Secure FileShare

Enable secure public internet access to your files with just two clicks

Attention!!! The only one instance of our website should be open in browser on your device!

Transfer file demo Share file demo

In modern digital society, privacy and data protection have become essential priorities for almost everyone. Our web application empowers you to take control of your online presence and share sensitive information securely. All that can be done in a very easy intuitive way, without any sophisticated software or techniques.

Key features:

1. Share any type of content via public url
2. Transfer files within your transfer group (P2P, P2nP transfer)
3. Strong end-to-end encryption
4. Unique option - share files directly from device, without upload to any cloud
5. Works on any device in any modern browser
6. Fully anonymous sharing, without possibility to track files ownership
7. A robust and dependable data transfer algorithm designed to perform seamlessly, even on slow or unstable networks
8. Remove public access to your files at any time

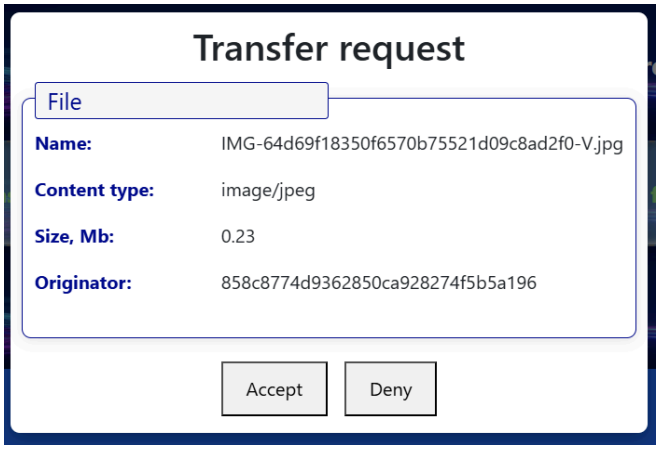
Possible Use cases:

1. Protect content shared via social media or other public channels with password and encryption
2. Effortlessly transfer files between your devices without worrying about network security—whether you're on public airport Wi-Fi, free hotel Wi-Fi, or any other hotspot.
3. Share sensitive information like passwords, access codes, bank card number etc.
4. Record audio/video message and leave it on any site that support comments (Facebook, Reddit, Amazon etc.)
5. share screenshots captured on your device
6. Share big files (up to 5Gb per day) for free
7. Transfer files without any size limits

Let's do a breakdown of the major features one by one:

The core element of file transfer is the Transfer Group, which is identified by its name. You can assign any name to your Transfer Group, but it's best to avoid overly common names like 'main' or 'My-group.' Using a generic name increases the risk of inadvertently receiving files from other users who may have chosen the same group name.
Your data will be encrypted during transfer, even if you haven't set a password (a password will be derived from the group name). However, we strongly recommend using a hard-to-crack password alongside the group name to ensure maximum security for your data transfer.
You only need to configure the transfer group once on each device. It will be saved and automatically applied every time you launch the Secure FileShare website.

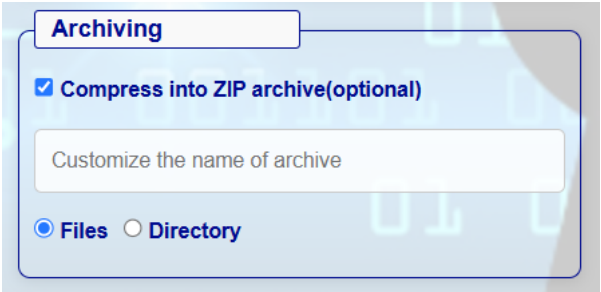
Select files for transfer by pressing  button or using drag-and-drop zone
To speedup your transfer and save network traffic you can create ZIP archive with customisable name (first selected file name or folder name will be used as an archive name otherwise)
At once the files are selected, the transfer will begin, a progress bar will be displayed, and all team members will receive a file transfer request:



A peer-to-peer connection will be established with each team member during the transfer, ensuring that no data is uploaded to any cloud. Additionally, the transfer only needs to be initiated once, as all team members will receive the data simultaneously (no need for separate transfers for each member)

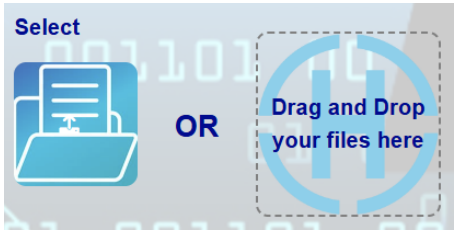
The key difference from File Transfer is the ability to generate a public URL, which can be shared and accessed by anyone who wishes to download the file. So you need some external channel to share that public URL (Telegram, Facebook etc.)
Use '**Protect with**' section to encrypt your file. You should only provide the password, after that encryption will be applied automatically.

Use '**Archiving**' section to speedup downloading and save network traffic by creating ZIP archive. Customise the name or your archive (first selected file name or folder name will be used as an archive name otherwise)

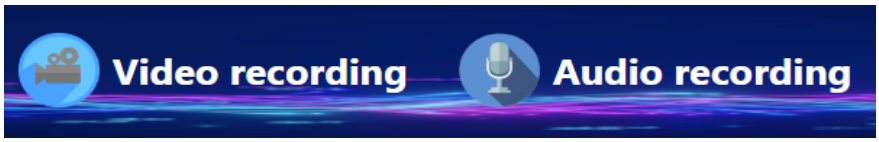


Enabled '**Share from device, without upload to cloud**' checkbox prevents caching of your files in cloud. They will be stored in the internal browser database and served directly from your device during downloading. Combined with encryption that feature provides the highest level of protection for your file. Attention!!! Our website should be always open in browser on your device to support sharing.

Use '**Select**' section or '**Drag and drop**' zone to choose files for sharing



Once files are selected, they will either be uploaded to the cloud or stored in the browser's internal storage. A new entry will be created in the Shared Content Manager, and a public access link will be automatically copied to your clipboard. You can paste this link anywhere, such as in social media comments, messaging apps, or any other platform.



What sets this apart from regular File Sharing is the ability to capture video or audio content directly from our website page using your device's camera(access to camera can be requested explicitly by the browser). The recorded content is then processed like any other file and transformed into a public URL for seamless sharing. This feature allows you to effortlessly create voice or video messages with optional protection, such as passwords plus end-to-end encryption. You can then share these messages on social media, e-commerce sites, messaging apps, or any platform that supports commenting.

Again very similar to regular File Sharing, but instead of file selection just press '**Ctrl+V**' (On macOS, you'll use `Command (⌘)+V` for pasting). If buffer contains some binary then it will be processed as any other file and transformed into a public URL for seamless sharing. The most popular application of this feature is the quick and seamless sharing of screenshots.

Shared content manager

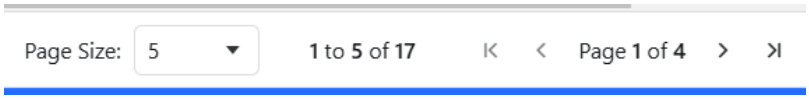
The Shared Content Manager is created to help you efficiently track and manage all files shared from your device. Every track record contains following fields:

1. File name
2. Size in Mb
3. Mime type
4. 'Created at' - actual time when the public URL was created
5. 'Public URL' with 'Expose workspace ID' checkbox - use button in that column to copy Public URL to keyboard buffer. If checkbox is selected then workspace ID will be automatically added to public URL. That enables you to share only the password through a secure channel, as the workspace ID will be extracted from

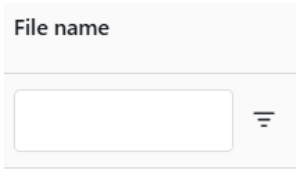
URL. Caution!!! Including the workspace ID in the Public URL significantly reduces the security of your protected content and makes it more vulnerable. Use this option carefully.

6. Credentials - use button in that column to copy protected URL credentials (workspace ID and password) that should be share with receivers via secure channel
7. 'Download' - use button in that column to test availability of your content shared via public URL. You chould be able to download content by opening public URL in a new browser tab
8. 'Cached in Cloud' - that column contains  icon if shared content is cached in cloud and empty if not. If content is not cached it can be downloaded directly from your device but our website should be always open in browser to directly support sharing
9. 'Remove' - You can revoke a public access to your files and clear the cloud cache with a single click at any time by pressing button in that column.

Shared Content Manager table supports pagination

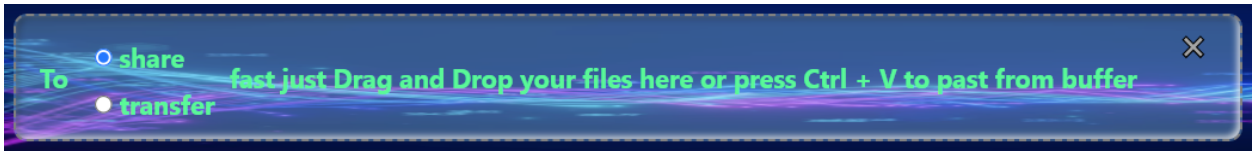


and 'search by name' filter



Also you can change default ordering or remove some columns

Fast access toolbar



Fast access toolbar use the following defaults:

- no encryption
- cache content in cloud

And provides extremely easy way to share or transfer your files.

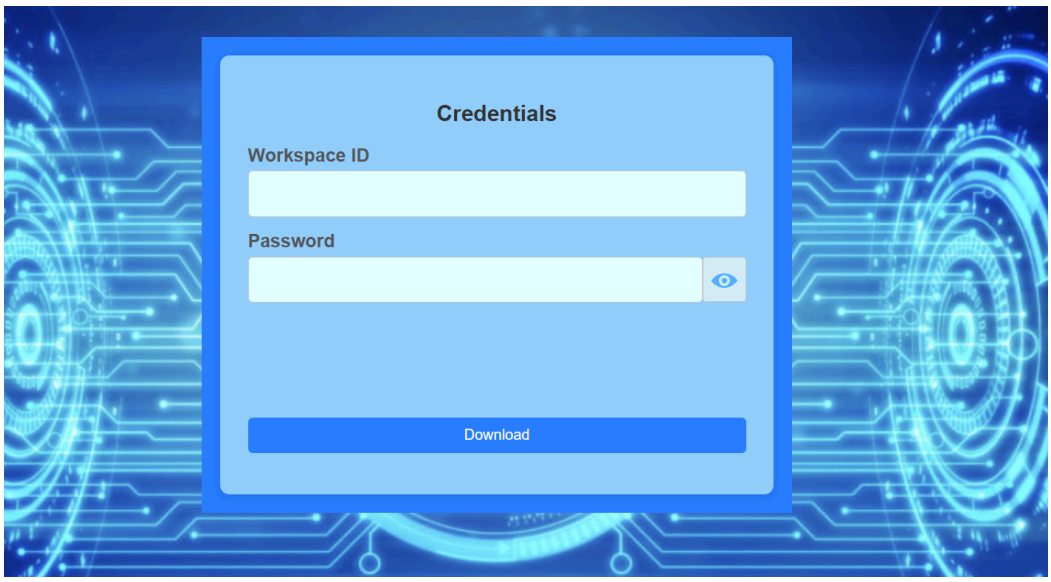
Eight reasons to start using our product:

1. Simplicity - enable secure public internet access to your files with just two clicks
2. Universal, cross-platform tool that can be used in modern browsers on any device, without necessity to install any additional software like http/sftp server, agent etc.
3. No need in public IP address or open ports on your machine even if '**Share from device, without upload to cloud**' option is selected
4. Several options for sharing with different security levels, include the highest Zero-trust security provided by '**Share from device, without upload to cloud**' feature
5. No registration required, use our product fully anonymously
6. We are using only secure https/wss protocols for data transfering
7. Secure FileShare is completely free
8. Out public URL completely hides the identity of content owner. No IP address leaks or any disclosure

Why our password protection is almost impossible to huck

We are talking about unique '**Share from device, without upload to cloud**' feature

1. Receiver (for instance friend of you) will be redirected to pre-download page after attempt to open short public link



2. Now He should enter credentials that you previously shared with him via a secure, reliable channel. **Never send credentials along with download link!!!**
3. Request Signature will be created based on provided workspace ID and password with strong and secure cryptography algorithm. So actual credentials are never sent via network or stored on any server in cloud
4. Signed download request will be sent via https POST channel to file owner.
5. File owner verify download request signature and initiate upload if signature is correct
6. File is splitted into chunks of equal size. Every chunk is encrypted before sending on owner side and then decrypted on receiver side
7. For better security download request has very short ttl(time to live)
8. Do not use “Expose workspace ID” option if your goal is an ultimate security and protection against brute force attacks

Enjoy our product and provide feedback on email: sf-share@gmail.com