WEB-BASED WORKFLOW

1 Getting Started

2 Contents
   2.1 Creating your Account .......................................................... 5
   2.2 Using Redmine ................................................................. 6
   2.3 Troubleshooting .............................................................. 15
   2.4 Overview ...................................................................... 15
   2.5 What if I don’t want to use encrypted email? ...................... 15
   2.6 Setting up Encrypted Email .............................................. 16
   2.7 Troubleshooting .............................................................. 18
   2.8 General Support ............................................................. 20
   2.9 First Time Contacting Us? ................................................. 21
Freedom of the Press Foundation uses a Redmine-based ticketing system for all support requests related to SecureDrop. This system offers simple, centralized assistance to the administrators who maintain SecureDrop instances and the journalists who use them. Running a SecureDrop is hard work. We at FPF are committed to offering support during installation and into the working life of an organization's SecureDrop instance.

Note: The support site is also available as a Tor Onion Service at http://sup6h5iyiyenvjxfbgrjynm5wsgijjoatvnvdgyyi7je3xqm4kh6uqd.onion/.
Current SecureDrop users should get started by creating an account. Support is available on the web or by encrypted email. The two support methods can also be used interchangeably.
2.1 Creating your Account

To get started, register your account on the Registration Page.

Make sure you

• Choose a strong passphrase;
• Use an email address that you check frequently;
• Pick a username that helps us identify you at a glance. We recommend using your first initial and your last name (e.g. “jsmith” for John Smith).

We manually confirm each new account. After submitting your registration, it will be reviewed by our team. When approved, you will receive an email notification stating that your account has been activated.
After your account is activated, you can login and continue to the next step.

### 2.2 Using Redmine

#### 2.2.1 Logging In

Once your account has been activated, go to the Support Page and log in with your new account.
After logging in, you will be taken to the Home page. In the top menu bar, you will see helpful links to a variety of resources. The most important links are:

- **Projects**: The list of projects you have access to.
- **My Page**: An overview of the open issues that were either created by you or are assigned to you.

Click on **Projects** in the top menu bar. You'll see a project for your SecureDrop instance listed underneath the parent SecureDrop project. Only Freedom of the Press Foundation staff and people within your organization have access to your instance’s project.
Click on the project link. You’ll be shown an **Overview** of the project and all of its issues.

To view the list of open issues, click the **Issues** button to open the issues pane.
2.2.2 Onboarding Issue

By the time you log in, we’ll have created an initial issue for onboarding, called “Onboarding Verification”. Please write a reply on this issue, which will let us know that you succeeded in logging in and finding your project page.

To write a reply, click Edit button at the top of the issue. Write your reply in the Notes text box, then click Submit.
We'll reply to the issue and start a little exchange to explain some features of the platform and answer any questions you might have. The goal here is to make sure you're comfortable and confident using the new Support site.
Once we're satisfied you're ready to use the new site, we'll close the issue.

Once we're finished with the onboarding issue, you're ready to use the Support site. If you want to additionally set up encrypted email notifications, head over to the Encrypted Email Overview.

The rest of this documentation is for your reference.

2.2.3 Key Features

Creating a new issue

To create a new issue, click New issue and fill out the Subject and Description fields. All other fields can be left blank, although you can assign a priority if you want. When we see the issue, we will respond and assign it to the appropriate person. If we're waiting for a reply from someone in your organization, we may assign it back to you.
Creating a new issue via email

Sending an email to support@freedom.press will automatically create a new issue in your project, using the subject line of the email for the Subject and the body of the email for the Description.

Enabling two-factor authentication

Two-factor authentication (2FA) protects your account in the event that your passphrase is compromised. Once enabled, you will be prompted to provide a one-time six digit code every time you log into the support portal, in addition to your passphrase.

To enable 2FA:

1. Choose an application to generate two-factor codes. We recommend the FreeOTP app for Android or iOS, but any app that implements the Time-based One Time Password (TOTP) algorithm should work.
2. If you are not already logged in, log into the support portal.
3. Click My account in the top right corner to navigate to your account settings. On the settings page, click Enable authenticator app.
4. You will see a page that shows a QR code, similar to the one below. Use your 2FA app’s QR code scanning function to scan the code on the page, or manually enter the 2FA secret (called a “plain text key” here) in the app.

5. Select the account you have just added to your 2FA app, and generate a new one-time token using the app. Enter it on the webpage and click **Activate**.

6. You should see a success message like the one below. Follow the recommendation and click **generate backup codes**.

```
✓ Two-factor authentication successfully enabled. It is recommended to generate backup codes for your account.
```

7. You will see a list of codes like the one below. Each code (e.g., ec96 a5d7 c678) can be used once instead
of a 2FA code during the login sequence. Store these codes securely and separately from your passphrase. The recommended method is to keep a printout of the recovery codes in a secure location.

8. Log out of your account and attempt to log in again. After entering your passphrase, you will additionally be prompted for a two-factor code, which you can generate using your 2FA app.

If you have to reset your 2FA settings at any time, you can use a recovery code. Once you are logged in, disable and then re-enable 2FA from your account settings.

Please do not hesitate to open a ticket or email us at securedrop@freedom.press (GPG-encrypted) if you encounter difficulties using 2FA on the support portal.

**Other account settings**

In addition to two-factor authentication, you can also configure your local time zone in the account settings.

We encourage you to leave the notification setting as the default: “For any event on all my projects”.
2.3 Troubleshooting

2.3.1 Email notifications

If you'd rather not receive emails for your own comments on issues, there's a setting for that. Go to the “My account” page, select ” I don't want to be notified of changes that I make myself” under “Email notifications” and hit Save.

2.3.2 Inline replies

When responding to issues, you should only use the “Quote” button if you want to make an inline reply. Otherwise, hit “Edit”.

2.3.3 Customizing “My Page”

There's a shortcut in the main menu called “My page”. Typically, this starts out as a list of issues that are assigned to you and issues that have been reported to you. However, it can be personalized further to include stuff like issues you're watching, documents, and the latest news from your project.

2.4 Overview

One of Redmine's strengths as a ticketing system is its powerful support for email-based workflow. You can use email to create new issues, reply to existing issues, and be notified of updates to issues that are relevant to you.

While many people find email-based workflows convenient, email is unfortunately insecure by default. Freedom of the Press Foundation takes the security of every SecureDrop instance seriously; therefore, we require the use of encryption for support requests because they may contain sensitive information about your SecureDrop instance.

The web interface workflow is automatically encrypted thanks to HTTPS. Supporting a secure email-based workflow is more difficult because email is unencrypted by default. Our solution is to combine Redmine's excellent email-based workflow with OpenPGP encryption, which we already use to communicate with many SecureDrop administrators and journalists.

2.5 What if I don't want to use encrypted email?

That's fine! You can do everything through the web interface that you can do through email.

If you don't do the setup process for receiving encrypted emails from our support server, you will still receive email alerts for changes to issues in your project, but the content of the email will not be included. This is called a “filtered” email.
We encourage you to use these filtered emails as a reminder to login to your Redmine account and check the content of the corresponding updates to an issue through the web interface. We like to think of them as “poor man’s push notifications”.

**Note:** We welcome feedback on how we could make notifications for this Redmine system more convenient for you.

### 2.6 Setting up Encrypted Email

In order to use this encrypted email workflow, you need to:

1. Provide your public key to the support server
2. Import the server’s public key into your local GPG keyring.

The following documentation explains how to perform these steps to get the encrypted email workflow working. This documentation assumes you are familiar with PGP/GPG. We encourage you to use your preferred GPG key management tool and email client.

If you do not know how to do things like import and export GPG keys, the encrypted email workflow is not for you. We recommend you stick to the web-based workflow.
2.6.1 Providing your public key

Start by navigating to support.freedom.press/pgp or click on the “PGP” menu option in the upper right corner of the support window.

In the PGP management window you will see two columns: one for your public key on the left, and one with the server’s public key on the right.

To provide your public key, start by exporting an ASCII-armored copy of your public key. Paste your armored public key into the empty text box on the left and hit Save.

---

To provide your public key, start by exporting an ASCII-armored copy of your public key. Paste your armored public key into the empty text box on the left and hit Save.
2.6.2 Importing the server’s public key

Now, import the public key for our Redmine server into your local GPG keyring. It is available on the right hand side of the page in the column with the heading “Redmine Server (support@freedom.press)”, in the text box labeled “Public GPG key”.

Select the entire public key and copy it to your clipboard. Import the copied public key into your local GPG keyring.

You can download the key or fetch it from a keyserv (fingerprint: D0E0B2F27B6A4E48278637D9EA33029EFBBA2E).

Todo: Add section on testing encrypted email after setting it up

2.7 Troubleshooting

2.7.1 Always sign and encrypt your emails

To maintain the security of conversations around support requests, you should always sign and encrypt your email to support@freedom.press if you have a Redmine account.

Our server is configured to reject emails that do not have a valid signature. We cannot reject unencrypted emails due to a limitation in the Redmine-OpenPGP plugin we are using, but we are logging them and will harangue you if you send us unencrypted email.
2.7.2 PGP/MIME vs. inline PGP

When you’re replying to Redmine via email, you must use PGP/MIME instead of inline PGP. The default settings for the Enigmail plugin in Thunderbird should work.

Check your mail client and GPG integration tool’s settings to ensure you are using PGP/MIME. One notable exception to this is Mailvelope, which cannot send PGP/MIME (you shouldn’t be using Mailvelope anyway).

2.7.3 Per-recipient Rules

You may not want to use these settings (PGP/MIME, always sign) for all of your email. If not, most email clients support the concept of “Per-recipient rules”, which allow you to configure specific settings on a per-recipient basis.

Below is an example of how to configure a per-recipient rule for support@freedom.press in Thunderbird/Enigmail. If you are not using Thunderbird/Enigmail, consult your mail client’s documentation.

**Thunderbird**

To check your global settings, go to Edit > Account Settings in Thunderbird. Navigate to the “OpenPGP Security” tab of the email account you are using for your Redmine account. Be sure that “Use PGP/MIME by default” is checked. If you do not want to enable “Sign messages by default” for everything, you should add a per-recipient rule for support@freedom.press.

To do so, go to Enigmail > Edit Per-Recipient Rules > Add, and enter support@freedom.press. Set to Apply rule if “Contains” the above address, select our key, change all of the defaults (Encryption, Signing, PGP/MIME) to “Always”, then click OK, and OK again. The per-recipient rule should look like this:
2.8 General Support

First time getting in touch with us about SecureDrop? Please start by submitting a request through the SecureDrop Contact Form.

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

Once you are initially onboarded, we will assign you to a project called “Support Triage” where you will be able open new issues. Any issues that you create will only be visible to Freedom of the Press Foundation staff and you.
2.9 First Time Contacting Us?

If this is your first time contacting FPF for assistance, or if you have questions about

- installing SecureDrop;
- an existing SecureDrop installation that was set up without our involvement; or
- inclusion in the SecureDrop Directory;

please contact us through the General Support channel.