SecureDrop Workstation Documentation

Release stable

SecureDrop

Nov 21, 2024

OVERVIEW

SecureDrop Workstation is a tool to enable journalists to communicate with anonymous sources and manage submitted documents, while providing mitigations against malware and other security risks. It is built on Qubes OS and requires a SecureDrop server setup.

Note

This documentation is also available as a Tor Onion Service at http://wcjrbbrllo2r554s542u55on6y4sf3aq2gheigjs3rpsfoa2qq3z2gqd.onion/en/stable/.

CHAPTER

ONE

INTRODUCTION

1.1 What is Qubes OS?

Qubes OS is an open source, security-focused operating system. It is very different than operating systems you may be familiar with already, because it consists of multiple isolated virtual machines that allow you to separate more trusted components, files, or programs on your computer from less trusted components, files, or programs.

Broadly speaking, this means that even if files in one of your virtual machines are exposed to malware, files in others still have some protection, which is not true of other operating systems.

1.2 What is SecureDrop Workstation?

SecureDrop Workstation is a project that uses Qubes to make SecureDrop faster and simpler for journalists to use.

A key feature of SecureDrop is that journalists can receive submissions from unknown sources without risking the security of their own machines and networks. Previously, SecureDrop accomplished this by using a physical airgap (the *Secure Viewing Station*), meaning that to view submissions, journalists would have to download them, transfer them to an encrypted USB drive, and physically take that drive to a separate, non-networked computer for decryption and viewing. SecureDrop Workstation combines all of those steps into one workflow on one machine: a Qubes computer that combines the *Journalist Workstation* and the *Secure Viewing Station*.

1.3 Who is behind SecureDrop Workstation?

SecureDrop and SecureDrop Workstation are open source projects of Freedom of the Press Foundation (FPF), a US-based nonprofit organization. You can support our work by contributing to SecureDrop and by making a donation.

Our work would not be possible without the larger open source community.

We're deeply grateful to the SecureDrop volunteer community for translating our software into many languages. Their work is enabled by Weblate, an open source platform for continuous localization. You can make a donation to support Weblate development.

Translation of SecureDrop is supported by Localization Lab. You can donate to support their important work to help bring open source software into many languages.

The backbone of SecureDrop Workstation is Qubes OS. FPF has directly sponsored Qubes OS development, and we encourage you to donate to Qubes OS as well.

We use the Python programming language and many tools in its ecosystem, which you can support by donating to the Python Software Foundation.

SecureDrop Workstation VMs are powered by Debian, Fedora, and Whonix, all of which rely on volunteer contributions and financial support. The GNOME project acts as an umbrella for many of the individual software components we rely on.

Finally, SecureDrop Workstation relies on many other open source projects such as grsecurity, GnuPG, Sequoia, LibreOffice, Audacious, and others. These projects, in turn, are built on open source foundations. Please consider directing time and financial support wherever it can make a positive difference.

For more information on SecureDrop Workstation, see our *FAQ*.

CHAPTER

TWO

SECUREDROP WORKSTATION ARCHITECTURE

2.1 SecureDrop Workstation networking architecture

One key security feature of Qubes OS is that it enables users to configure the appropriate level of network access for each VM. For example, you could have a VM for password storage that has no network access, a work VM that is firewalled to only connect to work servers, and a personal VM that always uses Tor.

SecureDrop Workstation tightly controls access to the network, in order to prevent the exfiltration of messages, replies, documents, or encryption keys by adversaries. Specifically, the following VMs have no network access:

- `sd-app`, which runs the SecureDrop Client, and holds decrypted messages, replies, and documents.
- `sd-viewer`, which is the template for disposable VMs used for opening documents from the SecureDrop Client.
- `sd-gpg`, which holds the *Submission Private Key* required to decrypt messages, replies, and documents.
- `sd-devices`, which passes exported documents through to USB devices like printers and encrypted flash drives.

By design, the Qubes OS host domain, `dom0`, also does not have Internet access.

Note

If you attempt to directly access the network in any of these VMs, it will not work. That is the expected behavior.

Because the SecureDrop Client must connect to the SecureDrop *Application Server* in order to send or retrieve messages, documents, and replies, it can communicate through Qubes-internal Remote Procedure Calls (RPCs) with another VM, `sd-proxy`, which can only access the open Internet through the Tor network, using the separate `sd-whonix` VM.

Like all networked VMs, `sd-whonix` uses the `sys-firewall` service to connect to the network, which is provided via `sys-net`. All four VMs must be running for the SecureDrop Client to successfully connect to the server.

Important

The `sd-whonix` VM contains a sensitive authentication token required to access the SecureDrop API via Tor, and should not be attached to VMs that are unrelated to SecureDrop.

Qubes OS ships with a Whonix service called `sys-whonix`. When troubleshooting connection issues specific to SecureDrop, `sys-whonix` is only relevant during updates of the Whonix VMs (e.g., while the preflight updater is running).

CHAPTER

THREE

SECUREDROP WORKSTATION PROJECT STATUS

SecureDrop Workstation is currently in active development.

Freedom of the Press Foundation had operated a pilot program with a limited number of organizations whose environments were especially well-suited for early testing of the Workstation. This pilot program has now ended.

With the 1.0.0 release, we're now switching to an open beta. If you are interested in using SecureDrop Workstation, please reach out to us via the support portal.

3.1 Is SecureDrop Workstation right for you?

Until SecureDrop Workstation reaches general availability, we would recommend against using it in production environments (outside of users who have already installed it as part of the pilot program).

That said, the project is entirely open source, and you can install it independently if you want to get a feel for how it all works.

If you're a journalist or news organization trying to decide if this is right for you, please note that SecureDrop Workstation should only be used by organizations that meet the following criteria:

- You have an existing SecureDrop Server in place
- You have fewer than 500 Sources on the Server
- You typically only interact with .pdf, .doc, and .jpg files via your SecureDrop (as opposed to large datasets or complex file formats, which are *not yet supported*)
- You have a functional *Secure Viewing Station* to fall back on
- Your journalists and support staff are comfortable trying a new operating system (Qubes OS), and are aware that they may need to troubleshoot with us or with your internal tech team if issues arise
- Your journalists don't rely on the features that are *not yet implemented*

If you do not meet the criteria above, you are likely to run into difficulties or frustrating experiences using the Workstation, and should consider waiting until it is more mature.

Warning

In its current state, if you have more than 500 Sources on your server you **will** experience significant performance issues using SecureDrop Workstation that may hinder your ability to use it at any functional level.

3.1.1 SecureDrop Workstation Feature Comparison

SecureDrop Workstation provides a faster and more streamlined way of interacting with sources and submissions, while preserving important security properties. That said, it is still under development, and not all features available on the Tails-based (existing) system are available in SecuredDrop Workstation. We are working towards feature parity, but in the meantime, there are some notable differences; see the *Limitations and known issues* page for more information.

3.2 Do you still need a Tails-based *Secure Viewing Station*?

For now, yes. There are still circumstances where the SecureDrop Workstation may not be able to retreive or show submissions. The main instances are either in situations where there are a substantial number of sources or submissions stored on the SecureDrop server, or in instances were you are trying to open a file type that the Workstation is not yet equipped to handle.

Once SecureDrop Workstation is more mature, you will be able to use it to view most submissions, but for now, having the *Secure Viewing Station* available as a backup is imperative.

3.3 Roadmap and Timeline

You can find information about our current development roadmap and timeline at the SecureDrop Development Wiki.

We encourage former pilot participants and open beta participants to file support tickets with us, to help us understand and prioritize your needs as we continue development.

CHAPTER

FOUR

LIMITATIONS AND KNOWN ISSUES

4.1 Reporting issues

Please report sensitive issues that are specific to your instance via the support portal.

Bugs and other issues that are not specific to your instance can be reported via GitHub using the following links:

- SecureDrop Workstation issues - issues related to the Qubes environment and workstation provisioning.
- SecureDrop Client issues - issues related to the *SecureDrop Client*.

If you encounter a security-related issue, please see SECURITY.md for instructions on how to privately report it.

4.2 Current known issues

- Searching/filtering by codename is not yet implemented.
- While failed file downloads are automatically retried, there is currently no mechanism cancelling in-progress downloads or viewing the progress or speed of a download. These features are planned.
- Updates are slow due to the number of VMs involved, and due to some updates being fetched over Tor. We have made improvements to the performance and reliability of the updater, and this work will continue.
- SecureDrop instances with very large numbers of sources may encounter UI performance issues. While performance improvements are on the roadmap, our recommendation is to delete information from the servers as regularly as possible, both for performance and security reasons.
- Printer support is limited to specific HP and Brother printer models, and printing different file types is not as reliable yet as under Tails. Support for additional non-networked printers will be added in a future release.
- Printing of individual files inside an archived submission is not yet supported.
- Currently, only app-based two-factor authentication (TOTP) is supported.
- The SecureDrop Client does not currently handle files that are "double-encrypted" (when a source pre-encrypts a submission locally before uploading it to SecureDrop). Until this is fully supported, we suggest using the Tails-based *Secure Viewing Station* for pre-encrypted submissions.
- There are a limited number of file types that can be viewed on SecureDrop Workstation. Some file types (such as *.eml*) are not yet supported for viewing, and must be exported via USB, and/or viewed using the Tails-based *Secure Viewing Station*. *Broader file type support is planned*.
- If the *Submission Key* for your SecureDrop server was rotated in the past, you must manually re-add the old key to your vault VM (*sd-gpg*) in order to view old submissions in SecureDrop Client. Contact Support for assistance.
- We do not support uninstalling SecureDrop Workstation without wiping all of Qubes OS. There is an `--uninstall` option for `sdw-admin`, but it is not officially supported and will leave behind sensitive material in

`/usr/share/securedrop-workstation-dom0-config` in `dom0`. If you need to decomission a SecureDrop Workstation, please contact us for assistance.

CHAPTER

FIVE

SUPPORTED FILETYPES

Currently-supported filetypes include:

- .txt, .csv, .pdf
- Microsoft Office files (.doc, .docx, .xls, .xlsx, .ppt, .pptx)
- OpenDocument files (.odt, .ods, .odp)
- Audio: .mp3, .mp4, .mpeg, .wav, .ogg (Ogg Vorbis)
- Video: .mp4, .webm, .mov (Quicktime), .avi (Audio Video Interleave - Microsoft), .wmv (Windows Media Video)
- Image: .gif, .png, .jpeg, .tiff, .svg, .ico, .webp, .heic, .avif
- Compressed archives: .zip, .tar.gz (although printer support for files inside an archive is still to be implemented)

A full list of supported filetypes can be found here.

Filetypes that are not yet supported for viewing on SecureDrop Workstation can be exported for use on the Tails-based Secure Viewing Station.

CHAPTER

SIX

STARTING QUBES

When turning on SecureDrop Workstation, you will be greeted with a password prompt. This is the full-disk encryption passphrase.

This passphrase protects your entire system. It is of the utmost importance to secure this passphrase. When not using SecureDrop Workstation, shut down the computer completely so as to take advantage of the protections offered by full-disk encryption.

After entering the passphrase, Qubes OS will boot. Log in with the username and password set up by your administrator.

CHAPTER

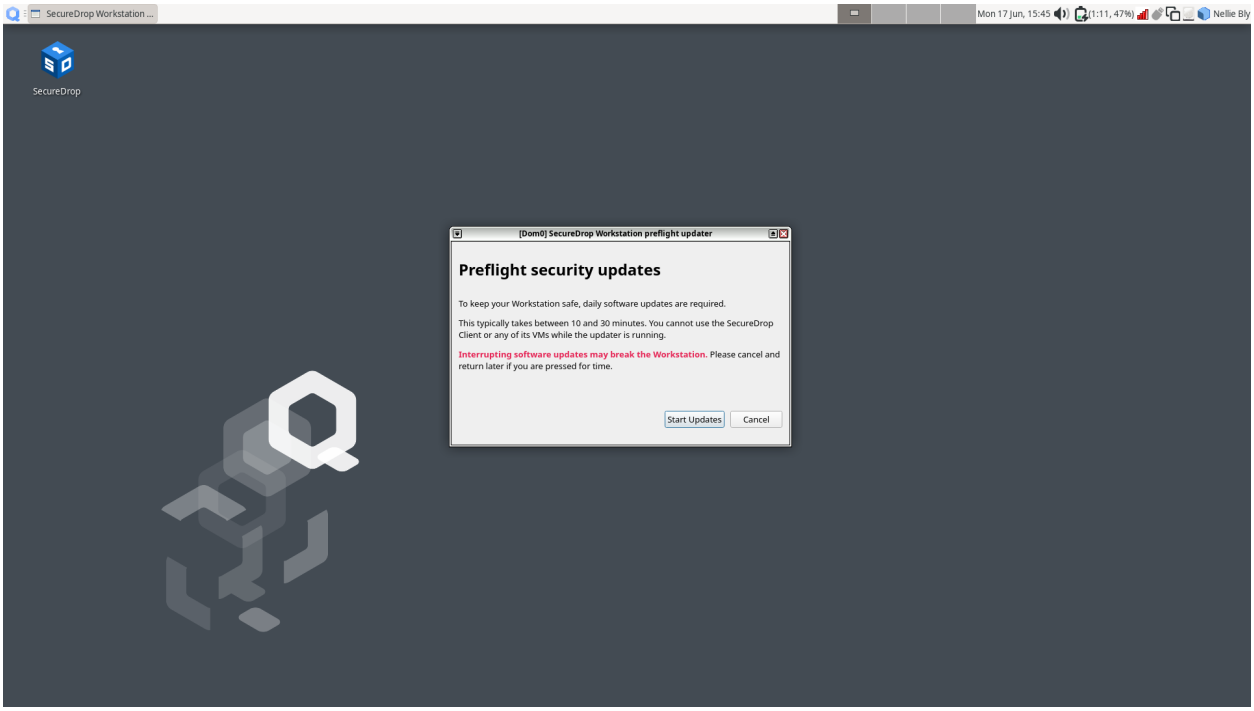
SEVEN

STARTING THE SECUREDROP CLIENT

After you log into Qubes, the SecureDrop Client app will start automatically. If you have previously exited the application, you can double-click on the **SecureDrop** desktop shortcut to launch it.

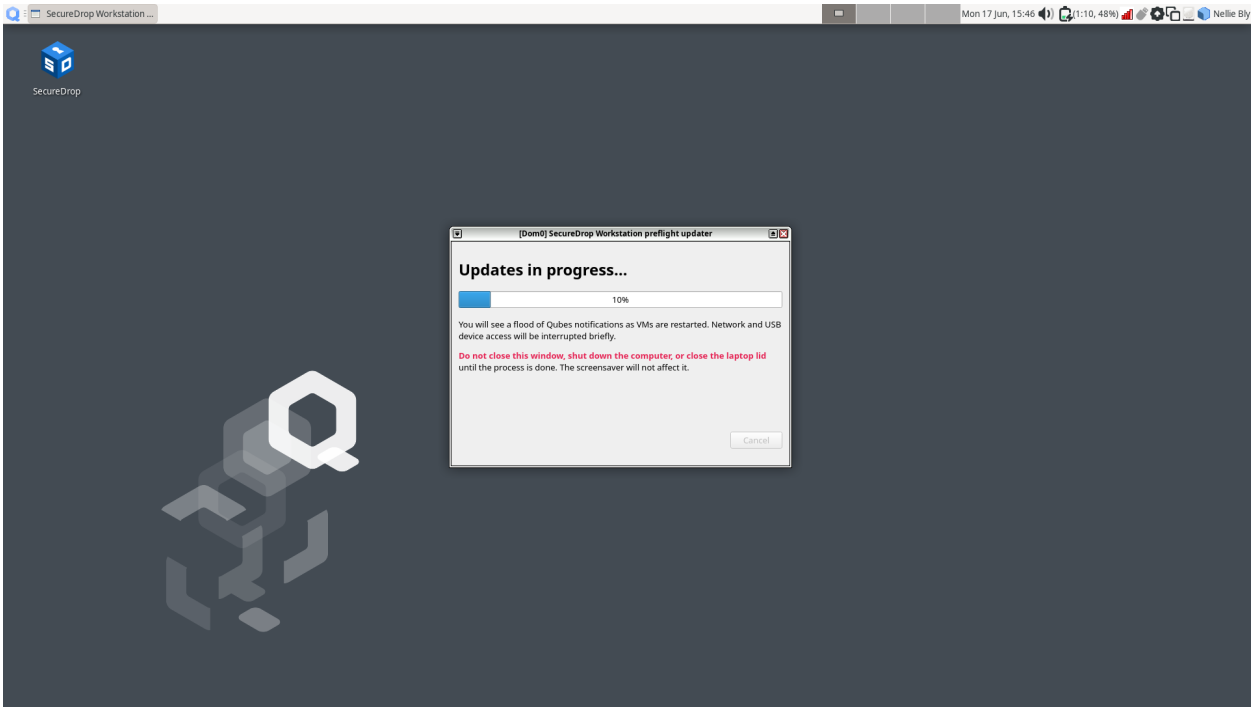
7.1 Performing updates

Unless the system has just been updated, SecureDrop Workstation will now prompt you to automatically download and apply any available security updates:



For security reasons, you will not be able to launch the SecureDrop Client until updates have been applied. This typically takes between 10 and 30 minutes.

Click "Start updates" if you are ready to start the process. (If you prefer to shut down the machine or do other work in Qubes OS instead, click "Cancel".) You will see a progress indicator until updates are completed:



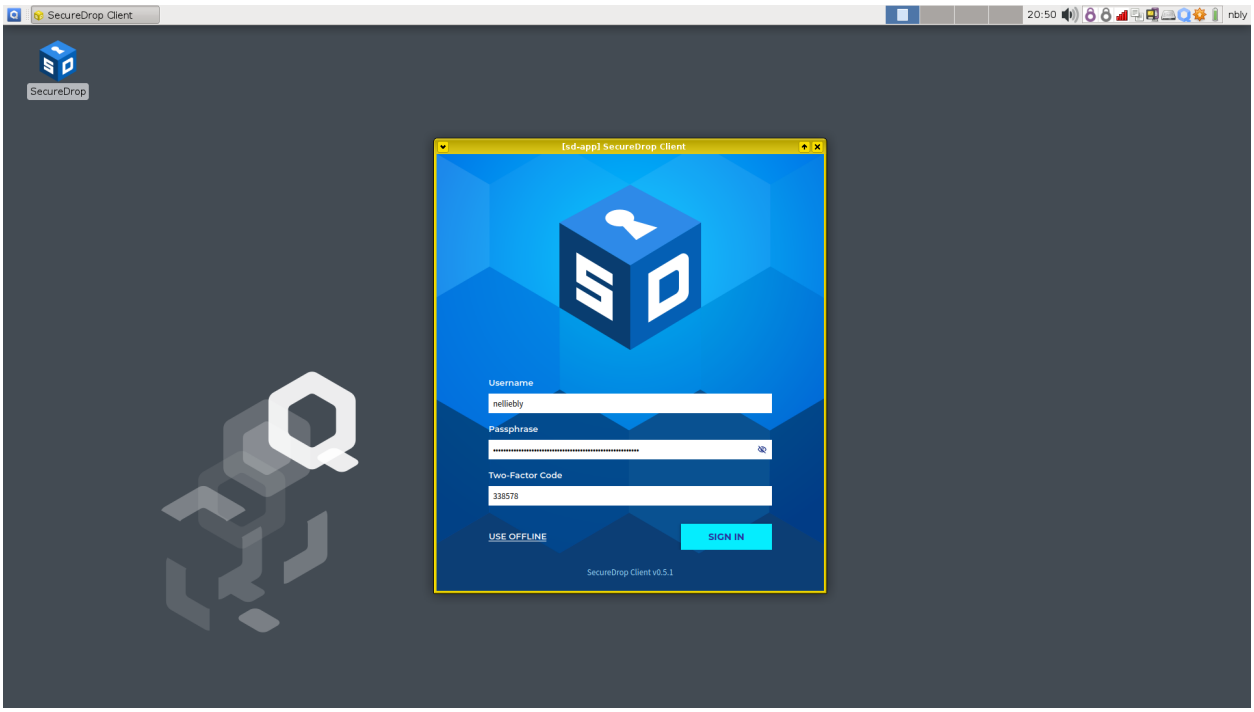
Important

> Allow the update process to complete fully, without closing or interrupting it, or you risk breaking important system components.

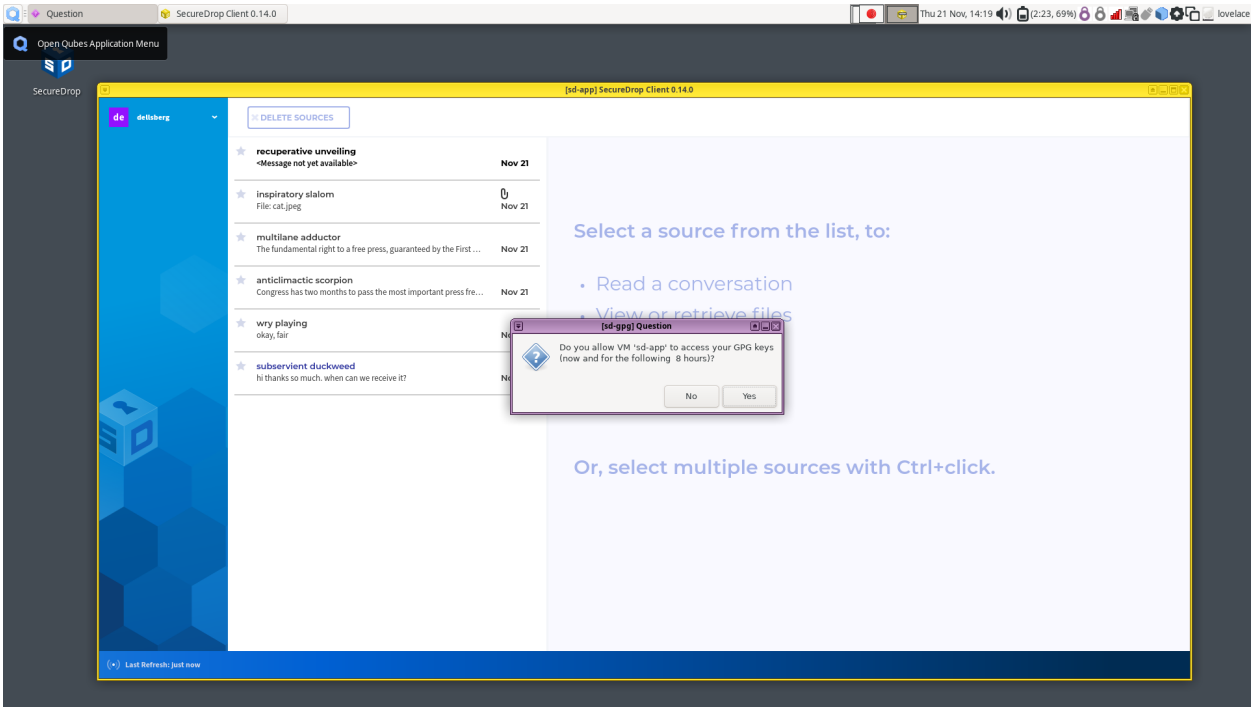
At the end of this process, SecureDrop Workstation may prompt you to reboot if core system components were updated. Once all steps in the update process have been completed, the SecureDrop Client will launch automatically.

7.2 Signing in

To sign in, enter the username and passphrase provided to you by your SecureDrop administrator, as well as the two-factor code using the method you have set up. If you have used SecureDrop before, these are the same credentials that you would use to log in to the Journalist Interface.



After signing in, you will be prompted by a dialog that says "Do you allow VM 'sd-app' to access your GPG keys (now and for the following 8 hours)?". Click **Yes.** This dialogue may appear immediately after signing in, or when you click on a source submission.



7.2.1 Troubleshooting tips

If you have trouble running the updater or logging in, please contact your administrator. Our *network troubleshooting guide* for administrators gives detailed steps for investigating connectivity issues.

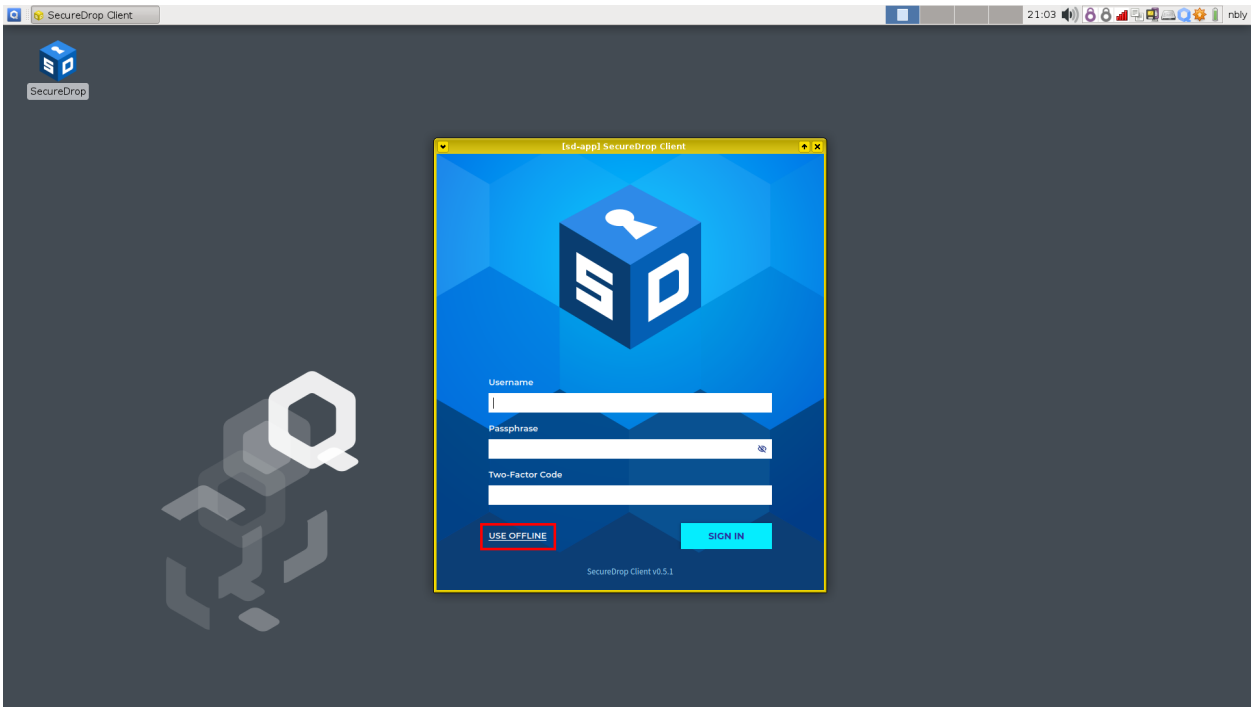
7.3 Seen and unseen submissions

Sources with submissions (messages or files) that have not been seen by any journalist user will be displayed in bold text in the source list.

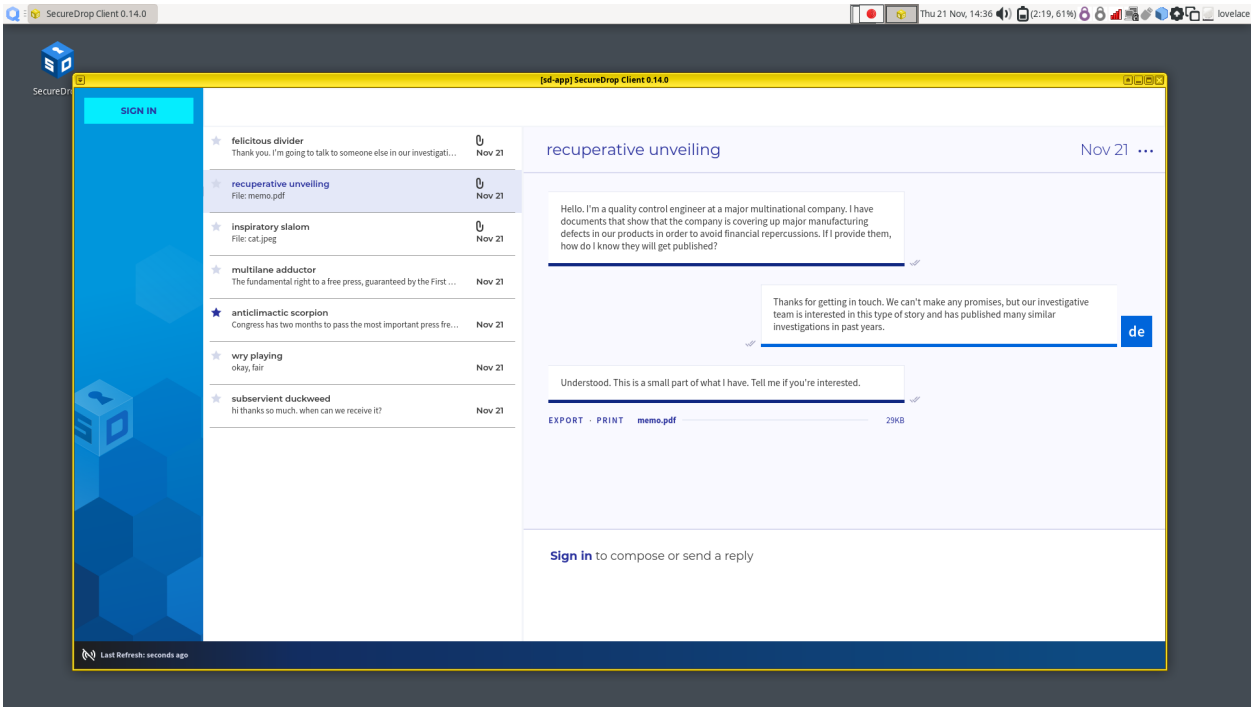
As soon as any journalist user clicks on a source with unseen submissions, it will be marked as seen (no longer displayed in bold text) for all users.

7.4 Working offline

Offline mode is available for circumstances where you wish to work offline or are unable to connect to the SecureDrop servers. In offline mode, any content that you have previously downloaded will be available. You will not be able to send or delete messages, and your actions will not impact the seen/unseen state of submissions.



Because SecureDrop Workstation allows you to download and decrypt submissions on one machine, submissions that you have downloaded are still available in offline mode and can be accessed even when you are not logged in.



Important

Protecting downloaded submissions is another reason why SecureDrop Workstation needs to be powered off completely when it is not in use.

CHAPTER

EIGHT

COMMUNICATING WITH SOURCES

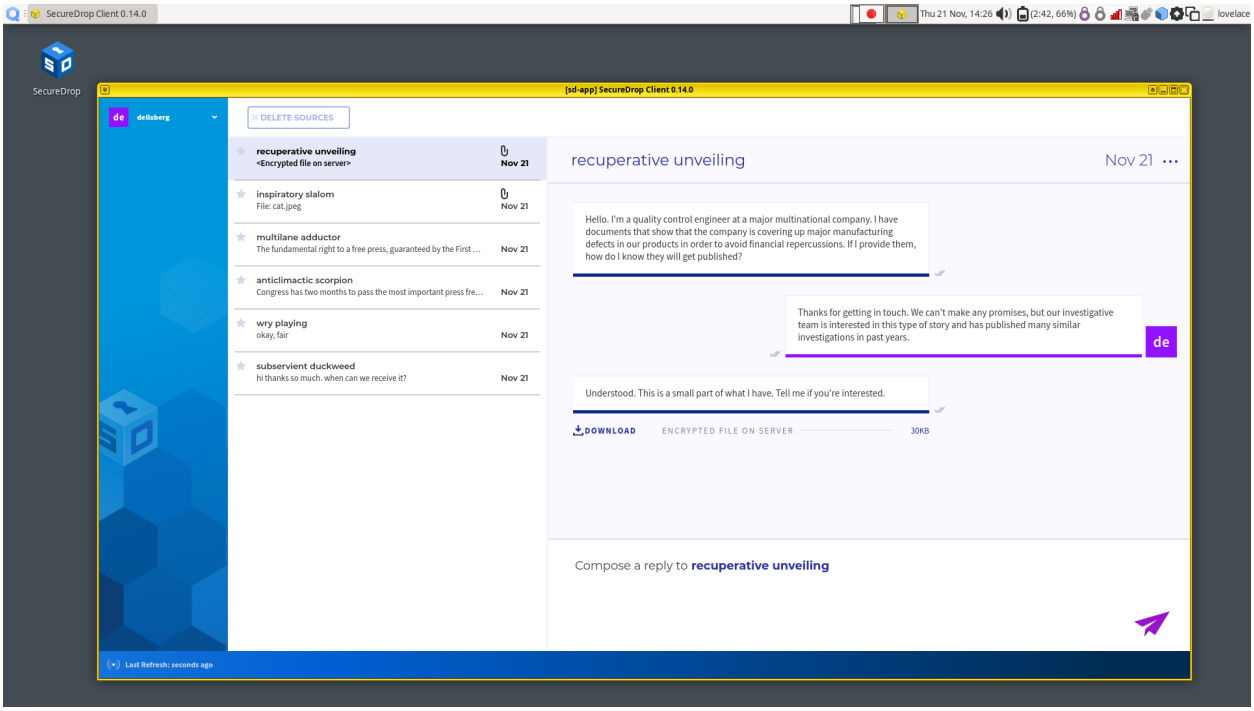
SecureDrop Workstation lets journalists check SecureDrop, decrypt and securely view submissions, and reply to sources, all on the same computer.

Once logged in, you will see a chat-like user interface:

- The leftmost panel shows your username, if you are logged in, or the sign-in button.
- The middle panel holds the list of sources that have submitted to your instance. Each source is identified to you with a two word pseudonym.
- The rightmost panel holds the conversation view. All parts of the conversation with a specific source (messages, files, and journalist replies) will be displayed here.
- The top panel holds a toolbar that allows you to apply actions to multiple sources at once. (Currently, "Delete Sources" is the only supported action.)
- The bottom status bar will alert you to any problems (such as lack of network connectivity or issues downloading a file).

8.1 Opening a conversation

To display a conversation in the conversation view, simply click a source in the source list.



Journalists sending replies are assigned different colors and identified with their initials. Move your mouse pointer over the initials to reveal the full name.

Note

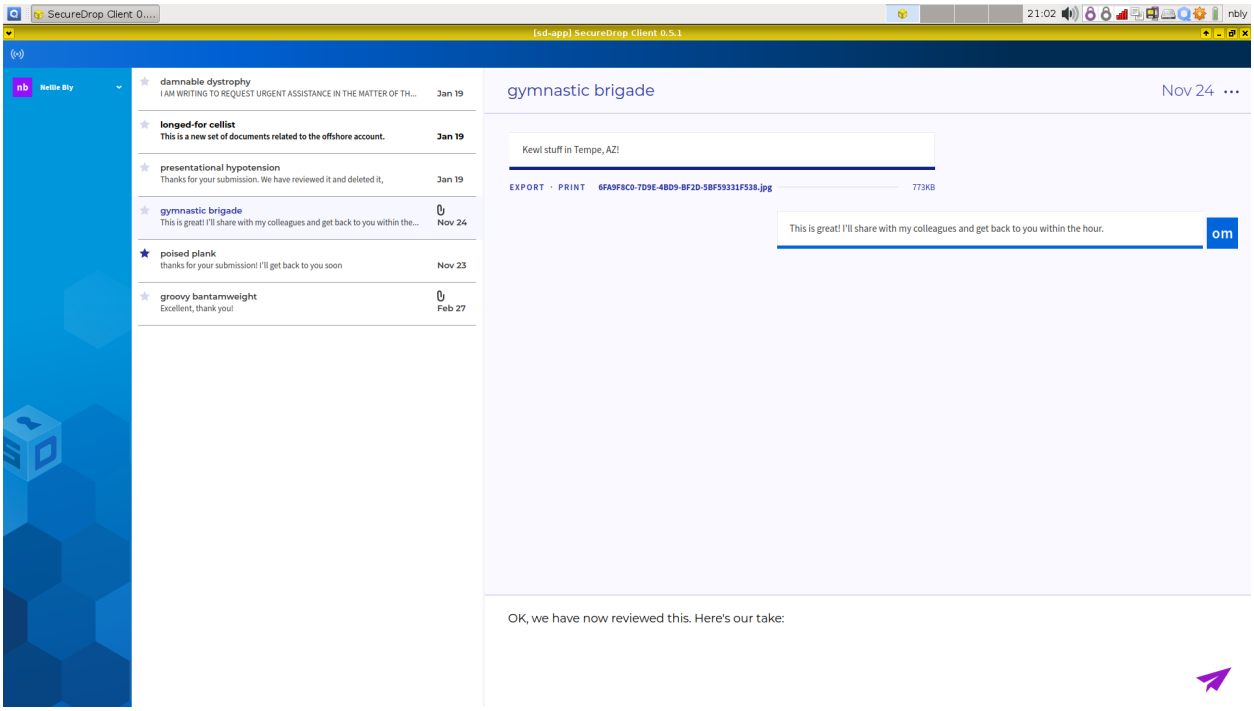
When you are prompted by a dialog that says "Do you allow VM 'sd-app' to access your GPG keys (now and for the following 28800 seconds)?", click **Yes**. This allows the SecureDrop Application VM access to the secure VM that holds your SecureDrop Submission Key.

8.2 Highlighting conversations

You can highlight important conversations by clicking on the star beside a source's name. Starred sources will be visible as starred to everyone in your organization.

8.3 Sending a reply

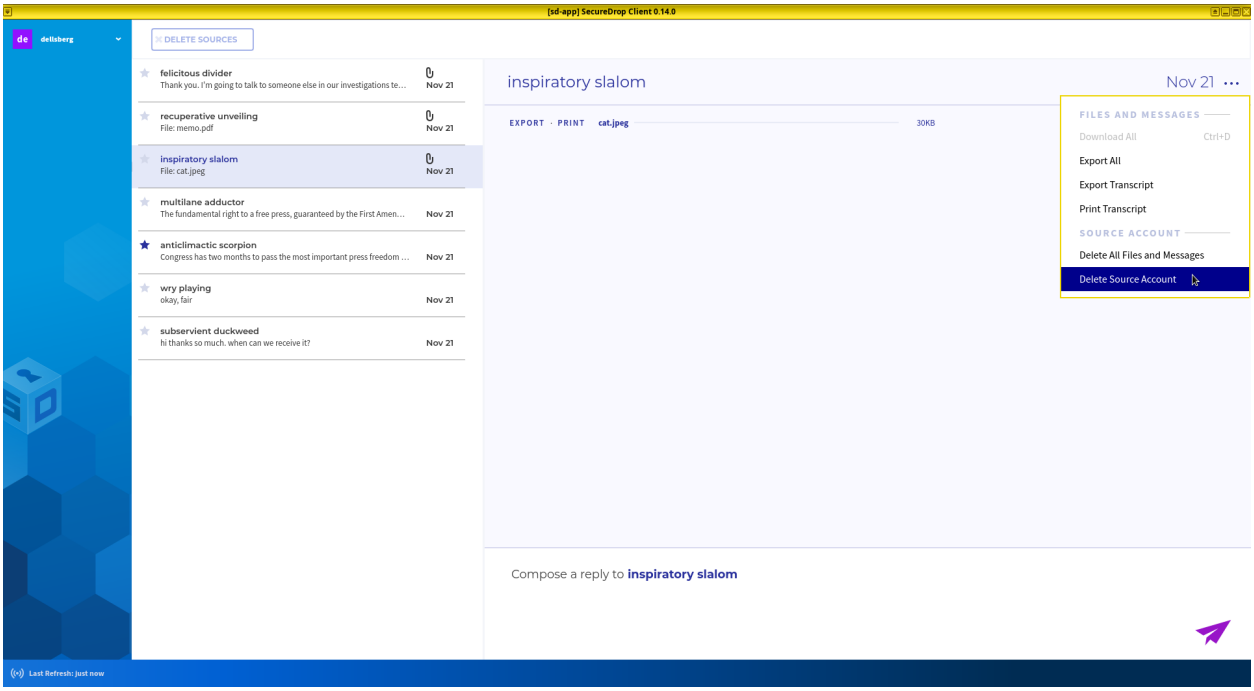
Compose a reply to the selected source in the text box at the bottom of the conversation view. Click the paper airplane icon or press "Ctrl+Enter" to send a reply. Any replies you did not send will be discarded when you exit the client.



8.4 Deleting conversations

8.4.1 Deleting a single conversation

You can delete a single source conversation by clicking on the three dots at the top right-hand side of the application window, beside the timestamp. You should see a dropdown menu with two options: **Files and messages** and **Entire source account**. In both cases, a confirmation dialog will appear before anything is deleted.



Click **Files and messages** to delete all files and messages (including journalist replies) associated with this source,

while keeping the source account active. The source will continue to appear in the source list, and will be able to communicate with you through the Source Interface.

Click **Entire source account** to also remove the source from the source list, and to prevent them from logging into the Source Interface. Their account will be completely removed from the system.

8.4.2 Deleting multiple conversations

You can also delete multiple source conversations at once. Hold down the Control (Ctrl) key and click on different rows to select (or deselect) sources from the list. (You can also Ctrl + drag the mouse, or Shift + select, to select a range of continuous sources.) Once you are finished selecting, click the "Delete Sources" toolbar button.

This action deletes the **entire source account**, meaning files and messages will be removed, and that source will no longer be able to log in using their codename.

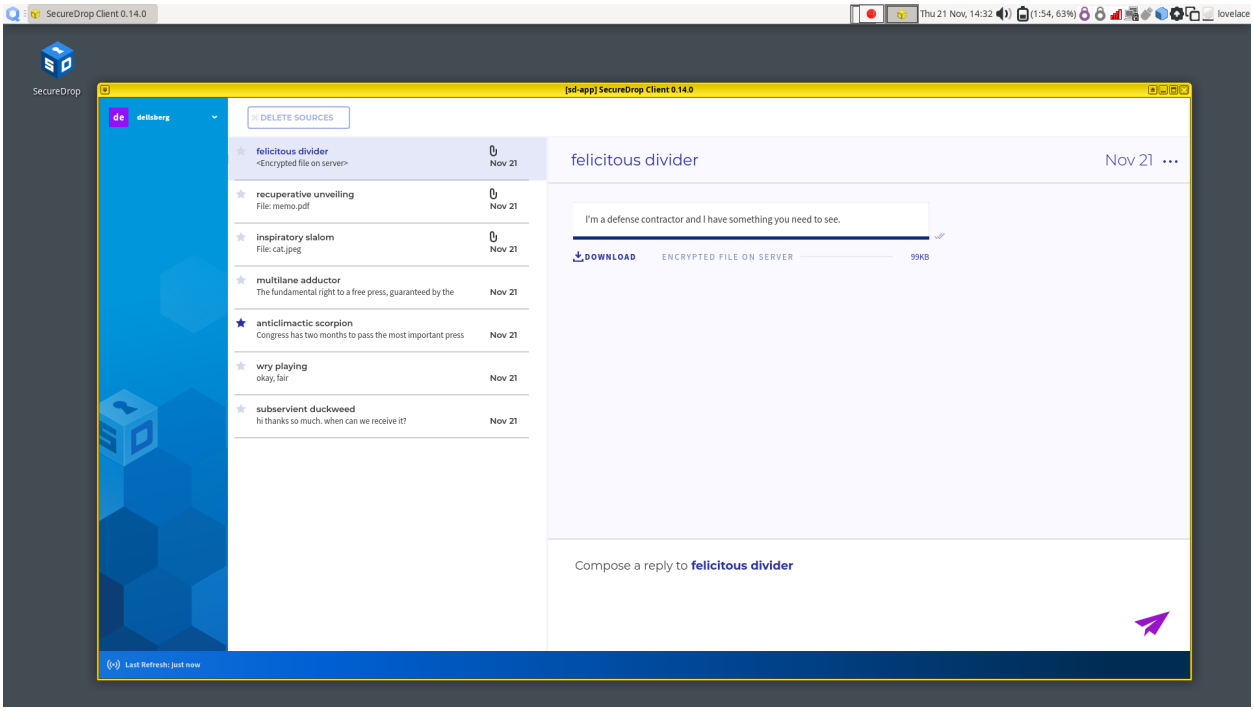
You will be shown a confirmation dialog before any sources are deleted. If you select a very large number of sources, you will also notice a brief time delay, to prevent unintentional deletion.

CHAPTER

NINE

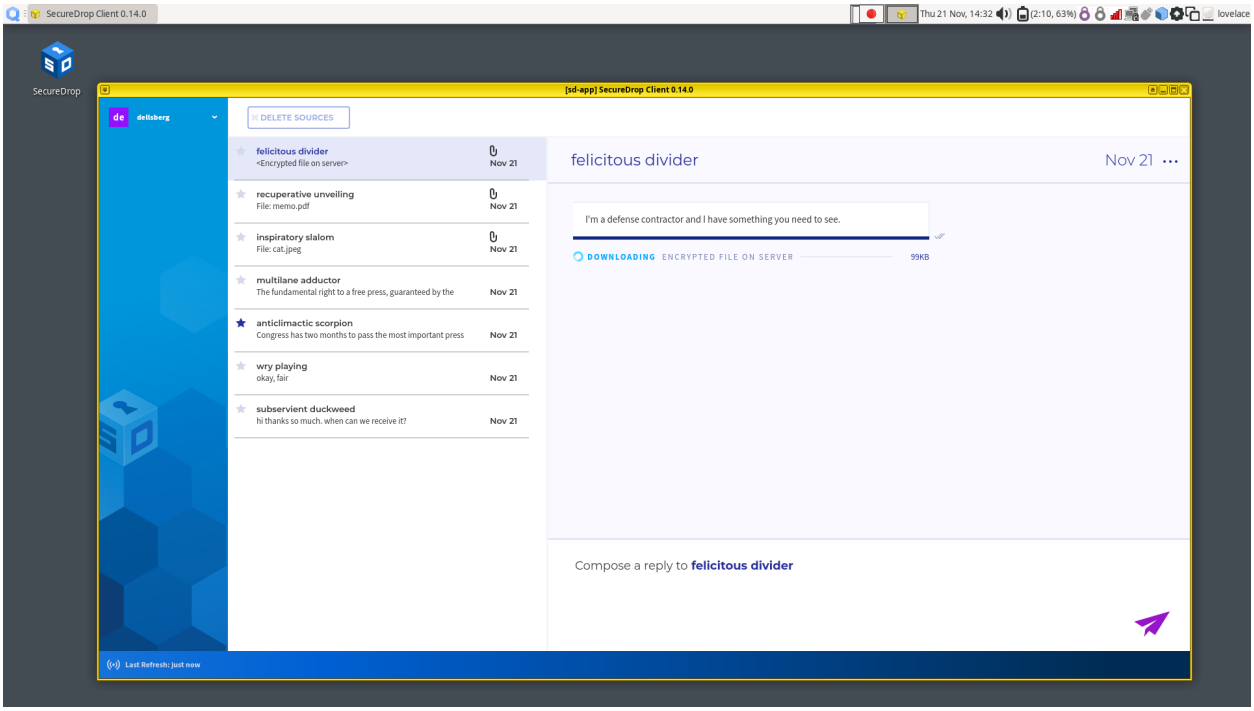
WORKING WITH SUBMISSIONS

When a source submits files, you will see a Download button in the conversation flow, a file size, and light-gray text that says “Encrypted file on server.”

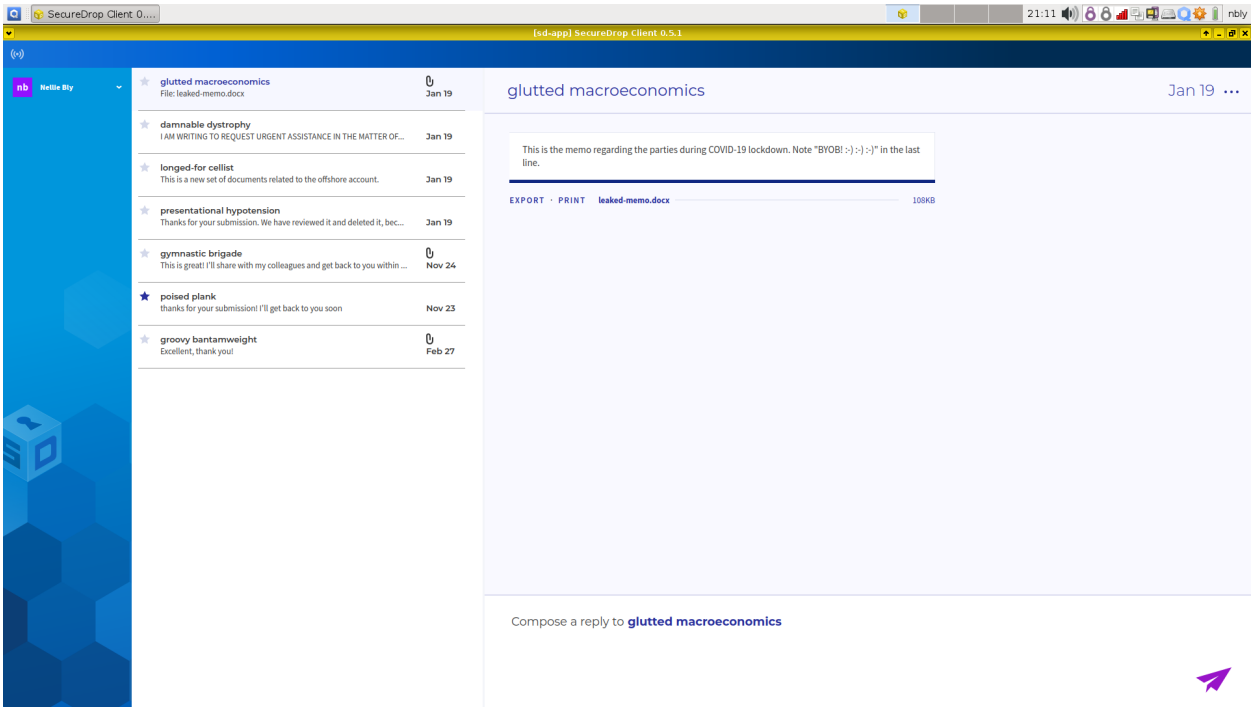


9.1 Downloading

To download a file, click the **Download** button. An animated spinner will indicate that the file is downloading:

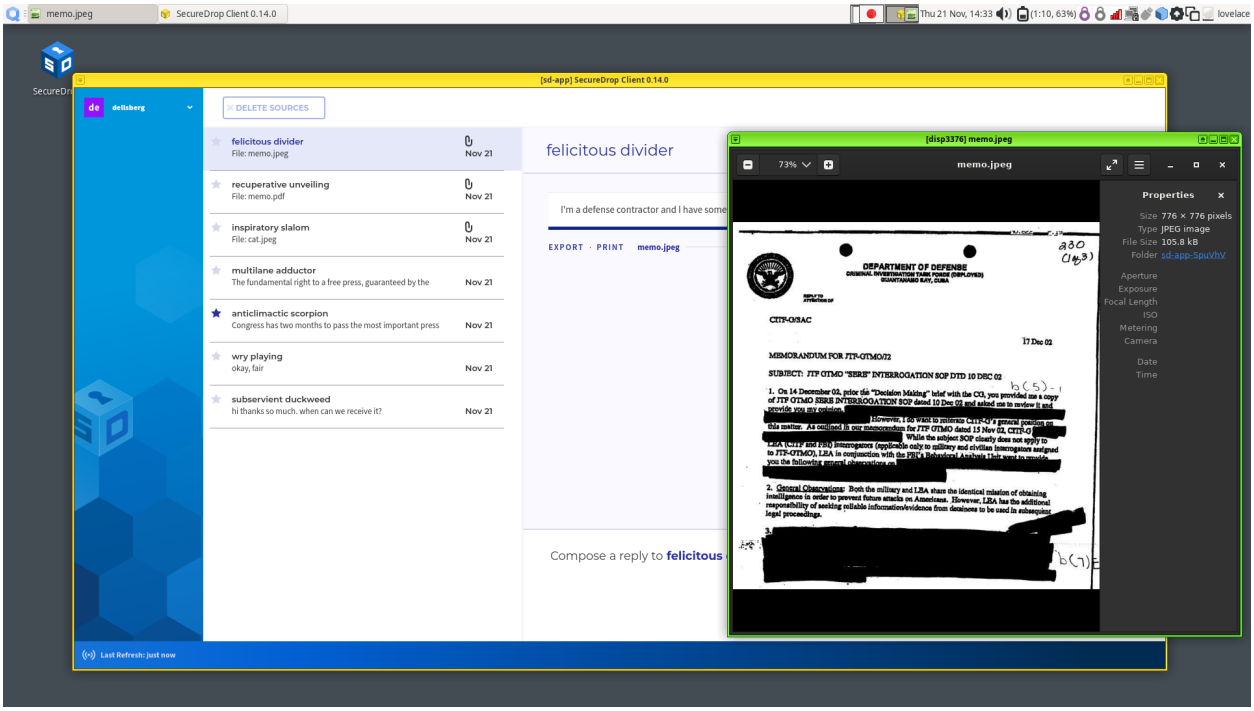


Once the file has been downloaded and decrypted, the filename will be visible, as will the action **Export** and **Print**. The displayed file size may increase after the download is complete, because the SecureDrop Client automatically decompresses the downloaded file.



9.2 Viewing

To view a downloaded submission, click its filename. This will open the file in a temporary environment, called a "disposable VM." The file you clicked on will open in a new window with a different colored border and a window title prefixed with "disp" (meaning disposable).



This disposable VM is a special isolated environment similar to the *Secure Viewing Station*; it does not have internet access, and isolates the files that you are viewing from other sensitive files and applications on the same computer.

> **Tip**
>
> In Qubes, window border colors are used to signify different virtual machines.

9.3 Printing

To print a document, click the **Print** button. Currently, printing is only supported with a specific HP printer model, and for security reasons you are required not to use a printer that has any wireless capabilities.

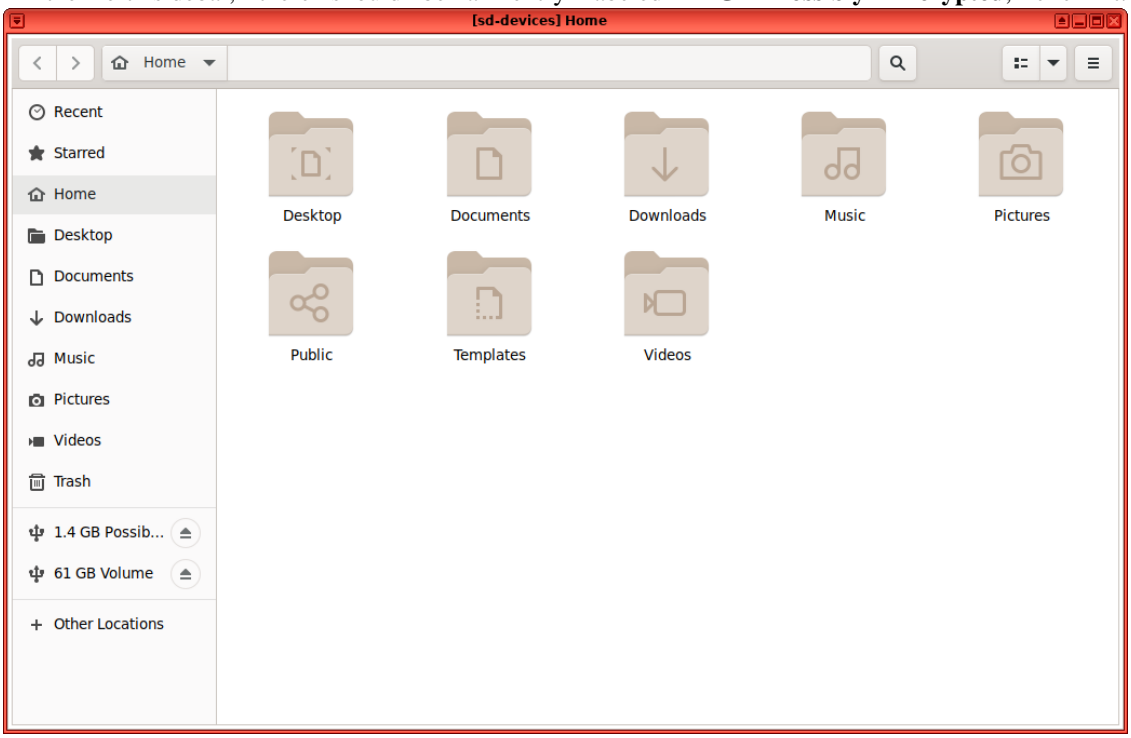
You should have access to a supported printer that has been set up by your administrator. The printer must be plugged into the computer's USB port.

9.4 Exporting to an Export USB

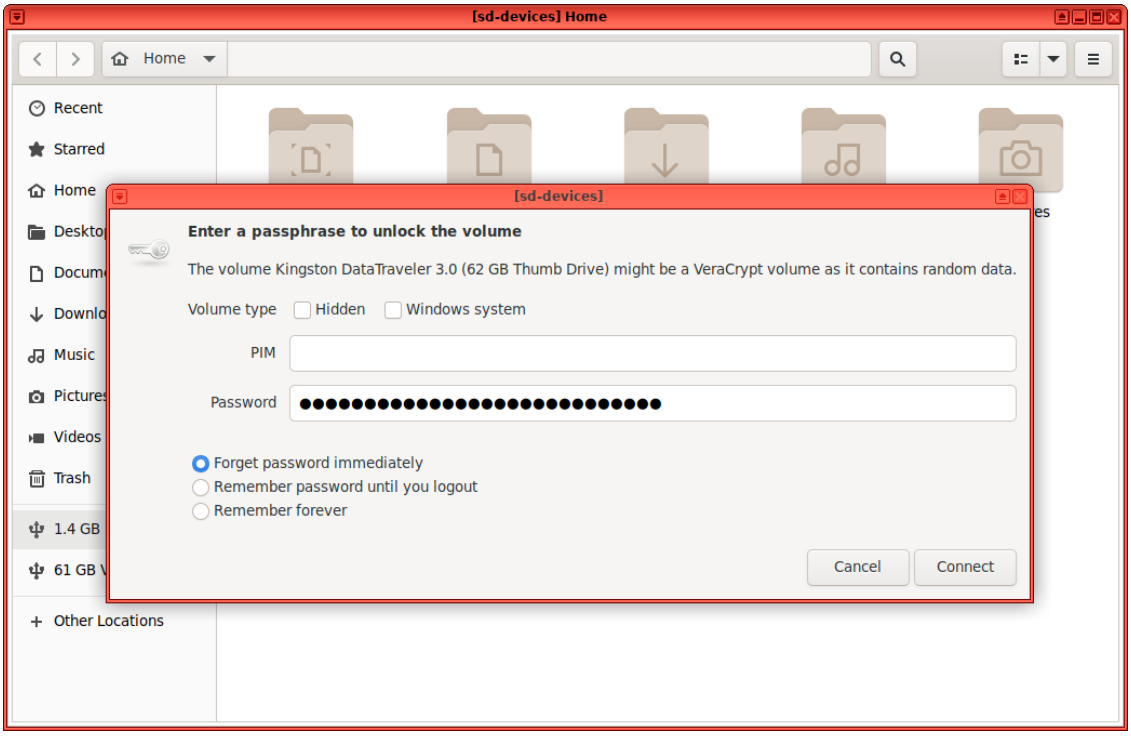
Currently, a LUKS- or VeraCrypt-encrypted USB drive is required for exporting submissions.

1. Insert the USB drive and wait for the `sd-devices` VM to start.
2. If your drive is using VeraCrypt, you will need to unlock it manually:
    1. Open the file menu by clicking on the **Q** application menu (in the top left), select **sd-devices** and click **Files**.

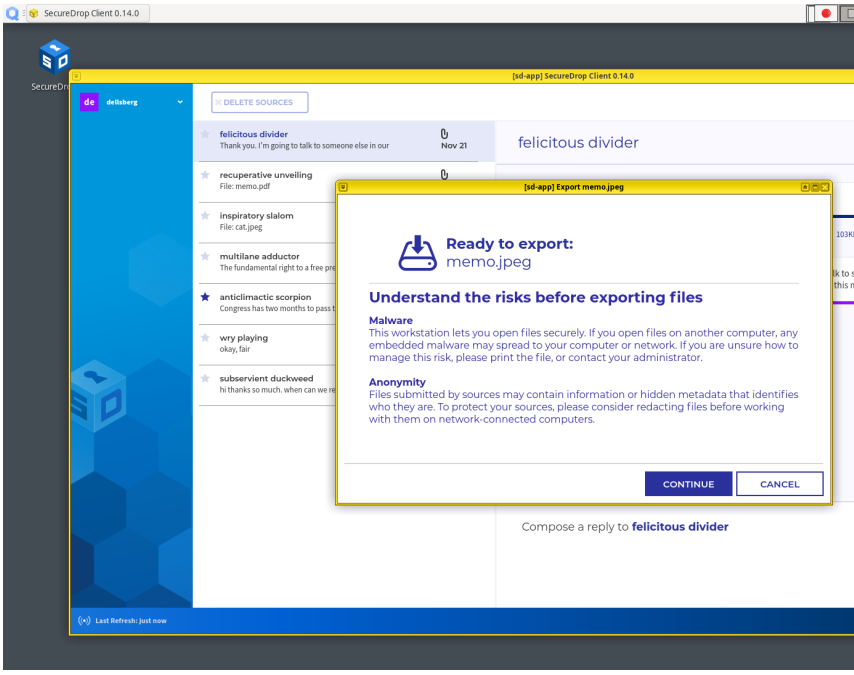
2. In the left sidebar, there should be an entry labeled **# GB Possibly Encrypted**, click it.



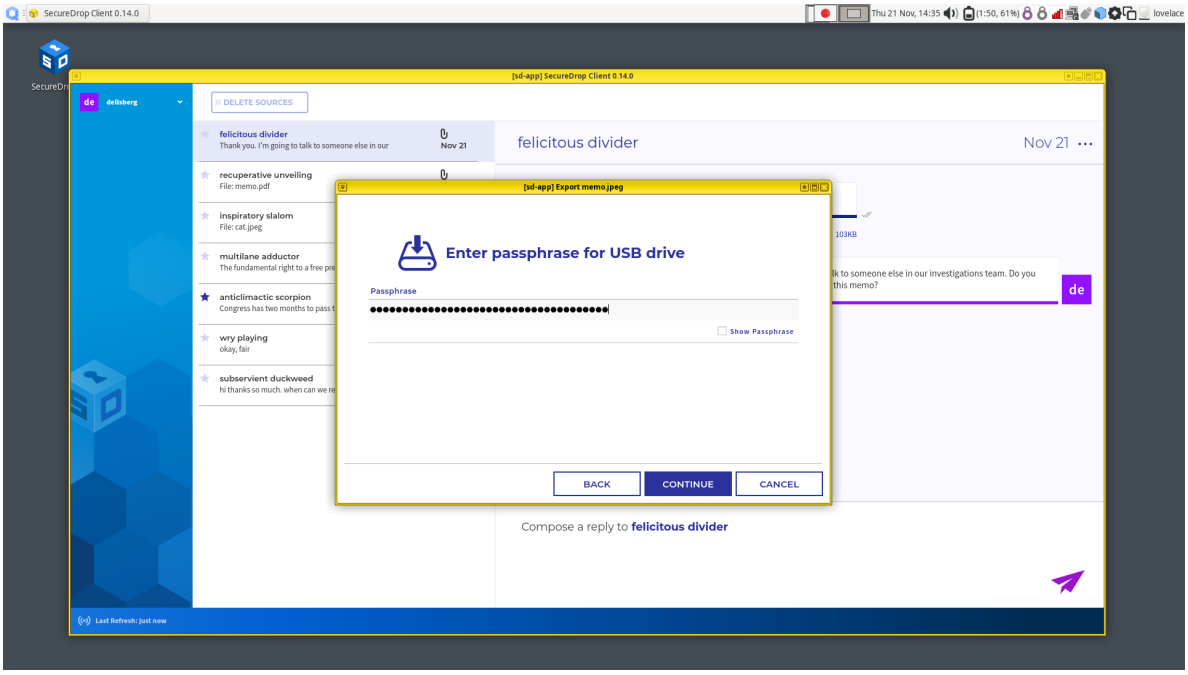
3. You will be prompted for the password configured for this USB drive:
   - Volume type: leave both unchecked
   - PIM: leave empty
   - Password: drive's password
   - Forget password immediately: selected



4. Click **Connect**.



3. Back in your source's conversation, click **Export**.
4. If you have not already unlocked your USB drive, you will be prompted for the password configured for this USB

drive. 

5. Once you see a message informing you that the export was successfully completed, you can safely unplug the USB drive. Alternatively, you can leave the drive plugged in and export additional files.

CHAPTER

TEN

ENDING YOUR SESSION

When you are finished using SecureDrop Workstation, close the SecureDrop Client window and shut the computer down completely. This is to take advantage of the protections of full-disk encryption, and to avoid unauthorized access to the Workstation and the files and materials on it, which include any messages and submissions that you have downloaded.

To shut down the computer, click your username in the top righthand corner of your screen, and select **Shut Down** from the menu.

CHAPTER

ELEVEN

FAQ

11.1 Frequently Asked Questions

11.1.1 How does SecureDrop Workstation work?

SecureDrop Workstation is a Qubes-based project. It consists of several different carefully-configured virtual machines (VMs), so that everything a journalist needs to use SecureDrop resides on one computer. Encryption and decryption happen with one click using a network-isolated VM that holds the SecureDrop Submission Key. Submissions can be viewed securely on the same machine thanks to a feature of Qubes that creates temporary VMs in which to view untrusted content without exposing the rest of your system to that content.

As a journalist, you will log into the SecureDrop application with the same credentials you previously used to log into the Journalist Interface. You will then be able to view, download, and reply to and submissions—all on the same device.

11.1.2 How is using Qubes different from using virtual machines?

Virtual machines that run on your Mac, Windows, or Linux machine (such as those created using VirtualBox, Parallels, and so on) are a "guest" on your machine, but still require a "host" operating system on top of which to run. These virtual machines are not designed as security tools; if the host OS is compromised, there are no protections for the guest OS, and some features (such as networking) allow communications between guest and host that can compromise the security of both.

In contrast, Qubes virtualization occurs at a lower level, under the Xen hypervisor. This means that virtual machines (VMs) in a Qubes environment can run operating systems that are independent of each other and are not reliant on a host OS.

In addition, these virtual machines can be used to quarantine specific functions of your computer. For example, network access is provided via two or more VMs, and you can control which applications or files have access to a networked environment by connecting to or disconnecting from these VMs.

Finally, Qubes is designed to make it more difficult for malware to remain on your machine. Each VM has read-only access to the root filesystem that provides its operating system, meaning that if a VM is infected with malware, it will be more difficult for that malware to persist across a reboot of that VM.

For more about the security features of Qubes, see the Qubes OS documentation.

11.1.3 How does the security of this system compare to using an air-gapped Secure Viewing Station?

The air-gapped Secure Viewing Station that is part of a SecureDrop setup offers strong protections against exfiltration of submissions or encryption keys by adversaries. It lacks important protections that SecureDrop Workstation provides. On the other hand, vulnerabilities in Qubes OS or Xen Hypervisor may have a greater security impact than vulnerabilities in Tails, the operating system used on a Secure Viewing Station.

A typical SVS USB drive may contain documents from multiple sources and always contains the highly sensitive private key needed to decrypt them. An adversary who does manage to achieve a security compromise (e.g., through a vulnerability in a file viewer application) can access these other files, and may be able to exfiltrate them.

In spite of the air-gap, this may be possible through physical channels used to transfer files off the SVS (e.g., USB drives), or by motivating the journalist user to perform an unsafe action (e.g., scanning a QR code).

Because the air-gapped SVS has no Internet access, updates can only be performed using another computer and a USB drive. In practice, newsrooms may not update their SVS in a timely manner, which can significantly worsen its security posture.

In SecureDrop Workstation, any document received via SecureDrop is opened in a disposable VM that has no Internet access and no access to other files submitted via SecureDrop. The encryption keys are stored in a separate, networkless VM from the SecureDrop Client app.

Because SecureDrop Workstation has Internet access, updates can be applied automatically as soon as they are available. SecureDrop Workstation enforces this by downloading and applying updates before the user logs into SecureDrop.

SecureDrop Workstation uses hardware-assisted virtualization, which allows us to use custom kernels for its VMs. These custom kernels use the grsecurity patches which are also used on the SecureDrop servers, and provide additional mitigation against security vulnerabilities.

An attacker able to exploit vulnerabilities in Qubes OS or Xen-based bare metal virtualization (likely in combination with other vulnerabilities, e.g., in a viewer application) may be able to exfiltrate information directly to the Internet. Qubes closely tracks any security vulnerabilities that may impact it, and the automatic update mechanism helps to ensure that, in the event of a vulnerability, every SecureDrop Workstation can be patched as quickly as possible.

For further technical detail on design rationale and mitigations, please consult our design document.

11.1.4 Can I install custom software on SecureDrop Workstation?

Right now, the project is designed to make the journalist experience easier by combining the functionality of the Journalist Workstation and Secure Viewing Station. The main focus is making sure that checking SecureDrop is easier and faster.

While we hope to add advanced tooling and document-processing options down the line, at this time we request that you do not change the configuration of the workstation or install additional software on it. If you have specific needs that you would like to discuss with us, please open an issue in our support portal or send us a GPG-encrypted email at support@freedom.press.

11.1.5 Why can't I save or print from the Viewer VM apps?

When you view a file on SecureDrop Workstation, it is opened in a disposable VM that cannot access the network or any peripherals. The VM and all its data will be destroyed the moment you close the viewer application.

You can save files from a viewer application, but copies saved inside a disposable VM will be deleted when you close the application, and the changes will not be applied to the main copy of the file stored on your computer.

You cannot print from the viewer application, because it does not have access to peripherals. This prevents malware from exfiltrating data (e.g., via attached USB devices), and from targeting hardware-level security vulnerabilities.

You *can* print files directly from the SecureDrop Client by clicking "Print" for a downloaded file, which will pass the file through to your USB printer without opening it in an interactive viewer application.

11.1.6 Why can't I copy and paste?

You should be able to copy and paste *within* any VM on the system, e.g., from one application running in `sd-app` to another.

Copy and paste between and to SecureDrop Workstation VMs is disabled for security reasons. The goal of this restriction is to minimize the risk of accidental pastes of sensitive content, and to reduce the attack surface for attempts to exfiltrate information.

Administrators can configure limited exceptions to this policy; please see the section *Managing Clipboard Access* of the admin guide for more information.

11.1.7 Why does it take so long to start the SecureDrop Client?

If the system has not been updated recently, the preflight updater will check for available security updates for all VMs used by SecureDrop Workstation, download, and apply them. This takes longer than for typical operating systems because of the number of VMs involved, and because some updates are performed over the Tor network.

These updates are essential to keep SecureDrop Workstation secure. Their speed is expected to be improved in subsequent releases of SecureDrop Workstation.

CHAPTER

TWELVE

SECUREDROP WORKSTATION INSTALLATION OVERVIEW

12.1 Overview

SecureDrop Workstation must be installed on a system running Qubes OS. The installation and configuration process should take between 4 and 6 hours, including time spent waiting for downloads and updates. At a high level, the tasks to be performed are as follows:

12.1.1 Pre-install tasks:

1. Rotate legacy passphrases (for pre-2018 installations)
2. Apply BIOS updates and check settings
3. Download and verify Qubes OS
4. Install Qubes OS
5. (Hardware-dependent) Apply USB fixes
6. Apply updates to system templates
7. Install and update Fedora 40 base template

12.1.2 Install tasks:

1. Copy the submission key
2. Copy *Journalist Interface* details
3. Copy SecureDrop login credentials
4. Download and install SecureDrop Workstation
5. Configure SecureDrop Workstation
6. Test the Workstation

12.2 Prerequisites

In order to install SecureDrop Workstation and configure it to use an existing SecureDrop instance, you will need the following:

- A Qubes-compatible computer with at least 16GB of RAM (32 GB is recommended). SecureDrop Workstation has mainly been tested against Lenovo T480, T490 and T14 - see Qubes' Hardware Compatibility List and the SecureDrop Workstation *Recommended hardware* page for more options .

- Qubes installation medium - this guide assumes the use of a USB 3.0 stick. Qubes may also be installed via optical media, which may make more sense depending on your security concerns.

  Note

  A USB stick with a Type-A connector is recommended, as USB-C ports may be disabled on your computer when the BIOS settings detailed below are applied.

- The SecureDrop instance's *Admin Workstation* and Secure Viewing Station (SVS) USBs, and the full GPG fingerprint of the submission key.
- (Optional, for a single-user workstation) The *Journalist Workstation* USB for the intended user of this workstation, if you want to import their SecureDrop login credentials into the workstation's password manager.
- The passphrases required to unlock the persistent volumes on each of these USB drives.
- A working computer (Linux is recommended and assumed in this guide) to use for verification and creation of the Qubes installation medium.

  Note

  A Tails USB can be used to perform the tasks below, but due to the size of the Qubes installation ISO, it may make sense to download it on another computer rather than via Tor, and then to use a USB stick to transfer it to Tails for verification and creation of the installation medium.

- A password manager or other system to generate and store strong passphrases for Qubes full disk encryption (FDE) and user accounts.

A basic knowledge of the Qubes OS is helpful.

CHAPTER

THIRTEEN

PRE-INSTALL TASKS

13.1 Apply BIOS updates and check settings

Before beginning the Qubes installation, make sure that your Qubes-compatible computer's BIOS is updated to the latest available version. If you're using one of the recommended ThinkPad T-series models, see the section on *Lenovo T series laptops*. The process will be different for other makes and models, and can usually be found on their respective support sites.

Once the BIOS is up-to-date, boot into the BIOS setup utility and update its settings. Note that not all BIOS versions will support the items listed, but if available following changes are recommended:

- Ensure the internal clock is correct.
- Set a password to access the BIOS (and record the password in your password manager).
- Disable BIOS downgrades.
- Enable Data Execution Prevention.
- Enable virtualization support (required for Qubes OS). - for Intel-based devices, **Intel VT-d** and **Intel VT-x** should be enabled - for AMD-based devices, **AMD-VI** and **AMD-V** should be enabled
- Disable unnecessary I/O options such as Wireless WAN and Bluetooth.
- Disable unnecessary network options such as Wake-on-LAN and UEFI network stacks.
- Disable Thunderbolt ports, or any other ports that allow Direct Memory Access (DMA).
- Enable any physical tamper detection options.
- Disable Computrace.
- Disable SecureBoot.

If the Qubes hardware compatibility list entry for your computer recommends the use of Legacy Mode for boot, change that setting in the BIOS as well.

13.2 Download and verify Qubes OS

On the working computer, download the Qubes OS ISO and cryptographic hash values for version `4.2.2` from https://www.qubes-os.org/downloads/. The ISO is 6.9 GB approximately, and may take some time to download based on the speed of your Internet connection.

Follow the linked instructions to verify the ISO. Ensure that the ISO and hash values are in the same directory, then run:

```
gpg --keyserver-options no-self-sigs-only,no-import-clean --fetch-keys https://keys.
↪qubes-os.org/keys/qubes-release-4.2-signing-key.asc
gpg -v --verify Qubes-R4.2.2-x86_64.iso.DIGESTS
sha256sum -c Qubes-R4.2.2-x86_64.iso.DIGESTS
```

The output should look like this:

```
gpg: requesting key from 'https://keys.qubes-os.org/keys/qubes-release-4.2-signing-key.
↪asc'
gpg: key E022E58F8E34D89F: public key "Qubes OS Release 4.2 Signing Key" imported
gpg: Total number processed: 1
gpg:               imported: 1
gpg: no ultimately trusted keys found

gpg: armor header: Hash: SHA256
gpg: original file name=''
gpg: Signature made Tue 25 Jun 2024 01:32:23 PM EDT
gpg:                using RSA key 9C884DF3F81064A569A4A9FAE022E58F8E34D89F
gpg: using pgp trust model
gpg: Good signature from "Qubes OS Release 4.2 Signing Key" [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: 9C88 4DF3 F810 64A5 69A4  A9FA E022 E58F 8E34 D89F
gpg: textmode signature, digest algorithm SHA256, key algorithm rsa4096
Qubes-R4.2.2-x86_64.iso: OK
sha256sum: WARNING: 20 lines are improperly formatted
```

Specifically, you will want to make sure that you see "Good signature" listed in the text. If it does not report a good signature, try deleting the ISO and downloading it again.

Once you've verified the ISO, copy it to your installation medium - for example, if using Linux and a USB stick, using the command:

```
sudo dd if=Qubes-R4.2.2-x86_64.iso of=/dev/sdX bs=1048576 && sync
```

where `if` is set to the path to your downloaded ISO file and `of` is set to the block device corresponding to your USB stick. Note that any data on the USB stick will be overwritten.

Caution

Make sure to verify that you have the correct device name using, for example, the `lsblk` command. You should write to the full device (eg. `/dev/sdc`) rather than to a partition (eg. `/dev/sdc1`).

13.3 Install Qubes OS (estimated wait time: 30-45 minutes)

Before starting the installation, please ensure that:

- the computer is charging
- all USB devices like YubiKeys, mice and keyboards are disconnected

To begin the Qubes installation, connect the Qubes install USB to your target computer and boot from it. You may need to bring up a boot menu at startup to do so - on Lenovo laptops, for example, you can do so by pressing **F12** on boot.

Follow the installation documentation to install Qubes on your computer, ensuring that you:

- Use English - United States as the setup language. (This requirement will be dropped in a future version).
- Use all available storage space for the installation (as the computer should be dedicated to SecureDrop Workstation).
- Set a strong full disk encryption (FDE) passphrase - a 6-word Diceware passphrase is recommended.
- Create an administrative account named `user` with a strong password.

Note

Qubes is not intended to have multiple user accounts, so your account name and password will be shared by all SecureDrop Workstation users. The password will be required to log in and unlock the screen during sessions - choosing something strong but memorable and easily typed is recommended!

Once the installation is complete, you will be prompted to reboot into Qubes. Reboot, removing the install USB when the computer restarts.

You will be prompted to enter the FDE passphrase set during installation.

After the disk is unlocked and Qubes starts, you will be prompted to complete the initial setup. Click the Qubes OS icon.

On the configuration screen, ensure that the following options are checked:

- Default Template should be set to "Fedora 40 Xfce"
- "Create default system qubes (sys-net, sys-firewall, default DispVM)"
- "Make sys-firewall and sys-usb disposable"

If there is a grayed out option "USB qube configuration disabled", make a note of this. An additional setup step will be required (see next section).

Finally, click **Finish Configuration** to set up the default system TemplateVMs and AppVMs.

Once the initial setup is complete, the login dialog will be displayed. Log in using the username and password set during installation.

13.4 (Hardware-dependent) Apply USB fixes

If, during the installation, you encountered the grayed out option "USB qube configuration disabled", you must now create a VM to access your USB devices. If you did not encounter this issue, you can skip this section.

To create a USB qube, open a `dom0` terminal by opening the **Q Menu**, selecting the gear icon on the left-hand side, then selecting **Other > Xfce Terminal**

Tip

For quicker access, you can add the `dom0` terminal to the "Favorites" section of the Qubes menu (identified by a bookmark symbol). Right-click the entry and select **Add to favorites**. To remove it at a later time, right-click the entry in your list of favorites and select **Remove from favorites**.

Run the following command:

```
sudo qubesctl state.sls qvm.sys-usb
```

After the command exits, confirm that you see an entry "Service: sys-usb" in the Qubes menu. If `sys-usb` is not running, you can start it with the command `qvm-start sys-usb` in `dom0`. Once `sys-usb` is running, click the devices widget in the upper right panel to expand a listing of all devices detected by Qubes OS.

Now, insert a safe USB device you intend to use with the SecureDrop Workstation. Click the devices widget again. Does the newly attached USB device appear in the list? If so, USB support is working and you can proceed with the installation. If you do encounter the error message "Denied qubes.InputKeyboard from sys-usb to dom0", you need to additionally enable USB keyboard support:

```
sudo qubesctl state.sls qvm.usb-keyboard
```

While we recommend against the use of a USB keyboard for security reasons, this error can also occur in combination with other USB devices on some hardware.

13.5 Apply `dom0` updates (estimated wait time: 15-30 minutes)

`dom0` is the most trusted domain on Qubes OS, and has privileged access to all other VMs. As such, it is important to ensure that all available security updates have been applied to `dom0` as the first step after the installation.

After logging in, use the network manager widget in the upper-right panel to configure your network connection.

Open a `dom0` terminal by opening the **Q Menu**, selecting the gear icon on the left-hand side, then selecting **Other > Xfce Terminal**. Run the following command:

```
sudo qubes-dom0-update -y
```

Wait for all updates to complete. If you encounter an error during this stage, please contact us for assistance, as it may not be safe to proceed with the installation.

After updating `dom0`, reboot the workstation to ensure that all updates have taken effect for your active session.

13.6 Apply updates to system templates (estimated wait time: 45-60 minutes)

After logging in again, confirm that the network manager successfully connects you to the configured network. If necessary, verify the network settings using the network manager widget.

- Next, configure Tor by selecting the Qubes menu (the **Q** icon in the upper left corner) and selecting **Q > Service > sys-whonix > Anon Connection Wizard**. In most cases, choosing the default **Connect** option is best. Click **Next**, then **Next** again. Then, if Tor connects successfully, click **Finish**. If Tor fails to connect, make sure your network conection is up and does not filter Tor connections, then try again.

  > **Note**
  >
  > If Tor connections are blocked on your network, you may need to configure Tor to use bridges in order to get a connection. For more information, see the Anon Connection Wizard documentation.

- Once Tor has connected, select the **Q Menu**, click the gear icon on the left-hand side, then select **Qubes Tools > Qubes Update** to update the system VMs. in the `[Dom0] Qubes Update` window, check all entries in the list above except for `dom0` (which you have already updated in the previous step). Then, click **Update**. The system's VMs will be updated sequentially - this may take some time. When the updates are complete, click **Next**. You

will then be prompted to **Finish and restart/shutdown 4 qubes.** Go ahead and do so, and allow time for them to restart.

CHAPTER

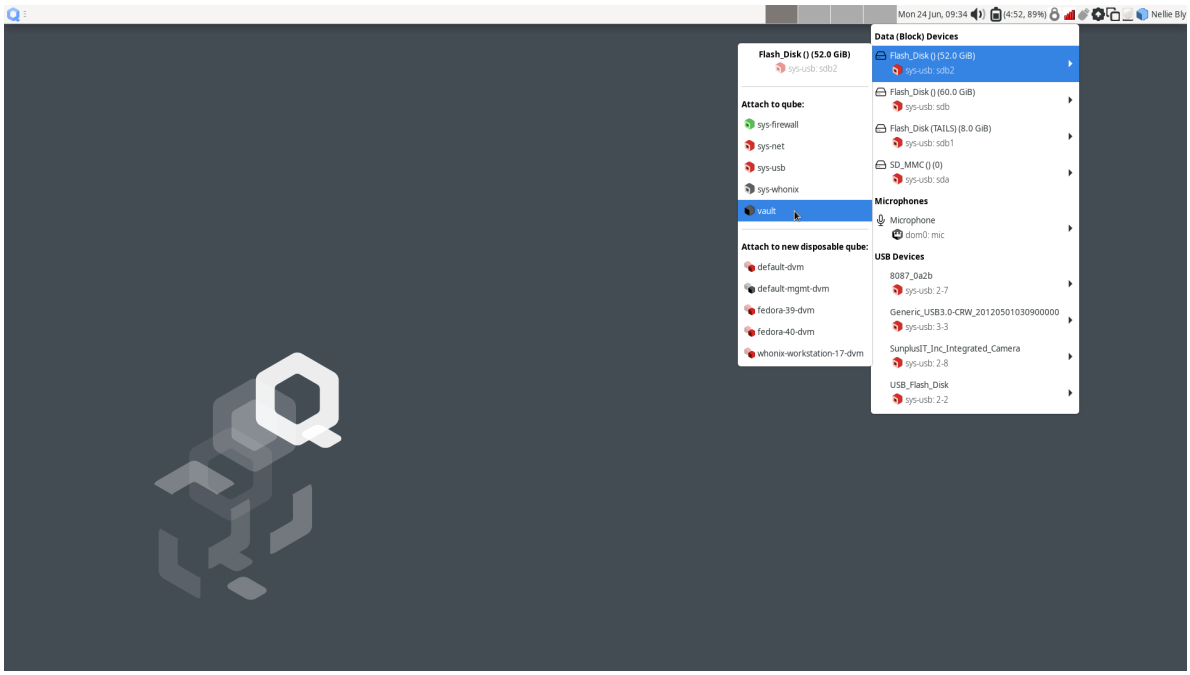
FOURTEEN

INSTALLING SECUREDROP WORKSTATION

14.1 Copy the submission key

In order to decrypt submissions, your SecureDrop Workstation will need a copy of the secret key from your SecureDrop instance's SVS. To protect this key and preserve the air gap, you will need to connect the SVS USB to a Qubes VM with no network access, and copy it from there to `dom0`. Note that you cannot directly copy and paste to the `dom0` VM from another VM - instead, follow the steps below to copy the file into `dom0`:

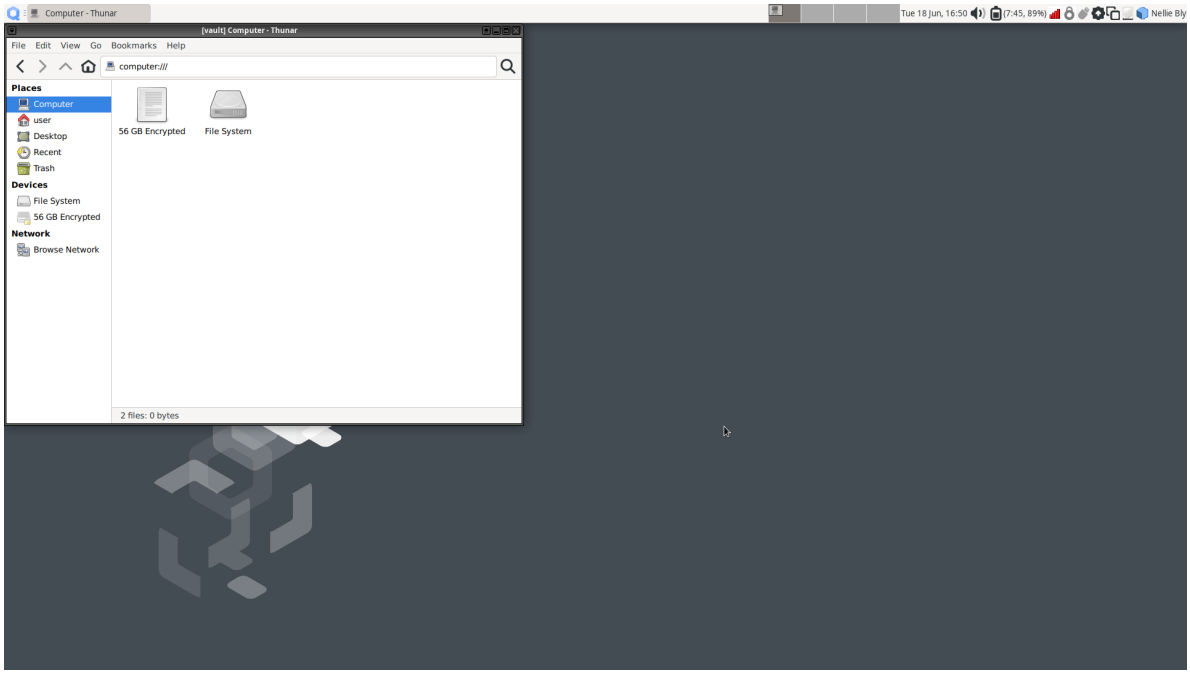
- First, use the network manager widget in the upper right panel to disable your network connection. These instructions refer to the `vault` VM, which has no network access by default, but if the SVS USB is attached to another VM by mistake, this will offer some protection against exfiltration.
- Next, choose **Q > Apps > vault > Thunar File Manager** to open the file manager in the `vault` VM.
- Connect the SVS USB to a USB port on the Qubes computer, then use the devices widget in the upper right panel to attach it to the `vault` VM. There will be three entries for the USB in the section titled **Data (Block) Devices**. Choose the *unlabeled* entry (*not* the one labeled "TAILS") annotated with a `sys-usb` text that ends with a number, like `sys-usb:sdb2`. That is the persistent volume.



- In the the `vault` file manager, select the persistent volume's listing in the lower left sidebar. It will be named `N GB encrypted`, where N is the size of the persistent volume. Enter the SVS persistent volume passphrase to

unlock and mount it. When asked if you would like to forget the password immediately or remember it until you logout, choose the option to **Forget password immediately**.

> **Note**
>
> You will receive a message that says **Failed to open directory "TailsData"**. This is normal behavior and will not cause any issues with the subsequent steps.



- Open a `dom0` terminal by opening the **Q Menu**, selecting the gear icon on the left-hand side, then selecting **Other > Xfce Terminal**. Once the Terminal window opens, run the following command to list the SVS submission key details, including its fingerprint:

```
qvm-run --pass-io vault \
  "gpg --homedir /run/media/user/TailsData/gnupg -K --fingerprint"
```

- Next, run the comand:

```
qvm-run --pass-io vault \
  "gpg --homedir /run/media/user/TailsData/gnupg --export-secret-keys --armor
↪<SVSFingerprint>" \
  > /tmp/sd-journalist.sec
```

  where `<SVSFingerprint>` is the submission key fingerprint, typed as a single unit without whitespace. This will copy the submission key in ASCII format to a temporary file in dom0, `/tmp/sd-journalist.sec`.

- Verify the that the file starts with `-----BEGIN PGP PRIVATE KEY BLOCK-----` using the command:

```
head -n 1 /tmp/sd-journalist.sec
```

- In the `vault` file manager, right-click on the **TailsData** sidebar entry, then select **Unmount** and disconnect the SVS USB.

14.2 Copy *Journalist Interface* details

SecureDrop Workstation connects to your SecureDrop instance's API via the *Journalist Interface*. In order to do so, it will need the *Journalist Interface* address and authentication info. As the clipboard from another VM cannot be copied into `dom0` directly, follow these steps to copy the file into place:

- Locate an *Admin Workstation* or *Journalist Workstation* USB drive. Both hold the address and authentication info for the *Journalist Interface*; if you also want to copy the journalist user's password database, use the *Journalist Workstation* USB drive.
- Connect the USB drive to a USB port on the Qubes computer, then use the devices widget in the upper right panel to attach it to the `vault` VM. There will be 3 listings for the USB in the widget: one for the base USB, one for the Tails partition on the USB, labeled `Tails`, and a 3rd unlabeled listing, for the persistent volume. Choose the third listing.
- In the the `vault` file manager, select the persistent volume's listing in the lower left sidebar. It will be named `` `N GB encrypted ``, where N is the size of the persistent volume. Enter the persistent volume passphrase to unlock and mount it. When prompted, select the option to **Forget password immediately**.
- Copy the *Journalist Interface* configuration file to `dom0`. If your SecureDrop instance uses v3 onion services, use the following command:

```
qvm-run --pass-io vault \
  "cat /run/media/user/TailsData/Persistent/securedrop/install_files/ansible-base/
↪app-journalist.auth_private" \
  > /tmp/journalist.txt
```

- Verify that the `/tmp/journalist.txt` file on `dom0` contains valid configuration information using the command `cat /tmp/journalist.txt` in the `dom0` terminal.
- If you used an *Admin Workstation* USB drive, or you don't intend to copy a password database to this workstation, safely disconnect the USB drive now. In the `vault` file manager, right-click on the **TailsData** sidebar entry, then select **Unmount** and disconnect the USB drive.

14.3 Copy SecureDrop login credentials

Users of SecureDrop Workstation must enter their username, passphrase and two-factor code to connect with the SecureDrop server. You can manage these passphrases using the KeePassXC password manager in the `vault` VM. If this laptop will be used by more than one journalist, we recommend that you shut down the `vault` VM now (using the Qube widget in the upper right panel), skip this section, and use a smartphone password manager instead.

In order to set up KeePassXC for easy use:

- Add KeePassXC to the application menu by selecting it from the list of available apps in **Q > Apps > vault > Settings > Applications** and pressing the button labeled **>** (do not press the button labeled **>>**, which will add *all* applications to the menu).
- Launch KeePassXC via **Q > Apps > vault > KeePassXC**. When prompted to enable automatic updates, decline. `vault` is networkless, so the built-in update check will fail; the app will be updated through system updates instead.
- Close the application.

Important

The *Admin Workstation* password database contains sensitive credentials not required by journalist users. Make sure to copy the credentials from the *Journalist Workstation* USB.

In order to copy a journalist's login credentials:

- If a *Journalist Workstation* USB is not currently attached, connect it, attach it to the `vault` VM, open it in the file manager, and enter its encryption passphrase.
- Locate the password database. It should be in the `Persistent` directory, and will typically be named `keepassx.kdbx` or similar.
- Open a second `vault` file manager window (`Ctrl + N` in the current window) and navigate to the **Home** directory.
- Drag and drop the password database to copy it.
- In the `vault` file manager, right-click on the **TailsData** sidebar entry, then select **Unmount** and disconnect the *Journalist Workstation* USB. Close this file manager window.
- In the file manager window that displays the home directory, open the copy you made of the password database by double-clicking it.
- If the database is passwordless, KeePassXC may display a security warning when opening it. To preserve convenient passwordless access, 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 selected when you open the database, but KeePassXC will remember the last selection.
- Inspect each section of the password database to ensure that it contains only the information required by the journalist user to log in.
- Close the application window and shut down the `vault` VM (using the Qube widget in the upper right panel).

14.4 Download and install SecureDrop Workstation

With the key and configuration available in `dom0`, you're ready to set up SecureDrop Workstation:

- First, re-enable the network connection using the network manager widget.
- Next, start a terminal in the network-attached `work` VM, via **Q > Apps > work > Xfce Terminal**.

Note

As the next steps include commands that must be typed exactly, you may want to open a browser in the `work` VM, open this documentation there, and copy-and-paste the commands below into your `work` terminal. Note that due to Qubes' default security settings you will *not* be able to paste commands into your `dom0` terminal. The `work` browser can be opened via **Q > Apps > work > Firefox**

- In the `work` terminal, run the following commands to download and add the SecureDrop signing key, which is needed to verify the SecureDrop Workstation package:

```
gpg --keyserver hkps://keys.openpgp.org --recv-key \
  "2359 E653 8C06 13E6 5295 5E6C 188E DD3B 7B22 E6A3"

gpg --armor --export 2359E6538C0613E652955E6C188EDD3B7B22E6A3 \
  > securedrop-release-key.pub

sudo rpmkeys --import securedrop-release-key.pub
```

- In the `work` terminal, open a text editor with escalated privileges (for example, with the command `sudo nano`) and create a file `/etc/yum.repos.d/securedrop-temp.repo` with the following contents:

```
[securedrop-workstation-temporary]
enabled=1
baseurl=https://yum.securedrop.org/workstation/dom0/f37
name=SecureDrop Workstation Qubes initial install bootstrap
```

- Download the SecureDrop Workstation config package to the curent working directory with the command:

```
dnf download securedrop-workstation-dom0-config
```

Note the release version number in the filename, you'll need it below. During the download, you may be prompted to confirm importing the Qubes OS Release 4 Signing Key. You can safely do so; it will not be used during the subsequent steps.

- Verify the package with the following command:

```
rpm -Kv securedrop-workstation-dom0-config-<versionNumber>-1.fc37.noarch.rpm
```

where <versionNumber> is the release version number you noted above. The command output should match the following text:

```
securedrop-workstation-dom0-config-<versionNumber>-1.fc37.noarch.rpm:
  Header V4 RSA/SHA512 Signature, key ID 7b22e6a3: OK
  Header SHA256 digest: OK
  Header SHA1 digest: OK
  Payload SHA256 digest: OK
  MD5 digest: OK
```

- If the package verification was successful, in the dom0 terminal, run the following command to transfer the RPM package to dom0:

```
qvm-run --pass-io work \
  "cat /home/user/securedrop-workstation-dom0-config-<versionNumber>-1.fc37.noarch.
↪rpm" \
  > securedrop-workstation.rpm
```

- Verify that the RPM was transferred correctly by running the following commands:
  - in the work terminal:

```
sha256sum securedrop-workstation-dom0-config-<versionNumber>-1.fc37.noarch.rpm
```

  - in the dom0 terminal:

```
sha256sum securedrop-workstation.rpm
```

If the hash output for both files matches, the RPM was transferred successfully.

- Install the RPM using the following command in the dom0 terminal:

```
sudo dnf install securedrop-workstation.rpm
```

When prompted, type **Y** and **Enter** to install the package.

- Shut down the work VM using the Qube widget in the top-right panel.

14.5 Configure SecureDrop Workstation (estimated wait time: 60-90 minutes)

Before setting up the set of VMs used by SecureDrop Workstation, you must configure the *Journalist Interface* connection and submission key.

- To add the submission key, run the following command in the dom0 terminal:

```
sudo cp /tmp/sd-journalist.sec /usr/share/securedrop-workstation-dom0-config/
```

- Your submission key has a unique fingerprint required for the configuration. Obtain the fingerprint by using this command:

```
gpg --with-colons --import-options import-show --dry-run --import /tmp/sd-
↪journalist.sec
```

  The fingerprint will be on a line that starts with `fpr`. For example, if the output included the line `fpr:::::::::65A1B5FF195B56353CC63DFFCC40EF1228271441:`, the fingerprint would be the character sequence `65A1B5FF195B56353CC63DFFCC40EF1228271441`.

- Next, create the SecureDrop Workstation configuration file:

```
cd /usr/share/securedrop-workstation-dom0-config
sudo cp config.json.example config.json
```

- The `config.json` file must be updated with the correct values for your instance. Open it with root privileges in a text editor such as `vi` or `nano` and update the following fields' values:
  - **submission_key_fpr**: use the value of the submission key fingerprint as displayed above
  - **hidserv.hostname**: use the hostname of the *Journalist Interface*, including the `.onion` TLD
  - **hidserv.key**: use the private v3 onion service authorization key value
  - **environment**: use the value `prod`

Note

You can find the values for the **hidserv.*** fields in the `/tmp/journalist.txt` file that you created in dom0 earlier. The file will be formatted as follows:

```
ONIONADDRESS:descriptor:x25519:AUTHTOKEN
```

- Verify that the configuration is valid using the command below in the dom0 terminal:

```
sdw-admin --validate
```

- Configure infinite scrollback for your terminal via **Edit > Preferences > General > Unlimited scrollback**. This helps to ensure that you will be able to review any error output printed to the terminal during the installation.
- Finally, in the dom0 terminal, run the command:

```
sdw-admin --apply
```

This command will take a considerable amount of time and approximately 4GB of bandwidth, as it sets up multiple VMs and installs supporting packages. When the command finishes, reboot the machine to complete the installation. Your SecureDrop Workstation is finally ready to use!

14.6 Test the Workstation

To start the SecureDrop Client, double-click the SecureDrop desktop icon that was set up by the previous command. The preflight updater will start and check for updates. The system should be up-to-date and no updates should be required, but if updates are available follow the instructions in the preflight updater to apply them.

Once the update check is complete, the SecureDrop Client will launch. Log in using an existing journalist account and verify that sources are listed and submissions can be downloaded, decrypted, and viewed.

14.7 Enable password copy and paste

If you use KeePassXC in the `vault` VM to manage login credentials, you can enable the user to copy passwords to the SecureDrop Client using inter-VM copy and paste. While this is relatively safe, we recommend reviewing the section *Managing Clipboard Access* of this guide, which goes into further detail on the security considerations for inter-VM copy and paste.

The password manager runs in the networkless `vault` VM, and the SecureDrop Client runs in the `sd-app` VM. To permit this one-directional clipboard use, issue the following command in `dom0`:

```
qvm-tags vault add sd-send-app-clipboard
```

Confirm that the tag was correctly applied using the `ls` subcommand:

```
qvm-tags vault ls
```

To revoke this configuration change later or correct a typo, you can use the `del` subcommand, e.g.:

```
qvm-tags vault del sd-send-app-clipboard
```

CHAPTER

FIFTEEN

TROUBLESHOOTING INSTALLATION ERRORS

15.1 "Failed to return clean data"

An error similar to the following may be displayed during an installation or update:

```
sd-log:
      ----------
      _error:
          Failed to return clean data
      retcode:
          None
      stderr:
      stdout:
          deploy
```

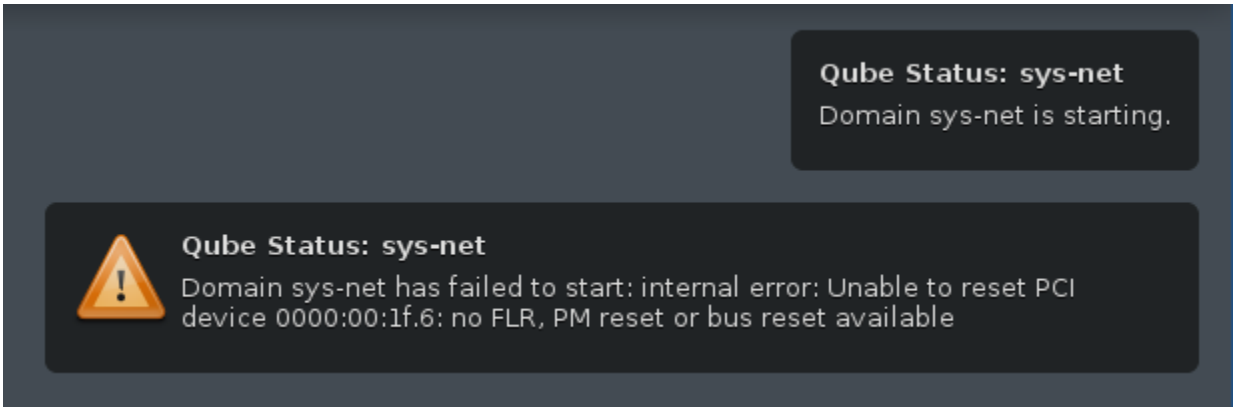
This is a transient error that may affect any of the SecureDrop Workstation VMs. To clear it, run the installation command or update again.

15.2 "Temporary failure resolving"

Transient network issues may cause an installation to fail. To work around this, verify that you have a working Internet connection, and re-run the `sdw-admin --apply` command.

15.3 "Unable to reset PCI device"

On some hardware, network devices (Ethernet and Wi-Fi) will not immediately work out of the box and require a one-time manual configuration on install. After Qubes starts for the first time, `sys-net` will fail to start:



Open a dom0 terminal via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal**, and run the following command to list the devices connected to the sys-net VM.

```
qvm-pci ls sys-net
```

This will return the two devices (Ethernet and WiFi) that are connected to sys-net:

```
BACKEND:DEVID  DESCRIPTION                                                    ␣
↪USED BY
dom0:00_14.3   Network controller: Intel Corporation                          ␣
↪sys-net
dom0:00_1f.6   Ethernet controller: Intel Corporation Ethernet Connection (5) I219-V ␣
↪sys-net
```

For both device IDs (e.g. dom0:00_1f.6 and dom0:00_14.3), you will need to detach and re-attach the device to sys-net, then restart sys-net as follows:

```
qvm-pci detach sys-net dom0:00_14.3
qvm-pci detach sys-net dom0:00_1f.6
qvm-pci attach sys-net --persistent --option no-strict-reset=True dom0:00_14.3
qvm-pci attach sys-net --persistent --option no-strict-reset=True dom0:00_1f.6
qvm-start sys-net
```

sys-net should now start, and network devices will be functional. This change is only required once on first install. See the Qubes documentation of this issue for more information.

15.4 Full system freezes

A known issue with some hardware results in Qubes fully freezing. If you encounter this issue, you will need to forcibly restart your computer, usually by holding down the power button.

When you boot up, you will see a black-and-white menu with the following options:

```
Qubes, with Xen hypervisor
Advanced options for Qubes (with Xen hypervisor)
UEFI Firmware Settings
```

While Qubes, with Xen hypervisor is selected, press e to edit the option. You should now see a rudimentary edit interface.

Find the line that starts with multiboot2 /xen- and ends with ${xen_rm_opts}. Use the arrow keys to move your cursor to before ${xen_rm_opts} and type cpufreq=xen:hwp=off (leave a space between off and the $.

Press Ctrl-x to continue with booting. This will fix the current boot, we now need to make the fix permanent.

Once Qubes has started and you have logged in, open a dom0 terminal via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal** and type sudo nano /etc/default/grub to start an editor.

Move your cursor to the bottom of the file and add: GRUB_CMDLINE_XEN_DEFAULT="$GRUB_CMDLINE_XEN_DEFAULT cpufreq=xen:hwp=off"

Press Ctrl-x, then y, and then Enter to save the file.

Finally, in the terminal run sudo grub2-mkconfig -o /boot/grub2/grub.cfg. The workaround will now automatically be applied going forwards.

15.4.1 Getting Support

If you have questions about this process or about any other aspect of SecureDrop Workstation, please reach out to us.

CHAPTER

SIXTEEN

RECOMMENDED HARDWARE

16.1 Qubes OS hardware requirements

In order to install and use SecureDrop Workstation, you will need a Qubes-Compatible computer with the following specifications:

- 64-bit Intel or AMD processor with virtualization support
- a minimum of 32GB RAM
- sufficient disk space for the Qubes OS base install and SecureDrop Workstation VMs (a 128GB or greater SSD is recommended)

We recommend against a device that requires an external USB keyboard for security reasons.

More information on hardware compatibility can be found on the Qubes OS System Requirements page, and information on specific systems can be found via the hardware compatibility list.

In order to print submissions, a supported non-networked printer is required. We have tested and recommend the HP LaserJet Pro M404n. More printer options will be added in future releases.

16.2 Lenovo X1 series laptops

16.2.1 Lenovo ThinkPad X1 Carbon (10th-generation)

The 10th-generation ThinkPad X1 Carbon **with a 12th-generation Intel Core processor** is a recommended option for the SecureDrop Workstation beginning with Qubes 4.1. If you plan to use it:

- If your laptop has come with Ubuntu preinstalled, run its **Software Updater** twice as follows:
  1. to install software updates, especially for the `fwupd` package; and then
  2. to run `fwupd` to update the BIOS automatically.

  If **Software Updater** offers to run `fwupd` during step (1), decline until step (2), to make sure `fwupd` itself has received its latest security updates.
- Otherwise, follow the instructions below to ensure that the BIOS is up to date.

You'll need to have a USB-to-Ethernet adapter on hand in order to *apply Qubes updates*, which will enable Wi-Fi and fix glitchy video rendering and cursor performance.

16.3 Lenovo T series laptops

16.3.1 Lenovo ThinkPad T14 (2nd-generation)

The 2nd-generation ThinkPad T14 **with an 11th-generation Intel Core processor** is a recommended option for the SecureDrop Workstation beginning with Qubes 4.1. If you plan to use it:

- If your laptop has come with Ubuntu preinstalled, run its **Software Updater** twice as follows:
  1. to install software updates, especially for the `fwupd` package; and then
  2. to run `fwupd` to update the BIOS automatically.

  If **Software Updater** offers to run `fwupd` during step (1), decline until step (2), to make sure `fwupd` itself has received its latest security updates.
- Otherwise, follow the instructions below to ensure that the BIOS is up to date.

The Ethernet and Wi-Fi controllers may not work without one-time manual configuration, as documented in the following sections.

Ethernet controller

After Qubes starts for the first time, when `sys-net` fails to start, follow the instructions below for the *Lenovo ThinkPad T490 (with 8th-generation Intel Core processor)*, but only for the `dom0:00_1f.6` Ethernet device.

16.3.2 Lenovo ThinkPad T490 (with 8th-generation Intel Core processor)

The ThinkPad T490 **with an 8th-generation Intel Core processor** is a recommended option for the SecureDrop Workstation. If you plan to use it, you should follow the instructions below to ensure that the BIOS is up to date and adequately configured before proceeding with the installation.

Caution

The versions of the T490 with 10th generation Intel Core processors are at present **untested and unsupported**. The Workstation has been tested on models 20N2002AUS & 20N20046US.

16.3.3 Lenovo ThinkPad T480

The ThinkPad T480 is also a recommended option for SecureDrop Workstation, as it is being used by the core team for development and testing. If you plan to use it, you should follow the instructions below to ensure that the BIOS is up to date and adequately configured before proceeding with the installation:

16.4 Upgrading the BIOS on Lenovo ThinkPad laptops

The instructions below assume the use of a Linux-based computer for the creation of a BIOS upgrade USB. To upgrade the BIOS:

- Locate the ThinkPad's "machine type" in its BIOS setup program:
  1. Boot (or reboot) the ThinkPad and follow the prompts to enter setup, usually via the <Enter> and <F1> keys.
  2. On the **Main** tab, look for the **Machine Type Model**. The first four characters, such as *20L5*, *20L6*, or *20S0*, are the machine type.
- Visit https://support.lenovo.com in the Linux-based computer. Type the machine type found above into the search bar, then press **Enter**.

- In the "Product Home" page, select **Drivers And Software** and choose **BIOS/UEFI**.
- Download the file called either **BIOS Update (Bootable CD)** or **BIOS Update (Utility & Bootable CD)**.

Note

A Tails USB can be used for the verification and conversion process described below, but the Lenovo support site blocks requests over Tor, preventing the ISO download. To work around this, either:

- download the BIOS ISO on a different computer and transfer it to Tails using a USB stick, or
- download the ISO in Tails using the Unsafe Browser as follows:
  - Start Tails with an administration password set and the Unsafe Browser enabled under "Additional Settings" on the Welcome Screen.
  - Open the Unsafe Browser: **Applications > Internet > Unsafe Browser** and find and download the ISO
  - Note the filename, as you'll need it for subsequent steps.
  - Leave the Unsafe Browser running, and open a terminal via **Applications > System Tools > Terminal**.
  - Copy the ISO to the desktop with the command:

    ```
    sudo cp /var/lib/unsafe-browser/chroot/home/clearnet/Downloads/<fileName.iso>
    ↪ ~amnesia/Desktop
    ```

  - Fix the ISO file's ownership with the command:

    ```
    sudo chown amnesia:amnesia ~amnesia/Desktop/<fileName.iso>
    ```

- Verify the checksum of the downloaded ISO file using the following command, comparing it against the checksum in the file listing above:

```
sha256sum /path/to/downloaded.iso
```

- Create a USB-bootable version of the ISO using the command:

```
geteltorito <path/to/CDISO> > usb-bios.iso
```

Note

To install the `geleltorito` utility on Debian-based systems, use the command

```
sudo apt install genisoimage
```

To install it on Fedora-based systems, use the command:

```
sudo dnf install geteltorito genisoimage
```

- Plug in a USB and check its device name with the `lsblk` command - use the root device name below, not a partition (eg. `/dev/sdc` instead of `/dev/sdc1`).
- Write the BIOS update ISO to the USB using the following command:

```
sudo dd if=usb-bios.iso of=/dev/sdX bs=1M && sync
```

where `sdX` is the device name verified above.

Caution

The dd command will wipe data on the targeted device. Make sure that you use the correct device name.

Once complete, remove the USB.

- Plug the USB into the ThinkPad.
- Boot the ThinkPad and follow the prompts to enter its startup and boot menus, likely via the <Enter> and <F12> keys, respectively.
- Follow the on-screen instructions to update the BIOS, including any mandatory reboots. Note that the instructions may refer to an update CD instead of your update USB.

16.5 USB-C ports

If you intend to use USB-C ports, please note that our recommended BIOS settings will disable dual USB-C/Thunderbolt ports (recognizable by the Thunderbolt logo next to the port). The T480, for example, includes two USB-C ports, specified as follows:

- 1 x USB 3.1 Gen 1 Type-C (Power Delivery, DisplayPort, Data transfer)
- 1 x USB 3.1 Gen 2 Type-C / Intel Thunderbolt 3 (Power Delivery, DisplayPort, Data transfer)

The first of these ports will continue to function as a USB-C port. After disabling Thunderbolt, the second port can no longer be used for Thunderbolt or for USB-C data transfer, but it can still be used for power delivery (i.e. to plug in your AC adapter). If you are unsure about the features of your laptop's USB-C ports, or if you are using a different make or model, please consult the technical specifications of your laptop for further information.

CHAPTER

SEVENTEEN

KEEPING THE WORKSTATION SECURE

The *SecureDrop Workstation* provides the combined functionality of the Tails-based *Journalist Workstation* and *Secure Viewing Station* (SVS). As such, it contains both a copy of the *Submission Private Key*, and encrypted and decrypted messages and submissions. It's critical to ensure that the same security practices that are used to protect the SVS are applied to the *SecureDrop Workstation* as well.

17.1 Physically secure the workstation

The *SecureDrop Workstation* computer is subject to similar security requirements as the *SVS*, with the additional requirement of a working Internet connection:

- It should be stored in a secure and locked room, with access restricted to users and administrators.
- The room may be monitored externally, but there should be no internal monitoring.
- A wired Internet connection that does not restrict Tor must be available for the workstation. This connection should either be dedicated to *SecureDrop Workstation*, or should be on a fully segregated subnet from the rest of the corporate network.
- Users should not bring other electronic devices into the room, with the exception of smartphones used for 2FA token generation. While in the room, smartphones should be set to airplane mode, and should not be used for any purpose other than 2FA.

17.2 Use strong passphrases

It is recommended to use strong Diceware-generated passphrases for all passwords in the system. The password manager included with current versions of Tails, KeepassXC, includes an option to generate Diceware passphrases, which may make the process easier for end users.

Passwords and other credentials in use by *SecureDrop Workstation* include:

- the Qubes full disk encryption (FDE) password, required to unlock system storage on boot. All users will need this password.
- the Qubes system user password, required to log in. All users will need this password
- *SecureDrop Client* login credentials. These are the same credentials that are used by journalists and administrators to log in to the *Journalist Interface*, and are unique per user.

17.3 Apply updates when prompted

SecureDrop Workstation includes an updater application that runs automatically on startup, checks for Qubes and SecureDrop updates, and prompts the user to apply them if found. Given the sensitive nature of the system, it is critical

that updates are applied when available. Administrators should ensure that users are aware of this requirement, and should periodically check to ensure that the system is up to date.

CHAPTER

EIGHTEEN

MANAGING CLIPBOARD ACCESS

Every VM in Qubes has its own clipboard, similar to the clipboard of a Mac, Windows or Linux computer. For example, if you used the default `work` VM to browse the web and wanted to copy text from one browser window to another, you would use the `Ctrl+C` and `Ctrl+V` keyboard shortcuts to copy and paste. This type of clipboard usage – copy and paste in the same VM – also works in all VMs that are part of SecureDrop Workstation.

In addition, Qubes supports copying information *between* VMs. This is done by using special keyboard shortcuts, `Ctrl+Shift+C` and `Ctrl+Shift+V`, in a four-step process. By default, this is disabled for all VMs that are part of SecureDrop Workstation, consistent with the principle of least privilege.

As an administrator, you should be aware of the following risks related to clipboard access before changing the default configuration:

1. It is dangerous to copy untrusted, unsanitized content *into* a secure environment. What looks like plain text may contain character sequences that exploit security vulnerabilities in the target environment.
2. The four-step process described above can be difficult to follow, and it is easy to make an operational mistake, such as pasting a password into a message to a source, or into a window belonging to a VM with network access.
3. Like any other part of the operating system, the implementation of Qubes clipboard itself may contain undiscovered security vulnerabilities that an adversary could exploit in an attempt to exfiltrate information.

With these considerations in mind, there are use cases where clipboard access may be an important part of your regular use of SecureDrop Workstation. For example:

- You may want to copy passwords from a password manager to the SecureDrop Client;
- You may want to copy a message you received via SecureDrop into a secure messaging app like Signal, to share it with another journalist.

To support these use cases, SecureDrop Workstation allows you to grant granular access to the `sd-app` clipboard (via the cross-VM clipboard) to selected VMs.

18.1 Configuring clipboard access to `sd-app`

The process for permitting the one-directional copying of passwords from a password manager in `vault` to the SecureDrop Client is *outlined in the installation docs*. In general, clipboard access to SecureDrop Workstation VMs is governed by *tags* that can be applied in `dom0` to selected VMs:

- the tag `sd-send-app-clipboard` can be used to tag a VM that should be able to send its clipboard contents *to* `sd-app` via the cross-VM clipboard;
- the tag `sd-receive-app-clipboard` can be used to tag a VM that should be able to receive its clipboard contents *from* `sd-app` via the cross-VM clipboard.

You can configure these tags for a given VM from the `dom0` terminal. Changes to tags take effect immediately, and any VM can have multiple tags.

Important

Make sure you fully understand technical and operational security risks before permitting clipboard access to any VM. The "send" and "receive" tags are separate so you can set up only the clipboard direction you need to support a given use case.

We recommend adding a note about any changes to the clipboard configuration to your internal documentation for SecureDrop. If you are unsure how to configure the clipboard to support a specific use case, please do not hesitate to contact us for assistance.

The general syntax for adding a tag is as follows, substituting `<VM name>` with the name of an existing VM in the system you want to grant access to the clipboard:

```
qvm-tags <VM name> add <tag name>
```

Confirm that the command was successfully applied using the `ls` subcommand:

```
qvm-tags <VM name> ls
```

The syntax for revoking a tag is as follows:

```
qvm-tags <VM name> del <tag name>
```

As before, confirm the operation via the `ls` subcommand.

As an example, if you had a custom VM called `work-signal` that runs the Signal messenger, and you wanted to copy and paste messages from the SecureDrop Client *into* Signal (and potentially other applications in that VM) but not *out* of Signal into the SecureDrop Client, you would issue the following commands:

```
qvm-tags work-signal add sd-receive-app-clipboard
qvm-tags work-signal ls
```

To review current clipboard permissions, you can use `qvm-ls` to print out a list of VMs that can receive or send clipboard contents:

```
qvm-ls --tags sd-receive-app-clipboard
qvm-ls --tags sd-send-app-clipboard
```

CHAPTER

NINETEEN

REVIEWING AND EXPORTING LOGS

SecureDrop Workstation aggregates system logs from all its VMs in the `sd-log` VM, in the folder `~/QubesIncomingLogs`, with one subfolder for each VM. You can inspect these logs directly in the `sd-log` VM, or you can copy them to another VM, e.g., for purposes of sharing logs with the SecureDrop development team.

Please note that while the logs do not include original filenames or message contents, they do contain sensitive information, e.g.:

- timing and usage information related to SecureDrop access
- the two-word designation for a given source
- metadata about submissions and replies
- error messages that disclose further details

For this reason, the `sd-log` VM is networkless, and you cannot copy files from `sd-log` to other VMs by default.

If you want to selectively enable copying logs to a single VM, you can use tags, similar to the method used for *managing clipboard access*. You can add and remove the permission just before each copying operation; the change will take effect immediately.

Important

Before copying logs to a networked VM, inspect them for sensitive information, and redact them as warranted.

To enable copying logs to a target VM, you can use a command like the following in `dom0`, substituting `<VM name>` with the name of the target VM (e.g., `work`):

```
qvm-tags <VM name> add sd-receive-logs
```

Verify that the tag was successfully applied using the `ls` subcommand:

```
qvm-tags <VM name> ls
```

To remove the permission, use this command in `dom0`:

```
qvm-tags <VM name> del sd-receive-logs
```

With the permission in effect, you can use the command `qvm-copy` in a terminal in `sd-log` to copy individual files to the target VM. For example, to copy a file `syslog-redacted.log`, you would use this command:

```
qvm-copy syslog-redacted.log
```

A graphical prompt will permit you to select any target VM that has the `sd-receive-logs` tag. Once successfully copied, the file can be found in the directory `~/QubesIncoming/sd-log` in the target VM. See the Qubes OS documentation on copying files for more information.

To review current copy permissions, you can use `qvm-ls` to print out a list of VMs that can receive files from `sd-log`:

```
qvm-ls --tags sd-receive-logs
```

CHAPTER

TWENTY

TROUBLESHOOTING CONNECTION PROBLEMS

Before troubleshooting connection problems, we recommend reading about the *networking architecture* of SecureDrop Workstation. If you are in a hurry, this guide offers quick diagnostic and remedial steps.

20.1 Step 1: Verify you are connected to the Internet

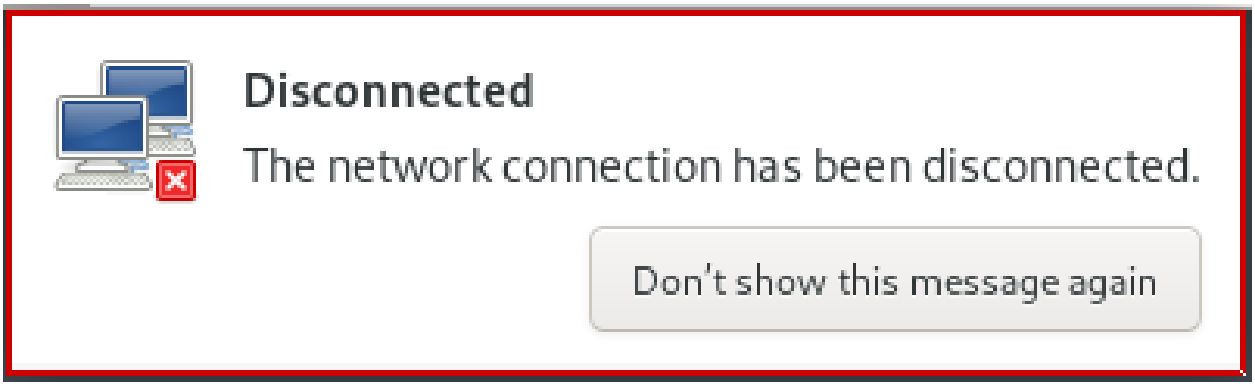
You can use both wireless and wired networks in Qubes. You can manage network access through the network manager, which you can find in the area populated with icons in the top right corner of your Qubes desktop, known as the *system tray*.

The network manager is the red icon, which looks like this for a wired connection (ordering of icons may vary):

It looks like this for a wireless connection:

It looks like this when you are not connected to the Internet at all:

When a network connection is lost, Qubes will display an alert like the following:

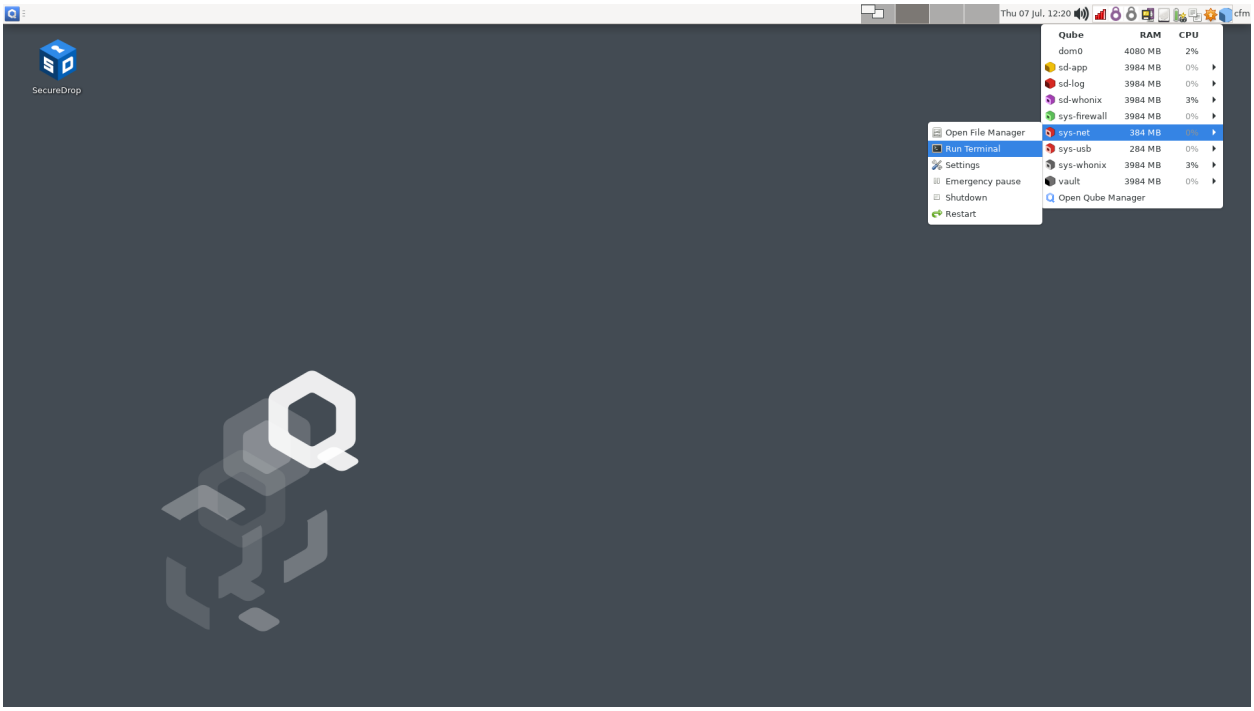


Common causes for lost connections include fully or partly unplugged network cables, lost power to networking equipment, and ISP service outages. When you see a lost connection notification, it is most likely due to one of these causes.

Important

Not all VMs in Qubes OS have Internet access. For example, opening a terminal via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal** opens a `dom0` terminal without Internet access. See our *networking architecture* overview for additional background.

If the network manager shows that you are connected to the Internet, you can verify whether your connection is working by opening a terminal in `sys-net`:



1. Click the "Q" icon in the in the system tray (top right area).
2. A list of running VMs should appear. Select `sys-net` from the list, and click **Run Terminal**.
3. In the terminal window, type the command `ping -c 5 google.com`.

You should see a sequence of lines starting with `64 bytes from` and ending with the number of milliseconds it took to complete the request. If you do not see similar output, your network access may be misconfigured, or the Internet may be wholly or partially unreachable. If using `8.8.8.8` instead of `google.com` works, it may suggest a problem at the DNS level in your network configuration.

If you have verified that you are able to connect to the Internet using `sys-net`, but you are experiencing other connectivity issues, move on to the next step.

20.2 Step 2: Troubleshooting login issues

Issues logging in may not be network-related. If you are experiencing connectivity issues before or after logging in, you can skip ahead to the next section.

Make sure that your username, passphrase, and two-factor code are correct.

Important

After a failed login, wait for a new two-factor code from your app before trying again.

You can reveal the passphrase by clicking the "eye" icon next to it in the login dialog (ensure you are in a fully private setting before doing so). Check for extra characters and end, or subtle differences like capitalization. Note that the spaces between words in SecureDrop passphrases are part of the passphrase.

If you use the two-factor app on your phone for other websites and services, make sure that you have selected the correct user account. It should be labeled **SecureDrop**.

If you have access to a Tails-based *Journalist Workstation*, verify whether you can access SecureDrop from Tails.

If you are certain that your credentials are correct but you are unable to log in, proceed to the next step.

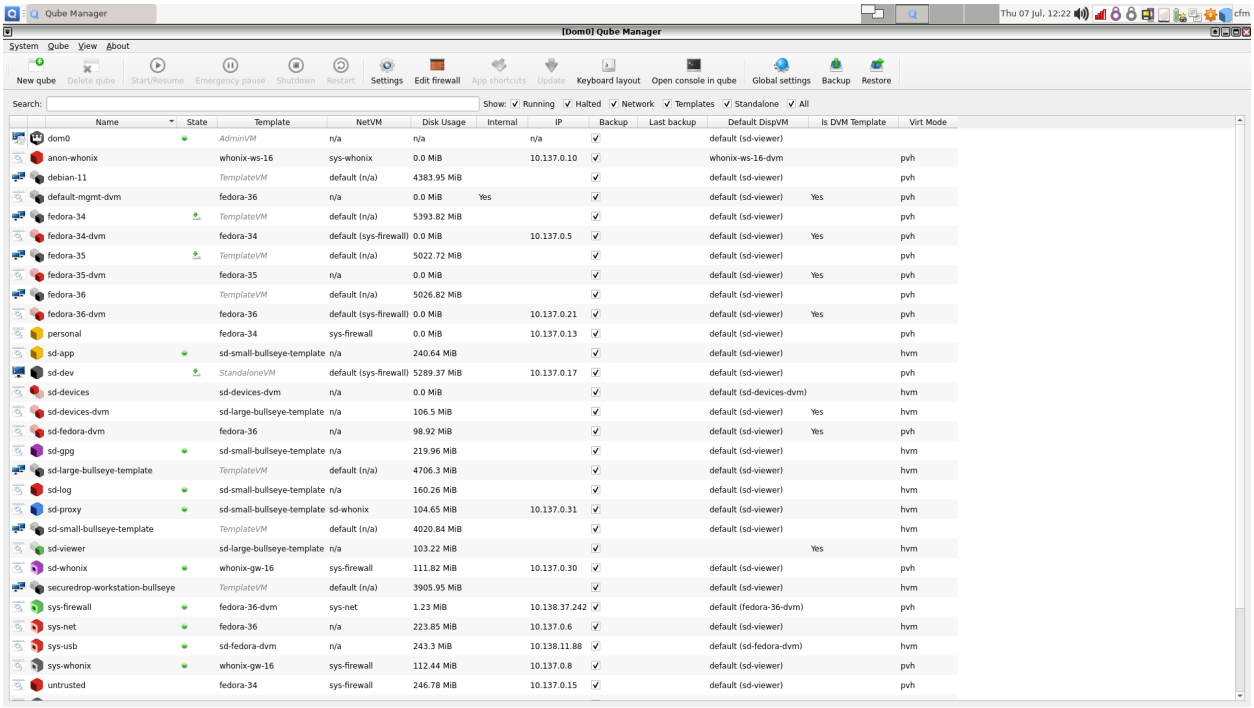
20.3 Step 3: Verify that all required VMs are running

The following VMs must be running for all actions requiring network connectivity to work (e.g., logging in, checking for messages, downloading documents, replying to sources, starring sources, deleting sources):

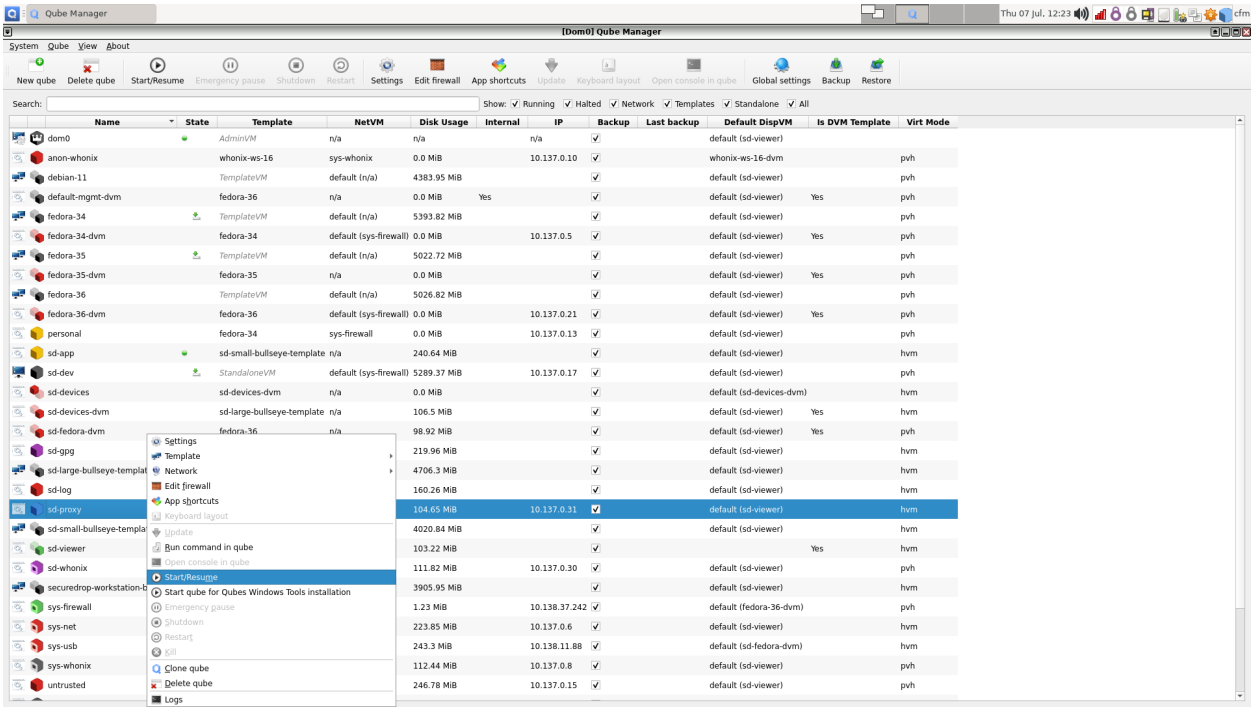
- `sd-app`
- `sd-gpg`
- `sd-log`
- `sd-proxy`
- `sd-whonix`
- `sys-firewall`
- `sys-net`
- `sys-whonix` (during updates)

You can verify whether a VM is running or not by clicking the "Q" icon in the system tray (top right). Only VMs that are currently running will appear in the list:

If a required VM is not running, you can launch it from the Qube Manager. Open the Qube Manager by clicking **Open Qube Manager** in the menu above. A window like the following should appear:



To start a VM, select it from the list, right-click it, and click **Start/Resume Qube**. Alternatively, you can click the "Play" button in the toolbar.



In ordinary use, VMs required by SecureDrop should be started on boot or when they are needed. If you repeatedly experience problems with a necessary VM not running, or if an error message is displayed when attempting to start the VM, please contact us for assistance.

If all required VMs are running, proceed to the next step.

20.4 Step 4: Verify that required VMs have connectivity

In step 1, you have already verified that you can connect to the Internet using `sys-net`. Now, test whether `sys-firewall`, `sd-whonix` and `sd-proxy` are working.

First, open a terminal in `sys-firewall` and run the `ping google.com` command. You should see similar output as in `sys-net` before.

Now, open a terminal in `sd-whonix` and run the following command:

```
wget -qO- https://check.torproject.org/ | cat | grep -m 1 "Congratulations"
```

This command contacts a service intended for web browsers to verify whether your Tor connection is working.

You should see the text “Congratulations. This browser is configured to use Tor.” or a similar message on the terminal.

If the output does not include the text “Congratulations”, keep the terminal window open and proceed to the next steps.

If the command does include the expected text in `sd-whonix`, also run it in `sd-proxy`. If it only fails in `sd-proxy`, your workstation may be misconfigured, or the proxy may have crashed. In that case, skip ahead to step 6. We also recommend that you contact us, so we can help identify the root cause.

20.5 Step 5: Restart Tor

If you have narrowed down the problem to `sd-whonix`, try restarting Tor. You can do this from within the `sd-whonix` terminal using the following command:

```
sudo systemctl restart tor
```

If this does not resolve the issue, proceed to the next step.

20.6 Step 6: Restart sd-proxy and sd-whonix

Restart `sd-proxy` and `sd-whonix` to attempt to restore connectivity:

1. Exit the SecureDrop app if it is running.
2. Click the "Q" icon in the system tray (top right).
3. Click **Run Qube Manager**
4. Right-click `sd-proxy` in the list of VMs. Click **Shutdown qube**.
5. Right-click `sd-whonix` in the list of VMs. Click **Shutdown qube**.
6. Right-click `sd-proxy` in the list of VMs. Click **Start/Resume qube**. The `sd-whonix` VM should start automatically.

If this does not resolve the issue, proceed to the next step.

20.7 Step 7: Restart sys-net and sys-firewall

Note

You will temporarily lose all Internet connectivity in Qubes OS during this step.

Using the same procedure as in the previous step, shut down `sd-proxy`, `sd-whonix` and `sys-whonix` (in this order). Attempt to shut down `sys-firewall`. You may see an error message telling you that other VMs still require access to `sys-firewall`. Save your work in those VMs, shut them down, and attempt to shut down `sys-firewall` again.

Finally, shut down `sys-net`. The network manager icon should disappear.

Now, start `sys-whonix`, which will bring up `sys-net` and `sys-firewall` at the same time. Start `sd-proxy`, which will bring up `sd-whonix`.

If this does not resolve the issue, please contact us for assistance.

20.8 Customizing Synchronization Timeouts

The SecureDrop Workstation Client application performs a synchronization on launch, which may time out in situations where there are a large number of sources on the server. To the extent possible, we recommend regularly removing sources that are no longer actively engaging with you, or any sources that appear to be spam.

If you are able to login to the Client application, but sources are not appearing, you may be reaching a timeout for the synchronization process. To temporarily increase the timeout, and give the system more time to finish synchronizing with the server, you can perform the following steps:

1. Log into the Qubes workstation
2. Start a system Terminal in `dom0` via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal**
3. Run the following commands:

```
qvm-service --enable sd-app SDEXTENDEDTIMEOUT_600
qvm-shutdown sd-app && sleep 5 && qvm-start sd-app
```

4. Start the SecureDrop Client application, like normal

These instructions will change the sync timeout to 10 minutes. If the sync fails to complete in that time, repeat the instructions, replacing the "600" with a larger value. We recommend increasing the number in increments of 100, and checking after each change to find the best value.

Once the synchronization has completed and the sources have loaded, we advise going through and removing any unnecessary sources.

20.9 Examining logs

You may wish to examine system logs on your own, or with our guidance. You can examine consolidated syslogs from all SecureDrop-related VMs in the `sd-log` VM. They can be found in the default user's `~/QubesIncomingLogs` directory.

In addition, you may want to examine `/var/log/syslog` in `sys-net` and `sys-firewall`.

CHAPTER

TWENTYONE

TROUBLESHOOTING SYSTEM UPDATES

After you log into Qubes, the SecureDrop Workstation preflight updater will prompt you to check for available system updates at least once per day.

If updates fail for any reason, the preflight updater will not launch the SecureDrop Client application until the underlying issue has been resolved. This is to ensure that the system is in a secure state before you interact with SecureDrop.

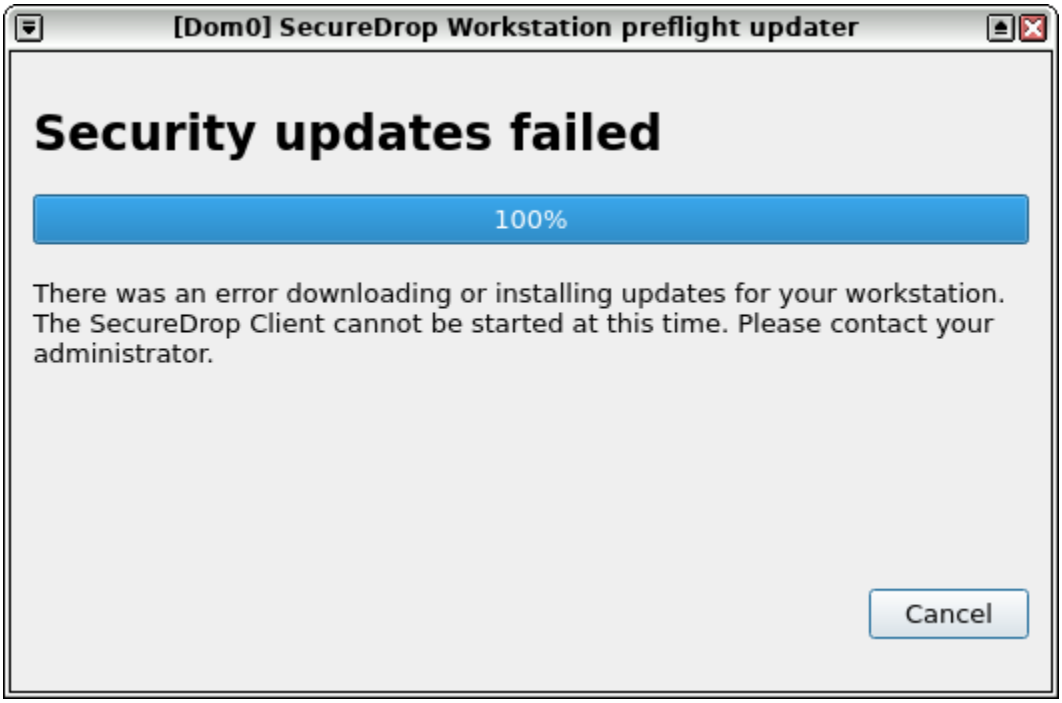


Fig. 1: The error displayed when the preflight updater does not successfully complete the update.

This guide offers troubleshooting steps for common update issues.

21.1 Step 1: Locate the updater log

The preflight updater runs in the `dom0` domain. It writes its log to `~/.securedrop_updater/logs/updater.log`. Log files are rotated hourly; if you have started the updater again since the error occurred, you may need to check the previous log file.

In order to examine the most recent log file:

1. Open a terminal in `dom0` via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal**.

2. Change to the `~/.securedrop_updater/logs/` directory:

   ```
   cd ~/.securedrop_updater/logs/
   ```

3. Display the most recent log file:

   ```
   cat updater.log
   ```

In order to locate a previous log file in the same directory:

1. Locate the most recently modified log file.

   ```
   ls -t updater.log* | head -n 2
   ```

2. Display the file that ends with a date and time stamp, e.g.:

   ```
   cat updater.log.2023-01-01_10
   ```

21.2 Step 2: Identify the cause(s) of the error

If the updater has run to completion, you should see a result line in the log file that looks similar to the following:

```
2023-03-30 20:12:11,821 - sd.sdw_updater_gui.UpdaterApp:71(upgrade_status)
INFO: Signal: upgrade_status {
'dom0': <UpdateStatus.UPDATES_OK: '0'>,
'apply_dom0': <UpdateStatus.UPDATES_OK: '0'>,
'fedora-40': <UpdateStatus.UPDATES_OK: '0'>,
'sd-large-bullseye-template': <UpdateStatus.UPDATES_OK: '0'>,
'whonix-gateway-17': <UpdateStatus.UPDATES_FAILED: '3'>,
'sd-small-bullseye-template': <UpdateStatus.UPDATES_OK: '0'>,
'recommended_action': <UpdateStatus.UPDATES_FAILED: '3'>}
```

In this example, the `whonix-gateway-17` VM has failed to update. This is indicated by the text `<UpdateStatus.UPDATES_FAILED: '3'>`.

It is possible that multiple steps have failed. Make note of any of the individual steps that have failed, other than `recommended_action`.

21.3 Step 3: Resolve the issue(s)

The resolution path will depend on which step(s) failed. Note that `dom0` and `apply_dom0` are separate steps.

21.3.1 `dom0` update failures

1. Open a terminal in `dom0` via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal**.
2. Perform an interactive `dom0` update by running the following command:

   ```
   sudo qubes-dom0-update
   ```

3. Follow the prompts to resolve any issues. If you are unsure on how to resolve an error, please contact us for assistance.
4. Reboot the system. `dom0` updates are often security-sensitive, and may require a reboot to take effect.

21.3.2 Expired SecureDrop Signing Key

If the update fails after running `sudo qubes-dom0-update` as described above, and the terminal console displays the following message:

```
1. Certificiate 188EDD3B7B22E6A3 invalid: certificate is not alive
    because: The primary key is not live
    because: Expired on 2023-07-04T10:52:20Z
2. Key 188EDD3B7B22E6A3 invalid: key is not alive
    because: The primary key is not live
    because: Expired on 2023-07-04T10:52:20Z
[...]
Error: GPG check FAILED
```

your system is trying to use an old copy of the SecureDrop Release Signing Key. The new, valid key will already be locally available on your system, so you can perform the following steps to remove the expired key and enable this updated key:

1. Open a terminal in `dom0` via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal**.
2. Run the following command:

   ```
   sudo rpm -q gpg-pubkey --qf '%{NAME}-%{VERSION}-%{RELEASE}\t%{SUMMARY}\n' | grep␣
   ↪SecureDrop
   ```

   The output should look similar to:

   ```
   gpg-pubkey-xxxxx-xxxxx        SecureDrop Release Signing Key <securedrop-release-
   ↪key-2021@freedom.press  public key
   ```

3. Make note of the KEY ID (in the format `gpg-pubkey-xxxxx-xxxxx`).
4. Run the following commands:

   ```
   sudo rpm -e gpg-pubkey-xxxxxx-xxxxxx # use KEY ID from step 3

   sudo rpm --import /etc/pki/rpm-GPG/RPM-GPG-KEY-securedrop-workstation
   ```

5. Reboot, then run updates again. If there are new errors, repeat the full troubleshooting process.

21.3.3 `sd-*-template` or `whonix-gateway-17` update failures

1. Click the Qubes menu and open a terminal in the impacted template. For example, if `whonix-gateway-17` failed to update, select its entry in the Qubes menu and click **Terminal**. (Be sure not to confuse it with the similarly named `whonix-workstation-17` template.)
2. Perform an interactive template update by running the the following commands:

   `sudo apt update`

   `sudo apt upgrade`

   The SecureDrop and Whonix templates are based on Debian GNU/Linux. The `apt update` comand will ensure the package index is up-to-date, and the `apt upgrade` comand will apply updates.
3. Follow the prompts to resolve any issues. If you are unsure on how to resolve an error, please contact us for assistance.

21.3.4 `fedora-40` update failures

1. Click the Qubes menu and open a terminal in the `fedora-40` template.
2. Perform an interactive template update by running the following command:

   ```
   sudo dnf update
   ```

3. Follow the prompts to resolve any issues. If you are unsure on how to resolve an error, please contact us or assistance.

21.3.5 `apply_dom0` update failures

The `apply_dom0` step applies any necessary configuration changes to the SecureDrop Workstation. If this step fails, this may indicate a misconfiguration, or it could be a result of download failures during the operation.

We recommend first re-running the updater by double-clicking the SecureDrop desktop icon. This may resolve transient network issues.

If this does not resolve the issue:

1. Locate the `updater-detail.log` file in the same directory as the `updater.log` file. This file contains more detailed information about the `apply_dom0` step.

   Like the `updater.log` file, this file is rotated hourly.

2. Copy this file to a networked VM by using the `qvm-copy-to-vm` command. For example, to copy the file to the `work` VM:

   ```
   qvm-copy-to-vm work ~/.securedrop_updater/logs/updater-detail.log
   ```

3. The file can now be found in `~/QubesIncoming/dom0/` in the `work` VM.

   Send us the file through a secure channel, such as our support portal. We will provide further instructions.

21.4 Step 4: Restart the updater

Click the SecureDrop desktop icon to restart the updater. If all issues have been resolved, the updater should run to completion and display a success message. If the issue persists, please contact us for assistance.

CHAPTER

TWENTYTWO

PROVISIONING EXPORT USB DEVICES

SecureDrop Workstation supports the export of submissions from the Qubes client to a LUKS- or VeraCrypt-encrypted USB *Export Device*.

22.1 Creating a LUKS-encrypted drive

Note

LUKS-encrypted devices can only be used with Linux-based systems such as Tails. For compatibility with macOS and Windows systems, use VeraCrypt.

In order to provision a LUKS-encrypted *Export Device* for use with SecureDrop Workstation, you will need a fresh USB stick and a Linux-based system. Tails is recommended - if available, the *Secure Viewing Station* can be used, adding the extra benefit of its airgap:

- First, boot into the *Secure Viewing Station*, without unlocking its persistent volume or setting an admin password.
- Next, open the Disks utility: **Applications > Utilities > Disks**.
- Connect the fresh USB stick and select it in the list in the left-hand panel.

Warning

The formatting operation will wipe any data on an existing partition. Make sure that you select the correct device!

- Click the interlocking gear icon under the drive volumes schematic in the right-hand panel and choose **Format Partition…**.
- Select the following options in the Format Volume dialog:
  - Volume Name: Transfer
  - Type: Ext4, with the "Password protect volume (LUKS)" option enabled
- Then, click **Next**. You will be prompted to set a password. This password should be strong - a 6-word Diceware passphrase is highly recommended.
- Once the password is set, click **Format**, then when prompted, click **Format** again. The formatting process should take only a few seconds.
- Once formatting is complete, you will need to provide the *Export Device* and its decryption password to the SecureDrop Workstation users. Make sure that they store it and its password securely, as it will contain decrypted submissions.

22.2 Creating a VeraCrypt-encrypted drive

- If it isn't already done, download and install the VeraCrypt software.
- Start VeraCrypt from your computer's application or software interface.
- Click **Create Volume**
- Select **Encrypt a non-system partition/drive** and click **Next**.
- Select **Standard VeraCrypt volume** and click **Next**
- Connect your fresh USB stick and click **Select Device...** to choose your USB.
  - You may see a warning that says "We strongly recommend that inexperienced users create a VeraCrypt file container on the selected device/partition, instead of attempting to encrypt the entire device/partition." We disagree with this recommendation, so click **Yes**.
  - Click **Next** to advance.

Warning

The formatting operation will wipe any data on an existing partition. Make sure that you select the correct device!

- You will be prompted to set a password. This password should be strong - a 6-word Diceware passphrase is highly recommended.
- You will be asked if you need to store large files, select **No** and click **Next**.
- Select the following options in the Volume Format dialog:
  - Filesystem: FAT
  - Quick Format: unselected
- Click **Next**. VeraCrypt will now collect entropy from your mouse movements. Randomly move your mouse cursor around the screen until the progress bar is filled up. Then click **Format**.
  - You will be reminded that all files on the device will be erased and lost and given a final confirmation to begin. Click **Yes**.
- Wait until VeraCrypt says "The VeraCrypt volume has been successfully created." Until this pops up, it may look like the program is frozen, but it's running in the background.
- Click **OK** and then **Exit** to finish formatting process.
- Once formatting is complete, you will need to provide the *Export Device* and its decryption password to the SecureDrop Workstation users. Make sure that they store it and its password securely, as it will contain decrypted submissions.

CHAPTER

TWENTYTHREE

BACKUP AND RESTORE

Qubes OS has a backup utility that allows for backup and restoration of user-specified VMs and templates.

SecureDrop Workstation requires only that you back up instance-specific secrets and configuration files, although you can optionally back up some additional local data.

To perform backups, you will need:

- a LUKS-encrypted USB or LUKS-encrypted external hard drive (of sufficient size, if backing up additional local data)
- a secure place to store backup credentials (such as a password manager on your primary laptop)

23.1 Backup

23.1.1 Preserve files from `dom0` and `sd-gpg`

Preserve configuration files and private key material by copying them into `dom0`.

In a `dom0` Terminal via **Q > Gear Icon (left-hand side) > Other Tools > Xfce Terminal**:

```
qvm-run --pass-io sd-gpg 'gpg -a --export-secret-keys' > sd-keys.asc
sudo mv sd-keys.asc /usr/share/securedrop-workstation-dom0-config/
cp -r /usr/share/securedrop-workstation-dom0-config ~
```

If you have made customizations to `dom0` (for example, custom RPC policy files):

```
mkdir ~/etc-qubes && cp -r /etc/qubes ~/etc-qubes
mkdir ~/etc-qubes-rpc && cp -r /etc/qubes-rpc ~/etc-qubes-rpc
```

23.1.2 Back up SecureDrop Workstation

Note

Backups contain sensitive data, and must be created and stored just as securely as SecureDrop Workstation itself.

If performing this backup as part of a migration (from one machine to another or from one version of Qubes OS to another), we suggest you retain the backup only during the migration process, and destroy it after the migration is complete. The easiest way to do this is to create a LUKS-encrypted drive, follow this guide to create your backup, and then wipe (reformat) or destroy the drive after you have successfully restored it onto the new machine, which should ideally happen the same day. In all cases, follow your organization's internal policies on handling sensitive assets and information.

If you are looking to back up your own customized components of SecureDrop Workstation for long-term storage, we suggest taking that backup separately from the backup of SecureDrop Workstation components so that you can avoid proliferating copies of sensitive assets.

Before starting your backup, decide whether you want to back up your data from `sd-app`. If you skip this step, the first time you log in, your submissions will re-download from your SecureDrop server.

Ensure your storage medium is plugged in, attached to `sd-devices`, and unlocked.

Navigate to **Q > Gear Icon (left-hand side) > Qubes Tools > Backup Qubes**, and move all VMs from "Selected" to "Available" by pressing the << button.

To target a VM for backup, highlight it and move it into the "Selected" column by pressing the > button. Select:

- `dom0`
- the `sd-app` VM (optional), noting the warning above
- any customized VMs (and their templates) that you may wish to preserve, noting the warning above.

You do not need to back up the other `sd-` VMs.

Click "Next", and in "Backup destination," specify the VM and directory corresponding to your storage medium's current mount point.

Set a strong, unique backup passphrase (7-word diceware), and ensure this passphrase is stored securely outside SecureDrop Workstation.

Note

This passphrase protects sensitive components of your SecureDrop instance, including the *Submission Private Key*, and unencrypted submissions (if `sd-app` is backed up). Ensure it is a very strong password and is stored securely.

Uncheck "save backup profile," then proceed with the backup.

Qubes OS recommends verifying the integrity of the backup once the backup completes, and this should be done on the same machine where the backup was created. This can be done by using the Restore Backup GUI tool and selecting "Verify backup integrity, but do not restore the data." For details, see the Qubes OS backup documentation.

Warning

Any files or data not mentioned above and not backed up elsewhere will be destroyed. Ensure that any other data on your system (for example, using KeepassXC in the `vault` VM, or data stored in other VMs) have been backed up and the integrity of the backup has been verified before proceeding.

23.2 Restore

23.2.1 Reinstall Qubes OS

To restore SecureDrop Workstation, follow our *pre-install tasks* to provision a Qubes OS system complete with updated base templates.

23.2.2 Rename or delete redundant AppVMs

By default, Qubes OS will create the AppVMs `personal`, `work`, `untrusted` and `vault` as part of the installation process. Rename or delete any of these newly created AppVMs whose names conflict with the AppVMs you intend to restore from a backup.

Example: If you wish to restore the `vault` VM, rename or delete the existing `vault` VM prior to restoring the backup. You can do so in **Q > Apps > vault > Settings** (the VM must not be running).

23.2.3 Restore Backup (SecureDrop Workstation components)

Plug in your backup medium and unlock it as during the backup. By default on a new system, your peripheral devices will be managed by a VM called `sys-usb`.

Navigate to **Q > Gear Icon (left-hand side) > Qubes Tools > Restore Backup**, and enter the location of the backup file. You do not need to adjust the default Restore options, unless you have made customizations to the backup. Enter the decryption/verification passphrase, and proceed to restoring the available qubes (which should include `dom0` and possibly `sd-app`).

We suggest restoring only those VMs, provisioning SecureDrop Workstation, and then restoring any customized VMs you may have had once that process is complete. This way SecureDrop Workstation is provisioned on a clean system and can implement the security measures it requires before any additional VMs are configured.

Note

When migrating to a newer version of Qubes OS (for example, Qubes 4.1 to Qubes 4.2), you may notice that the original templates for certain VMs are not present on your new machine. For the purposes of this guide (optional `sd-app` backup), this is not a problem. Allow the VM to be restored with the default template suggested by the operating system (the current Fedora base template). **Do not start the VM.** Continue through the reinstallation process. The correct template will be configured as you follow the rest of these instructions.

If you are restoring your own customized VMs and templates, you will need to take additional steps. You may decide to create new templates for your custom VMs and provision them with the necessary applications/customizations (recommended), or you may upgrade your existing templates following the upstream documentation (Fedora templates, Debian templates), then upgrade their package repositories to the Qubes 4.2 repositories using:

```
sudo qubes-dom0-update -y qubes-dist-upgrade
qubes-dist-upgrade --template-standalone --upgrade
```

More information can be found in the upstream documentation. Contact Support with any questions.

23.2.4 Reinstall SecureDrop Workstation

If you do not already have a `work` VM, create it with default networking settings:

```
qvm-create -l blue work
```

Then, *download and verify* the SecureDrop Workstation .rpm to the `work` VM and copy it to `dom0`.

Once you have a valid .rpm file in `dom0`, install the .rpm by running:

```
sudo dnf install securedrop-workstation.rpm
```

Retrieve the previous SecureDrop Workstation configuration from the backup folder on `dom0`. From the `dom0` home directory:

```
ls -d */*/* | grep home-restore
```

You should see a directory called `home-restore-$YYYY-MM-DD-HHMMSS/dom0-home/$USERNAME`. We will call this `$RESTORE_DIR` in the instructions below.

```
sudo cp ~/$RESTORE_DIR/securedrop-workstation-dom0-config/{sd-journalist.sec,
↪config.json,sd-keys.asc} /usr/share/securedrop-workstation-dom0-config/
```

Optionally, inspect each file before proceeding. The first file should be an ASCII-armored GPG private key file. The second file should follow the format of the example configuration file, with values for its fields (e.g., `hostname`, `submission_key_fpr`) specific to your configuration. The file may be formatted in a single line without whitespace. The third file is a backup of key material from `sd-gpg` and will be moved into that VM when you have reprovisioned the system.

Verify that the configuration is valid:

```
sdw-admin --validate
```

If the above command prints `OK`, the configuration is valid.

Reinstall SecureDrop Workstation:

```
sdw-admin --apply
```

23.2.5 Restore additional keys to sd-gpg

In a `dom0` terminal:

```
qvm-copy-to-vm sd-gpg $RESTORE_DIR/securedrop-workstation-dom0-config/sd-keys.
↪asc
qvm-run sd-gpg 'gpg --import /home/user/QubesIncoming/dom0/sd-keys.asc'
```

23.2.6 Restore Customized VMs, RPC Policies

At this stage, you should have a functional SecureDrop Workstation. You may restore any additional customizations or additional VMs, being mindful that you are responsible for the security implications of customizing this system.

Customizations in `dom0` must be restored manually, meaning that any RPC policies you have added will need to be moved into place from the `$RESTORE_DIR`.

Once you are finished with the `$RESTORE_DIR` and have verified that your system works (download, decrypt, sync), you may delete the `$RESTORE_DIR`.

23.2.7 (Post-Migration Instructions) Destroy backup medium

Wipe (reformat) the LUKS-encrypted storage device that you used to store SecureDrop Workstation configuration material, overwriting the LUKS header and all data with a new encrypted partition, or physically destroy the backup medium, to ensure you are not proliferating copies of sensitive data.

- genindex
- search