SecureDrop Workstation Documentation

Release 0.0.1

SecureDrop

Jul 22, 2020
Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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.
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 pilot 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.

For more information on SecureDrop Workstation, see our FAQ.
Starting Qubes

Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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.
Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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.
3.1 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.

3.2 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.

3.2.1 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.
3.3 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.

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 4

Communicating with sources

Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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 consisting of three panels. The small panel on the left shows your username, if you are logged in, or the sign-in button.
The source list in the middle panel shows sources that have submitted to your instance. Each source is identified to you with a two word pseudonym.

In the righthand panel, the conversation view allows you to see your conversation history with a particular source.

4.1 Opening a conversation

Clicking on a source will display their messages to you in the conversation view. Replies that you or anyone from your organization has sent will also appear in the conversation flow.

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.

4.2 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.

4.3 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.
4.3.1 Sources without reply keys

You may sometimes see the text “Awaiting encryption key from server” in a grayed out reply box for a source. This typically happens in the following situations:

- A source has just contacted your SecureDrop moments ago, and the server has not created an encryption key yet. If you are logged in, the key will be automatically fetched as soon as it becomes available, usually within a few seconds. At that point, the reply box will become available.

- Your SecureDrop server is experiencing a surge of traffic, and the generation of encryption keys has been temporarily disabled. You have to manually flag the source for reply, and the source has to log in again before you can respond. This cannot currently be done from the SecureDrop Client.

4.4 Deleting a conversation

You can delete a source conversation by clicking on the three dots at the top righthand side of the application window, beside the timestamp, and clicking “Delete source account”.

**Important:** Deleting a source conversation deletes the conversation for everyone at your organization, and also prevents the source from logging in again using their current codename.
Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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.”
5.1 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.
5.2 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.

### 5.3 Printing

To print a document, click the **Print** button. Currently, printing is only supported with select printers from Brother and HP, 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.

### 5.4 Exporting to an Export USB

Currently, a LUKS-encrypted USB drive is required for exporting submissions. A Linux-based system such as Tails is required to configure and use a LUKS-encrypted drive, meaning that for the time being, you will only be able to export to a Linux environment where these drives can be read. For assistance with this, see your SecureDrop administrator.

Once you have provisioned a LUKS-encrypted export drive, insert the drive and click **Export**.

You will be prompted for the password configured for this USB drive.
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.
Ending your session

**Warning:** SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our [blog post](#) for more information.

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.
7.1 Frequently Asked Questions

7.1.1 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.

7.1.2 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.

### 7.1.3 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.

### 7.1.4 Can I install custom software on SecureDrop Workstation?

Right now, the pilot 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.

### 7.1.5 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.

### 7.1.6 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.

### 7.1.7 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.
Recommended hardware

Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

8.1 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 16GB RAM (32GB recommended for production use)
- sufficient disk space for the Qubes OS base install and SecureDrop Workstation VMs (a 128GB or greater SSD is recommended)

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. Supported models currently include:

- Brother HL-L2320D
- HP LaserJet Pro M404n

More printer options will be added in future releases.

8.2 Lenovo ThinkPad T480

The ThinkPad T480 is 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 before proceeding with the installation:
8.2.1 Upgrading the T480 BIOS

The instructions below assume the use of a Linux-based computer for the creation of a BIOS upgrade USB. To upgrade the T480 BIOS:

- Locate the machine type of the T480 - it be found via the Main tab in Thinkpad Setup (accessed by pressing Enter on startup). For recent T480s, it will be a string like 20L5 or 20L6.
- 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 T480 Product Home page, select Drivers And Software and choose BIOS/UEFI.
- Expand the BIOS Update listing and download the BIOS Update (Bootable CD) file.

**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 geelortorito 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 T480 and boot it, pressing **F12** on startup. Select the USB’s listing in the boot menu.

• 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.

### 8.2.2 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 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.
9.1 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:

9.1.1 Pre-install tasks:

1. Verify the SecureDrop server configuration
2. Apply BIOS updates and check settings
3. Download and verify Qubes OS
4. Install Qubes OS
5. Apply updates to system templates
6. Install Fedora 31 base template

9.1.2 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

9.2 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 6th-gen T480 and X1 models - 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.

9.3 Pre-install tasks

9.3.1 Verify the SecureDrop server configuration

In order to be used with SecureDrop Workstation, your instance must be running the latest version of SecureDrop, and the server configuration must have been updated to allow for HTTP DELETE requests. The configuration change to enable this was added in the 0.13.0 version of SecureDrop, released on May 29 2019. If your instance was created using this or a later version, it has the necessary changes. If not, then the ./securedrop-admin install command must have been run from an Admin Workstation updated with the 0.13.0 code or later. To check this:

- Use an Admin Workstation USB to boot into Tails, with the persistent volume unlocked and an administration password set.
- Navigate to Applications System Tools Terminal to open a terminal.
• Verify that the Journalist Interface Apache configuration allows for HTTP DELETE using the following command:

```
ssh app "grep '^\s<LimitExcept GET POST HEAD DELETE>$' /etc/apache2/sites-enabled/journalist.conf"
```

• If your instance is configured correctly, this command will output two lines as follows:

```
<LimitExcept GET POST HEAD DELETE>
<LimitExcept GET POST HEAD DELETE>
```

• If not, then you will need to:
  – Update the Admin Workstation to the current SecureDrop release version, by following the applicable upgrade guide in our documentation.
  – Back up the SecureDrop instance, using the server backup instructions.
  – Verify that the configuration stored on the Admin Workstation is correct by running `cd ~/Persistent/securedrop && ./securedrop-admin sdconfig`. This command will display each setting in turn - to accept without changing, press Enter for each.
  – Update the instance configuration by running `./securedrop-admin install`.

• When the instance configuration is up to date, continue with the SecureDrop Workstation installation.

### 9.3.2 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 the recommended ThinkPad T480, see the [Upgrading the T480 BIOS](#) section in this documentation. 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 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.
9.3.3 Download and verify Qubes OS

On the working computer, download the latest stable Qubes OS ISO (4.0.3 at time of writing) from https://www.qubes-os.org/downloads/. The ISO is 4.5GB approximately, and may take some time to download based on the speed of your Internet connection.

Follow the linked instructions to verify the ISO.

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-R4.0.3-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`).

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

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 all available storage space for the installation (as the computer should be dedicated to SecureDrop Workstation).
- Set a strong 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 this 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.

Note: On first booting into a Qubes OS 4.0.3 installation, you may be prompted to enter the FDE passphrase at a command-line prompt rather than via the GUI. The next system update will restore the GUI prompt.

After the disk is unlocked and Qubes starts, you will be prompted to complete the initial setup. Click the Qubes OS icon, then accept the default options and click Done. 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.
9.3.5 Apply updates to system templates (estimated wait time: 45-60 minutes)

Before installing SecureDrop Workstation, you must set up network and Tor access, then update the system VMs:

- After logging in, use the network manager widget in the upper-right panel to configure your network connection.
- Next, configure Tor by selecting the Qubes menu (the Q icon in the upper left corner) and selecting Service: sys-whonix > 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 connection 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 Q > System Tools > Qubes Update to update the system VMs. In the [Dom0] Qubes Updater window, first check Enable updates for qubes without known available updates, then check all entries in the list above. Then, click Next. The system’s VMs will be updated sequentially - this may take some time. When the updates are complete, click Finish.

9.3.6 Install Fedora 31 template

See Upgrading to Fedora 31.

9.4 Install tasks

9.4.1 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 > Domain: vault > vault: Files 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 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 vault file manager, select + Other Locations, then click the persistent volume’s listing in the right panel. 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.

• Open a dom0 terminal via Q > Terminal Emulator, and 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 command:

```
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 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, select + Other Locations and eject the TailsData volume, then disconnect the SVS USB.

### 9.4.2 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 vault file manager, select + Other Locations, then click the persistent volume’s listing in the right panel. 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.

• 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
```

If your instance uses legacy v2 onion services, use the following command instead:

```
qvm-run --pass-io vault
  "cat /run/media/user/TailsData/Persistent/securedrop/install_files/ansible-base/app-journalist-aths"
> /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, select + Other Locations and eject the TailsData volume, then disconnect the USB drive.

### 9.4.3 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 > Domain: vault > vault: Qube 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 > Domain: vault > 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, select + Other Locations and eject the TailsData volume, then 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).

9.4.4 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 > Domain:work > work: 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 > Domain: work > 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 \  "2224 5C81 E3BA EB41 38B3 6061 310F 5612 00F4 AD77"
gpg --armor --export 22245C81E3BAEB4138B36061310F561200F4AD77 \  > 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 gedit) 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/f25
name=SecureDrop Workstation Qubes initial install bootstrap
```

• Download the SecureDrop Workstation config package to the current working directory with the command:

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

Note the release version number in the filename, you’ll need it below.

• Verify the package with the following command:
```
rpm -Kv securedrop-workstation-dom0-config-<versionNumber>-1.fc25.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.fc25.noarch.rpm:
  Header V4 RSA/SHA256 Signature, key ID 00f4ad77: OK
  Header SHA1 digest: OK
  V4 RSA/SHA256 Signature, key ID 00f4ad77: 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.fc25.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.fc25.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.

### 9.4.5 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-fingerprint --with-colons /tmp/sd-journalist.sec
```

The fingerprint will be on a line that starts with `fpr`. For example, if the output included the line `fpr: : : : : : : 65A1B5FF195B56353CC63DFCC40EF1228271441:`, the fingerprint would be the character sequence `65A1B5FF195B56353CC63DFCC40EF1228271441`.

• 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 value of the v2 HidServAuth token for the Journalist Interface, or the v3 private authorization key value if your SecureDrop instance uses v3 onion services
  - `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:

If your instance uses v2 onion services, the file will be formatted as follows:

```
HidServAuth ONIONADDRESS.onion AUTHTOKEN # comments, can be ignored
```

If your instance uses v3 onion services, 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:

```
securedrop-admin --validate
```

- Finally, in the `dom0` terminal, run the command:

```
securedrop-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 it completes, your SecureDrop Workstation is finally ready to use!

### 9.4.6 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.

### 9.4.7 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

9.5 Troubleshooting installation errors

9.5.1 “Recurse failed: none of the specified sources were found”

An error similar to the following may be displayed during the installation, after which the installation will fail:

```
_____ID: dom0-securedrop-launcher-directory
Function: file.recurse
    Name: /opt/securedrop/launcher
    Result: False
    Comment: Recurse failed: none of the specified sources were found
    Started: 20:52:46.766870
    Duration: 2.371 ms
    Changes:
```

To clear this error, clear the Salt cache and resynchronize by running the following commands in a `dom0` terminal:

```
sudo rm -rf /var/cache/salt
sudo qubesctl saltutil.sync_all refresh=true
```

Then, run `securedrop-admin --apply again`.

9.5.2 “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.
9.5.3 “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 `securedrop-admin --apply` command.

9.6 Uninstalling SecureDrop Workstation

To uninstall SecureDrop Workstation, open a `dom0` terminal and run the following command:

```
securedrop-admin --uninstall
```

This will remove all associated VMs and configuration details, and uninstall the `dom0` SecureDrop Workstation package.

The submission key and `config.json` file will still be present in `dom0` in `/usr/share/securedrop-workstation-dom0-config`. To delete them, use the command:

```
sudo shred /usr/share/securedrop-workstation-dom0-config/{config.json, sd-journalist. --sec}
```
CHAPTER 10

Keeping the Workstation secure

Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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.

10.1 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.

10.2 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.

### 10.3 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 11

Managing Clipboard Access

Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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.
11.1 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
```
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:
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
```
Troubleshooting connection problems

Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

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.

13.1 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):

15:37

It looks like this for a wireless connection:

16:03

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

16:10

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 the Qubes menu (top left) and clicking **Terminal Emulator** 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.

### 13.2 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.

### 13.3 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.

13.3.1 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:

```
curl -s 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.

13.3.2 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.

13.3.3 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.

13.3.4 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.

13.3.5 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 14

Provisioning Export USB devices

**Warning:** SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

SecureDrop Workstation supports the export of submissions from the Qubes client to an encrypted USB *Export Device*.

**Note:** Currently only LUKS-encrypted devices are supported, which effectively restricts the *Export Device* to use with Linux-based systems such as Tails. Support for Veracrypt-encrypted devices is planned, which will allow the use of the *Export Device* with MacOS and Windows systems.

In order to provision an *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.
CHAPTER 15

Limitations and known issues

**Warning:** SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

15.1 Reporting issues

For the duration of the pilot, bugs and other issues found in SecureDrop Workstation should be reported by pilot participants via the support portal. Issues that are not instance-specific will be added to the appropriate public issue tracker by the developers, for example:

- SecureDrop Workstation issues - issues related to the Qubes environment and workstation provisioning.
- SecureDrop Client issues - issues related to the SecureDrop Client.
- SecureDrop Export issues - issues related to printing and exporting submissions.

15.2 Current known issues

- Updates are slow due to the number of VMs involved, and due to some updates being fetched over Tor. We are investigating various strategies to improve performance and reliability of the updater.
- Currently, only LUKS-encrypted Export Devices are supported. VeraCrypt support will be added in a future release.
- Printer support is limited to specific models by Brother and HP, 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.
- “Flag for reply” functionality is not implemented in the SecureDrop Client. This is used when a source’s reply key was not created on their first submission and needs to be created on their next visit. If you are logged into the SecureDrop Client, and the reply feature for a source is disabled for more than a minute, they must be flagged for reply in the Journalist Interface - see the SecureDrop “Flag for Reply” documentation for more information.
• Currently, only app-based two-factor authentication (TOTP) is supported.

• The SecureDrop Client can only be configured with a single Submission Key. If the Submission Key for your SecureDrop server was rotated in the past, and submissions encrypted with the old key are still on your server, you will not be able to open them with the SecureDrop Client.
Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

Note: This advisory was written in May 2020, and will be removed when a new version of Qubes that contains the Fedora 31 template is released.

16.1 Why do I need to upgrade?

SecureDrop Workstation makes use of several Fedora-based VMs which are part of a Qubes installation by default, including sys-firewall, sys-net, sys-usb, work, and vault. In Qubes 4.0.3, these VMs are based on a Fedora 30 template.

As of May 26, 2020, Fedora 30 templates are end-of-life. If you are provisioning SecureDrop Workstation for the first time, you will need to update your Fedora template manually from Fedora 31 before installing SecureDrop Workstation.

If you are an existing SecureDrop Workstation user, SecureDrop Workstation will install the template automatically when updates are applied, but you should also manually configure VMs not managed by SecureDrop Workstation to use the Fedora 31 template.

16.2 Install Fedora-31 template

In a dom0 terminal (Qubes Application Menu > Terminal Emulator), type the following to download the Fedora 31 template:
sudo qubes-dom0-update qubes-template-fedora-31

You will see some information from the package manager, including a progress bar.

When the download has concluded, you will be prompted to install the package. Type `y` to proceed with the installation.

### 16.3 Update the Fedora-31 template

Once the template installation is complete, update the template using the Qubes Updater. Click `Q > System Tools > Qubes Update` in the application menu. Click the checkbox “Enable updates for qubes without known updates” option, and click the checkbox next to `fedora-31`. Click `Next` and wait for any available updates to be downloaded and applied.

### 16.4 Configure VMs to use the new template

To apply the template to VMs that currently use an older version, open the Qube Manager via `Q > System Tools > Qube Manager`. All VMs will be visible at a glance; to change a VM’s settings, right-click it and select `Qube Settings`.

In the Qube Settings window, select `fedora-31` from the drop-down menu beside `Template`, then click `OK`.

You should perform this process for:

- `work`
- `vault`
- `sys-net`
- `sys-usb`
• `sys-firewall`.

Existing SecureDrop Workstation users may perform this process for `work` and `vault` only, as the other VMs will be updated by SecureDrop Workstation.

Reboot the system to ensure the changes take effect. Alternatively, you can restart only the VMs you have updated.

**Tip:** You can also use the Qubes Template Manager (also in `Q > System Tools`) to make template changes. However, note that it will not allow you to make template changes for VMs that are currently running, so you may have to manually shut down VMs in the correct order to do so.

### 16.5 Getting Support

If you are part of the SecureDrop Workstation Pilot and you have questions about this process or about any other aspect of SecureDrop Workstation, please reach out to us.
17 SecureDrop Workstation Architecture

Warning: SecureDrop Workstation is in a limited beta phase, and is not recommended for general use at this time. See our blog post for more information.

17.1 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).

- genindex
- search