CYBERVORE

FRAGGLEdrive™

The disappearing, disk drive that renders your data useless to hackers

FRAGGLEdrive™/FRAGGLEstorm™ Quick Start Installation & Setup Guide

FRAGGLEdrive™ protects critical data by combining identity access management (IAM), NIST AES-256 encryption, and secure file fragmentation. By distributing encrypted 'fragments' across local storage and diverse cloud services, FRAGGLEdrive™ establishes a virtual safety deposit box where your files remain ultra-secure and private. This quick guide is to assist with the installation.

Install FRAGGLEdrive™ in minutes, map your first business line's storage, and see what an unreadable breach looks like — at no cost for 30 days. Thank you for using FRAGGLEdrive™!

PRE-INSTALLATION CHECKLIST

Follow these key steps to ensure a smooth setup process:

• Check and Update the OS: Run your 'Windows Update' on your PC/laptop to ensure Windows 11 has the latest cumulative and security releases.

• Prepare for a Software Installation: Temporarily turn off heavy antivirus programs and close other active applications to prevent installer blocks.

• Admin Access: Log in with an administrator account or be ready to right-click the setup file and choose Run as administrator.

- ✓ Gather Cloud Credentials: Collect usernames and passwords for your active cloud storage accounts that you want to use for your FRAGGLEdrive™ storage (e.g., OneDrive, Google Drive, Dropbox, Wasabi S3, Box). FRAGGLEdrive™ can support multiple storage locations and up to 70 cloud storage services. This will reduce installation and setup time.

• Install Guardian App: Download the free Okta/Auth0 Guardian authentication app for your smartphone from your mobile provider's app store.



FRAGGLEdrive/FRAGGLEstorm APPLICATION INSTALLATION WIZARD

Once the checklist is complete, proceed with the wizard-based installation:

• Sign Up and Download Now: Obtain the software license from Cybervore.com for 30 days free. Upon registration, you will receive an email containing a secure download link, your license key, and password.

• Launch Setup: Download the compressed archive file (usually saved in your Downloads folder). Open the ZIP folder and double-click the .exe executable to run the setup.

• Accept Terms: Click **Next** to begin, carefully read the License Agreement, choose I accept..., and then select **Next**.

• Select Directory: The recommended default destination is C:\Program Files\Cybervore\Fragglestorm\. Click **Next**, then click **Install**, and once the progress bar completes, select **Finish**.

• Install WinFsp (a Microsoft© program): The software relies on WinFsp 2023. The secondary setup wizard will open automatically. Click **Next**, accept the default features, click **Next**, click Install, then click **Finish**.

• System Reboot: To complete the driver installation and system integration, you must restart your PC.

FRAGGLEDRIVE™ QUICK START INSTALLATION GUIDE SECURITY SOLUTION SETUP & OPERATIONS

SYSTEM SETUP & SECURITY OPERATIONS

After your computer restarts, complete the registration and storage integration:

• Activate License: Log back into your PC. In the Validation window, click OK. Enter the License ID and Password you received by email, then click **Next**.

• Configure Virtual Drive: In the FRAGGLEdrive™ setup wizard, assign a Display Name (e.g., MySecureFiles). This will appear as the drive letter or disk label in Windows File Explorer.

• Set Fragment Count: Choose the number of fragments to split files into across your storage providers. The recommended value is 16.

• Connect Storage Providers: Choose your target storage locations. You can connect Box, Dropbox, Google Drive, Wasabi, or a Local folder on the PC or laptop. Grant 'yes' to enable API/rClone authorization for cloud integrations when that provider requests permission.

• Enable Encryption: Select the Enable Encryption box, then create a unique, strong master encryption password. **Note: This password cannot be recovered; store it in a secure location.**

• Confirm Settings: Enable 'Auto Mount (Y)' to allow the drive to connect automatically at startup. Check the configuration summary, then click **Add Drive**.

MULTI FACTOR AUTHENTICATION (MFA) INTEGRATION

To enable two-factor security for your files, click Sign Up and Continue on your PC.

- Launch the Guardian App on your smartphone, select Add, and scan the QR code on your monitor. Once complete, your PC will display 'Logged in Successfully!'. You must use this app to authenticate every time you 'log in' to your PC/laptop to unlock and access your secure FRAGGLEdrive™ and data storage.

FRAGGLEdrive™ SYSTEM OPERATIONS

Once configured, FRAGGLEdrive™ runs seamlessly in the background. A key logo indicates normal green operational status in the Windows system tray. The drive icon displays three distinct system modes:

• Green (Normal): FRAGGLEdrive™ is mounted and operational.

• Orange (Synchronizing): FRAGGLEdrive(s) are actively syncing with your providers.

• Red (Alert): System requires attention or has hit a connectivity obstacle.

System Tray Menu Commands (Right-Click Bottom Tray Icon):



• FRAGGLEdrive(s): View the mount status of your drives (Green = mounted and accessible in File Explorer, Red = unmounted and hidden). Each FRAGGLEdrive™ must be mounted to be accessed, so we recommend setting automount to 'on'. You will see each active drive on 'This PC' as pictured.

• Login / Logout: FRAGGLEdrive(s) is not visible or accessible if the authorized user is not logged in or mounted. Logging out immediately disables your FRAGGLEdrive and removes all metadata and paths.

- ✓ 'Logging in' prompt is activated by right-clicking the green key in the bottom tray. MFA verification requires your smartphone. (We recommend you log in whenever you want to access your data, and to log out when you would like to secure it.

• Shutdown: Closes FRAGGLEdrive™ operations, locking all data securely offline. Must restart Fragglestorm to restart.

• Settings / Help: Manage drive options or access direct technical support and services from Cybervore.

FRAGGLEdrive™ and FRAGGLEstorm™ are trademarks of Cybervore, Inc. © 2026 Cybervore, Inc. All Rights Reserved.