How To Use *Save* by OpenArchive

This guide will help new users set up and use OpenArchive's secure mobile archiving app **Save** (Secure, Archive, Verify, Encrypt). It will also explain the various features **Save** offers and provide an overview of the settings to help you customize your experience.

WHAT *Save* Can Do

Save is an app for Android and iOS that helps you preserve and protect your mobile multimedia. We built **Save** with and for those working in archival, human rights, journalism, and activist spaces in order to fill critical security, verification, preservation, and accessibility gaps in their workflows.

Save is a secure workflow tool that will help you safely send mobile media from your phone to either public or private servers while collecting contextual metadata to help you verify the media.

Save enables you to:

- Upload your verified mobile media to three types of servers; Nextcloud or any webDAV-compatible server (you have full control + it is secure & open source) and the Internet Archive (free public or paid private).
- Control access to and create in-app project folders to help you stay secure and organized.
- Add critical metadata like notes and location information to individual or batch uploads.
- Authenticate and verify your media with sha256 hashes automatically and optional Proofmode.
- Protect your media in transit with automatic Transport Layer Security and optional Tor (the onion router).
- Easily add Creative Commons licenses, allowing others to know your intentions for reuse of your media.

WHAT *Save* Cannot Do

- **Save** DOES NOT provide an archive to store your media or personal information
- **Save** DOES NOT store your media or personal information anywhere else
- **Save** DOES NOT yet have a killswitch or ability to mask the app on your phone (but these features are coming soon)

HOW To Install, Set Up *Save*, & Connect to Servers

Step 1: Download *Save* on your phone (search "OpenArchive" and "save" to find it quickly)

Download the *Save* app for Android from [Google Play.](#)

Download the *Save* app for iPhone from the [App Store](#).

After installation, select 'open'.

Step 2: Swipe through the welcome screens

Upon first opening *Save*, you'll be greeted with a series of screens that welcome you to the app. To begin, tap 'Get Started.'

These screens give you a quick overview of how you can:
- connect to a private server or the Internet Archive;
- organize your media into custom folders and add context-setting metadata like location and notes and flag significant content;
- ensure authenticity to support verification workflows;
- and how to enable Tor to encrypt your media for safer transit.

Step 3: Connect to a Server

To archive your media, you will now need to connect to a server. You can choose to connect to a private open-source server like [Nextcloud,](#) or share publicly for free or privately via their paid Vault on the [Internet Archive](#) (see the bottom of this document for more information about the different servers and when to use each). Choose your preferred server* and connect.

* Important note on connecting to servers:
Note that you will need to have created an account with an Nextcloud instance or at the Internet Archive.

Step 4: Add a folder

Tap the plus icon at the bottom of your screen. First-time users will be prompted to add a folder to store media on the server. You can create a new folder or browse existing folders on the chosen server.

Step 5: Add media, metadata, & flag significant content
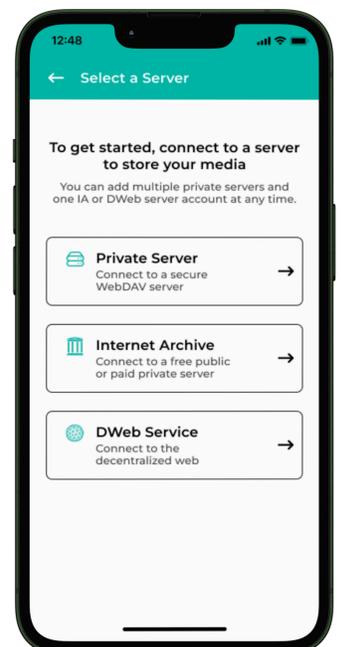
Tap the plus icon to select media from your camera roll or gallery for uploading. After you've chosen your media, you can edit one file or bulk/batch edit as many files as you like. Here you can add location and notes information. You can also tap the "significant content" flag to identify sensitive media that will then be stored in a separate subfolder to alert viewers that this content may be violent or disturbing before they see it (you can also use this feature as a way to save "favorites" from within the bulk upload). You will be able to see the upload progress from your home screen.

Step 6: Add media from other apps like audio files or documents

Along with uploading media from your camera roll, you can also use *Save* to upload other types of files on your phone, such as documents, voice notes, etc. Long-press and hold the plus icon and then add media by choosing "files". Then select the files from your phone to upload. Once chosen, you can edit the metadata for these files and upload them just as you would photos or videos.

How to Customize *Save's* Settings
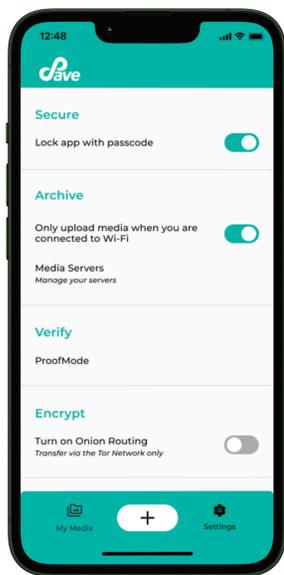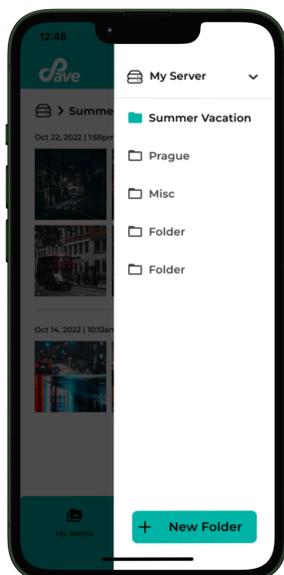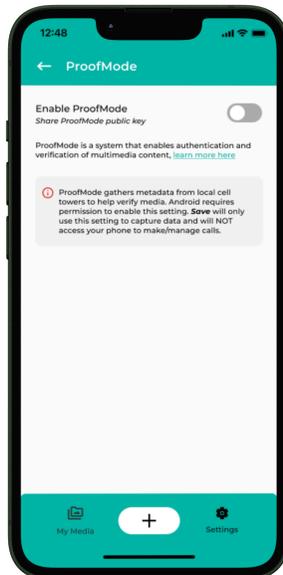
Secure	Archive	Verify	Encrypt
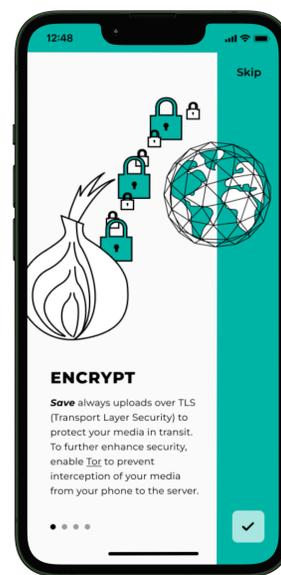
Save offers some powerful settings that allow you to customize the app to your needs. To get to the settings, touch the cogwheel at the bottom right of your screen.

You will then be taken to a setting page that offers options to do the following:

Secure
- Lock the app with your passcode or biometric ID

- Hide app content in background

Archive
- Choose **servers** to see which servers you are connected to and your login information for each server. You can also disconnect the server(s) from the app.
- Choose **folders** to remove* or archive a folder.
  - *Removing a folder removes the folder and its thumbnails from your phone. However, it will NOT remove any media or files from the server or your phone's camera roll/other file folders or from the server you send it to.
  - Archiving a folder will move it from the active workspace view and save it for later access. You can then access archived folders from this screen by tapping "View Archived Folders".
- Once you add a server or folder, you will be prompted to choose a [Creative Commons license](#) for the media on that server or in that folder. A Creative Commons license allows you to share your intentions for future use, republishing, remixing, and distribution of your media. For ease of use, you have the option to enable the same Creative Commons license for all folders per chosen server, or you can tap an individual folder and set unique Creative Commons licenses for that specific folder.

Verify
- Whenever sending media to a server via *Save*, it is always packaged with a sha256 hash, which we encourage you to share publicly online for future verification.
- You can use [Proofmode](#) to notarize and add more metadata to your media. Please note that you will need to record your media in-app when running Proofmode in order for it to add extra metadata to the media at point-of-capture to further corroborate/verify your media's built-in metadata (exif data). Note that *Save* does not store your photos and videos within the app.

Encrypt
- Your media is always sent over [Transport Layer Security (TLS)](#) and you can have additional security by choosing to only send media over the [Tor](#) network.

Device Settings

- Choose your theme
- Choose whether to only upload media while using a WiFi connection

WHERE Your Media Goes

Save** does not store your media. When using **Save**, you have full agency over the lifecycle of your media: you can decide where to store it and how you want to share it in the future.

The app connects to two different types of servers, so you can choose which works best for you:

1) [Nextcloud](): Secure, private, paid, and open source WebDAV-compatible, or;
2) [Internet Archive](), a nonprofit archive offering **free public** or **paid private** servers.

Keep in touch!

Website: [open-archive.org]()
Mastodon: [https://mstdn.social/@OpenArchive]()
Bluesky: [@OpenArchive]()
Pixelfed: [@OpenArchive]()
Instagram: [@open__archive]()
Email: [info[at]open-archive.org]()