use the command as above so that you append the key, instead of replacing the file. While you are still on the *Application Server*, you can then delete the file newkey.pub from wherever you scp'd it to (i.e. your home directory). Repeat this process with the *Monitor Server*.

4. Rename SSH keys. Exit all SSH sessions and, on your *Admin Workstation*, rename id_rsa and id_rsa.pub (the old SSH keys) to something else. For example,

   ```
   mv /home/amnesia/.ssh/id_rsa /home/amnesia/.ssh/id_rsa_old
   mv /home/amnesia/.ssh/id_rsa.pub /home/amnesia/.ssh/id_rsa_old.pub
   ```

   Then, rename your newkey and newkey.pub to id_rsa and id_rsa.pub.

5. Test SSH connection. Test that you can still ssh into the *Application and Monitor Servers* (you can test with ssh app host and ssh mon host).

6. Restrict SSH access to the new key.

   > **Important**
   >
   > If you have other users who also have SSH access to the *Application* and *Monitor Servers*, the next step will revoke their access. Their public keys will have to be re-appended to the authorized_keys file on each server, as in step 3.

   From an *Admin Workstation*, run

   ```
   securedrop-admin reset_admin_access
   ```

   This removes all other SSH keys, except for the new key that you are currently using, from the list of authorized keys on the *Application* and *Monitor Servers*.

1.57.3 Rotate the *Submission Key*

The *Submission Private Key* is held on the airgapped *Secure Viewing Station*, and is not normally accessed by SecureDrop users anywhere but on the *SVS*. Therefore, we recommend rotating the *Submission Key* under the following circumstances:

- If the user's departure was not amicable
- If the user is still holding on to any *Secure Viewing Station* USB drive or backup
- If you have any other reason to believe the *Submission Private Key* or the entire *Secure Viewing Station* USB may have been copied or compromised.

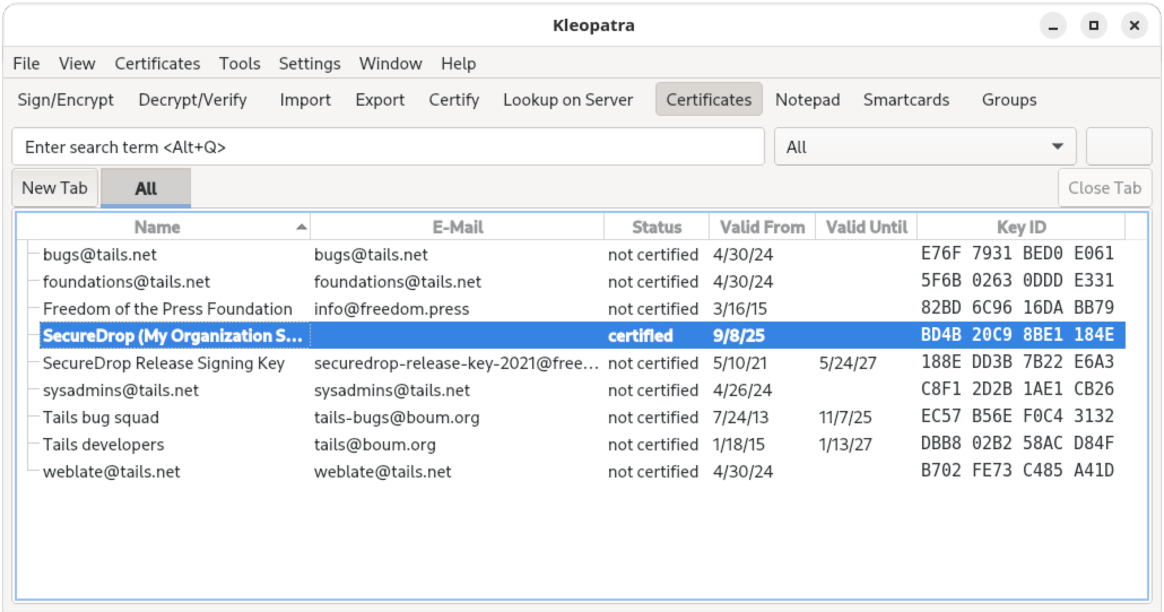
You should still keep the old key on the *Secure Viewing Station*, or else you will not be able to decrypt submissions that were sent to you while that key was in effect.

You will need:

- The *Admin Workstation*
- The *Secure Viewing Station*
- A *Transfer Device* (LUKS-encrypted USB drive)

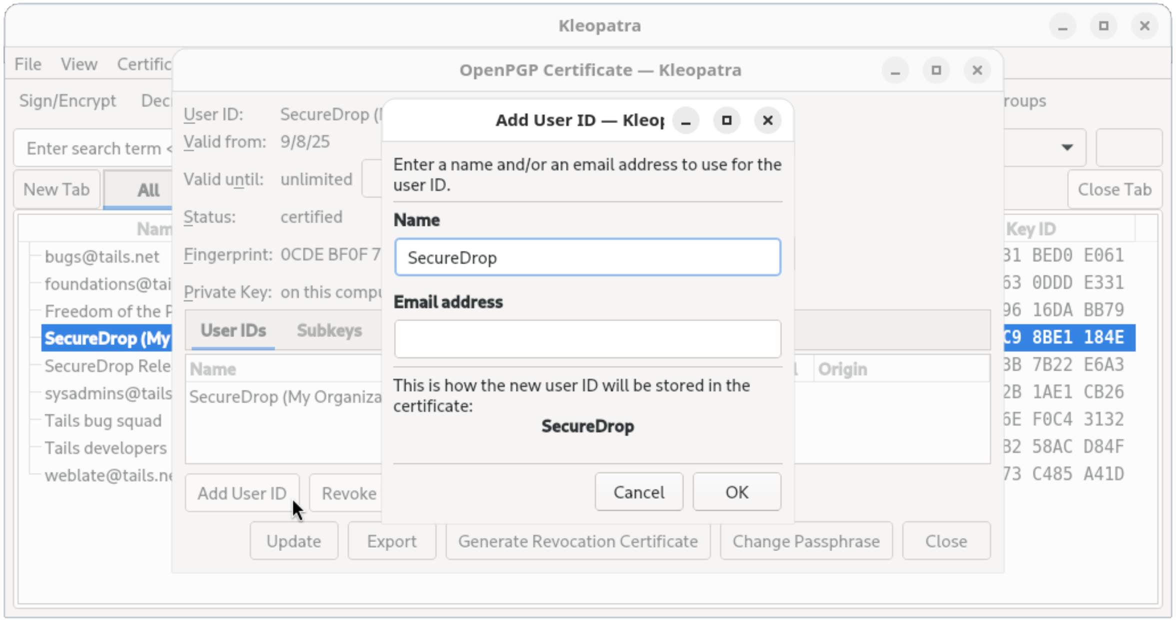
On the Secure Viewing Station

1. From the *Secure Viewing Station* Apps Menu, choose **Accessories ▶ Kleopatra**, and select the *Submission Key* from the list of available keys.


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards Groups
Enter search term <Alt+Q>
All
New Tab
All
Close Tab

Name	E-Mail	Status	Valid From	Valid Until	Key ID
bugs@tails.net	bugs@tails.net	not certified	4/30/24		E76F 7931 BED0 E061
foundations@tails.net	foundations@tails.net	not certified	4/30/24		5F6B 0263 0DDD E331
Freedom of the Press Foundation	info@freedom.press	not certified	3/16/15		82BD 6C96 16DA BB79
SecureDrop (My Organization S...		certified	9/8/25		BD4B 20C9 8BE1 184E
SecureDrop Release Signing Key	securedrop-release-key-2021@free...	not certified	5/10/21	5/24/27	188E DD3B 7B22 E6A3
sysadmins@tails.net	sysadmins@tails.net	not certified	4/26/24		C8F1 2D2B 1AE1 CB26
Tails bug squad	tails-bugs@boum.org	not certified	7/24/13	11/7/25	EC57 B56E F0C4 3132
Tails developers	tails@boum.org	not certified	1/18/15	1/13/27	DBB8 02B2 58AC D84F
weblate@tails.net	weblate@tails.net	not certified	4/30/24		B702 FE73 C485 A41D

2. From the details view that appears, click the **Add User ID** button.



User ID: SecureDrop (

Valid from: 9/8/25

Valid until: unlimited

Status: certified

Fingerprint: 0CDE BF0F 7

Private Key: on this compu

SecureDrop (My Organiza

Enter a name and/or an email address to use for the user ID.

Name

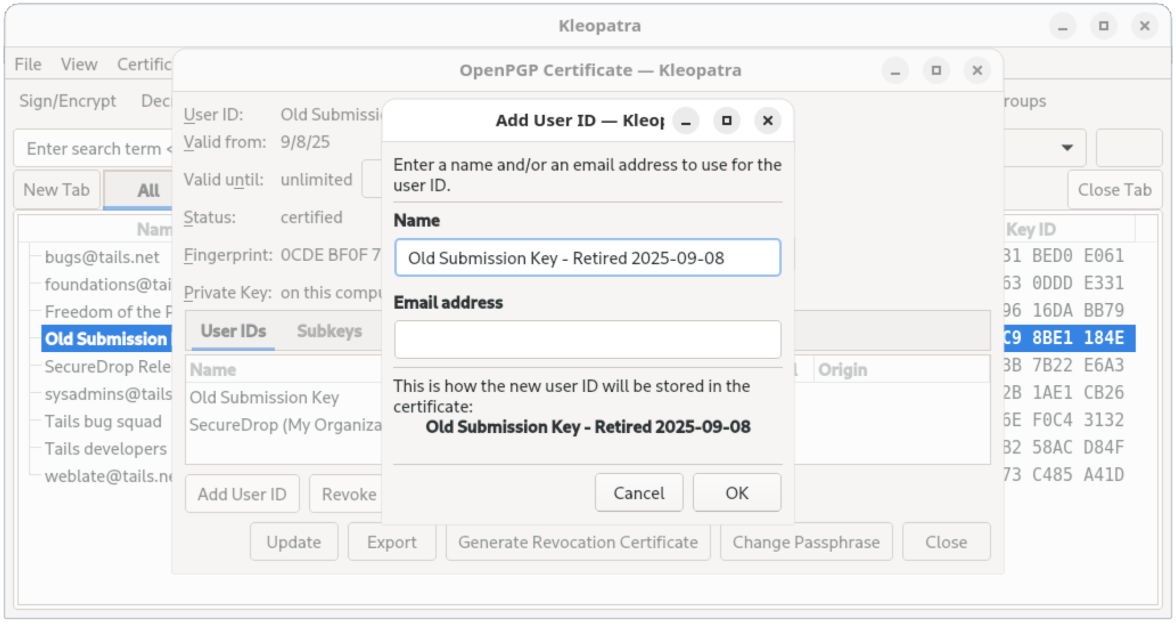
SecureDrop

Email address

This is how the new user ID will be stored in the certificate:

SecureDrop

3. Set the name field to "Old SecureDrop Submission Key - Retired ", and add the date of retirement. Click **OK** to add this information to the key.



Add User ID — Kleopatra

Enter a name and/or an email address to use for the user ID.

Name

Old Submission Key - Retired 2025-09-08

Email address

This is how the new user ID will be stored in the certificate:
Old Submission Key - Retired 2025-09-08

User ID: Old Submissi
Valid from: 9/8/25
Valid until: unlimited
Status: certified
Fingerprint: 0CDE BF0F 7
Private Key: on this compu

Note

This is a local-only change to stop you from mixing up the old and new keys

4. Return to the Terminal, then run:

```
gpg --list-keys
```

In the output, locate the Retired SecureDrop Submission Key. It should look similar to this:

```
pub   rsa4096/0x1CB396626CA370AB 2022-08-16 [SC]
      Key fingerprint = 6A7F 116B 3C22 4F36 7275 236A 1CB3 9662 6CA3 70AB
uid          [ultimate] OLD SecureDrop Submission Key (Retired 2022-08-16)
uid          [ultimate] SecureDrop (SecureDrop Submission Key)
sub   rsa4096/0x228C92459E3D16DE 2022-08-16 [E]
```

Make note of the ID of the key, which is the portion of the key after the slash in the first line. In this example, the key ID would be: `0x1CB396626CA370AB`

5. Generate a revocation certificate, by running the command below (replacing <KEY_ID> with the ID you noted in the step above):

```
gpg --output revoke.asc --gen-revoke <KEY_ID>
```

This will launch an interactive prompt, where you can supply the following values:

```
Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
```

(continues on next page)

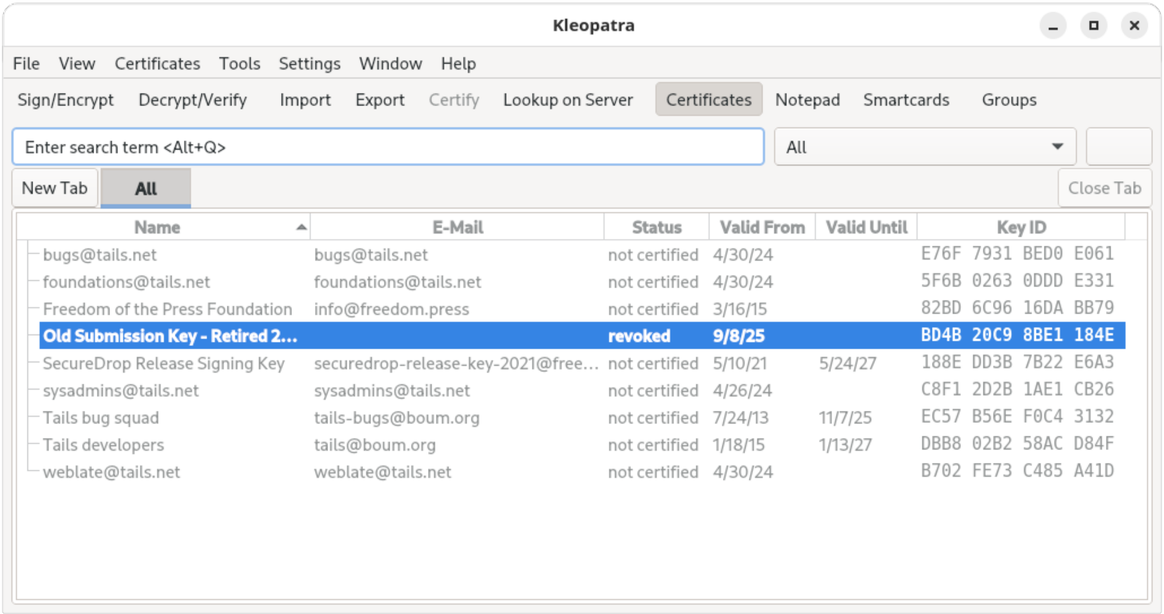
(continued from previous page)

```
(Probably you want to select 1 here)
Your decision? 2
Enter an optional description; end it with an empty line:
> <Just Press Enter>
Reason for revocation: Key is superseded
(No description given)
Is this okay? (y/N) y
ASCII armored output forced.
Revocation certificate created.
```

6. Import the revocation certificate:

```
gpg --import revoke.asc
```

7. Return to Kleopatra, and make sure the key is now marked as **Revoked**.


Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards Groups
Enter search term <Alt+Q>
All
New Tab
All
Close Tab

Name	E-Mail	Status	Valid From	Valid Until	Key ID
bugs@tails.net	bugs@tails.net	not certified	4/30/24		E76F 7931 BED0 E061
foundations@tails.net	foundations@tails.net	not certified	4/30/24		5F6B 0263 0DDD E331
Freedom of the Press Foundation	info@freedom.press	not certified	3/16/15		82BD 6C96 16DA BB79
Old Submission Key - Retired 2...		**revoked**	**9/8/25**		**BD4B 20C9 8BE1 184E**
SecureDrop Release Signing Key	securedrop-release-key-2021@free...	not certified	5/10/21	5/24/27	188E DD3B 7B22 E6A3
sysadmins@tails.net	sysadmins@tails.net	not certified	4/26/24		C8F1 2D2B 1AE1 CB26
Tails bug squad	tails-bugs@boum.org	not certified	7/24/13	11/7/25	EC57 B56E F0C4 3132
Tails developers	tails@boum.org	not certified	1/18/15	1/13/27	DBB8 02B2 58AC D84F
weblate@tails.net	weblate@tails.net	not certified	4/30/24		B702 FE73 C485 A41D

8. Now *follow the instructions* to create a PGP key on the *Secure Viewing Station*. This will be your new *Submission Key*. Copy the fingerprint and new *Submission Public Key* to your *Transfer Device*.

On the Admin Workstation

Important

Ensure that your *Admin Workstation* is *up-to-date* before performing these steps.

1. Take the *Transfer Device* with the new *Submission Public Key* and fingerprint to your *Admin Workstation*. As you did during the initial install, copy the public key, `SecureDrop.asc`, to the `~/.config/securedrop-admin` directory, replacing the existing public key file that is there.

2. From a Terminal, run:

```
securedrop-admin sdconfig
```

If the new public key that you placed in `~/.config/securedrop-admin` has the same name as the old public key, `SecureDrop.asc`, the only part of the configuration you will change is the SecureDrop *Submission Key* fingerprint, which you will update with the fingerprint of your new key.

3. Once you have completed the above, run:

   ```
   securedrop-admin install
   ```

   to push the changes to the server.

   You may want to immediately create a test submission, then use a Journalist account to log into the *Journalist Interface*, download your submission, and take it to the *Secure Viewing Station*.

Return to the Secure Viewing Station

1. On the *Secure Viewing Station,* decrypt the test submission you made to ensure that your new key is working properly.
2. **Do not delete your old submission key!** You'll want to maintain it on the *SVS* so that you can still decrypt old submissions that were made before you changed keys.
3. If you have any other *Admin Workstations*, make sure that you have copied the new *Submission Public Key* into the `~/.config/securedrop-admin` directory, replacing the old public key file, and updated the *Submission Public Key* fingerprint by running

   ```
   securedrop-admin sdconfig
   ```

   and updating the fingerprint when prompted. You do not have to run `securedrop-admin install` again, since you have already pushed the changes to the server.

1.57.4 Getting Support

If you have any questions about the steps in this guide, we're here to help:

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.58 Investigating Logs

When troubleshooting issues with your SecureDrop instance, be sure to examine all relevant log files on both servers. To work with logs, it is helpful to be familiar with commands like `less`, `tail` and `grep`; to inspect older, archived logs (names end with `.gz`) you can use commands like `zless` and `zgrep` to avoid manually decompressing each file.

Note

You can use the `securedrop-admin` tool to extract logs to send to Freedom of the Press Foundation for analysis. Run the following command on your *Admin Workstation*:

```
securedrop-admin logs
```

This command will produce encrypted tarballs containing logs from each server. See the command output for more information.

1.58.1 Logs to examine on both servers

- /var/log/kern.log: Use this file to investigate kernel-related issues, including warnings or errors specific to AppArmor or grsecurity (a set of patches applied to the kernels for additional security hardening)
- /var/log/syslog: Use this file to investigate most other system issues, including iptables configuration problems or Tor network issues. Use search patterns, e.g., search for "app Tor" to find log entries specific to Tor.

1.58.2 *Application Server* Logs

See the directory /var/log/apache2/* for web server access and error logs. In production systems, logging is only enabled for the *Journalist Interface* to the files journalist-access.log and journalist-error.log, and the logs do not contain IP address information.

When investigating an application error on the *Source Interface* (e.g., if you see an "Internal Server Error" when submitting a document), it can make sense to temporarily enable error logging. To do so:

1. Log into your *Application Server* from your *Admin Workstation* via ssh app
2. Edit the file /etc/apache2/sites-enabled/source.conf (requires sudo)
3. Comment out the old ErrorLog and LogLevel directives, e.g., like so:

```
# Enabling logging for error investigation, 2020-04-18, ~admin
#
# ErrorLog /dev/null
# LogLevel critical
```

4. Add the desired new logging configuration in the same location (inside the <VirtualHost> block), e.g.:

```
ErrorLog /var/log/apache2/source-error.log
LogLevel debug
```

5. Save the file and reload the configuration with sudo systemctl reload apache2
6. Visit the Source Interface and reproduce the error
7. Inspect the log file /var/log/apache2/source-error.log for any details
8. Remember to set the configuration back to the default values once your investigation is complete.

Note that the debug logging level is highly verbose; if you want to adjust it, see the Apache documentation for more information about the different logging levels.

If you encounter an application error, and you have not modified the application code, please be sure to file an issue or contact us via securedrop@freedom.press (GPG encrypted).

1.58.3 *Monitor Server* Logs

- /var/ossec/logs/ossec.log: Examine this file to investigate problems with OSSEC itself not functioning as expected (e.g., you are not seeing alerts when you would expect them to).
- /var/ossec/logs/alerts/alerts.log: This file contains the most recent alerts generated by OSSEC. If you have correctly configured OSSEC emails, the text of these alerts should correspond to the text of the emails.
- /var/log/mail.log and /var/log/procmail.log: These files contain information about email delivery and email processing (for encrypting the alerts). Investigate these files if you believe OSSEC is correctly configured, but you are not receiving emails.

1.59 OSSEC Guide

1.59.1 Setting up OSSEC alerts

OSSEC is an open source host-based intrusion detection system (IDS) that SecureDrop uses to perform log analysis, file integrity checking, policy monitoring, rootkit detection, and real-time alerting. It is installed on the *Monitor Server* and constitutes that machine's main function. OSSEC works in a server-agent scheme; that is, the OSSEC server extends its existing functions to the *Application Server* through an agent installed on that server, covering monitoring for both machines.

In order to receive email alerts from OSSEC, you need to supply several settings to Ansible in the playbook for your environment. If you don't already have a working mail server or don't know what to do, then see the section below about using Gmail as a fallback option. We assume that you're working out of the 'securedrop' directory you cloned the code into, and that this configuration is happening prior to installing SecureDrop.

Receiving email alerts from OSSEC requires that you have an SMTP relay to route the emails. You can use an SMTP relay hosted internally, if one is available to you, or you can use a third-party SMTP relay such as Gmail. The SMTP relay does not have to be on the same domain as the destination email address, i.e. smtp.gmail.com can be the SMTP relay and the destination address can be securedrop@freedom.press.

What you need:

- The *OSSEC Alert Public Key* and its fingerprint
- The email address that will receive alerts from OSSEC
- The reachable hostname of your SMTP relay
- The secure SMTP port of your SMTP relay (typically 25, 587, or 465; must support TLS encryption)
- An email username to authenticate to the SMTP relay
- The domain name of the email used to send OSSEC alerts
- The password of the email used to send OSSEC alerts

While there are risks involved with receiving these alerts, such as information leakage through metadata, we feel the benefit of knowing how the SecureDrop servers are functioning is worth it. If a third-party SMTP relay is used, that relay will be able to learn information such as the IP address the alerts were sent from, the subject of the alerts, and the destination email address the alerts were sent to. Only the body of an alert email is encrypted with the recipient's GPG key. A third-party SMTP relay could also prevent you from receiving any or specific alerts.

The SMTP relay that you use should support SASL authentication and SMTP TLS protocols TLSv1.2, TLSv1.1, and TLSv1. Most enterprise email solutions should be able to meet those requirements.

These values must be set in the *configuration playbook* by running the `securedrop-admin sdconfig` command, which will prompt for each of the items listed above. Please note, this command updates the configuration, but does not apply it to the servers. Any time you make changes to the configuration it is necessary to deploy them with the `securedrop-admin install` command.

If you don't know what value to enter for one of these, please ask your organization's email admin for the full configuration before proceeding. It is better to get these right the first time rather than changing them after SecureDrop is installed. If you're not sure of the correct SMTP relay port number, you can use a simple mail client such as Thunderbird to test different settings or a port scanning tool such as nmap to see what's open. You could also use telnet to make sure you can connect to an SMTP server, which will always transmit a reply code of 220 meaning "Service ready" upon a successful connection.

The SMTP relay mail server hostname is often, but not always, different from the SASL domain, e.g. smtp.gmail.com and gmail.com.

In some cases, authentication or transport encryption mechanisms will vary and you may require later edits to the Postfix configuration (mainly /etc/postfix/main.cf) on the *Monitor Server* in order to get alerts to work. You can consult

Postfix's official documentation for help, although we've described some common scenarios in the *troubleshooting section*.

If you have your *OSSEC Alert Public Key* public key handy, copy it to `~/.config/securedrop-admin` and then specify the filename, e.g. `ossec.pub`, when prompted by `securedrop-admin sdconfig`.

If you don't have your GPG key ready, you can run GnuPG on the command line in order to find, import, and export your public key. It's best to copy the key from a trusted and verified source, but you can also request it from keyservers using the known fingerprint. Looking it up by email address or a shorter key ID format could cause you to obtain a wrong, malicious, or expired key. Instead, we recommend you type out your fingerprint in groups of four (just like GPG prints it) enclosed by double quotes. The reason we suggest this formatting for the fingerprint is simply because it's easiest to type and verify correctly. In the code below simply replace `<fingerprint>` with your full, space-separated fingerprint:

Download your key and import it into the local keyring:

```
gpg --recv-key "<fingerprint>"
```

Note

It is important you type this out correctly. If you are not copy-pasting this command, we recommend you double-check you have entered it correctly before pressing enter.

Again, when passing the full public key fingerprint to the `--recv-key` command, GPG will implicitly verify that the fingerprint of the key received matches the argument passed.

Caution

If GPG warns you that the fingerprint of the key received does not match the one requested **do not** proceed with the installation. If this happens, please email us at securedrop@freedom.press.

Next we export the key to a local file.

```
gpg --export -a "<fingerprint>" > ossec.pub
```

Copy the key to a directory where it's accessible by the SecureDrop installation:

```
cp ossec.pub ~/.config/securedrop-admin/
```

The fingerprint is a unique identifier for an encryption (public) key. The short and long key ids correspond to the last 8 and 16 hexadecimal digits of the fingerprint, respectively, and are thus a subset of the fingerprint. The full fingerprint must be the entire 40 hexadecimal digit GPG fingerprint for this same key, with all capital letters and no spaces. The following command will retrieve and format the fingerprint per our requirements:

```
gpg --with-colons --fingerprint "<fingerprint>" | grep "^fpr" | cut -d: -f10
```

Next you must specify the e-mail that you'll be using to receive alerts. This could be your work email, or an alias for a group of IT admins at your organization. It helps for your mail client to have the ability to filter the numerous messages from OSSEC into a separate folder.

Now you can move on to the SMTP and SASL settings, which are straightforward. These correspond to the outgoing e-mail address used to send the alerts instead of where you're receiving them. If that e-mail is ossec@news-org.com, the SASL Username would be OSSEC and the SASL Domain would be news-org.com.

After setting those values, securedrop-admin sdconfig will exit and return you to the command line. In most cases, you will then be ready to *proceed with the installation*.

The Postfix configuration enforces certificate verification, and requires both a valid certificate and STARTTLS support on the SMTP relay. By default the system CAs will be used for validating the relay certificate. If you need to provide a custom CA to perform the validation, copy the cert file to ~/.config/securedrop-admin add a new variable to ~/.config/securedrop-admin/site-specific:

```
smtp_relay_cert_override_file: MyOrg.crt
```

where MyOrg.crt is the filename. The file will be copied to the server in /etc/ssl/certs_local and the system CAs will be ignored when validating the SMTP relay TLS certificate. Be sure to save ~/.config/securedrop-admin/site-specific when you are finished.

Using Gmail for OSSEC alerts

It's easy to get SecureDrop to use Google's servers to deliver the alerts, but it's not ideal from a security perspective. This option should be regarded as a backup plan. Keep in mind that you're leaking metadata about the timing of alerts to a third party — the alerts are encrypted and only readable to you, however that timing may prove useful to an attacker.

First you should sign up for a new account. While it's technically possible to use an existing Gmail account, it's best to compartmentalize these alerts from any of your other activities. Choose a strong and random passphrase for the new account.

Next, enable Google's 2-Step Verification. This is required in order to use SMTP with a username and password, which is needed for SecureDrop.

After enabling 2-Step Verification, you'll then need to generate a new app password to use exclusively with SecureDrop. To do so, open the app password settings. From there, click "Select App", choose "Custom", assign it a name (such as "SecureDrop"), then click "Generate."

This will provide you with a 16-character password that you will need to use for the SMTP settings to enable OSSEC alerts.

> **Tip**
>
> SMTP through Gmail will only work with a generated app password. The password for the Gmail account itself is not sufficient, and will not allow mail to be sent. In order to be able to create an app password, you must have 2-Step Verification enabled on the Gmail account.

Once the account is created you can log out and run securedrop-admin sdconfig, setting the SASL username as your new Gmail username (without the domain), the SASL domain to be either gmail.com or your custom Google Apps domain, and then finally your SASL password. Remember to use the app password generated from the 2-step config, as the primary account password won't work. The SMTP relay will be smtp.gmail.com and the SMTP relay port is 587.

Configuring fingerprint verification

If you run your own mail server, you may wish to increase the security level used by Postfix for sending mail to fingerprint, rather than secure. Doing so will require an exact match for the fingerprint of TLS certificate on the SMTP relay. The advantage to fingerprint verification is additional security, but the disadvantage is potential maintenance cost if the fingerprint changes often. If you manage the mail server and handle the certificate rotation, you should update the SecureDrop configuration whenever the certificate changes, so that OSSEC alerts continue to send. Using fingerprint verification does not work well for popular mail relays such as smtp.gmail.com, as those fingerprints can change frequently, due to load balancing or other factors.

You can retrieve the fingerprint of your SMTP relay by running the command below (all on one line). Please note that you will need to replace smtp.gmail.com and 587 with the correct domain and port for your SMTP relay.

```
openssl s_client -connect smtp.gmail.com:587 -starttls smtp < /dev/null 2>/dev/null |
    openssl x509 -fingerprint -noout -in /dev/stdin | cut -d'=' -f2
```

If you are using Tails, you will not be able to connect directly with `openssl s_client` due to the default firewall rules. To get around this, proxy the requests over Tor by adding `torify` at the beginning of the command. The output of the command above should look like the following:

```
6D:87:EE:CB:D0:37:2F:88:B8:29:06:FB:35:F4:65:00:7F:FD:84:29
```

Finally, add a new variable to `~/.config/securedrop-admin/site-specific` as `smtp_relay_fingerprint`, like so:

```
smtp_relay_fingerprint: "6D:87:EE:CB:D0:37:2F:88:B8:29:06:FB:35:F4:65:00:7F:FD:84:29"
```

Specifying the fingerprint will configure Postfix to use it for verification on the next playbook run. (To disable fingerprint verification, simply delete the variable line you added, and rerun the playbooks.) Save `~/.config/securedrop-admin/site-specific`, exit the editor and *proceed with the installation* by running the playbooks.

1.59.2 Troubleshooting

Some OSSEC alerts should begin to arrive as soon as the installation has finished.

The easiest way to test that OSSEC is working is to SSH to the Monitor Server and run `systemctl restart ossec`. This will trigger an Alert level 3 saying: "Ossec server started."

So you've finished installing SecureDrop, but you haven't received any OSSEC alerts. First, check your spam/junk folder. If they're not in there, then most likely there is a problem with the email configuration. In order to find out what's wrong, you'll have to SSH to the Monitor Server and take a look at the logs. To examine the mail log created by Postfix, run the following command:

```
tail /var/log/mail.log
```

The output will show you attempts to send the alerts and provide hints as to what went wrong. Here's a few possibilities and how to fix them:

Problem	Solution
Connection timed out	Check that the hostname and port is correct in the relayhost line of `/etc/postfix/main.cf`
Server certificate not verified	Check that the relay certificate is valid (for more detailed help, see *Troubleshooting SMTP TLS*). Consider adding `smtp_relay_cert_override_file` to `prod_specific.yml` as described above.
Authentication failure	Edit `/etc/postfix/sasl_passwd` and make sure the username, domain and password are correct. Run `postmap /etc/postfix/sasl_passwd` to update when finished.

After making changes to the Postfix configuration, you should run `systemctl reload postfix` and test the new settings by restarting the OSSEC service.

Tip

If you change the SMTP relay port after installation for any reason, you must update the SMTP relay port using `securedrop-admin sdconfig` and deploy using `securedrop-admin install`.

Useful log files for OSSEC

Other log files that may contain useful information:

/var/log/procmail.log
Includes lines for sending mail containing OSSEC alerts.

/var/log/syslog
Messages related to grsecurity, AppArmor and iptables.

/var/ossec/logs/ossec.log
OSSEC's general operation is covered here.

/var/ossec/logs/alerts/alerts.log
Contains details of every recent OSSEC alert.

Tip

Remember to encrypt any log files before sending via email, for example to securedrop@freedom.press, in order to protect security-related information about your organization's SecureDrop instance.

Not receiving emails

Some mail servers require that the sending email address match the account that authenticated to send mail. By default the *Monitor Server* will use `ossec@ossec.server` for the from line, but your mail provider may not support the mismatch between the domain of that value and your real mail host. If the Admin email address (configured as `ossec_alert_email` in `~/.config/securedrop-admin/site-specific`) does not start receiving OSSEC alerts updates shortly after the first playbook run, try setting `ossec_from_address` in `~/.config/securedrop-admin/site-specific` to the full email address used for sending the alerts, then run the playbook again.

Message failed to encrypt

If OSSEC cannot encrypt the alert to the *OSSEC Alert Public Key* for the Admin email address (configured as `ossec_alert_email` in `~/.config/securedrop-admin/site-specific`), the system will send a static message instead of the scheduled alert:

> Failed to encrypt OSSEC alert. Investigate the mailing configuration on the Monitor Server.

Check the GPG configuration vars in `~/.config/securedrop-admin/site-specific`. In particular, make sure the GPG fingerprint matches that of the public key file you exported.

Troubleshooting SMTP TLS

Your choice of SMTP relay server must support STARTTLS and have a valid server certificate. By default, the *Monitor Server*'s Postfix configuration will try to validate the server certificate using the default root store (in Ubuntu, this is maintained in the `ca-certificates` package). You can override this by setting `smtp_relay_cert_override_file` as described earlier in this document.

In either situation, it can be helpful to use the `openssl` command line tool to verify that you can successfully connect to your chosen SMTP relay securely. We recommend doing this before running the playbook, but it can also be useful as part of troubleshooting OSSEC email send failures.

In either case, start by attempting to make a STARTTLS connection to your chosen `smtp_relay:smtp_relay_port` (get the values from your `group_vars/all/site-specific` file). On a machine running Ubuntu, run the following `openssl` command, replacing `smtp_relay` and `smtp_relay_port` with your specific values:

```
openssl s_client -showcerts -starttls smtp -connect smtp_relay:smtp_relay_port < /dev/
↪null 2> /dev/null
```

Note that you will not be able to run this command on the Application Server because of the firewall rules. You can run it on the Monitor Server, but you will need to run it as the Postfix user (again, due to the firewall rules):

```
sudo -u postfix openssl s_client -showcerts -starttls smtp -connect smtp.gmail.com:587 <␣
↪/dev/null 2> /dev/null
```

If the command fails with "Could not connect" or a similar message, then this mail server does not support STARTTLS. Verify that the values you are using for `smtp_relay` and `smtp_relay_port` are correct. If they are, you should contact the admin of that relay and talk to them about supporting STARTTLS, or consider using another relay that already has support.

If the command succeeds, the first line of the output should be "CONNECTED" followed by a lot of diagnostic information about the connection. You should look for the line that starts with "Verify return code", which is usually one of the last lines of the output. Since we did not give `openssl` any information about how to verify certificates in the previous command, it should be a non-zero value (indicating verification failed). In my case, it is `Verify return code:  20 (unable to get local issuer certificate)`, which indicates that openssl does not know how to build the certificate chain to a trusted root.

If you are using the default verification setup, you can check whether your cert is verifiable by the default root store with `-CApath`:

```
openssl s_client -CApath /etc/ssl/certs -showcerts -starttls smtp -connect smtp_
↪relay:smtp_relay_port < /dev/null 2> /dev/null
```

For example, if I'm testing Gmail as my SMTP relay (`smtp.gmail.com:587`), running the `openssl` with the default root store results in `Verify return code: 0 (ok)` because their certificate is valid and signed by one of the roots in the default store. This indicates that can be successfully used to securely relay email in the default configuration of the *Monitor Server*.

If your SMTP relay server does not successfully verify, you should use the return code and its text description to help you diagnose the cause. Your cert may be expired, in which case you should renew it. It may not be signed by a trusted CA, in which case you should obtain a signature from a trusted CA and install it on the mail server. It may not have the right hostnames in the Common Name or Subject Alternative Names, in which case you will need to generate a new CSR with the correct hostnames and then obtain a new certificate and install it. Etc., etc.

If you are *not* using the default verification setup, and intentionally do not want to use a certificate signed by one of the default CA's in Ubuntu, you can still use `openssl` to test whether you can successfully negotiate a secure connection. Begin by copying your certificate file (`smtp_relay_cert_override_file` from `group_vars/all/site-specific`) to the computer you are using for testing. You can use `-CAfile` to test if your connection will succeed using your custom root certificate:

```
openssl s_client -CAfile /path/to/smtp_relay_cert_override_file -showcerts -starttls␣
↪smtp -connect smtp_relay:smtp_relay_port < /dev/null 2> /dev/null
```

Finally, if you have a specific server in mind but are not sure what certificate you need to verify the connection, you can use the output of `openssl s_client` to figure it out. Since we have `-showcerts` turned on, `openssl` prints the entire certificate chain it receives from the server. A properly configured server will provide all of the certificates in the chain up to the root cert, which needs to be identified as "trusted" for the verification to succeed. To see the chain, find the part of the output that start with `Certificate chain`. It will look something like this (example from `smtp.gmail.com`, with certificate contents snipped for brevity):

```
---
Certificate chain
0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=smtp.gmail.com
i:/C=US/O=Google Inc/CN=Google Internet Authority G2
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2
i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA
i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
---
```

The certificates are in reverse order from leaf to root. `openssl` handily prints the Subject (`s:`) and Issuer (`i:`) information for each cert. In order to find the root certificate, look at the Issuer of the last certificate. In this case, that's `Equifax Secure Certificate Authority`. This is the root certificate that issued the first certificate in the chain, and it is what you need to tell Postfix to use in order to trust the whole connection.

Actually obtaining this certificate and establishing trust in it is beyond the scope of this document. Typically, if you are using your own SMTP relay with a custom CA, you will be able to obtain this certificate from an intranet portal or someone on your IT staff. For a well-known global CA, you can obtain it from the CA's website. For example, a quick search for "Equifax Secure Certificate Authority" finds the web page of GeoTrust's Root Certificates, which have accompanying background information and are available for download.

Once you have the root certificate file, you can use `-CAfile` to test that it will successfully verify the connection.

1.59.3 Analyzing the alerts

Understanding the contents of the OSSEC alerts requires a background and knowledge in Linux systems administration. They may be confusing, and at first it will be hard to tell between a genuine problem and a fluke. You should examine these alerts regularly to ensure that the SecureDrop environment has not been compromised in any way, and follow up on any particularly concerning messages with direct investigation.

An initial SecureDrop install will generate quite a few alerts as OSSEC is installed early in the install process. As part of the administration of a SecureDrop instance, regularly looking through the generated alerts provides administrators with information on the overall health of the SecureDrop instance.

OSSEC alerts will range from a severity level of 1 (lowest) to 14 (highest), and as a baseline, you should expect to see the following alerts:

Common OSSEC alerts

Package updates

The SecureDrop *Application* and *Monitor Servers* check for package updates every day. As updates are automatically installed, OSSEC will notice and send out alerts. You may see any number of these alerts in the email, as several alerts can be batched in a single email. You should also see them in an email named `Daily Report:  File Changes`. To verify this activity matches the package history, you can review the logs in `/var/log/apt/history.log`.

```
Received From: (app)
Rule: 2902 fired (level 7) -> "New dpkg (Debian Package) installed."
Portion of the log(s):

status installed <package name> <version>
```

In addition to letting you know what packages were updated, OSSEC will send alerts about the specific changes to the files in these packages.

```
Received From: (app)
Rule: 550 fired (level 7) -> "Integrity checksum changed."
Portion of the log(s):

Integrity checksum changed for: '/usr/sbin/<binary name>'
Old md5sum was: '<old md5sum>'
New md5sum is : '<new md5sum>'
Old sha1sum was: '<old sha1sum>'
New sha1sum is : '<new sha1sum>'
```

It may seem redundant to receive both `New dpkg (Debian Package) installed` and `Integrity checksum changed` alerts. This happens because OSSEC's alerts do not track root causation: OSSEC doesn't "know" that files have changed because new packages have been installed or updated, so it reports both sets of events independently. As a result, these clusters of alerts are normal and expected: they tell you that your SecureDrop servers are properly up-to-date and patched.

Keep an eye out for *exceptions* to this rule as you analyze your OSSEC alerts. Surprising changes to configuration files, or new or changed files unrelated to the daily updates, may warrant further investigation.

Occasionally your SecureDrop Servers will send an alert for failing to connect to Tor relays. Since SecureDrop runs as a Tor Onion Service, it is possible for Tor connections to timeout or become overloaded.

```
Received From: (app)
Rule: 1002 fired (level 2) -> "Unknown problem somewhere in the system."
Portion of the log(s):

[warn] Your Guard <name> ($fingerprint) is failing a very large amount of
circuits. Most likely this means the Tor network is overloaded, but it
could also mean an attack against you or potentially the guard itself.
```

This alert is common but if you see them for sustained periods of time (several times a day), please contact us at the SecureDrop Support Portal or at securedrop@freedom.press for help.

Daily reports

On days where file integrity checksums have changed or users have logged into `app` or `mon` servers, you will receive emails entitled `Daily report: File changes` or `Daily report: Successful logins`. These emails may be a more convenient format should you not have continuous access to the inbox or GPG key.

Action: periodically review these daily reports to ensure file changes correspond to platform updates and logins correspond to authorized admin activity on the SecureDrop servers.

If you have any suggestions on how to further tune or improve the alerting, you can open an issue on GitHub.

Uncommon OSSEC alerts

Data integrity

SecureDrop runs automatic checks for submission data integrity problems. For example, secure deletion of large submissions could potentially be interrupted:

```
Received From: (app) 10.20.2.2->/opt/venvs/securedrop-app-code/bin/python3 /var/www/
↪securedrop/manage.py check-disconnected-fs-submissions
Rule: 400801 fired (level 1) -> "Indicates that there are files in the submission area␣
↪without corresponding submissions in the database."
Portion of the log(s):

ossec: output: '/opt/venvs/securedrop-app-code/bin/python3 /var/www/securedrop/manage.py␣
↪check-disconnected-fs-submissions': There are files in the submission area with no␣
↪corresponding records in the database. Run "manage.py list-disconnected-fs-submissions
↪" for details.
```

To resolve the issue, you can *clean them up*.

Instance misconfigurations

In addition, SecureDrop performs a small set of daily configuration checks to ensure that the iptables rules configured on the *Application* and *Monitor Server* match the expected configuration. If they do not, you may receive a level 12 alert like the following:

```
Received From: (app) 10.20.2.2->/var/ossec/checksdconfig.py
Rule: 400900 fired (level 12) ->
"Indicates a problem with the configuration of the SecureDrop servers."
Portion of the log(s):
```

(continues on next page)

(continued from previous page)

```
ossec: output: '/var/ossec/checksdconfig.py': System configuration error:
The iptables default drop rules are incorrect.
```

Alternatively, the error text may say: `The iptables rules have not been configured.` To resolve the issue, you can reinstate the standard iptables rules by *updating the system configuration*.

`securedrop-admin` commands

OSSEC will send an alert when the *securedrop-admin* tool is used to backup, restore, or change the system configuration:

```
Rule: 400001 fired (level 13) -> "Ansible playbook run on server (securedrop-admin␣
↪install, backup, or restore)."
```

Action: You should ensure that this action was performed by you or a fellow administrator.

If you believe that the system is behaving abnormally, you should contact us at the SecureDrop Support Portal or securedrop@freedom.press for help.

1.60 Backing Up and Restoring Servers

Maintaining regular backups helps guard against data loss and hardware failure. Having a recent backup will allow you to redeploy SecureDrop without changing onion URLs, recreating journalist accounts, or losing previous submissions from sources.

Note

Only the *Application Server* is backed up and restored, including historical submissions and both *Source Interface* and *Journalist Interface* URLs. The *Monitor Server* needs to be configured from scratch in the event of a hardware migration.

1.60.1 Minimizing Disk Use

Since the backup and restore operations both involve transferring *all* of your SecureDrop's stored submissions over Tor, the process can take a long time.

Encouraging journalists to regularly delete older, unneeded submissions from the *Journalist Interface* will save time and improve reliability when doing backups.

Tip

Although it varies, the average throughput of an onion service is about 3 Mbps, or roughly 90 minutes for 2GB. Plan your backup and restore accordingly.

On the *Application Server*, open a Terminal via **Apps** ▶ **System Tools** ▶ **Console** on the Admin Workstation and run

```
ssh app sudo du -sh /var/lib/securedrop/store
```

Compare the output of this command (which approximates the size of a backup archive) to the amount of free space on your Tails persistent volume via Tails' **Disks** utility to ensure you have sufficient space to perform a backup.

If you find you cannot perform a backup or restore due to this constraint, and have already deleted old submissions from the *Journalist Interface*, contact us through the SecureDrop Support Portal.

Note

Submissions are deleted asynchronously and one at a time, so if you delete a lot of submissions through the *Journalist Interface*, it may take a while for all of the submissions to actually be deleted. SecureDrop uses `shred` to securely erase files, which takes significantly more time than normal file deletion. You can monitor the progress of queued deletion jobs by logging in to the *Application Server* over SSH and running:

```
sudo journalctl -u securedrop_rqworker
```

1.60.2 Backing Up

Check Connectivity

Open a Terminal via **Apps** ▶ **System Tools** ▶ **Console** on your *Admin Workstation* and verify it is able to run Ansible and connect to the SecureDrop servers.

```
ssh app uptime
```

If this command fails, see *Troubleshooting*.

Create the Backup

When you are ready to begin the backup, run

```
securedrop-admin backup
```

The backup command will display updates on its progress as the backup is created. Run time will vary depending on connectivity and the number of submissions saved on the *Application Server*.

When the backup action is complete, the backup will be stored as a compressed archive in `~/.config/securedrop-admin`. The filename will begin `sd-backup`, followed by a timestamp of when the backup was initiated, and ending with `.tar.gz`. You can find the full path to the backup archive in the output of the backup command.

Warning

The backup file contains sensitive information! It should only be stored on the *Admin Workstation*, or on a *dedicated encrypted backup USB*.

Note

When dealing with larger backups, the `securedrop-admin backup` command may fail with a `MemoryError` at this stage of the operation: “Fetch the backup tarball back to the Admin Workstation”.

If this happens, a backup was successfully generated, but it is still on the server. Run this command from your `~/.config/securedrop-admin` directory to copy the backup your *Admin Workstation*:

```
rsync -av --progress --partial app:$(ssh app ls -1rt /tmp/sd-backup* | tail -1) ~/.
↪config/securedrop-admin/
```

If the transfer fails or is interrupted, you can simply run this command again to resume it.

Note that this method will only work if you have first run the `securedrop-admin backup` command, and the backup has successfully progressed at least until the "Fetch the backup tarball" stage.

1.60.3 Restoring from a Backup

Prerequisites

To perform a restore, boot into the *Admin Workstation* and ensure that your `.tar.gz` backup archive has been copied to `~/.config/securedrop-admin`. (If you are using the same *Admin Workstation* as you did when you took the backup, the archive will already be in place).

If you are restoring data onto an existing instance (for example, for data recovery purposes), see *Restoring a Backup on an Existing Instance*.

If you are reinstalling SecureDrop and then restoring from a backup (for example, for hardware migration, operating system upgrade, or disaster recovery purposes), see *Migrating Using a Backup*.

For other data recovery scenarios, see *Additional Information* or contact Support.

Restoring a Backup on an Existing Instance

To restore an existing instance to a previous state, run the command:

```
securedrop-admin restore sd-backup-2020-07-22--01-06-25.tar.gz
```

Make sure to replace `sd-backup-2020-07-22--01-06-25.tar.gz` with the filename for your backup archive.

This command attempts to restore submissions, source and journalist accounts, and configuration details for the onion services used by the web interfaces and SSH (if configured).

1.60.4 Migrating Using a Backup

Moving a SecureDrop instance to new hardware involves:

- Backing up the old instance and preserving configuration and credentials from the *Admin Workstation*;
- Installing SecureDrop on new hardware;
- Restoring the backup to the new instance and repairing credentials.

Note

If you need to restore from a backup from an instance configured to use SSH-over-LAN onto an SSH-over-Tor instance, you must either first update the target instance to use SSH-over-LAN or perform a data-only backup. See *Data-only Restores* for more information.

Note

The instructions below assume that you are using the same *Admin Workstation* that was used to manage your old instance. If you are using a new *Admin Workstation* you will need to first install the *securedrop-admin package and prerequisites* on it. Then you may copy the config directory `~/.config/securedrop-admin` and backup archive from the old *Admin Workstation* to the new workstation (using an encrypted *Transfer Device*), and proceed with the instructions below.

1. If you have not already done so, *back up the existing installation*. The instructions below assume that the backup has been created and renamed `sd-backup-old.tar.gz`.

2. Move the existing *Admin Workstation* SSH configuration out of the way via the Terminal via **Apps ▶ System Tools ▶ Console**, using the commands:

   ```
   ssh-add -D
   find ~/.ssh/ -type f -exec mv {} {}.bak \;
   ```

   > **Note**
   >
   > You will be generating fresh SSH credentials for the servers, and any other *Admin Workstation* USBs will have to be *provisioned with updated credentials*.

3. Ensure your *Admin Workstation* is connected to a LAN port on your network firewall, and *configure the Admin Workstation's IP address*.

4. Install Ubuntu 24.04 on the *Application* and *Monitor Servers*, following the *server setup instructions* to install with the correct settings, test connectivity, and set up SSH keys to allow for *Admin Workstation* access.

   > **Note**
   >
   > You may need to wait approximately 10-15 minutes after installing Ubuntu 24.04 for the servers to become reachable via SSH.

5. Reinstall SecureDrop on the servers, following the *installation instructions*. During the configuration stage (`securedrop-admin sdconfig`), the values will be prepopulated based on the old instance's configuration, which is still stored in `~/.config/securedrop-admin`. Press **Enter** to accept each value.

   Proceed through the installation by running `securedrop-admin install` then `securedrop-admin localconfig`. If SSH-over-Tor is configured, run `ssh app uptime` and `ssh mon uptime` in the Terminal to verify SSH connectivity.

6. Restore from the old instance's backup (e.g. `sd-backup-old.tar.gz`) using the Terminal command:

   ```
   securedrop-admin restore sd-backup-old.tar.gz
   ```

   The restore task will proceed for some time, removing v2 services if a v2+v3 backup was used.

7. Synchronize the server and *Admin Workstation's* web interface config and authentication keys using the Terminal commands:

   ```
   securedrop-admin install
   securedrop-admin localconfig
   ```

8. *Test the new instance* to verify that the web interfaces are available and the servers can be reached via SSH.

9. If you have migrated to new hardware, ensure your old servers have been decommissioned and/or destroyed by following the relevant sections of *our decommissioning documentation*.

Repair Additional Admin Workstations

If you have additional *Admin Workstation* USBs, they will no longer have valid SSH credentials and will need to be repaired. In these steps, the "primary *Admin Workstation*" is the one which you used to complete the above migration process.

1. Prepare a fresh *LUKS-encrypted USB*. You may record the passphrase in your primary *Admin Workstation* KeePassXC password manager.

2. Copy the following files from your primary *Admin Workstation* onto the LUKS-encrypted USB:

   - `~/.config/securedrop-admin/tor_v3_keys.json`
   - `~/.config/securedrop-admin/mon-ssh.auth_private`
   - `~/.ssh/id_rsa.pub`
   - `~/.ssh/id_rsa`

   > **Note**
   >
   > Alternatively, if you wish to use different SSH credentials for each *Admin Workstation*, you may do so. In this case, copy only the first two files above to your additional *Admin Workstations*.
   >
   > Generate per-machine SSH keys and use a clean LUKS-encrypted USB drive to transfer the public portions of those keys to your primary *Admin Workstation*, where you will then add them to the servers' `authorized_keys` files, as described *here*. You may also contact Support for assistance.

3. Boot into each additional *Admin Workstation*. Set an administration password and unlock the persistent volume on the Tails welcome screen. Once logged in, attach the LUKS-encrypted USB and unlock it.
4. Ensure that this *Admin Workstation* is using an up-to-date version of Tails and is running the latest SecureDrop application code, 2.13.0.
5. As you did with the primary *Admin Workstation*, archive the existing SSH configuration:

   ```
   ssh-add -D
   find ~/.ssh/ -type f -exec mv {} {}.bak \;
   ```

6. From the LUKS-encrypted USB, copy `~/.ssh/id_rsa` and `~/.ssh/id_rsa.pub` to the `~/.ssh/` directory.
7. From the LUKS-encrypted USB, copy `tor_v3_keys.json` and `mon-ssh.auth_private` to the `~/.config/securedrop-admin` directory.
8. In the Terminal, type the following commands:

   ```
   securedrop-admin localconfig
   ```

9. Test connectivity to each server by running `ssh app uptime` and `ssh mon uptime`.
10. Once all *Admin Workstations* have been updated, securely wipe the files on the LUKS-encrypted USB, by right-clicking them in the file manager and selecting **Wipe**. Then, reformat the device using the **Disks** utility.

1.60.5 Additional Information

Data-Only Restores

The `restore` command normally restores both the data and the Tor configuration of an instance, including the .onion URLs for your instance.

You may, however, restore data, such as submissions and journalist and source accounts, without altering an instance's Tor configuration, with the following command:

```
securedrop-admin restore --preserve-tor-config sd-backup-2020-07-22--01-06-25.tar.gz
```

This is a suitable option if you have a backup archive taken from an instance with v2 onion services, and wish to restore it to an instance that is now using v3 onion services.

If you require any assistance with migration or data recovery, please contact Support.

1.61 Backing Up and Restoring Workstations

1.61.1 Backup the Workstations

Note

This workflow will create a single USB drive with the data backed up from all Tails drives. If instead you'd like to create a single duplicate Tails drive, you should follow the official documentation maintained by the Tails project.

Now that you have set up the *Secure Viewing Station*, the *Admin Workstation*, and your *Journalist Workstations*, it is important you make a backup. Your USB drive may wear out, a journalist might lose their drive, or something completely unexpected may happen.

In all these cases, it is useful to have a backup of your data for each device.

What You Need

1. You will need your *existing SecureDrop Tails USB sticks* (*Admin Workstation*, *Journalist Workstation*, and *Secure Viewing Station*).
2. You will also need an *airgapped machine* to perform the backups. The *Secure Viewing Station* may be used for this task.
3. You will also need a "primary" Tails USB, which we will use to perform the backups.
4. You also need at least one USB drive to backup the data from your current SecureDrop Tails USB sticks.

Warning

An airgapped machine (such as the *Secure Viewing Station*) is required in order to perform these backups safely. By isolating the machine from all network access, you reduce the exposure of sensitive data to networked computers, thereby reducing the threat of compromise by adversaries who wish to gain access to your SecureDrop instance.

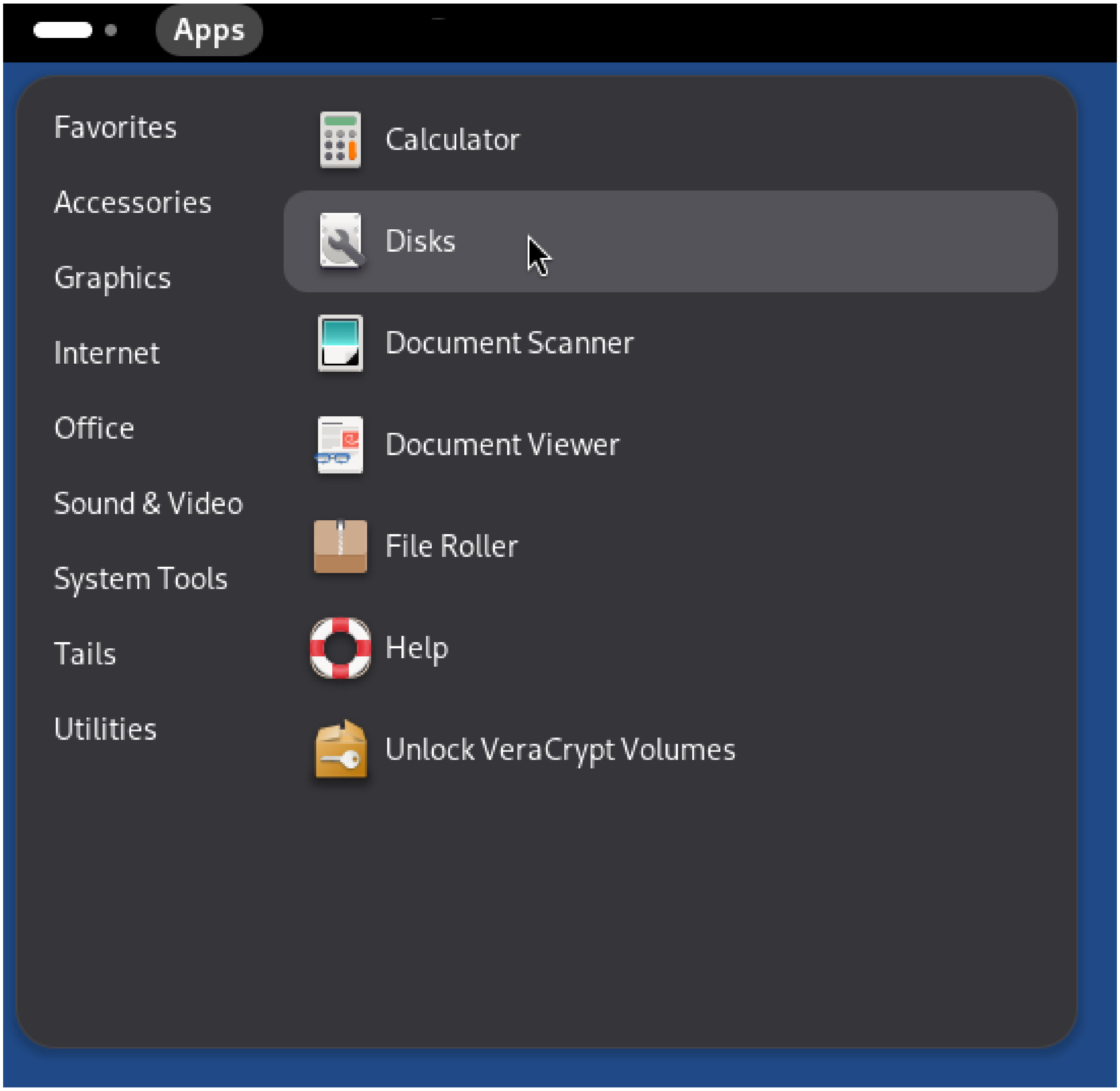
The airgapped machine should have 3 USB ports, so you can plug in the *primary Tails USB* drive, the Tails drive you want to backup, and the *backup drive* at the same time. If you don't have 3 USB ports available you can use a USB hub which may reduce transfer speeds.

Note

The steps in this section should be performed for each *Secure Viewing Station*, *Journalist Workstation*, and *Admin Workstation* USB drive in your organization.

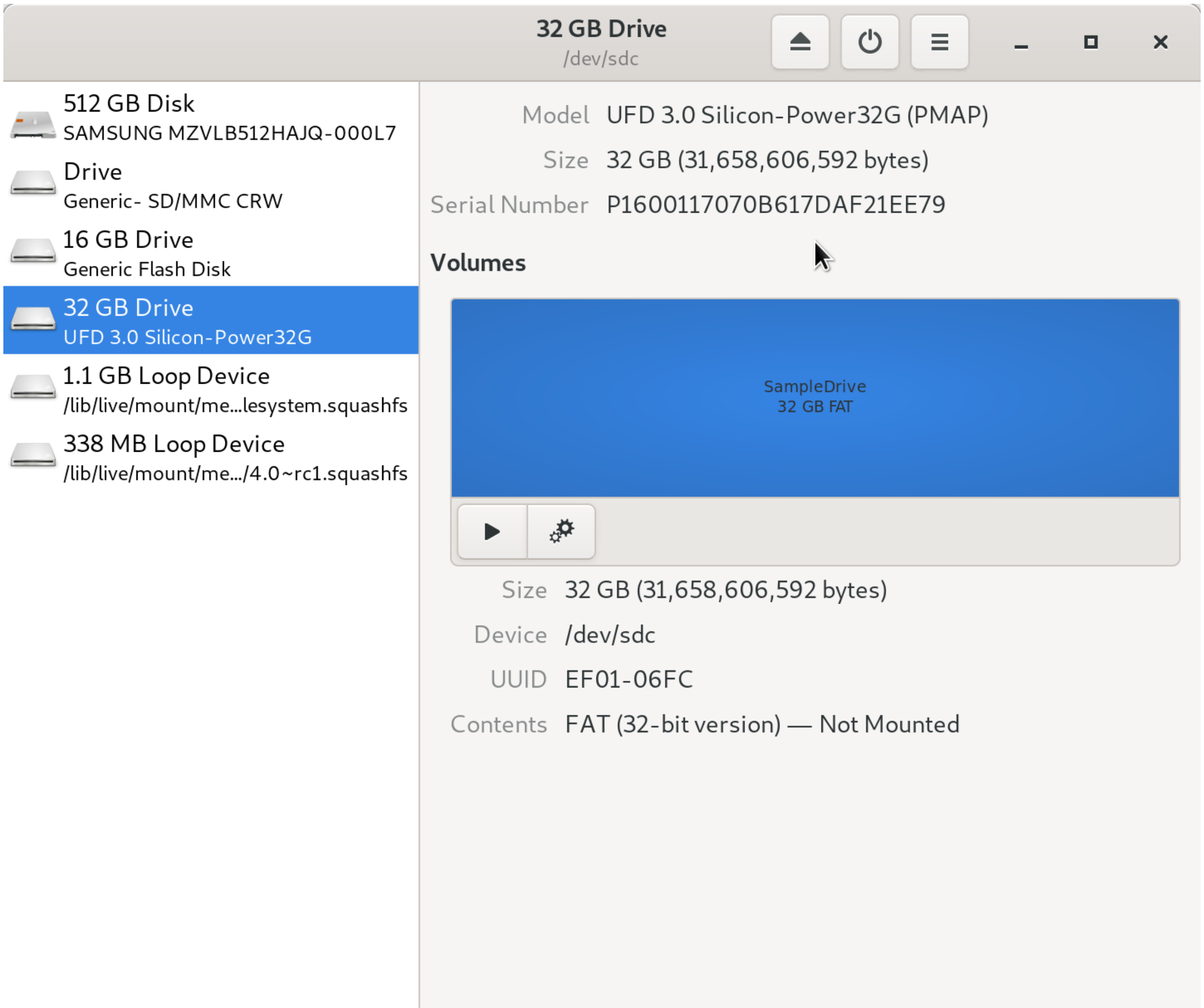
Preparing the Backup Device

First you must boot the *primary Tails USB* drive. Ensure you set an administrator password set at the login screen. Then navigate to **Apps** ▶ **Utilities** ▶ **Disks**.



Insert the USB drive you wish to use as a backup drive.

Select the drive from the list of drives in the left column.



32 GB Drive
/dev/sdc

512 GB Disk
SAMSUNG MZVLB512HAJQ-000L7

Drive
Generic- SD/MMC CRW

16 GB Drive
Generic Flash Disk

32 GB Drive
UFD 3.0 Silicon-Power32G

1.1 GB Loop Device
/lib/live/mount/me...lesystem.squashfs

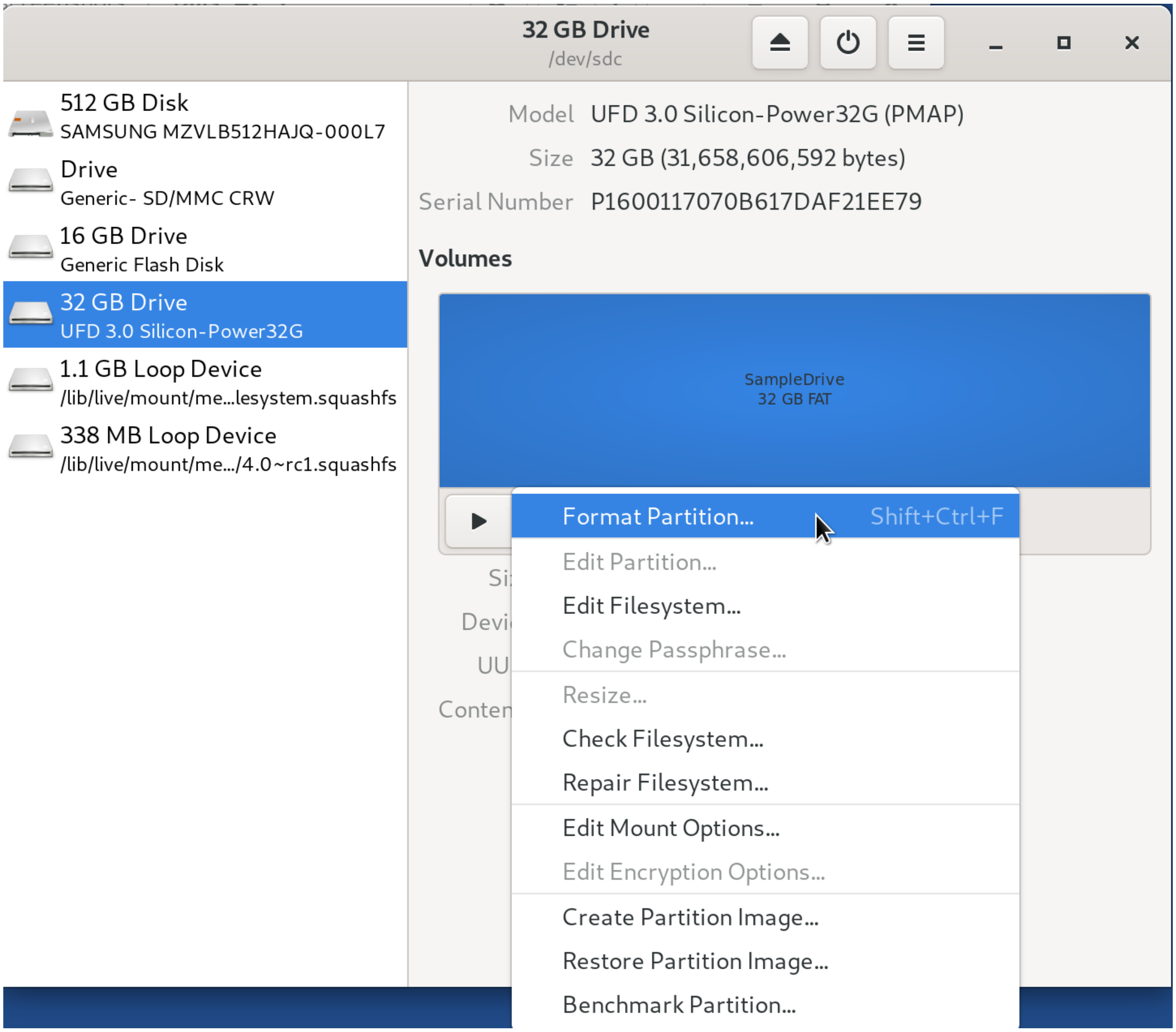
338 MB Loop Device
/lib/live/mount/me.../4.0~rc1.squashfs

Model	UFD 3.0 Silicon-Power32G (PMAP)
Size	32 GB (31,658,606,592 bytes)
Serial Number	P1600117070B617DAF21EE79

Volumes

Size	32 GB (31,658,606,592 bytes)
Device	/dev/sdc
UUID	EF01-06FC
Contents	FAT (32-bit version) — Not Mounted

Click the button with the two cogs and click **Format Partition. . .** .

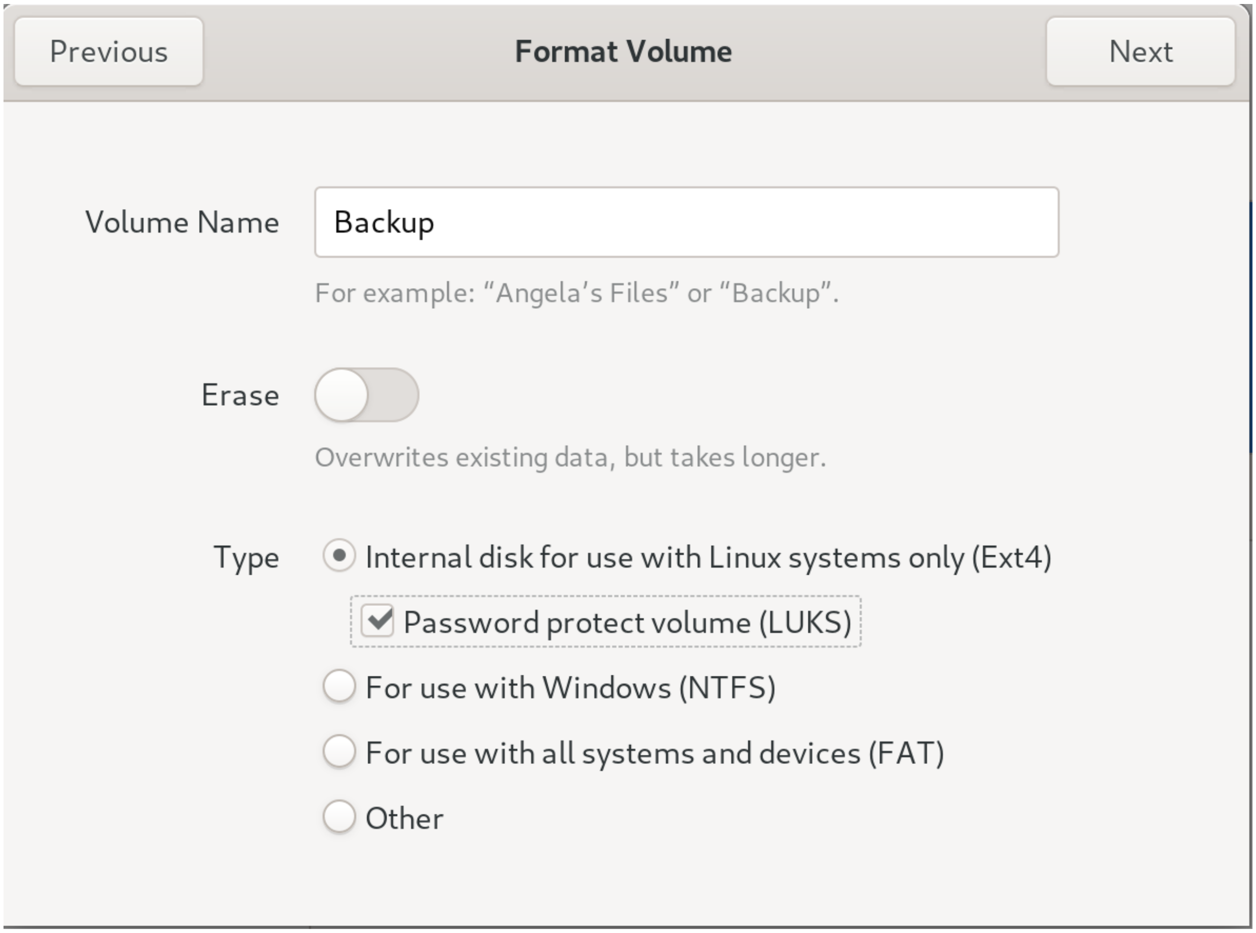


Model UFD 3.0 Silicon-Power32G (PMAP)

Size 32 GB (31,658,606,592 bytes)

Serial Number P1600117070B617DAF21EE79

Fill out the form as follows:



Volume Name: Backup

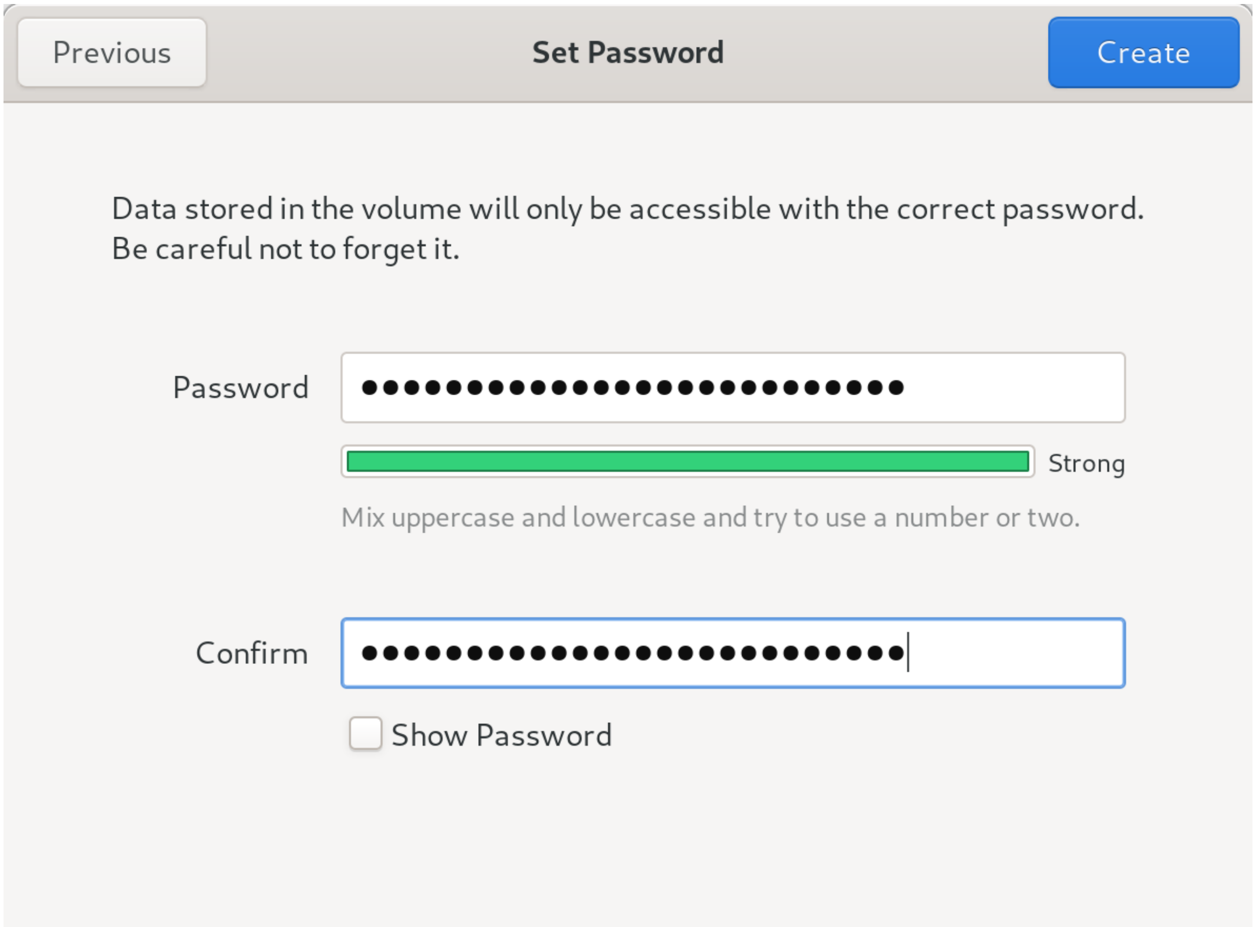
For example: "Angela's Files" or "Backup".

Erase ○

Overwrites existing data, but takes longer.

Type
● Internal disk for use with Linux systems only (Ext4)
☑ Password protect volume (LUKS)
○ For use with Windows (NTFS)
○ For use with all systems and devices (FAT)
○ Other

- **Erase**: *Don't overwrite existing data (Quick)*
- **Type: *Internal disk for use with other Linux systems only (Ext4)*, and** make sure *Password protect volume (LUKS)* is checked
- **Name**: *Backup*



Data stored in the volume will only be accessible with the correct password. Be careful not to forget it.

Password ●●●●●●●●●●●●●●●●●●●●●●●●●●

Mix uppercase and lowercase and try to use a number or two.

Confirm ●●●●●●●●●●●●●●●●●●●●●●●●●●

□ Show Password

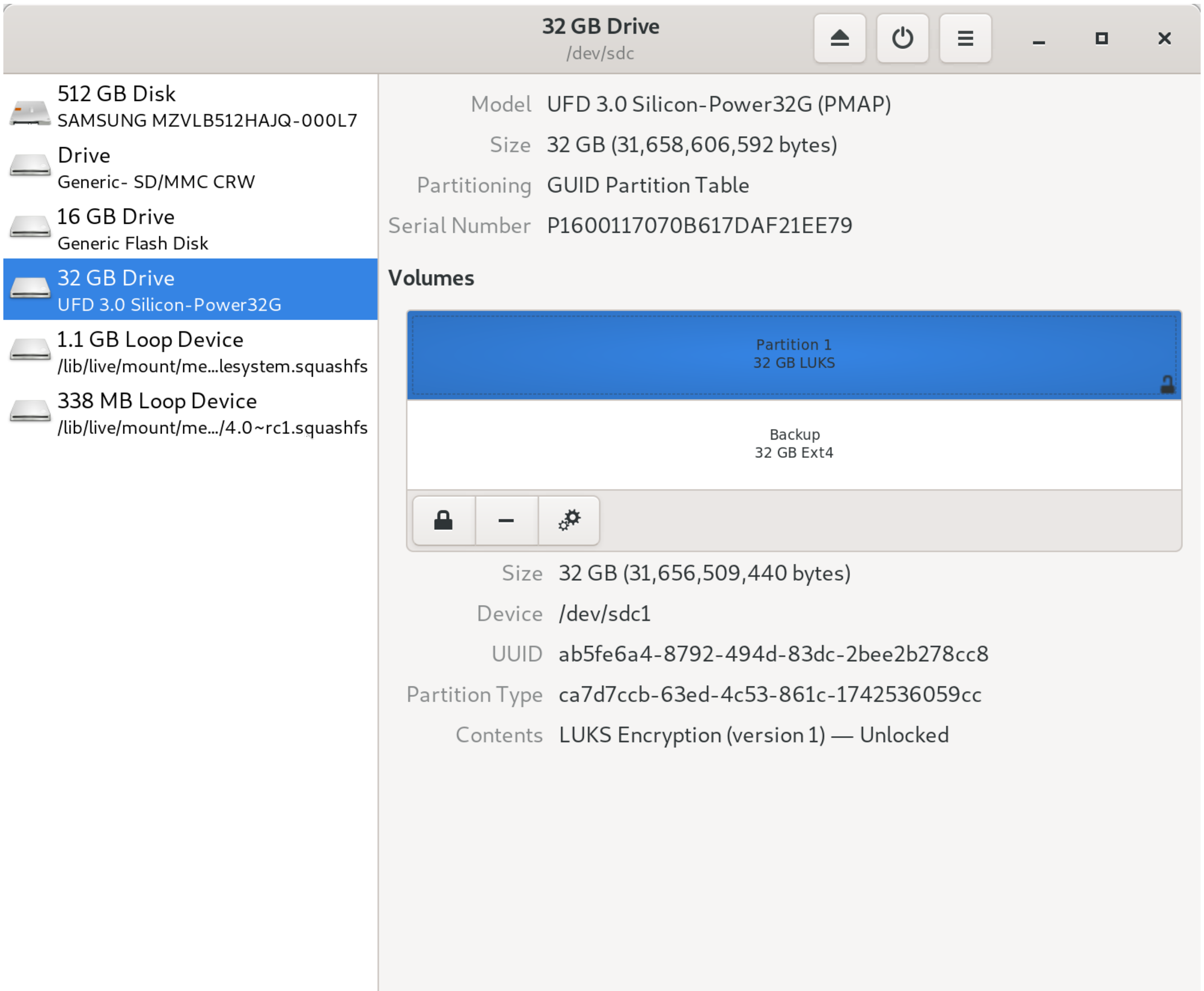
Warning

Since this will serve as a long-term backup, **make sure to use a strong passphrase**.

Click **Format**.

A dialog box will appear asking you **Are you sure you want to format the volume?** appears, click **Format**.

Once completed, you will see two partitions appear:



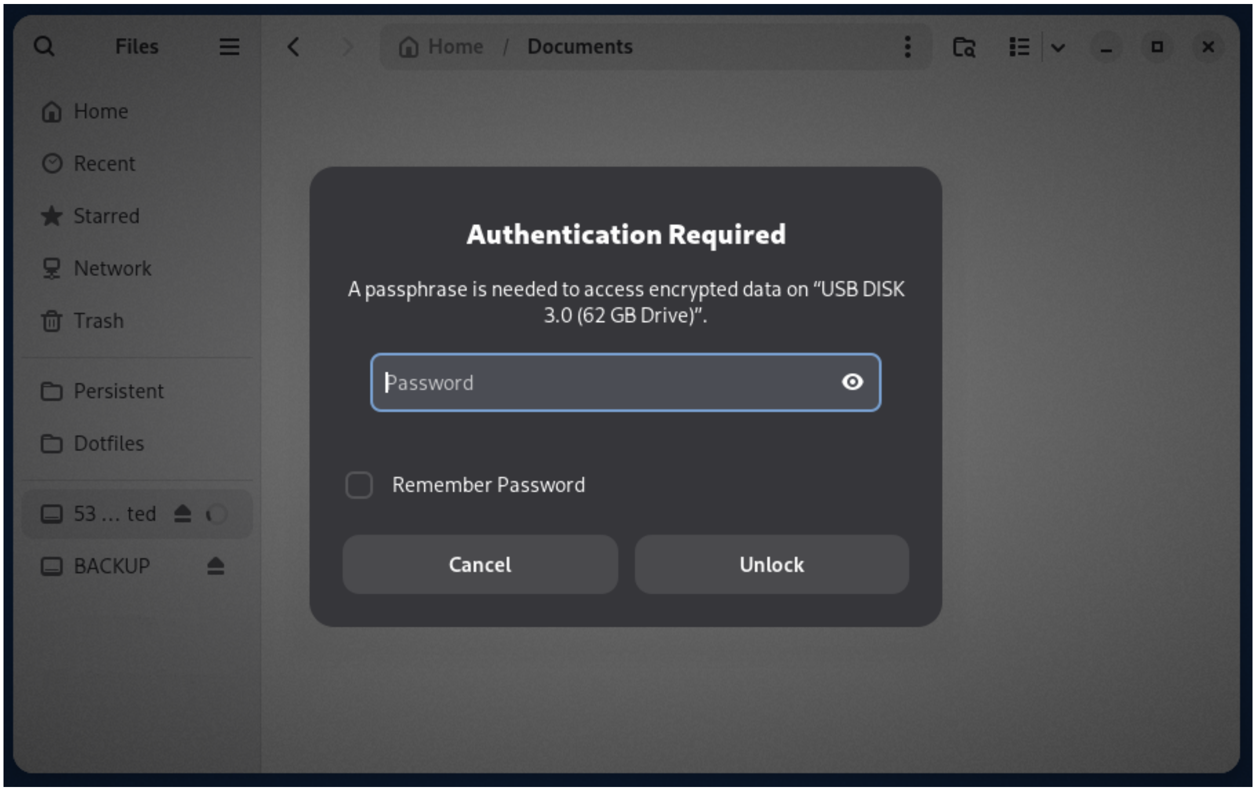
512 GB Disk
SAMSUNG MZVLB512HAJQ-000L7
Drive
Generic- SD/MMC CRW
16 GB Drive
Generic Flash Disk
32 GB Drive
UFD 3.0 Silicon-Power32G
1.1 GB Loop Device
/lib/live/mount/me...lesystem.squashfs
338 MB Loop Device
/lib/live/mount/me.../4.0~rc1.squashfs

Model	UFD 3.0 Silicon-Power32G (PMAP)
Size	32 GB (31,658,606,592 bytes)
Partitioning	GUID Partition Table
Serial Number	P1600117070B617DAF21EE79

Size	32 GB (31,656,509,440 bytes)
Device	/dev/sdc1
UUID	ab5fe6a4-8792-494d-83dc-2bee2b278cc8
Partition Type	ca7d7ccb-63ed-4c53-861c-1742536059cc
Contents	LUKS Encryption (version 1) — Unlocked

Now that you made the backup device, plug in the device you want to backup. Then, open the File Manager: **Apps** ▶ **Accessories** ▶ **Files**.

Click on the disk on the left side column. Fill in the passphrase you set up when you *created your Tails devices*.



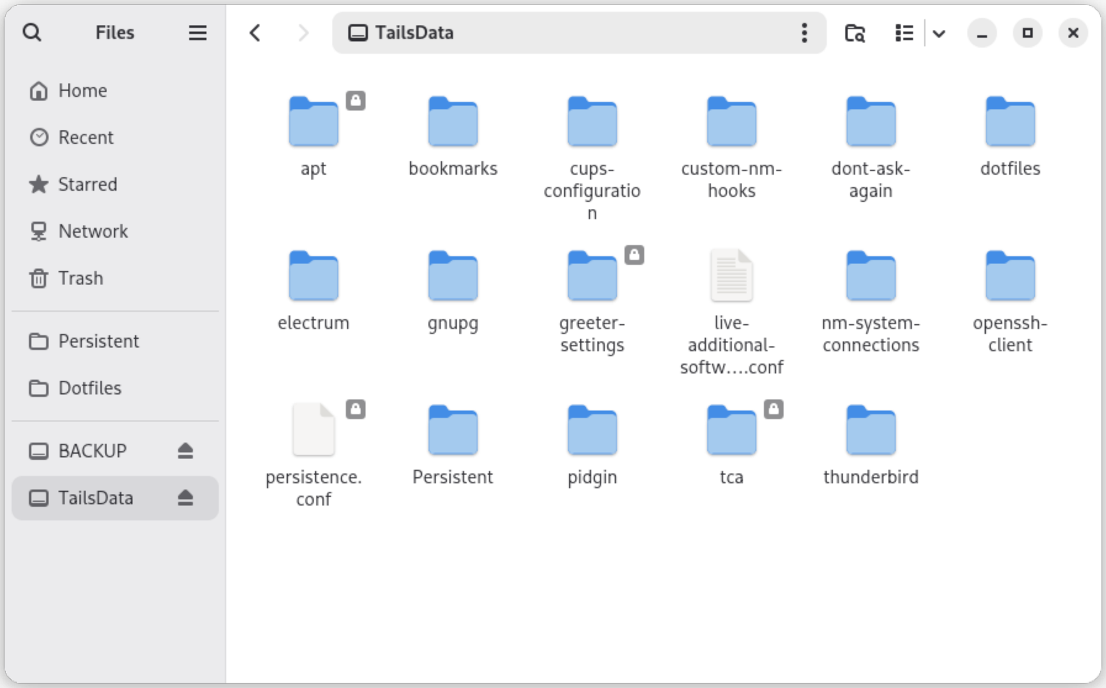
Authentication Required

A passphrase is needed to access encrypted data on “USB DISK 3.0 (62 GB Drive)”.

Password

You should now have both the Backup and TailsData partition to be backed up mounted and ready to access.

Create the backup using Rsync



Open a terminal by going to **Apps** ► **System Tools** ► **Console**.

Next, create a directory on the Backup USB for the device to be backed up - the command below creates a directory named `admin-backup`:

```
mkdir /media/amnesia/Backup/admin-backup
```

Then, copy the contents of the device's persistent volume to the directory using `rsync`:

```
sudo bash -c "rsync -a --info=progress2 --no-specials --no-devices \
    /media/amnesia/TailsData/ /media/amnesia/Backup/admin-backup/ && sync"
```

> **Note**
>
> Please make sure to include the trailing / in the directory paths in the command above, otherwise the files will not be backed up correctly.

Once complete, unmount the TailsData partition by clicking the Eject button beside its entry in the lefthand column of the file manager. When its entry is no longer shown in the lefthand column, it is save to remove the *Admin Workstation* USB.

Repeat these steps for every device, making a new folder on the backup device for each device you back up.

Finally, once you have completed the steps described in this section for each USB drive, unmount the Backup partition by clicking its Eject button. Wait until the Backup USB can be safely removed, and store it somewhere safely.

Note

After the Eject button is clicked, it may be take some time before the drive can be safely removed. Wait until its entry is removed from the lefthand column of the file manager.

1.61.2 Restoring a Workstation from a Backup

To recreate a backed-up *Admin Workstation*, *Journalist Workstation*, or *Secure Viewing Station* Tails USB, you will need

- your Backup USB containing the persistent volume to be restored,
- a blank USB stick to be set up as the new workstation USB,
- an airgapped machine and a USB with Tails already installed, referred to as the host Tails USB in this document. The host Tails USB is only used to transfer files between the Backup USB and the new workstation USB.

The process will require 3 USB ports - if necessary, you can use a USB hub. We recommend labeling USB devices before use, as it can be easy to confuse them.

Prepare the new Tails USB

Follow the guide to *creating a Tails USB* to install Tails and create a persistent volume on the blank USB stick to create the new workstation USB.

Open the Backup USB and new Tails Persistent Volume

First, boot up the host Tails USB on the airgapped machine, making sure to set an administration password on the Tails Welcome Screen dialog.

Then, navigate to **Places ▸ Computer** to open the file manager, and insert the Backup USB. Click its entry in the lefthand column and enter its decryption passphrase when prompted. Its volume name (`Backup` in the instructions above) will appear in place of the generic `N.M GB Encrypted` name.

Next, insert the new workstation USB, and click its entry in the lefthand column. When prompted, enter its persistent volume's passphrase. The volume name `TailsData` will appear in the lefthand column.

Copy the Backup to the New Workstation USB's Persistent Volume

Open a terminal by navigating to **Apps ▸ System Tools ▸ Console** . Next, use the `rsync` command to copy the appropriate backup folder to the new workstation USB's persistent volume. For example, if the backup folder to be copied is named `admin-backup`, run the following command:

```
sudo bash -c "rsync -a --info=progress2 --no-specials --no-devices \
    /media/amnesia/Backup/admin-backup/ /media/amnesia/TailsData/ && sync"
```

Note

Please make sure to include the trailing `/` in the directory paths in the command above, otherwise the backup files will not be restored correctly.

Once the command is complete, click the Eject button for the `TailsData` volume in the lefthand column of the file manager, wait for the `TailsData` entry to disappear from the column, and remove the new workstation USB.

You may now repeat the restore process for any other USBs that you wish to restore, or shut down the host Tails USB and test your new workstation USB by booting it with persistence unlocked and verifying its functionality.

1.62 Updating Tails USBs

You are responsible for keeping your Tails USBs updated.

There are two ways to perform updates: via the Tails graphical installer and manually. The manual update process will work on any Tails USB. The graphical installer requires an Internet connection to notify you when updates are available, so it is only suitable for internet-connected Tails workstations (such as the *Admin Workstation* and the *Journalist Workstation*).

Because the *Secure Viewing Station* (SVS) is airgapped, it cannot receive update notifications, so it will need to be updated manually.

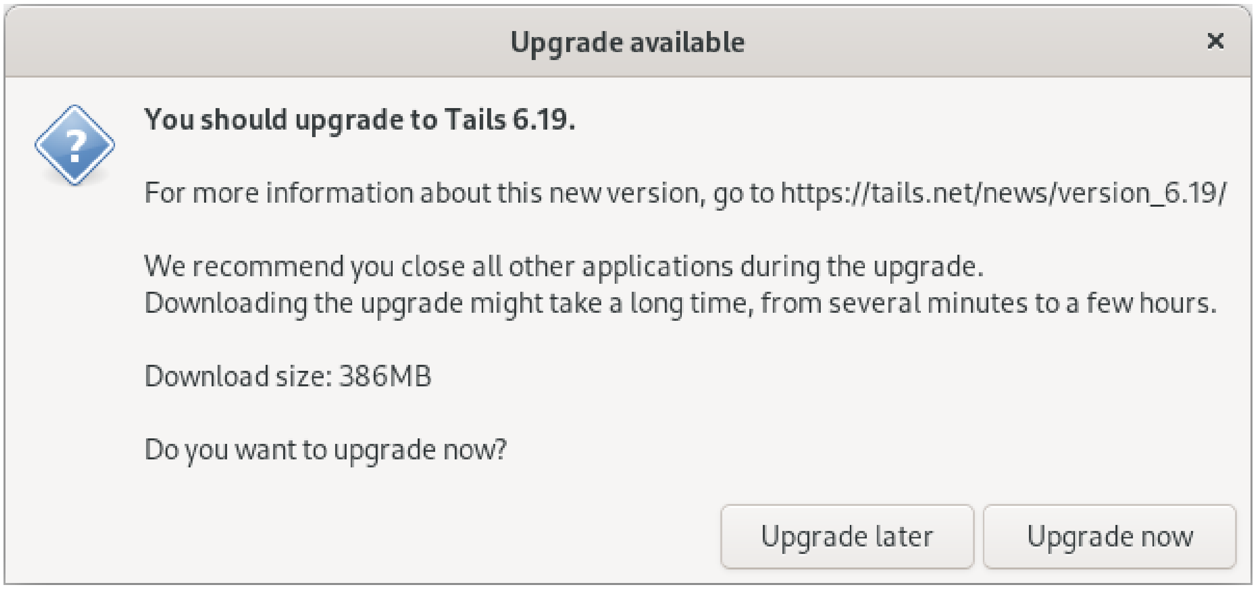
Important

The *SVS* stores some of SecureDrop's most sensitive data (decrypted submissions, the *Submission Private Key*), so we **strongly** encourage you to manually update the *SVS* whenever a new version of Tails is released.

The Tails project typically releases updates every 6 to 8 weeks. Occasionally they release a new version ahead of the normal cycle in order to address a security issue. For regular Tails OS and security information, check out the Tails Security page and subscribe to the Tails RSS/Atom feed.

1.62.1 Update via Graphical Installer

For Internet-connected Tails workstations, you'll see a notification when a new version of Tails is available.



You should upgrade to Tails 6.19.

For more information about this new version, go to https://tails.net/news/version_6.19/

We recommend you close all other applications during the upgrade.
Downloading the upgrade might take a long time, from several minutes to a few hours.

Download size: 386MB

Do you want to upgrade now?

We recommend that you *back up your existing configuration* and update as soon as possible. It usually takes some time for updates to download, so keep that in mind when choosing when to update.

1.62.2 Update Manually

The process for manually updating a Tails USB is:

1. Recommended: *Make a backup of the USB you want to update*.
2. Install the *latest version of Tails* on your *primary Tails USB* or a blank USB stick.

3. Use the *primary Tails USB* to *perform a manual update of your desired Tails USB* on a fully offline (airgapped) computer, such as the computer used for the *Secure Viewing Station*.

What you need

1. Your *Admin Workstation* computer to download the latest version of Tails
2. A *primary Tails USB* stick (you may still have one; it was used to create the *Admin Workstation*, *Secure Viewing Station*, and *Journalist Workstation* Tails USBs during the initial SecureDrop install process)
3. The Tails USB that you want to update
4. A Backup USB to back up the data on your existing Tails USBs
5. An airgapped computer, such as the computer used for the *Secure Viewing Station*, to perform the update

1. Back up your Tails USB

Follow the instructions to *back up your existing Tails USB*.

2. Get the latest version of Tails

If you have an existing *primary Tails USB* and the version of Tails you are updating to supports automatic updates, boot into it on your *Admin Workstation* computer and follow the graphical updater prompts that guide you through the update process.

Alternatively, you can also download and *install the newest version of Tails from scratch* (as you did when you first installed SecureDrop). This may be faster if your *primary Tails USB* has not been updated in a while, and is necessary for Tails releases that do not support automatic updates.

3. Perform airgapped update

In this step, use the up-to-date *primary Tails USB* to update your desired Tails USB.

Warning

The entire *Secure Viewing Station* is designed to be airgapped, so the *SVS* Tails USB must **never** be plugged into a computer with a network connection.

Use an airgapped computer, such as the *Secure Viewing Station* computer, to perform the steps in this section.

Plug your *primary Tails USB* into the airgapped computer and boot into Tails.

You can then perform the manual update steps. In the Tails Cloner, do **not** click the checkbox labeled “Clone the current persistent storage”. This refers to the persistent storage of your *primary Tails USB*. If you leave the checkbox unchecked, the persistent storage of the USB drive you are updating will be preserved.

While writing to the USB disk, Tails may appear to be frozen, or a dialog may appear warning that the application is unresponsive. In the latter case, click **Wait** (repeatedly if needed) until the operation is complete.

If you encounter issues

If you run into issues, you can always restore your data from the backup device following the instructions *here*.

If you continue to have problems, you can contact us through the SecureDrop Support Portal.

1.63 Updates over Tor

In case of censorship or blocking of the SecureDrop APT repository (`apt.freedom.press`), which provides automatic updates, Tor can be configured to provide unrestricted access.

Note

This is only meant as a temporary measure. SecureDrop generally expects an unfiltered internet connection. If you are facing long-term censorship, *please contact us* for other options.

1.63.1 Configuring updates over Tor

These steps will need to be applied to both the *Application Server* and the *Monitor Server*.

As mentioned earlier, this is meant to be a temporary measure. Notably, running `securedrop-admin install` will overwrite these changes.

1. From your *Admin Workstation*, SSH into the *Application Server* or *Monitor Server* using `ssh app` or `ssh mon`.
2. Run `sudo nano /etc/tor/torrc` to edit the Tor configuration. Replace the first line of `SocksPort 0` with `SocksPort 127.0.0.1:9050` and save the file.
3. Run `sudo systemctl reload tor@default` for the new configuration to take effect.
4. Run `sudo apt-get install apt-transport-tor --yes`.
5. Run `sudo nano /etc/apt/sources.list.d/apt_freedom_press.list` to edit the URL to begin with a "tor+" prefix. The new contents should be:

```
deb [arch=amd64] tor+https://apt.freedom.press noble main
```

6. Run `sudo apt update` and verify there are no error messages. This checks that fetching updates works

1.63.2 Disabling updates over Tor

From your *Admin Workstation*, run `securedrop-admin install`. This will overwrite all the above changes.

1.64 Troubleshooting Kernel Updates

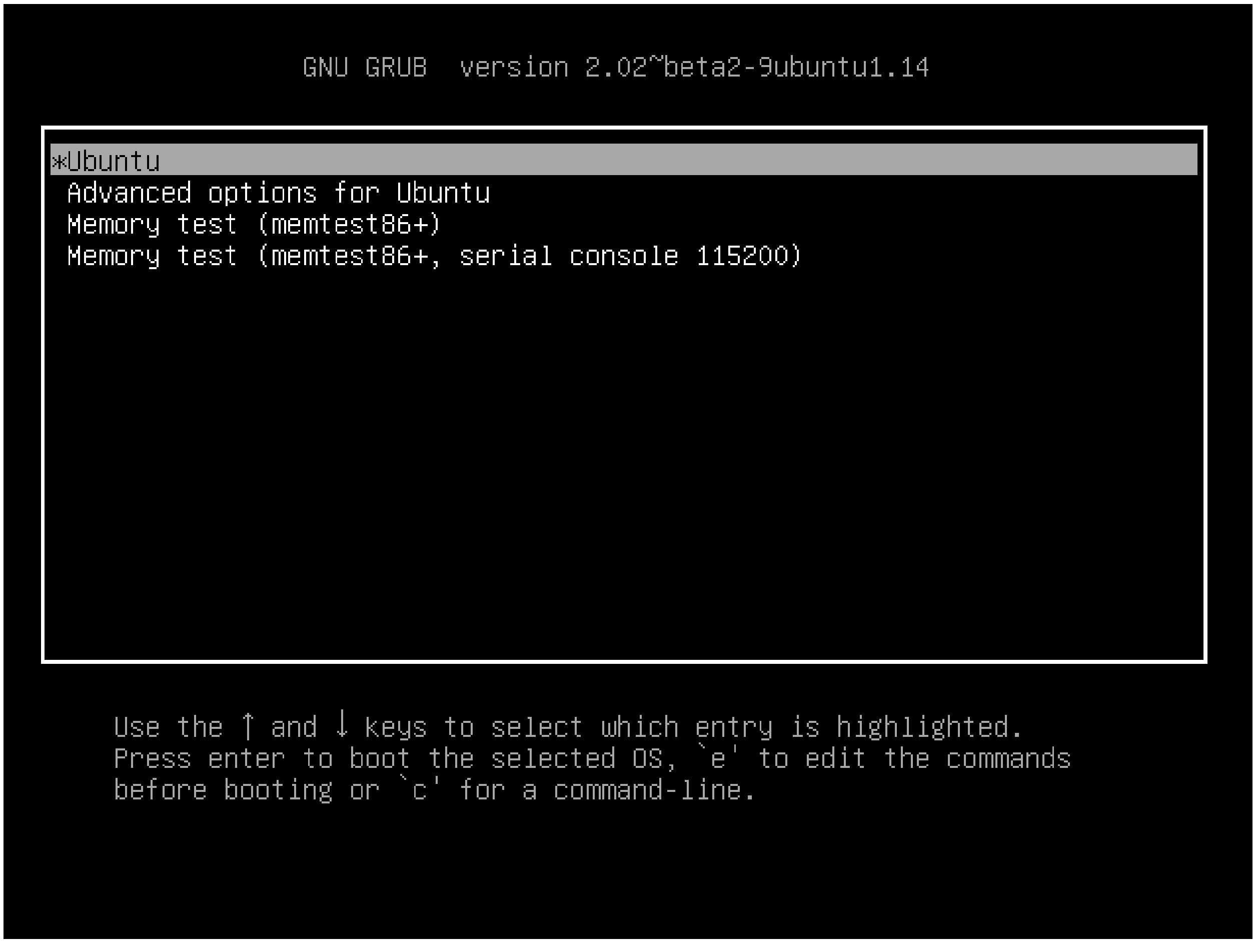
Kernel updates address known bugs and security vulnerabilities in the Linux kernel. They may be installed automatically on your *Application* and *Monitor Servers* as part of a SecureDrop release. All kernel updates are tested extensively against *recommended hardware*. If things do go wrong (e.g., the server does not boot after a kernel update), the following instructions will help you to roll back to the previous, working kernel. You can then *report compatibility issues* to us so we can work together to resolve them as quickly as possible.

First, you need to physically access each server. Power down the server (safely if possible), attach required peripherals (keyboard, monitor), and power the server back up.

If you have access to the password for your admin user, you can use it to log into each server without the use of two-factor authentication, which was disabled for keyboard logins in SecureDrop 0.8.0. You may have saved the password in the KeePassXC database on your *Admin Workstation*. If you do not have the password, you can boot into single user mode instead.

1.64.1 Boot into Single User Mode

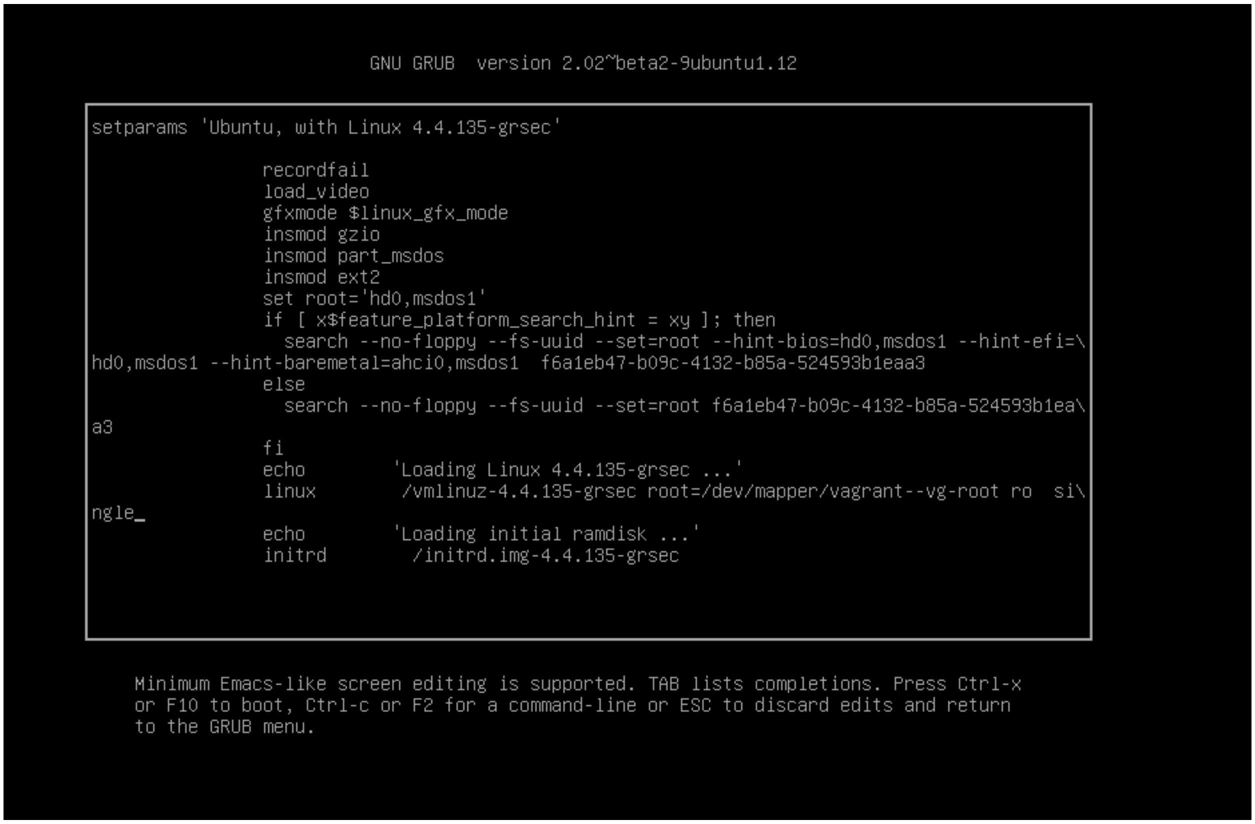
To access single user mode, you will have to edit the boot options for the new kernel. You can do so using the GRUB bootloader, pictured below:



```
                   GNU GRUB  version 2.02~beta2-9ubuntu1.14

 *Ubuntu
  Advanced options for Ubuntu
  Memory test (memtest86+)
  Memory test (memtest86+, serial console 115200)

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, `e' to edit the commands
     before booting or `c' for a command-line.
```

Press any key quickly just once. You will only have about 2 to 3 seconds before Ubuntu starts booting. If you miss that window, just log in normally and reboot safely, provided you can log in. Do not unplug or forcibly shut down the server.

Once you hit a key, you will be able to interact with the menu with the up (↑) and down (↓) keys. Select "Ubuntu" as shown above, and press "e" to edit the boot options. In the line that begins with "linux", add the word "single" at the end. When you are done, the output on your console should look similar to the screenshot below.



```
                        GNU GRUB  version 2.02~beta2-9ubuntu1.12

setparams 'Ubuntu, with Linux 4.4.135-grsec'

                recordfail
                load_video
                gfxmode $linux_gfx_mode
                insmod gzio
                insmod part_msdos
                insmod ext2
                set root='hd0,msdos1'
                if [ x$feature_platform_search_hint = xy ]; then
                  search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-efi=\
hd0,msdos1 --hint-baremetal=ahci0,msdos1  f6a1eb47-b09c-4132-b85a-524593b1eaa3
                else
                  search --no-floppy --fs-uuid --set=root f6a1eb47-b09c-4132-b85a-524593b1ea\
a3
                fi
                echo        'Loading Linux 4.4.135-grsec ...'
                linux        /vmlinuz-4.4.135-grsec root=/dev/mapper/vagrant--vg-root ro  si\
ngle_
                echo        'Loading initial ramdisk ...'
                initrd        /initrd.img-4.4.135-grsec


    Minimum Emacs-like screen editing is supported. TAB lists completions. Press Ctrl-x
    or F10 to boot, Ctrl-c or F2 for a command-line or ESC to discard edits and return
    to the GRUB menu.
```

Press the “F10” key to boot.

1.64.2 Test the New Kernel

Observe the boot process. It is possible that the system will fail to boot completely; if so, the log information will help us to understand what is happening.

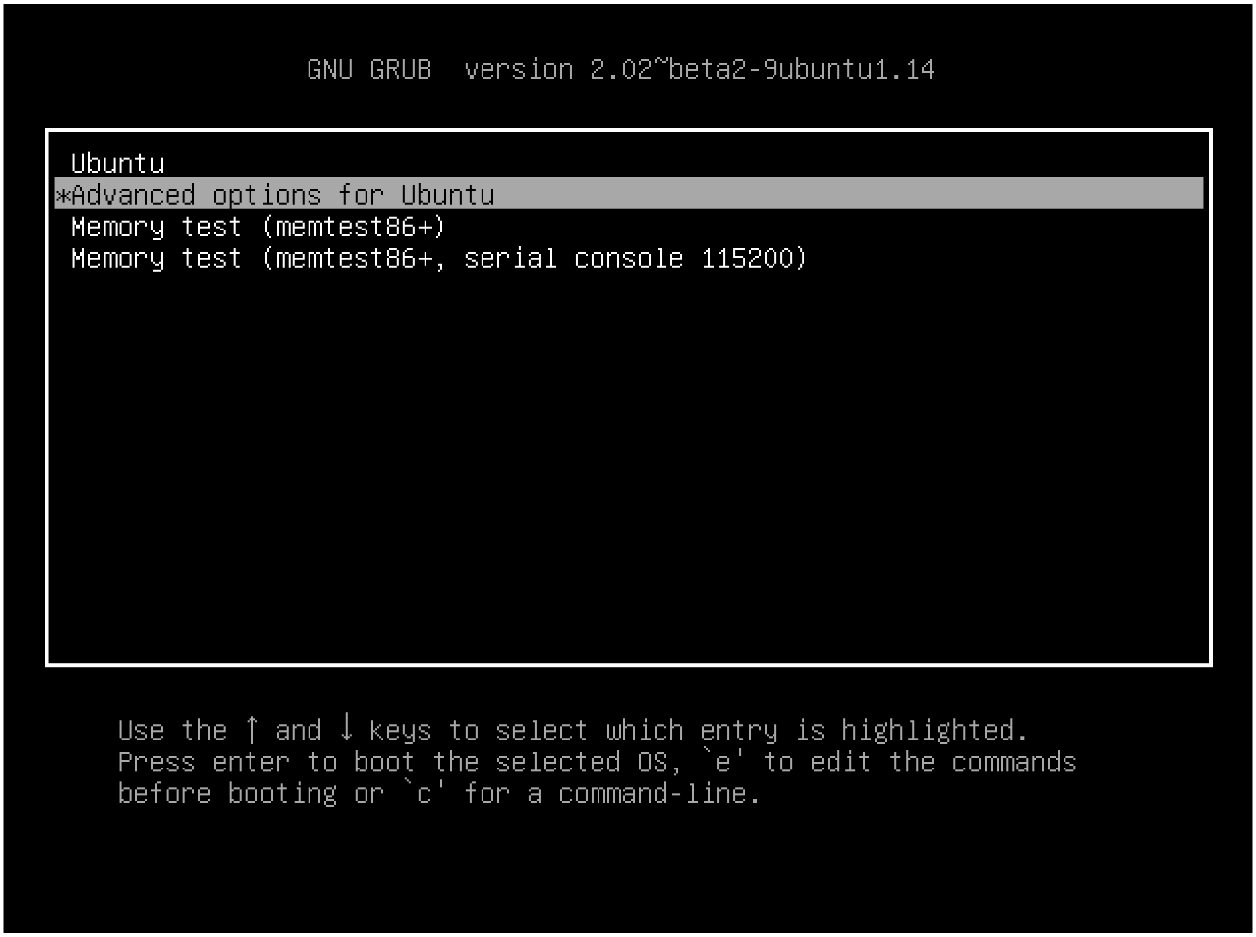
Provided that you can log in, check if you have network access. Try a command such as `sudo host freedom.press`. If you don’t have network access, it is most likely due to the upgraded kernel missing a network driver for your hardware.

If everything appears to be operating normally, the outage may not be kernel-related. In that case, you may still wish to follow the steps at the end of this document to send us log information along with an issue report, and we will help you investigate.

If you are experiencing network issues or other kernel problems, we recommend that you roll back to an older kernel, and that you report the issue to us immediately.

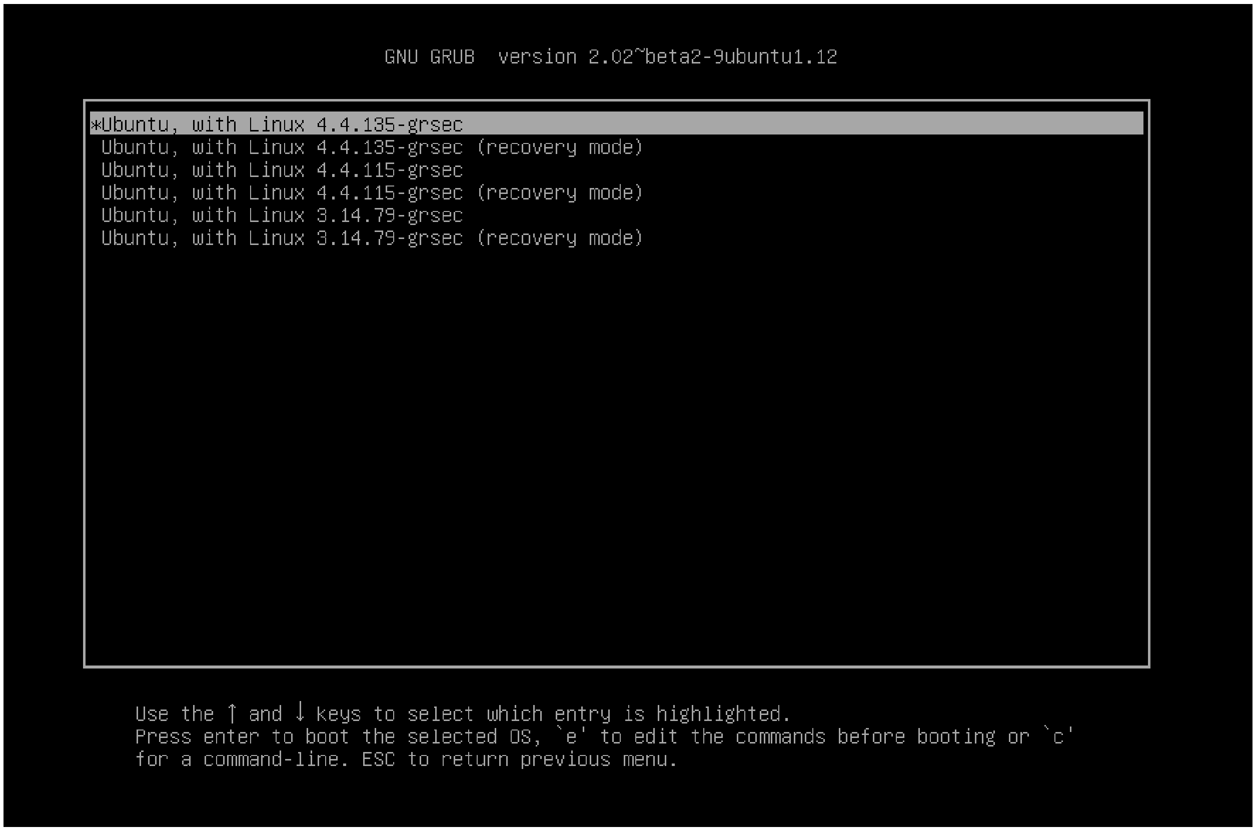
1.64.3 Compare the Behavior of the Old Kernel

Reboot the server in a safe way with `sudo reboot`. After the BIOS screen, you can select a different kernel from the GRUB boot menu by selecting **Advanced options for Ubuntu**, pictured below.



```
                    GNU GRUB  version 2.02~beta2-9ubuntu1.14

 Ubuntu
*Advanced options for Ubuntu
 Memory test (memtest86+)
 Memory test (memtest86+, serial console 115200)


    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands
    before booting or `c' for a command-line.
```

The next menu should give you a list of kernels, similar to the one pictured below:



```
                         GNU GRUB  version 2.02~beta2-9ubuntu1.12

*Ubuntu, with Linux 4.4.135-grsec
 Ubuntu, with Linux 4.4.135-grsec (recovery mode)
 Ubuntu, with Linux 4.4.115-grsec
 Ubuntu, with Linux 4.4.115-grsec (recovery mode)
 Ubuntu, with Linux 3.14.79-grsec
 Ubuntu, with Linux 3.14.79-grsec (recovery mode)

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands before booting or `c'
    for a command-line. ESC to return previous menu.
```

Choose the option with the previous kernel version. If unsure, please consult the release notes for the most recent release of SecureDrop, which will include details about kernel version changes.

As before, you may need to edit the kernel options to enter single user mode. The boot process should proceed normally. Wait until you get a login prompt and log in.

Once you are logged in, check to see if you have network access. If you do, then your instance is having an issue with the newer kernel. In that case, we need to temporarily set an older kernel as the default.

1.64.4 Roll Back to the Old Kernel

> **Important**
>
> It is of critical importance for the security of your instance that we work together to resolve any compatibility issues. Rolling back to an older version is only a stopgap measure to avoid a prolonged outage of your SecureDrop instance.

Inspect the file `/boot/grub/grub.cfg`. You should find a `menuentry` line with the same text that you selected during boot, e.g.:

```
submenu 'Advanced options for Ubuntu'...

  menuentry 'Ubuntu, with Linux 4.xxx.xx-grsec...
```

Take note of its position among the other submenu entries (it will most likely be third). Then edit the GRUB configuration:

```
sudo nano /etc/default/grub
```

Make a backup of the file or take a note of the current value of GRUB_DEFAULT somewhere, so you can restore the previous behavior easily at a later point.

Once you have done so, set the GRUB_DEFAULT variable to point to the index of the menu and submenu. Note that the index starts at 0, so for a typical setup, the line in /etc/default/grub would look like this:

```
GRUB_DEFAULT="1>2"
```

The "1" means the second entry of the main menu ("Advanced options"), the "2" means the third entry of the submenu. Again, update these numbers consistent with your configuration.

Caution

Ensure that you have chosen the right index for the main menu and the submenu, and double-check that you are beginning the count at 0, not 1; otherwise, you may boot into the wrong kernel.

This change still has to be applied to take effect on the next boot:

```
sudo update-grub
```

Now you can reboot into the old, working kernel.

```
sudo reboot
```

The server should come up automatically. From here on, you should be able to perform all administrative tasks via SSH as usual. If you want additional confirmation of the kernel version, the command `uname -r` should display the expected kernel version number.

Please notify us of the compatibility issue so we can help you resolve it ASAP.

1.64.5 Report Compatibility Issues

If you have encountered issues with a kernel update, it is important that you report them to us so that we may incorporate any necessary changes to our updated kernel, and so that we can work with you to switch back to the new kernel as soon as possible.

Run the following commands via SSH from the *Admin Workstation*:

```
source /usr/share/securedrop-admin/venv/bin/activate
cd /usr/share/securedrop-admin/ansible-base
ansible all -b -m setup > ~/server-facts.log
```

Please also send us a copy of /var/log/syslog and /var/log/dmesg for analysis.

You can share server-facts.log, syslog and dmesg with us as follows:

- If you are a member of our Support Portal, please create a new issue and attach the files to it.
- Alternatively, email us at securedrop@freedom.press (GPG encrypted) with the subject "SecureDrop kernel facts" and the files attached.

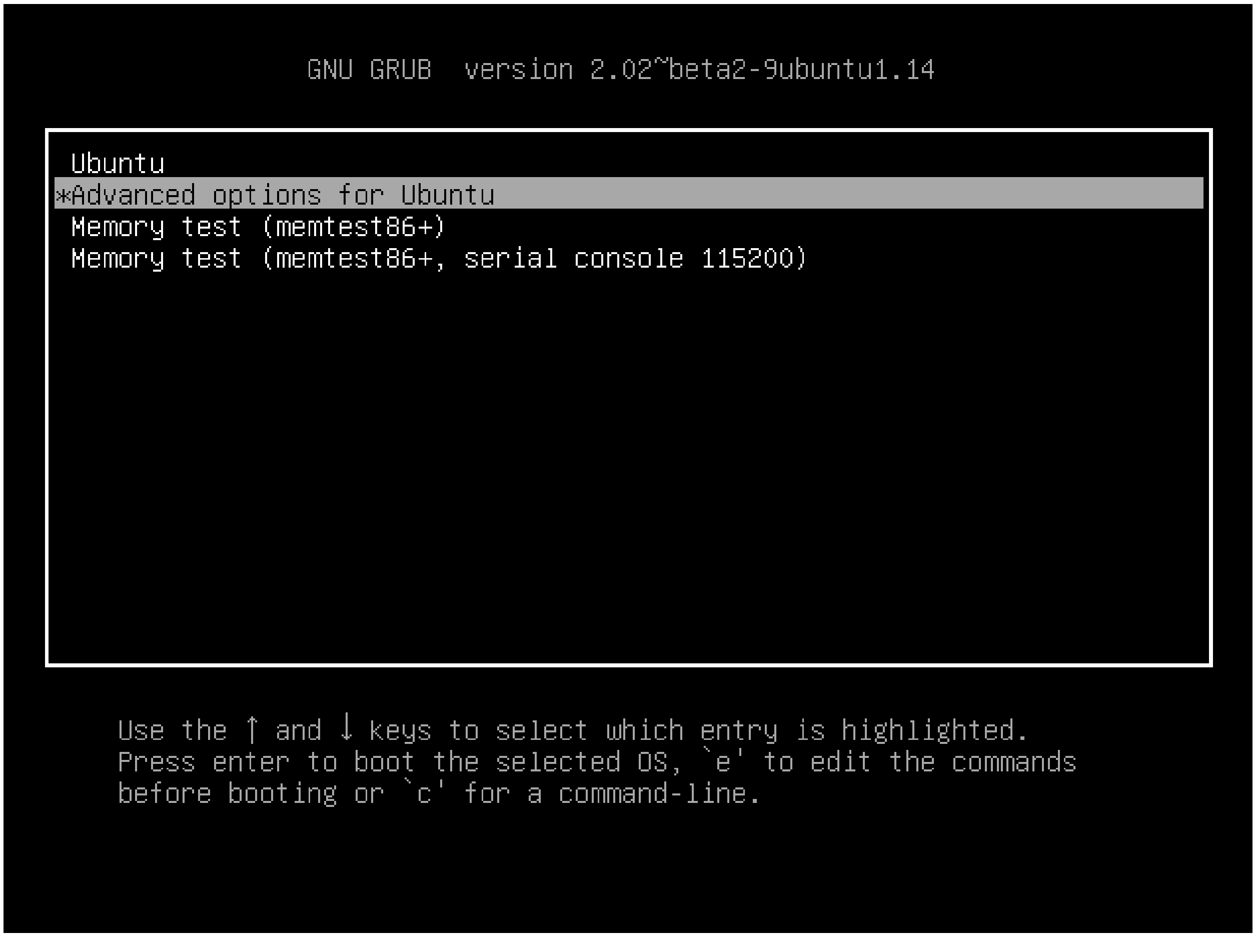
Once we get your information, we can try to provide assistance to resolve compatibility issues.

1.64.6 Test and Enable an Updated Kernel

If you have changed your default kernel, we urge you to test an updated kernel as soon as it becomes available in a future SecureDrop release. Note that an update may be enforced as part of a release to protect the security of your instance. Please consult the release notes for details about kernel updates.

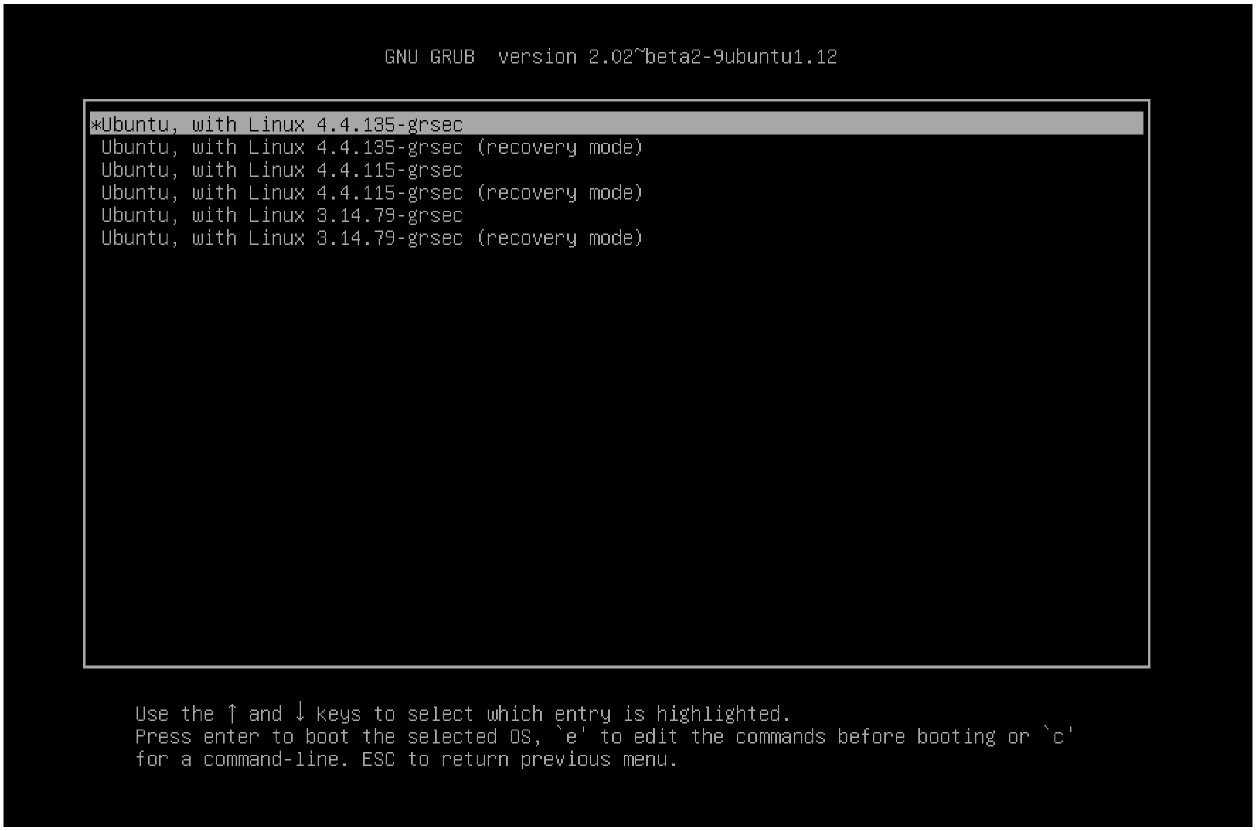
You can test a kernel update without downtime for your instance by booting your *Monitor Server* with the new kernel. Log into your *Monitor Server* using the *Admin Workstation*. Shut down the server safely using the command `sudo poweroff`. Ensure that the server is fully powered off.

Attach required peripherals and power the server back up. After the GRUB bootloader appears, select **Advanced options for Ubuntu**, pictured below.



```
                GNU GRUB  version 2.02~beta2-9ubuntu1.14

 Ubuntu
*Advanced options for Ubuntu
 Memory test (memtest86+)
 Memory test (memtest86+, serial console 115200)

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, `e' to edit the commands
    before booting or `c' for a command-line.
```

If a SecureDrop release with a kernel update has been installed on your system, the updated kernel version will be available in the list of options:



```
GNU GRUB  version 2.02~beta2-9ubuntu1.12

*Ubuntu, with Linux 4.4.135-grsec
 Ubuntu, with Linux 4.4.135-grsec (recovery mode)
 Ubuntu, with Linux 4.4.115-grsec
 Ubuntu, with Linux 4.4.115-grsec (recovery mode)
 Ubuntu, with Linux 3.14.79-grsec
 Ubuntu, with Linux 3.14.79-grsec (recovery mode)

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, `e' to edit the commands before booting or `c'
for a command-line. ESC to return previous menu.
```

Select the new kernel (you do not need to use the version with recovery mode). If you do not know your admin account password, you can *boot into single user mode* by editing the boot options. Otherwise, press enter to boot.

Verify that you can boot successfully, and that you have network access (`sudo host freedom.press`). If you still encounter problems with the new kernel, please *report compatibility issues* at your earliest convenience, and reboot the server into the old kernel for now.

If the update resolved compatibility issues with an earlier kernel version, you can make the new kernel the default. Edit the file `/etc/default/grub`, e.g., by issuing the following command:

```
sudo nano /etc/default/grub
```

Make a backup of the file or take a note of the current value of `GRUB_DEFAULT` somewhere, so you can restore the previous behavior if needed. Change the line to `GRUB_DEFAULT=0`. This configures the bootloader to default to loading the most recent kernel version installed on your server.

This change still has to be applied to take effect on the next boot:

```
sudo update-grub
```

Safely shut down the *Monitor Server*, remove attached peripherals, and reboot it. Verify that it is working correctly by logging in using your *Admin Workstation*. If everything is working as expected, you can make the same change to `/etc/default/grub` on your *Application Server* as well. Remember to again run the command `sudo update-grub` when you are done.

You can make the change on the *Application Server* from your *Admin Workstation* and reboot the server using the command `sudo reboot`.

Subsequent kernel updates will again be applied automatically.

1.65 Rebuilding an *Admin Workstation* USB

In cases where an *Admin Workstation* USB stick has been lost or destroyed, and no backup exists, it is possible to rebuild one. In order to do so, you'll need

- physical access to the SecureDrop servers
- 2 USB sticks:
  - Tails Template USB
  - 1 replacement *Admin Workstation* USB (USB3 and 16GB or better recommended)

The process requires experience with the Linux command line and Tails, and can take up to 3 hours. If a backup of the SecureDrop application server is available, *reinstalling the instance and restoring the backup* may be simpler. An outline of the steps involved in rebuilding an *Admin Workstation* is as follows:

1. Prepare the USB sticks.
2. (Optional) Boot the *Application* and *Monitor Server* in single user mode and reset the shell admin account password.
3. Set up SSH access for the new *Admin Workstation*.
4. Retrieve SecureDrop configuration settings from the *Application* and *Monitor Server*.
5. Back up and configure the SecureDrop application.
6. Run `securedrop-admin install` and `securedrop-admin localconfig` from the new *Admin Workstation*.
7. Configure SSH-over-TOR.
8. Complete post-rebuild tasks.

> **Important**
>
> The rebuild process involves temporarily removing `iptables` rules on the *Application* and *Monitor Servers*, weakening their security. Because of this, it's important to complete the rebuild process promptly, to avoid leaving the servers in an insecure state.

1.65.1 Step 1: Prepare the USB sticks

First, create a new Tails *create a new Admin Workstation USB* and set up a persistent volume with a strong passphrase.

Once persistence has been set up, start up the *Admin Workstation* with persistence enabled, *install the SecureDrop application code, and set up the KeePassXC database*.

The *Admin Workstation* uses SSH with key authentication to connect to the servers, so you'll need to create a new SSH keypair for your SecureDrop instance. To do so, open a terminal by navigating to **Apps ▸ System Tools ▸ Console**, and run the following command:

```
ssh-keygen -t rsa -b 4096
```

When prompted to `Enter file in which to save the key`, Press **Enter** to use the default location. When prompted for a passphrase, it's safe to leave it blank.

1.65.2 Step 2: (Optional) Boot the servers in single-user mode

If you do not have the original password for the shell admin account on the *Application* and *Monitor Servers*, you'll need to reset the password on each server by booting in single user mode. In order to do so, you'll need physical access to the server, a keyboard, and a monitor.

First, connect a monitor and keyboard to the *Monitor Server*. Then reboot the server. Enter the GRUB menu (instructions vary by hardware), ensure the **Ubuntu** entry is highlighted, and press **e** to edit boot options.

In the boot options for Ubuntu, find the line that starts with `linux` and ends with `noefi ipv6.disable=1 quiet`. Add `single` after `quiet`, separated by a space, and press **F10** to boot in single user mode.

Reset the SecureDrop admin user's password

Once the root prompt appears, you'll need to reset the password for the SecureDrop admin user. By default this user is named *sdadmin* and has UID 1000. However it may have been named differently during the installation of your instance. You can use the command `getent passwd 1000` to check the username corresponding to UID 1000. Once you have the correct username, reset its password using the *passwd* command, for example:

```
passwd sdadmin
```

Important

Make sure to select a strong password, and record it in the *Admin Workstation's* KeePassXC database.

Finally, reboot the *Monitor Server* and verify that you can log in at the console using the new password.

Repeat the process for the *Application Server*. Use the same username and password as for the *Monitor Server* - this is required in order for the `securedrop-admin install` command to work correctly.

1.65.3 Step 3: Set up *Admin Workstation* access

Next, you'll configure the servers to allow temporary SSH access from the new *Admin Workstation*.

First, start the new *Admin Workstation* with persistence enabled and an administration password set.

Next, connect the new *Admin Workstation* to the *Hardware Firewall* via the appropriate Ethernet port, and set up its static IP address. For more information on how to do so, see *this section in the firewall setup documentation*. If you do not know the correct static IP address for the *Admin Workstation*, and you are using a recommended pfSense-based *Hardware Firewall*, you can retrieve the address by logging into its admin interface and checking the settings under **Firewall ▶ Aliases**.

Note

If you do not have login credentials for your pfSense firewall, check its user manual for instructions on resetting the administration password.

Next, determine whether your instance was set up to allow administrative access via SSH over Tor, or via SSH over LAN. If you don't know which option was originally chosen, you can check as follows:

1. Log in to the *Application Server* via the console using the adminstration username and password.
2. Check to see if an SSH hidden proxy service exists, using the command `sudo cat /var/lib/tor/services/sshv3/hostname`. If this file exists and includes an Onion URL, your instance is set up to use SSH over Tor and you should configure temporary SSH access using *these instructions*. If not, your instance is set up to use SSH over LAN, and you should follow *these instructions instead*.

Configuring access for an SSH-over-Tor instance

Direct SSH access is disabled when the SSH-over-Tor option is selected during installation. To temporarily re-enable it, you'll need to update `iptables` rules and change the sshd daemon's configuration.

First, log on to the *Application Server* via the console, and run the following commands, substituting the *Admin Workstation's* static IP for `<admin_static_ip>`:

```
sudo iptables -I INPUT -p tcp --dport 22 -s <admin_static_ip> \
  -m state --state NEW,ESTABLISHED -j ACCEPT
sudo iptables -I OUTPUT -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT
```

Next, edit the file `/etc/ssh/sshd_config`, changing the line:

```
ListenAddress 127.0.0.1:22
```

to:

```
ListenAddress 0.0.0.0:22
```

and deleting the line:

```
PasswordAuthentication no
```

Restart `sshd` using the command `sudo systemctl restart ssh`.

Then, use the command `ip a` to note the local IP address of the default Ethernet interface. You'll need it in the next step.

Repeat the process above for the *Monitor Server*, making sure to note its local IP address as well.

Once the *Monitor Server* has been configured, proceed to *enable access from the new Admin Workstation*.

Configuring access for an SSH-over-LAN instance

First, log on to the *Application Server* via the console and edit the file `/etc/ssh/sshd_config`, deleting the line:

```
PasswordAuthentication no
```

Restart `sshd` using the command `sudo systemctl restart ssh`.

Then, use the command `ip a` to note the local IP address for the default Ethernet interface. You'll need it in the next step.

Repeat the process above for the *Monitor Server*, making sure to note its local IP address as well.

Enabling access from the new *Admin Workstation*

From the *Admin Workstation*, open a terminal and copy the *Admin Workstation's* SSH public key to the servers, substituting the values for the server administration username and server IP addresses in the commands below and entering the admin account's password when prompted:

```
ssh-copy-id <admin-username>@<application-server-ip>
ssh-copy-id <admin-username>@<monitor-server-ip>
```

Next, create a file `~/.ssh/config` with contents as below, again substituting the appropriate values for your servers:

```
Host app
  User <admin-username>
  Hostname <application-server-ip>
  ProxyCommand none

Host mon
  User <admin-username>
  Hostname <monitor-server-ip>
  ProxyCommand none
```

Finally, test direct SSH access from the terminal, using the commands `ssh app` and `ssh mon`. It should be possible to connect without entering a password.

1.65.4 Step 4: Retrieve SecureDrop configuration info from the servers

In addition to the account and networking information retrieved from the servers so far, you'll need to retrieve the following files and info:

- GPG *Submission Public Key*, *OSSEC Alert Public Key*, and (optional) *Journalist Alert Public Key*
- OSSEC alert configuration details
- (Optional) HTTPS configuration details

Retrieve GPG Public Keys

Copy the *Submission Public Key* with the following commands:

```
echo "$(ssh app sudo cat /var/lib/tor/services/sourcev3/hostname)" > /tmp/sourcev3
cd ~/.config/securedrop-admin
curl http://$(cat /tmp/sourcev3)/public-key > SecureDrop.asc
gpg --import SecureDrop.asc
```

Validate that the imported key's fingerprint matches the one on your SecureDrop install. You can do this by running the command:

```
gpg --with-fingerprint --import-options import-show --dry-run --import SecureDrop.asc
```

Then, compare the returned fingerprint value with that advertised by your *Source Interface*, using the command:

```
curl http://$(cat /tmp/sourcev3)/metadata
```

Next, note the OSSEC Alerts email address (`OSSEC_EMAIL`) and, if applicable, the Journalist Alerts email address (`JOURNALIST_EMAIL`):

```
ssh mon sudo cat /var/ossec/send_encrypted_alarm.sh | grep _EMAIL= | cut -f7 -d' '
```

Import the *OSSEC Alert Public Key* using the following commands (substituting the appropriate email address for `alerts@example.com`):

```
ssh mon sudo gpg --homedir=/var/ossec/.gnupg --export --armor alerts@example.com > ossec.
↪pub
gpg --import ossec.pub
```

If a Journalist Alerts address has been configured, repeat this step for the *Journalist Alert Public Key*, naming it `journalist.pub` or similar.

You will require the fingerprints for these keys during the next step, which you can obtain via the command:

```
gpg -k --fingerprint
```

Retrieve OSSEC alert configuration details

You'll also need to retrieve the following configuration information:

- SMTP server
- SMTP port
- SASL username
- SASL domain
- SASL password

To retrieve these values, use the following command in the terminal:

```
ssh mon sudo cat /etc/postfix/sasl_passwd
```

This will return a line like:

```
[smtp.gmail.com]:587 testossec@gmail.com:AwfulPassword
```

In this example, `smtp.gmail.com` is the SMTP server, `587` is the SMTP port, `testossec` is the SASL username, `gmail.com` is the SASL domain, and `AwfulPassword` is the SASL password.

(Optional) Retrieve HTTPS certificate files

If your *Source Interface* was configured to use HTTPS, you will need to copy three related files from the *Application Server* to the *Admin Workstation*.

To retrieve these files, use the commands:

```
cd ~/.config/securedrop-admin
ssh app sudo tar -c -C /var/lib ssl/  | tar xvf -
```

These commands will create a directory named `~/.config/securedrop-admin/ssl` on the *Admin Workstation*, containing your instance's SSL certificate, certificate key, and chain file. When prompted for the names of these files during the next step, you should specify them relative to the `~/.config/securedrop-admin/` directory, i.e. as `ssl/mydomain.crt`.

1.65.5 Step 5: Configure and back up the Application Server

Next, configure the SecureDrop application using the files and info retrieved in the previous steps. To do so, connect to the Tor network on the *Admin Workstation*, open a Terminal and run the following commands:

```
securedrop-admin sdconfig
```

The `sdconfig` command will prompt you to fill in configuration details about your instance. Use the information retrieved in the previous steps. When prompted whether or not to enable SSH-over-Tor, type **no**.

Next, back up the Application server by running the following command in the terminal:

```
securedrop-admin backup
```

Ensure the backup command completes successfully.

1.65.6 Step 6: Use the installer to complete the configuration

Run:

```
securedrop-admin install
```

Once the command completes successfully, run

```
securedrop-admin localconfig
```

Once this command is complete:

- verify that the *SecureDrop Menu* for the *Source* and *Journalist Interfaces* works correctly, opening their respective homepages in Tor Browser.

To revert the changes made to enable temporary local SSH access, you should reboot the servers, by issuing the following commands in a terminal:

```
ssh app sudo reboot
ssh mon sudo reboot
```

1.65.7 Step 7: Set up SSH-over Tor

> **Note**
>
> Without performing this step, you will not be able to access your SecureDrop servers from outside the local network. See *SSH Over Local Network* for more information.

Rerun the command:

```
securedrop-admin sdconfig
```

Press "Enter" to use the pre-populated values, but when asked whether to configure SSH-over-Tor, type **yes** (recommended).

Then, re-run

```
securedrop-admin install
```

When the installation completes, run:

```
securedrop-admin localconfig
```

Once this command completes:

- verify that the Hostname references in `~/.ssh/config` have been updated to refer to Onion URLs instead of direct IP addresses
- verify that you can connect to the servers using `ssh app` and `ssh mon`
- verify that the *SecureDrop Menu* for the *Source* and *Journalist Interfaces* works correctly, opening their respective homepages in Tor Browser.

1.65.8 Step 8: Post-rebuild tasks

Important

Rebuilding an Admin Workstation makes changes that will prevent your other Tails workstations from connecting to your SecureDrop servers. If you rebuild your Admin Workstation, you must also provision all other existing Tails Workstation USBs with updated Tor credentials (see below).

We recommend completing the following tasks after the rebuild:

- Set up a new administration account on the *Journalist Interface*, by following *these instructions*
- Verify that submissions can be decrypted, by going through the decryption workflow with a new submission.
- Back up your *Admin Workstation* using the process *documented here*.
- Delete invalid admin accounts in the *Journalist Interface*.
- Restrict SSH access to the *Application* and *Monitor Servers* to valid *Admin Workstations*. If your new *Admin Workstation* USB stick is the only one that should have SSH access to the servers, you can remove access for any previous *Admin Workstations* from the terminal, using the commands:

  ```
  securedrop-admin reset_admin_access
  ```

  You can also selectively remove invalid keys by logging on to the *Application* and *Monitor Servers* and editing the file ~/.ssh/authorized_keys, making sure not to remove the public key belonging to your new *Admin Workstation*.
- *Back up the Application server* once SSH-over-Tor has been restored. Ensure that server and workstation backups happen regularly.
- Provision all other Tails Workstation USBs (*Journalist* and/or *Admin Workstations*) with updated Tor credentials, so that they can access SecureDrop after this rebuild.

  You will need to copy the following file(s) to all other *Admin* and *Journalist Workstations*, replacing the existing files of the same name:

  ```
  ~/.config/securedrop-admin/app-journalist.auth_private
  ~/.config/securedrop-admin/tor-v3-keys.json # for Admin Workstations only
  ```

  You may copy these files using a *Transfer Device* (which must be wiped afterwards), or boot into each of your additional Tails workstations, plug in and unlock your *Admin Workstation*'s encrypted partition via the **Places** app, and manually copy the file(s) from the Admin Workstation to the same directory on the target Tails workstation.

1.66 BIOS Updates on the Servers

Below are the steps for updating the BIOS on the *Application* and *Monitor Servers*. We provide instructions for Intel and ASUS NUC devices, in accordance with *our hardware recommendations*. You should also update the BIOS on other computers such as the *Admin Workstation,* but those instructions will vary depending on the manufacturer and model of your device.

1.66.1 What you need

1. A clean USB device to download the BIOS file
2. An Internet-connected workstation, such as the *Admin Workstation*

3. A UPS (uninterrupted power supply), such as a surge-protecting power supply with a backup battery (This is not required, but strongly recommended)
4. A keyboard and monitor

1.66.2 Perform Backups

If you are updating the BIOS on an existing SecureDrop system, we recommend you *back up the Application Server* before proceeding.

1.66.3 Prepare the USB Stick

Using the Disks application, delete existing partitions on the USB device, if applicable, and reformat the entire device with one FAT32 partition. Note that you will lose access to all existing data on this USB stick.

1.66.4 Download and Verify Appropriate BIOS Files

For Intel and ASUS NUC Devices

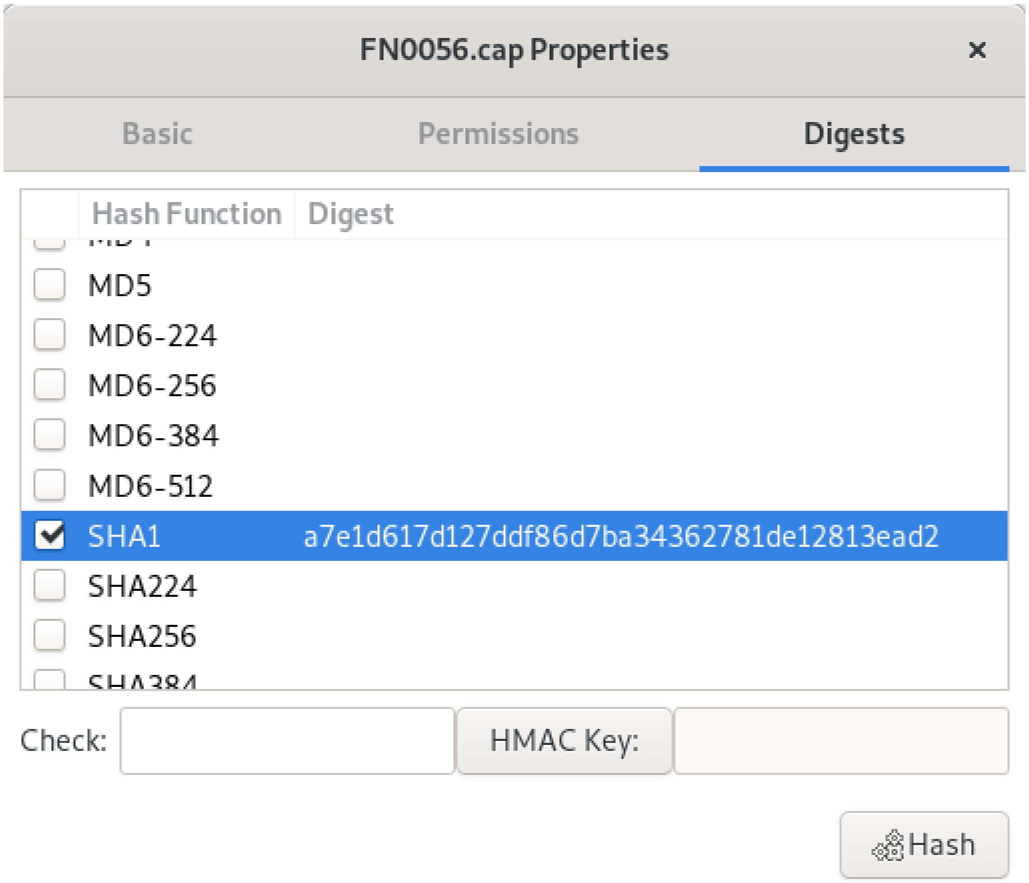
Check the make and model of your servers, and follow the F7 BIOS update method in the documentation. The exact instructions vary by model:

- BIOS update instructions for Intel NUC with Intel Visual BIOS
- BIOS update instructions for Intel NUC with Aptio V UEFI Firmware Core
- BIOS update instructions for ASUS NUCs

Each make and model of NUC will offer different file types; proceed to either the Intel or ASUS Download Center and download the file indicated in the documentation for the F7 method (e.g., `.bio` or `.cap`).

> **Warning**
>
> Do not download BIOS updates from anywhere other than the manufacturer's website. Be sure that you are on the correct website and that it has a valid SSL Certificate. Intel's SSL Certificate is issued to *.intel.com and signed by DigiCert. ASUS' SSL Certificate is issued to *.asus.com and signed by Amazon. Be sure you download the files specific to the model of your servers.

Intel provides an SHA1 checksum on the download page, while ASUS offers a SHA-256 checksum. Once you have downloaded the file, using the **Files** application, browse to the file, right click and select **Properties ▶ Digests**, select either SHA1 or SHA256 depending on which is available to you, and click Hash. Compare the result in the Digest column to the checksum listed on the manufacturer's website. If these two values do not match, do not proceed, and contact support@freedom.press. Tails provides a detailed explanation of this process. (Note that the hash in the screenshot below is an example only, and will not match your specific file.)



FN0056.cap Properties

	Hash Function	Digest
□	MD5	
□	MD6-224	
□	MD6-256	
□	MD6-384	
□	MD6-512	
☑	SHA1	a7e1d617d127ddf86d7ba34362781de12813ead2
□	SHA224	
□	SHA256	
□	SHA384	

Once you have verified the hash, copy the file to your USB device.

1.66.5 Update the BIOS

Power off the *Monitor Server*. We recommend plugging it into an uninterrupted power supply (UPS). Plug in the keyboard, monitor, and USB key, and power on the server, then press F7 when prompted to enter the BIOS Update tool.

Select the USB device and navigate to the file you have downloaded, then hit **Enter**. The update will take several minutes–do not interrupt the update or unplug the server during this time.

Repeat these steps on the *Application Server*.

1.67 Decommission SecureDrop

The following steps will guide you through the decommissioning of your SecureDrop instance.

1. **Put a notice in advance on your landing page to inform sources that your instance will soon be retired.** You may want to direct them to other secure methods of contacting you.
2. **Locate and create an inventory of all your hardware.**
    - *Journalist Workstation* USBs
    - *Admin Workstation* USBs
    - *Secure Viewing Station* USB

- *Secure Viewing Station* computer
- *Transfer* and *Export Devices* (USBs, optical drives, or external drives)
- Backup USBs/other storage media
- Servers
- Firewall

You may also want to inventory credentials, such as the email address or alias and PGP key used for receiving OSSEC alerts, in order to retire them.

> **Note**
>
> The recommended SecureDrop setup includes only one *Secure Viewing Station* USB. However, if you have been working remotely or have a non-standard setup, you may have more than one *SVS USB*. It is important that you locate all of these USBs, since they hold the most sensitive data.

3. **Optional: Save a backup.** If you want to save a backup of the *Application Server* (for example, to reinstall SecureDrop in the future using the same *.onion* address), follow our *backup guidelines*. Once the backup has been created, you can move it off of the *Admin Workstation* USB and onto an encrypted device, such as a LUKS-encrypted drive. You will also require a backup of the *Submission Key* found on the *SVS*.

   If you do not require a server backup, you may choose to download specific submissions, and store them in a secure manner (such as on an encrypted drive). If you export and store these submissions without first decrypting them on the *SVS*, be sure you maintain access to the *Submission Private Key* found on the *SVS* so that you can decrypt them at a later time.

4. **Optional: Delete submissions on the server.** Log into the *Journalist Interface* and delete all sources to take advantage of SecureDrop's secure deletion properties. Note that depending on the number of sources on your server, it may take anywhere from several minutes to an hour or more for the submissions to be completely deleted from the server.

   You can either leave the server ample time to complete this operation, or monitor the progress by SSHing to the Application server and running

   ```
   sudo journalctl -f
   ```

   You will see repeated log lines that contain the following:

   ```
   [Timestamp] app python [...] INFO Clearing shredder
   [Timestamp] app python [...] INFO Files to delete: <number>
   ```

   When the number of files to delete reaches 0, the process is complete.

5. **Disconnect the firewall and the servers from the internet.** Be sure to inform your network administrator of any changes to devices on your network.

6. **Wipe and destroy the USB drives.** Because the USB drives used for SecureDrop are all LUKS-encrypted, reformatting the USB drives (in particular, overwriting a portion of internal storage called the **LUKS header**) should be sufficient to make any existing data on those drives unrecoverable.

   For example, you could use your *Template Tails USB* to launch Gnome Disks, insert and identify the USB drive you are trying to erase, and reformat this drive with a new, LUKS-encrypted partition, erasing the existing partition data.

> **Caution**
>
> Be **very** sure you are reformatting the right drive. You may want to use the Secure Viewing Station laptop for this procedure to reduce the risk of accidentally erasing a drive on your regular-use machine.

You may also choose to destroy the drives by physical means, such as using a hammer or purpose-built shredder to pulverize or destroy the drive.

7. **Wipe and destroy the storage drives on the servers.** SecureDrop submissions are stored GPG-encrypted on the *Application Server*. Unless your SecureDrop *Submission Key* is compromised (or a significant vulnerability in GPG is discovered), access to the servers does not guarantee access to the submissions and messages you have received.

   That said, there may still be some sensitive information on the servers, including system logs and the SecureDrop database, which would yield information on the number of submissions and replies stored on the server. This risk is partially mitigated by securely deleting submissions from the server, as described in a previous step; however, physically destroying or encrypting the storage drives on the servers are the best ways to ensure that data on the drives cannot be recovered.

   Physically destroying SSD drives is not as straightforward as destroying older hard drives, but drives can be pulverized, shredded, or incinerated, as long as the flash chips are destroyed.

   If those options are not available, you may choose instead to write over the information on the existing drives. Most SSDs support ATA Secure Erase, although the implementation of this feature varies by manufacturer.

   Another option is to re-install a clean version of Ubuntu server with full- disk encryption enabled. During the disk-partitioning portion of the installation wizard, select *Guided - use entire disk and set up encrypted LVM*. You will need to reclaim the space that was taken up by your previous installation, so whenever prompted to unmount and reclaim unused partitions, select “yes.”

8. **Destroy other Transfer or Export media, if applicable.**

9. **Optional: Factory-reset the firewall.**

10. **Update your Landing Page (tips page) to reflect the fact that your organization no longer has SecureDrop.**

11. **Notify the SecureDrop Support team that your instance is no longer active.** If you have any questions about the decommissioning process, or about other secure communications options, please feel free to contact us at securedrop@freedom.press (GPG encrypted) or via the support portal.

1.68 Upgrade from 2.12.10 to 2.13.0

1.68.1 Changes in SecureDrop 2.13.0

SecureDrop 2.13.0 marks a major change from previous versions: the `securedrop-admin` tool is now provided as a Debian package installed on Tails using `apt` and available system-wide, instead of being run directly from a cloned version of the SecureDrop Git repository.

Some key changes you should be aware of:

- The `~/Persistent/securedrop` directory is no longer used.
- The `securedrop-admin` utility is installed in the default path and can be run as `securedrop-admin <command>` in a terminal window.
- Configuration and backup files will now be stored in `~/.config/securedrop-admin`.
- The GUI updater is no longer required.

For more details, see the announcement for this release.

1.68.2 Update Workstations to SecureDrop 2.13.0

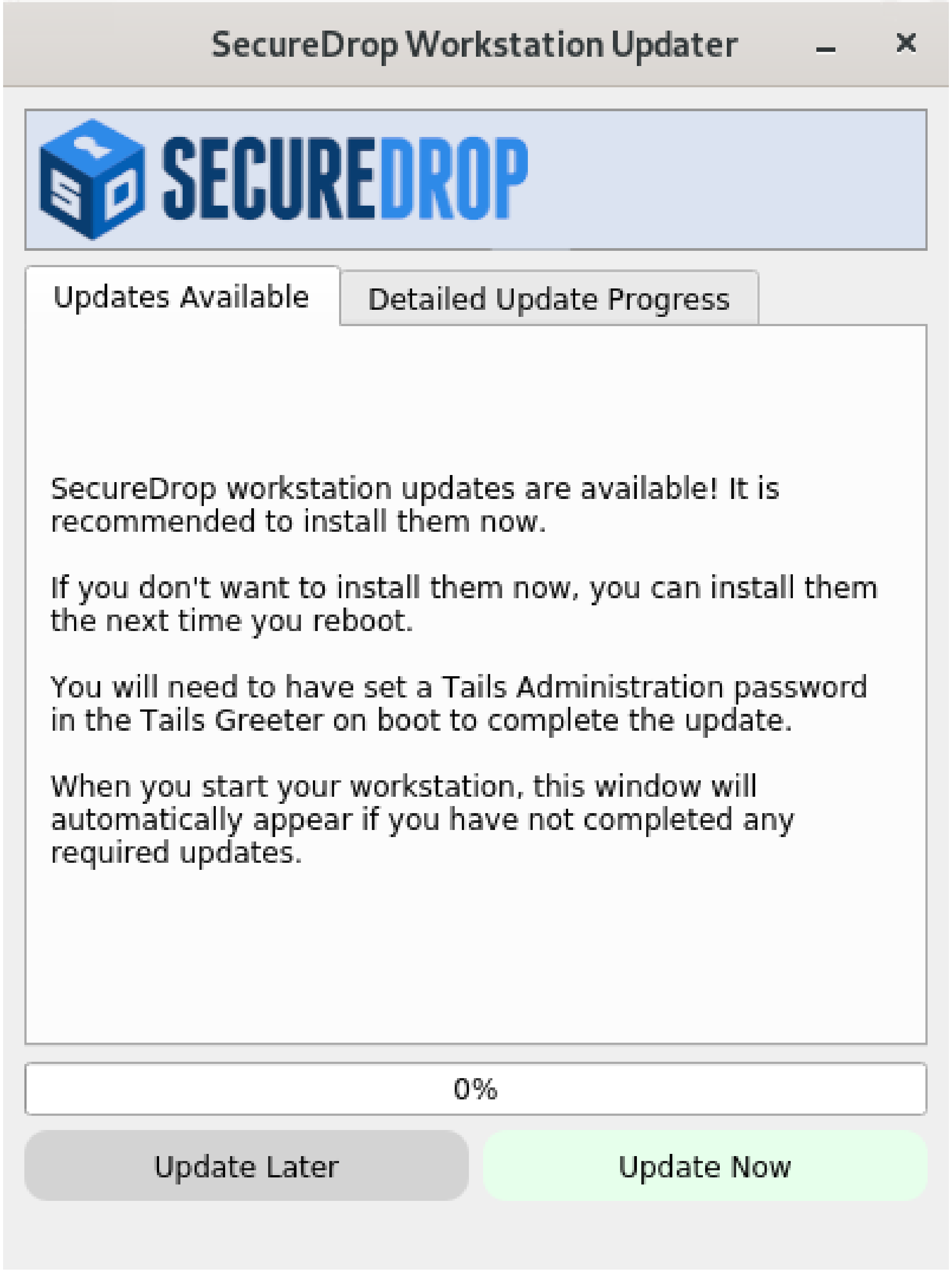
Important

We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.13.0 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.13.0 by clicking "Update Now":



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.13.0
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.13.0
```

Important

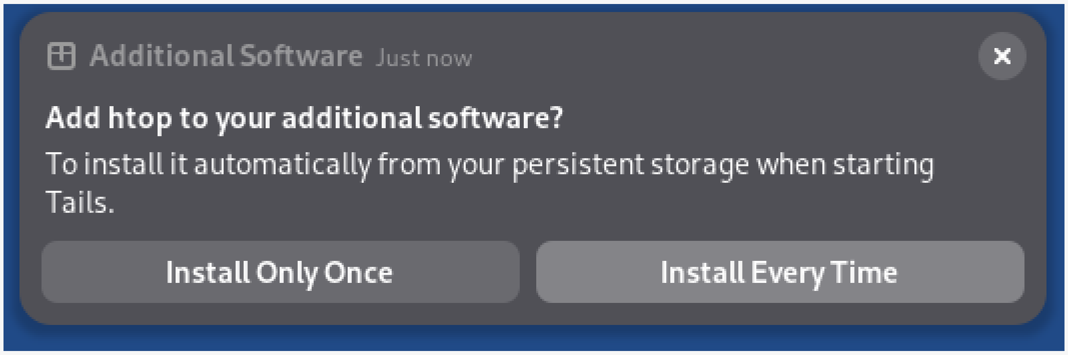
If you do see the warning "refname '2.13.0' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Next, run the following commands:

```
sudo apt update
./securedrop-admin setup
```

Note

The apt persistence feature will prompt to install the package automatically from persistent storage on each boot. Click **Install Every Time**:



Additional Software Just now

Add htop to your additional software?

To install it automatically from your persistent storage when starting Tails.

When the *./securedrop-admin setup* command has completed, reboot the the workstation to complete the upgrade.

1.68.3 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.69 Upgrade from 2.12.9 to 2.12.10

This version of SecureDrop coincides with the release of Tails 7. SecureDrop 2.12.10 adds compatibility with Tails 7, but is not compatible with earlier versions of Tails. Consequently, your *Journalist* and *Admin Workstations* Tails USBs also require a manual upgrade to Tails 7. To complete the entire upgrade process successfully, you must follow the steps below in order.

1.69.1 Update Workstations to Tails 7 and SecureDrop 2.12.10

Warning

We **strongly** recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

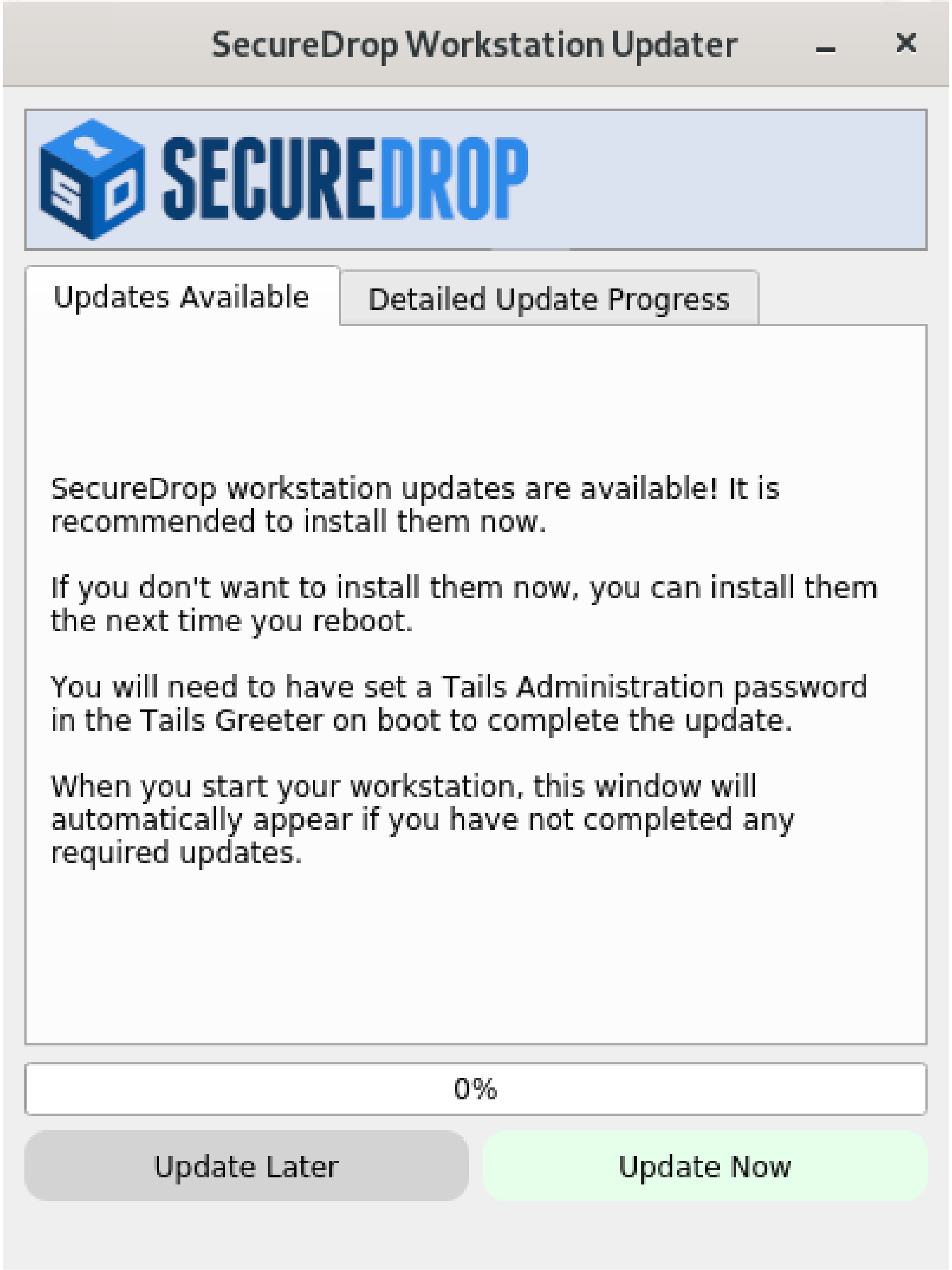
1. Begin upgrade to SecureDrop 2.12.10 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Important

Only begin the upgrade using the graphical updater if you are prepared to subsequently upgrade the Tails USB to Tails 7.

If you are ready, select the “Detailed Update Progress” tab and initiate the update to 2.12.10 by clicking “Update Now”:



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

The updater will fail with the following error:

```
This version of securedrop-admin requires Tails 7 or later.
```

This error is expected and you should proceed to the next step.

2. Create Tails 7 USB drive

To manually upgrade each Tails 6 USB to Tails 7, you can use a fresh Tails 7 USB and the Tails Cloner tool. This process will upgrade Tails and preserve your Persistent Storage, where SecureDrop lives.

Obtain a new USB drive and install Tails 7 on it. The Tails website has detailed and up-to-date instructions on how to download and verify Tails, and how to create a Tails USB drive. Follow the instructions at these links to create a fresh Tails 7 USB drive, and then return to this page:

- Download and verify the Tails image file
- Install onto a USB drive

Important

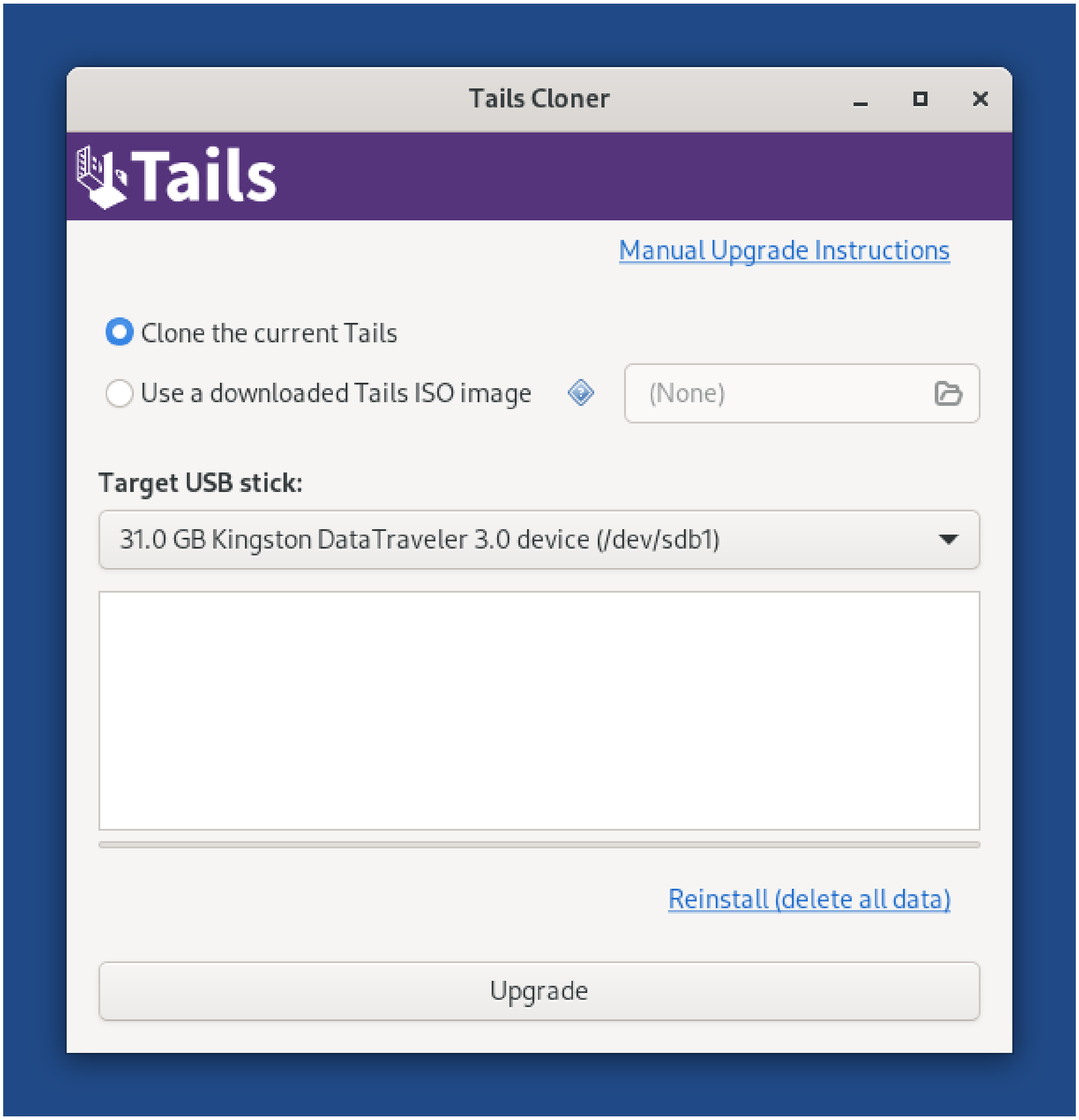
Make sure you verify the Tails .img file using one of the methods described on the Tails website.

3. Upgrade Tails 6 USB drives manually using Tails Cloner

You now have a new Tails 7 USB and several Tails 6 USBs (all your *Admin* and *Journalist Workstations*). A Tails 6 USB can be upgraded using the Tails Cloner tool running on the Tails 7 USB as described in the following steps. You will need to repeat the process to upgrade each *Admin* and *Journalist Workstation* to Tails 7.

- **3.1.** Plug your new Tails 7 USB into an airgapped computer, such as your *Secure Viewing Station* computer, and boot into Tails 7.
- **3.2.** At the Tails welcome screen, select your language and keyboard layout, if needed, and then click "Start Tails". Do not select "Create Persistent Storage".
- **3.3.** Once Tails has started, attach the Tails 6 USB you wish to upgrade (either a *Admin* or *Journalist Workstation*) to the computer.
- **3.4.** Open the Tails Cloner tool via **Apps ▶ Tails ▶ Tails Cloner**.

  The Tails Cloner will detect your attached Tails 6 USB and designate it the "Target USB stick". The upgrade process will clone the Tails 7 system from the booted Tails 7 USB to the attached Tails 6 USB, leaving the Persistent Storage intact.



● Clone the current Tails

○ Use a downloaded Tails ISO image (None)

Target USB stick: 31.0 GB Kingston DataTraveler 3.0 device (/dev/sdb1)

- **3.5.** Click “Upgrade” to begin this process.
- **3.6.** Once the process is complete, you can close the Tails Cloner and remove the newly-upgraded *Admin* or *Journalist Workstation* USB drive. Be careful not to accidentally remove the Tails 7 USB that was used to boot the computer.

You can repeat these steps on another Tails 6 USB without rebooting. Attach another Tails 6 USB and re-open the Tails Cloner, returning to step **3.3**.

4. Complete upgrade to SecureDrop 2.12.10

Reboot each *Journalist* and *Admin Workstation* after successfully upgrading to Tails 7 and run the following commands to complete the upgrade to SecureDrop 2.12.10:

```
cd ~/Persistent/securedrop
sudo apt update
```

(continues on next page)

(continued from previous page)

```
./securedrop-admin setup
./securedrop-admin tailsconfig
```

The *sudo apt update* or *./securedrop-admin setup* commands may fail due to a background *apt-get* process running after Tails starts up. If you encounter an error related to *apt* package updates, wait a few minutes and try again. If you continue to encounter the same error, you can safely kill the interfering background *apt* process by running:

```
sudo killall apt-get
sudo dpkg --configure -a
```

Then try re-running the command that failed and continue.

1.69.2 Rollback: Restore a broken upgrade

If you ran the SecureDrop graphical updater but are unable to upgrade the Tails USB to Tails 7, the affected SecureDrop *Journalist* or *Admin Workstation* will no longer work. You can fix this by rolling back an affected *Journalist* or *Admin Workstation* to SecureDrop version 2.12.9.

First delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.12.9
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the most recent release compatible with Tails 6:

```
git checkout 2.12.9
```

Important

If you do see the warning "refname '2.12.9' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.69.3 Getting Support

Should you require further help with either the SecureDrop 2.12.10 or Tails 7 upgrades, please reach out to support:

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.70 Upgrade from 2.12.8 to 2.12.9

1.70.1 Migrating to Ubuntu 24.04 (Noble)

Following an automatic upgrade period in which all known, actively maintained SecureDrops have been upgraded to Ubuntu Noble, SecureDrop 2.12.9 disables automatic upgrades from Ubuntu Focal to Noble. If you are using SecureDrop and are still running Ubuntu Focal, you are no longer receiving important Ubuntu security updates. Please *contact support* for information about backing up and performing a reinstall using Ubuntu Noble.

1.70.2 Update Workstations to SecureDrop 2.12.9

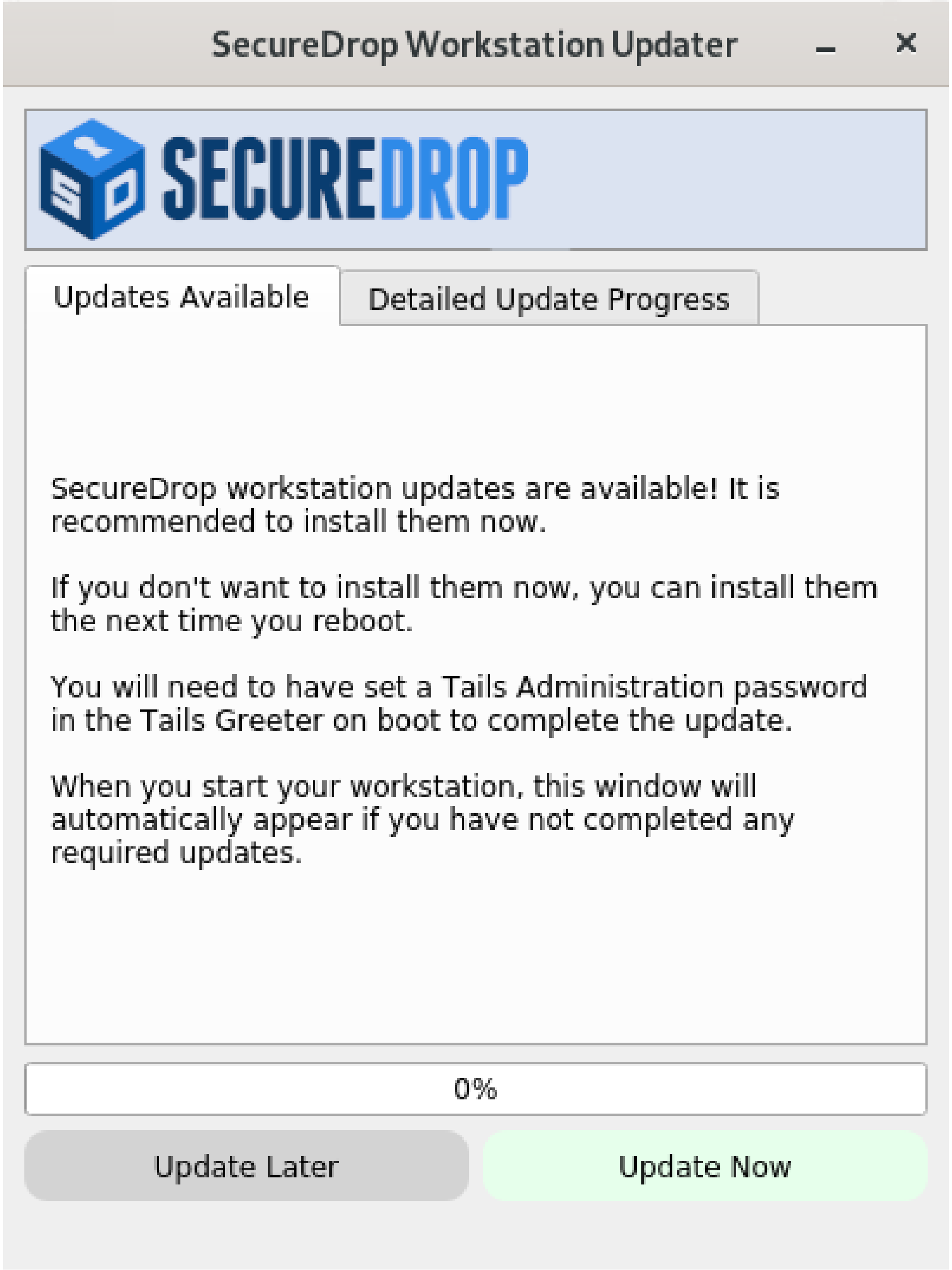
Important

We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.12.9 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.12.9 by clicking “Update Now”:



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.12.9
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.12.9
```

Important

If you do see the warning "refname '2.12.9' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.70.3 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.71 Upgrade from 2.12.3 to 2.12.8

1.71.1 Migrating to Ubuntu 24.04 (Noble)

The 2.12.8 release of SecureDrop enabled upgrades for 100% of Application and Monitor servers, marking the end of the automated process to upgrade SecureDrop servers to Ubuntu 24.04 (Noble). Versions 2.12.4 to 2.12.8 consisted solely of configuration changes to trigger progressive phases of this automated upgrade process for servers.

If you find yourself manually updating your workstations, it is perfectly safe to go directly from version 2.12.3 to version 2.12.8 using the instructions below.

1.71.2 Update Workstations to SecureDrop 2.12.8

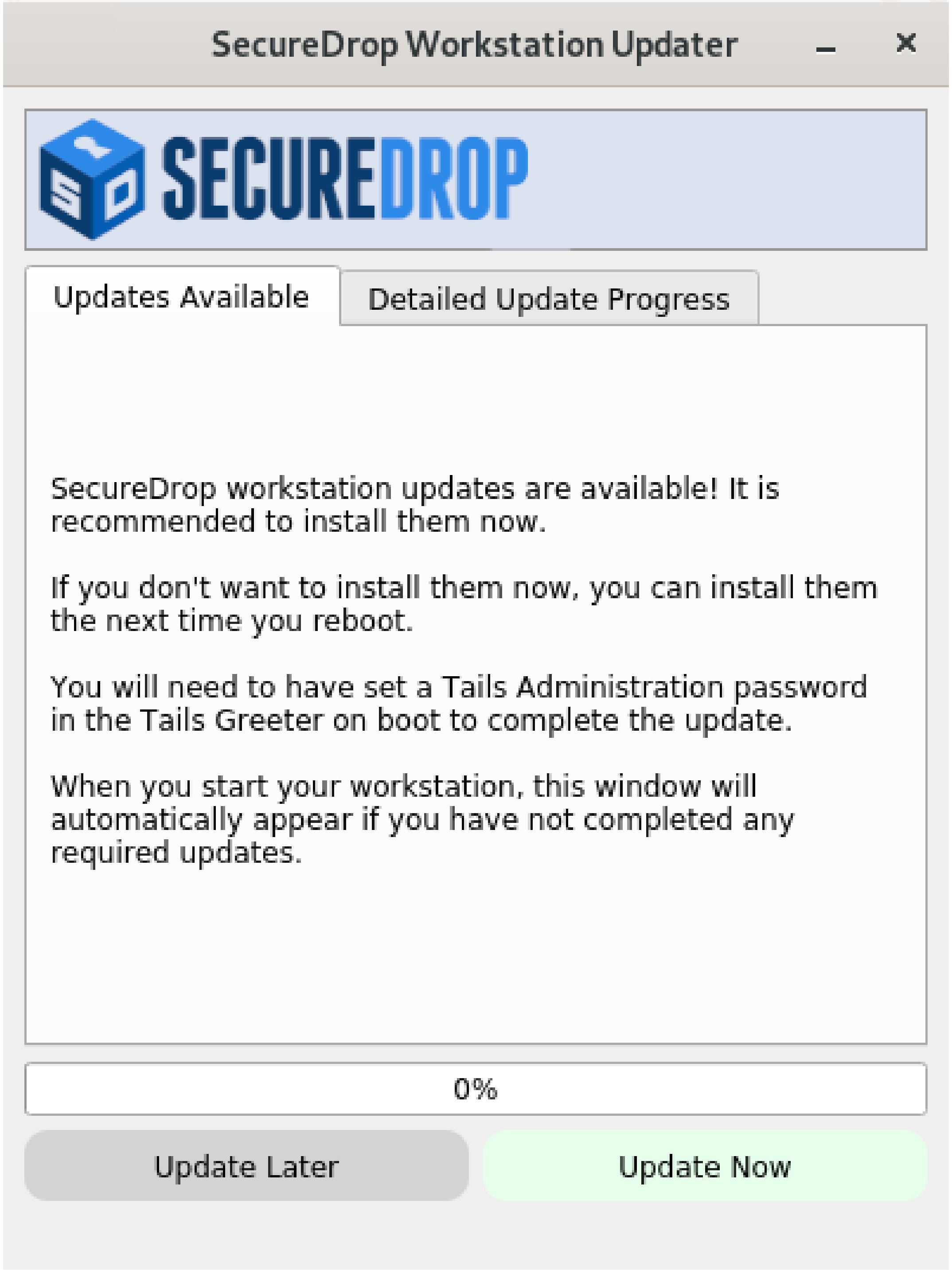
Important

We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.12.8 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.12.8 by clicking "Update Now":



SecureDrop Workstation Updater

SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.12.8
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.12.8
```

Important

If you do see the warning "refname '2.12.8' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.71.3 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.72 Upgrade from 2.12.2 to 2.12.3

1.72.1 Migrating to Ubuntu 24.04 (Noble)

After an initial set of successfully fully automated upgrades to Ubuntu 24.04 (Noble) with the 2.12.2 release, we are now enabling the next batch of automated uprades. In practice, this will result in approximately 40% of *Application Servers* being upgraded.

This release also addresses an issue where some SecureDrop instances that failed the pre-upgrade migration check could remain in a state with automatic updates disabled. The SecureDrop team is monitoring known servers; if we believe this bug as affected you, we will reach out with steps to re-enable automatic updates.

1.72.2 Update Workstations to SecureDrop 2.12.3

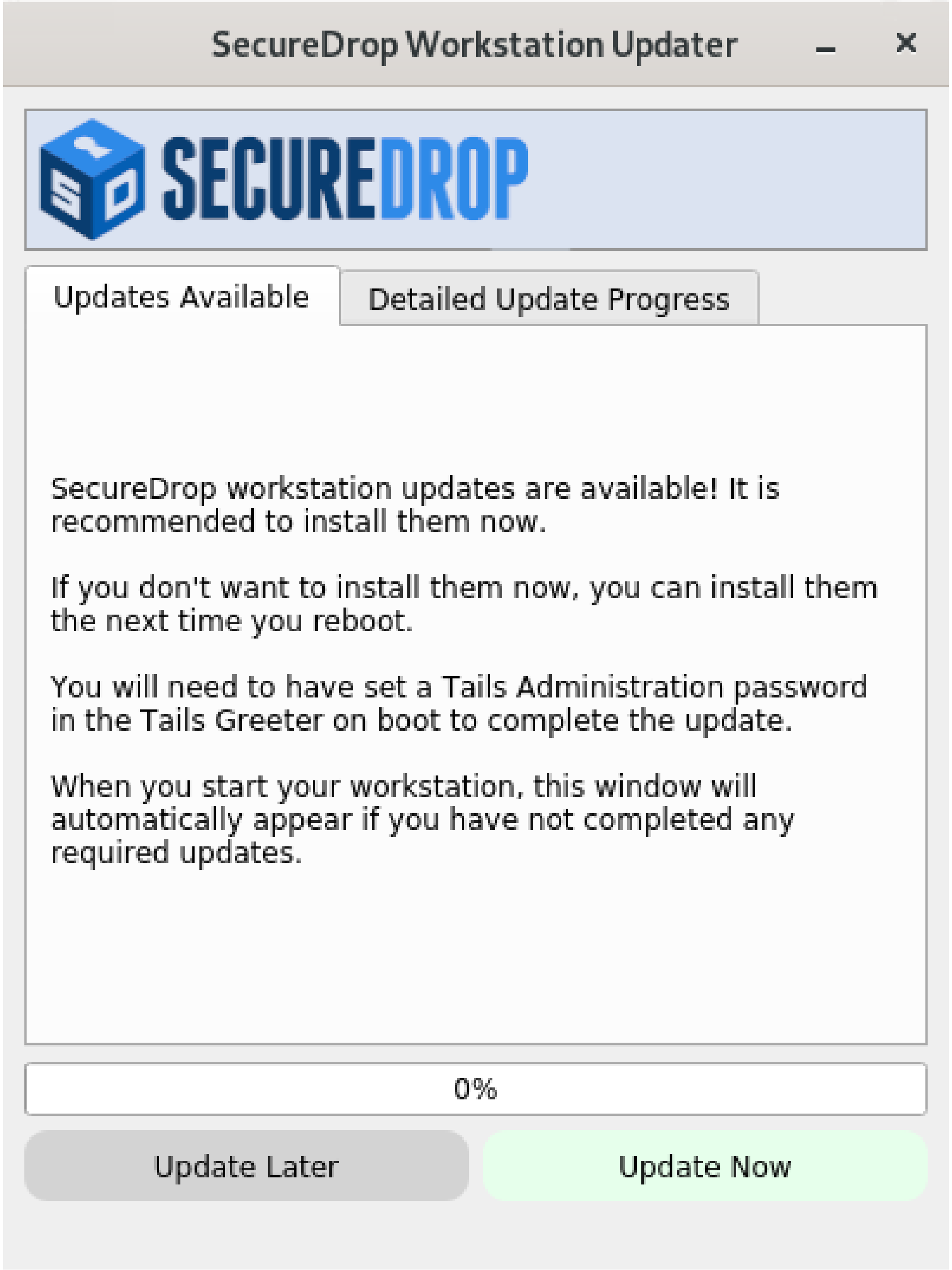
Important

We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.12.3 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.12.3 by clicking "Update Now":



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.12.3
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.12.3
```

Important

If you do see the warning "refname '2.12.3' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.72.3 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.73 Upgrade from 2.12.1 to 2.12.2

1.73.1 Migrating to Ubuntu 24.04 (Noble)

Following a successful period of semiautomated migrations to Ubuntu Noble, we are beginning the first phase of automated upgrades. Approximately 20% of *Application Servers* will be automatically upgraded.

1.73.2 Update Workstations to SecureDrop 2.12.2

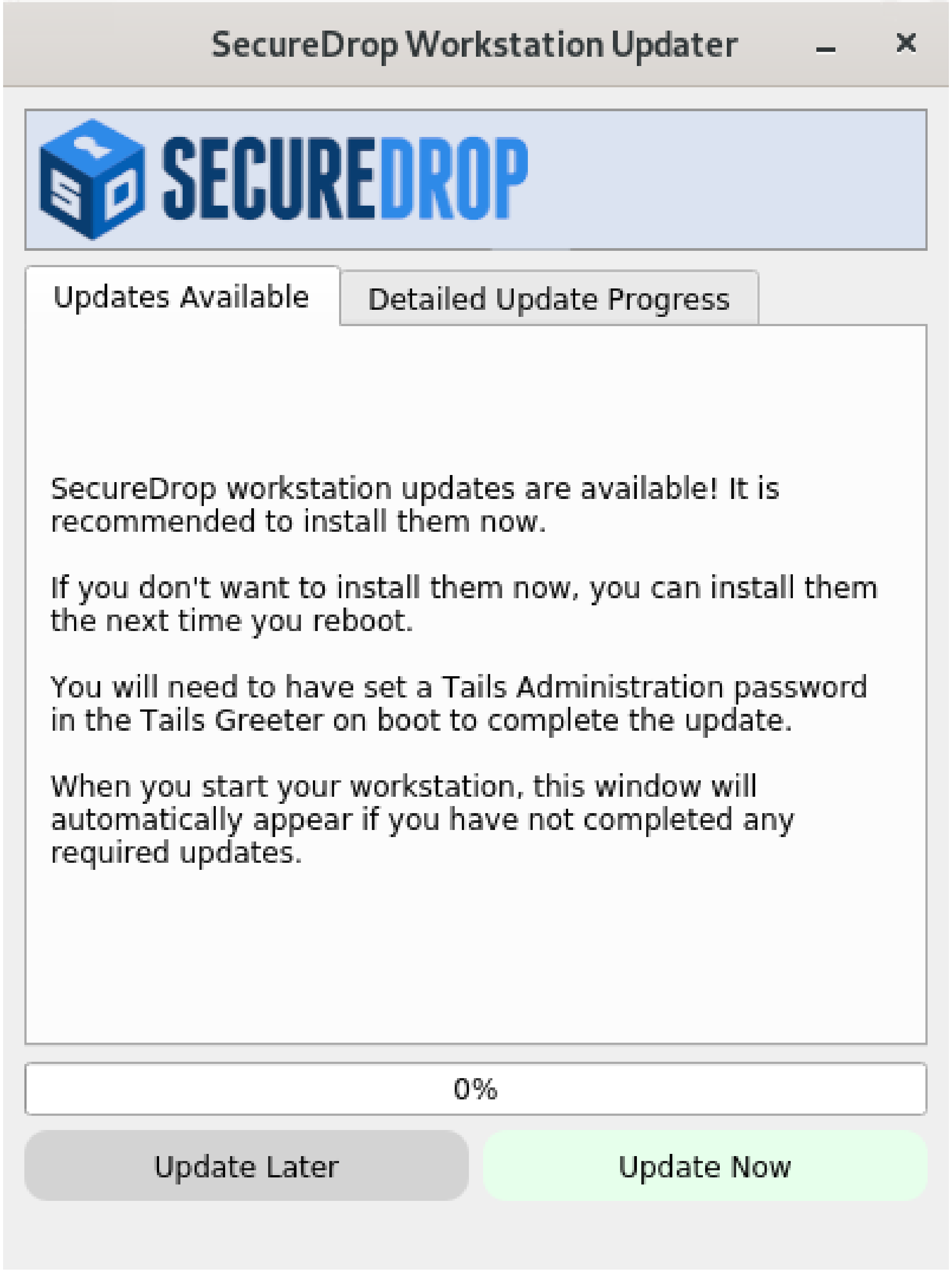
Important

We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.12.2 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.12.2 by clicking "Update Now":



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.12.2
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.12.2
```

Important

If you do see the warning "refname '2.12.2' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.73.3 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.74 Upgrade from 2.12.0 to 2.12.1

SecureDrop 2.12.1 is an Admin Workstation-only release, which improves the reliability of the semiautomated Ubuntu Noble upgrade when using SSH-over-Tor.

1.74.1 Migrating to Ubuntu 24.04 (Noble)

As a reminder, it is necessary to upgrade your SecureDrop Servers to Ubuntu 24.04 (Noble) due to the upcoming end-of-life for Ubuntu 20.04 (Focal).

Administrators have two options, on the following timeline:

- **semiautomated, through April 15, 2025:** Administrators can manually trigger the upgrade and observe the process.

- **fully automated, after April 15, 2025:** The SecureDrop team will push an update in mid- to late-April that automatically begins the upgrade process on all servers.

To determine which option is best for you, and to learn more about how the upgrade works, please review the Ubuntu 24.04 (Noble) migration guide at your earliest convenience.

1.74.2 Servers to Remain on 2.12.0

As this is an Admin Workstation-only release, servers will not receive an update and will remain on version 2.12.0. Please note, upgrading to SecureDrop 2.12.0 does not automatically upgrade your server to Ubuntu 24.04.

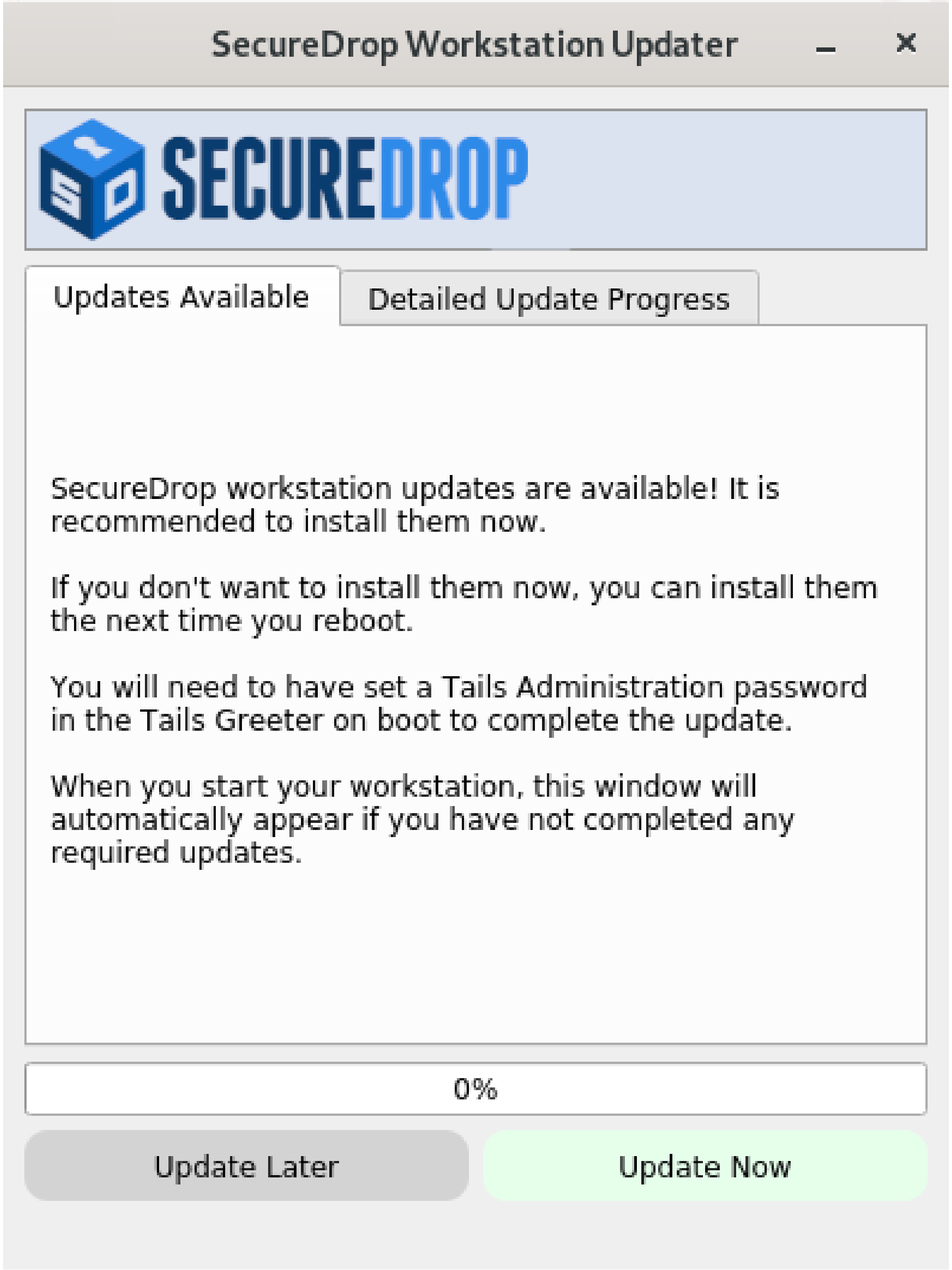
1.74.3 Update Workstations to SecureDrop 2.12.1

> **Important**
>
> We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.12.1 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.12.1 by clicking “Update Now”:



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.12.1
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.12.1
```

Important

If you do see the warning "refname '2.12.1' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.74.4 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.75 Upgrade from 2.11.1 to 2.12.0

1.75.1 Migrating to Ubuntu 24.04 (Noble)

The SecureDrop 2.12.0 release provides the foundation necessary to safely upgrade your SecureDrop Servers to Ubuntu 24.04 (Noble), which is necessary due to the upcoming end-of-life for Ubuntu 20.04 (Focal).

Administrators have two options, on the following timeline:

- **semiautomated, through April 15, 2025:** Administrators can manually trigger the upgrade and observe the process.
- **fully automated, after April 15, 2025:** The SecureDrop team will push an update in mid- to late-April that automatically begins the upgrade process on all servers.

To determine which option is best for you, and to learn more about how the upgrade works, please review the Ubuntu 24.04 (Noble) migration guide at your earliest convenience.

1.75.2 Update Servers to SecureDrop 2.12.0

Servers will be updated to the latest version of SecureDrop automatically within 24 hours of the release. Please note, upgrading to SecureDrop 2.12.0 does not automatically upgrade your server to Ubuntu 24.04.

1.75.3 Update Workstations to SecureDrop 2.12.0

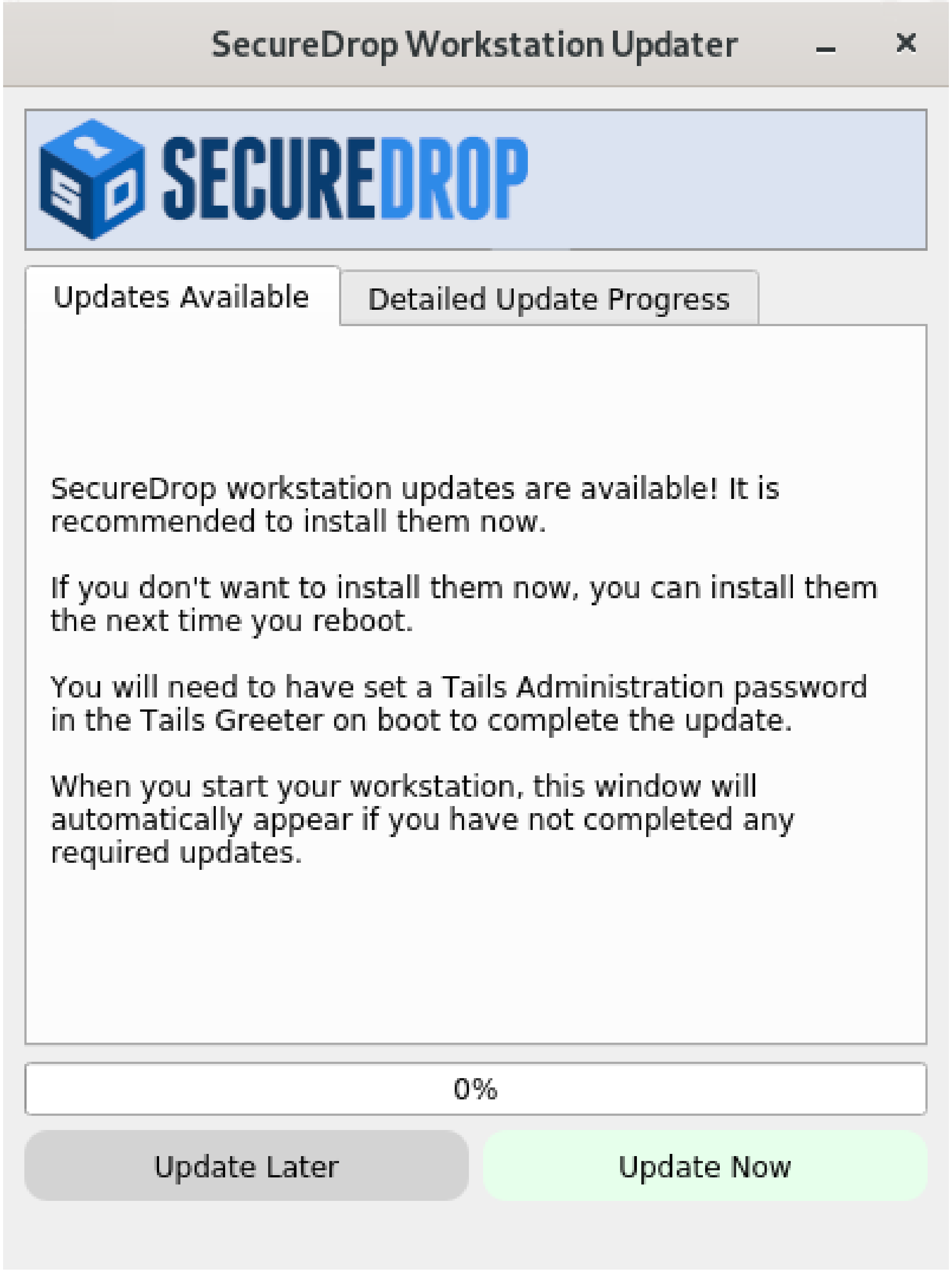
Important

We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.12.0 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.12.0 by clicking “Update Now”:



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.12.0
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.12.0
```

Important

If you do see the warning "refname '2.12.0' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.75.4 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

1.76 Upgrade from 2.11.0 to 2.11.1

1.76.1 Preparing for the Ubuntu 24.04 (Noble) migration

The 2.11.1 release includes a number of features that will help ensure your SecureDrop server is prepared for the automated migration to Ubuntu 24.04 (Noble) in early 2025.

SecureDrop 2.11.1 will automatically run checks to ensure all servers are ready for migration to Ubuntu 24.04 (Noble). If issues are found, a banner will be displayed in the Journalist Interface to both admins and journalists. Administrators are encouraged to review the Ubuntu 24.04 (Noble) migration guide explaining how to resolve any errors and perform any necessary steps before Jan. 31st, 2025.

We will have more details on the migration itself early next year.

1.76.2 Update Servers to SecureDrop 2.11.1

Servers running Ubuntu 20.04 will be updated to the latest version of SecureDrop automatically within 24 hours of the release.

1.76.3 Update Workstations to SecureDrop 2.11.1

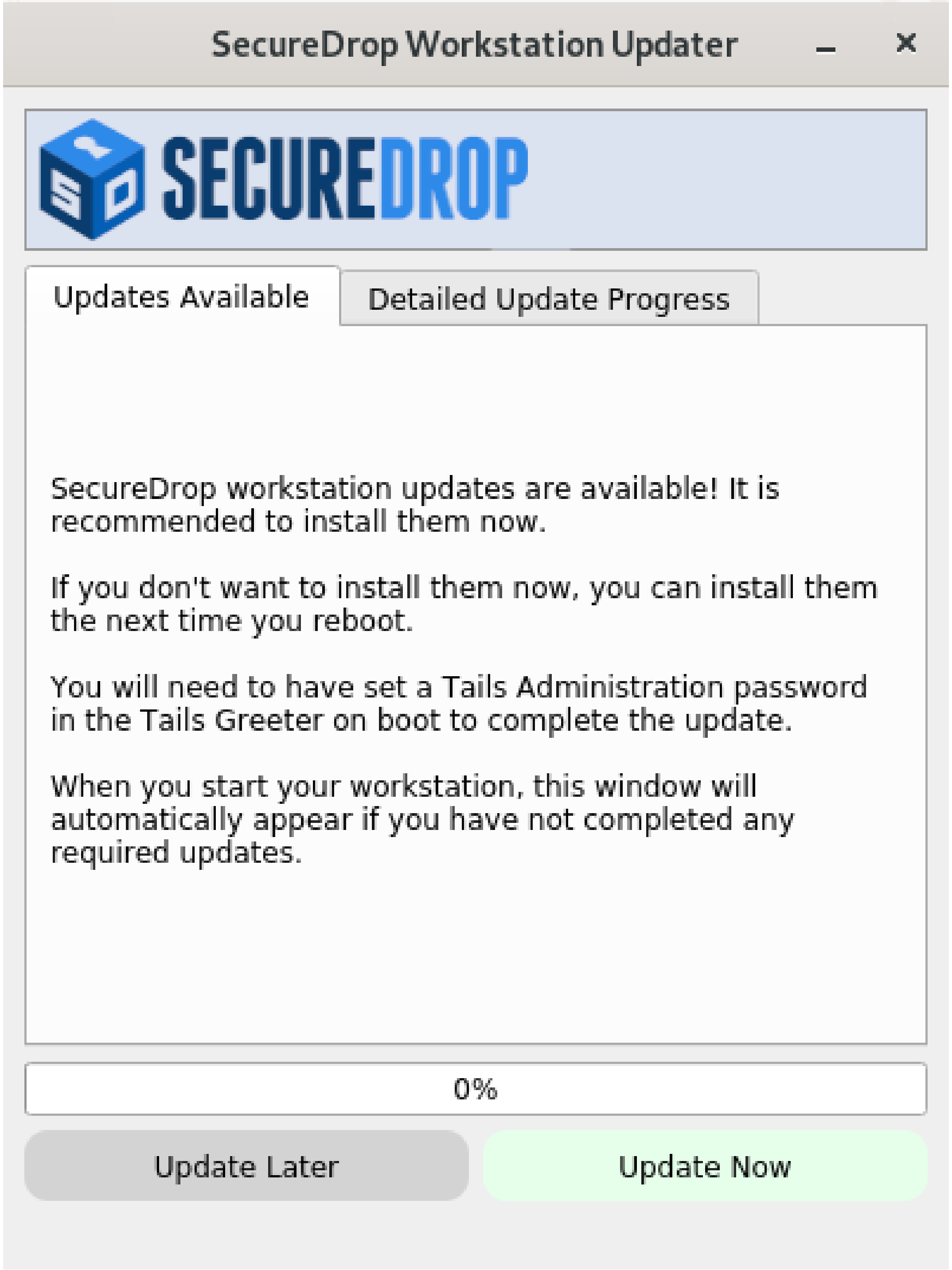
Important

We recommend backing up your workstations prior to any upgrades. See our *backup instructions* for more information.

Update to SecureDrop 2.11.1 using the graphical updater

On the next boot of your SecureDrop *Journalist* and *Admin Workstations*, the *SecureDrop Workstation Updater* will alert you to workstation updates. You must have configured an administrator password on the Tails welcome screen in order to use the graphical updater.

Perform the update to 2.11.1 by clicking “Update Now”:



SecureDrop workstation updates are available! It is recommended to install them now.

If you don't want to install them now, you can install them the next time you reboot.

You will need to have set a Tails Administration password in the Tails Greeter on boot to complete the update.

When you start your workstation, this window will automatically appear if you have not completed any required updates.

Fallback: Perform a manual update

If the graphical updater fails and you want to perform a manual update instead, first delete the graphical updater's temporary flag file, if it exists (the `.` before `securedrop` is not a typo):

```
rm ~/Persistent/.securedrop/securedrop_update.flag
```

This will prevent the graphical updater from attempting to re-apply the failed update and has no bearing on future

updates. You can now perform a manual update by running the following commands:

```
cd ~/Persistent/securedrop
git fetch --tags
gpg --keyserver hkps://keys.openpgp.org --recv-key \
 "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"
git tag -v 2.11.1
```

The output should include the following two lines:

```
gpg:                using RSA key 2359E6538C0613E652955E6C188EDD3B7B22E6A3
gpg: Good signature from "SecureDrop Release Signing Key <securedrop-release-key-
↪2021@freedom.press>" [unknown]
```

Please verify that each character of the fingerprint above matches what is on the screen of your workstation. A warning that the key is not certified is normal and expected. If the output includes the lines above, you can check out the new release:

```
git checkout 2.11.1
```

Important

If you do see the warning "refname '2.11.1' is ambiguous" in the output, we recommend that you contact us immediately at securedrop@freedom.press (GPG encrypted).

Finally, run the following commands:

```
sudo apt update
./securedrop-admin setup
./securedrop-admin tailsconfig
```

1.76.4 Getting Support

Should you require further support with your SecureDrop installation, we are happy to help!

- If you are already in touch with us for support via Signal, please contact us there.
- If you would like to request support, please contact us by e-mail at securedrop@freedom.press (PGP encrypted), or by using the (Get Help with SecureDrop) contact form. - The Freedom of the Press Foundation offers training and priority support services. See https://securedrop.org/priority-support/ for more information.

CHAPTER TWO

GET INVOLVED

SecureDrop is an open source project. If you would like to contribute to SecureDrop, please see our developer documentation.

Two versions of this documentation are available, and can be selected in the lower left corner using the version dropdown menu:

- `latest` - built from the `develop` branch of the SecureDrop repository, containing updates that have been tested but not yet released.
- `stable` - built from the `stable` branch of the SecureDrop repository, and up to date with the most recent release, 2.13.0.