



GHFS Backup Manager

User Guide

Version 1.0

Last updated: 2026-01-14

1. What is GHFS Backup Manager?

GHFS Backup Manager is a Windows application that helps you back up important folders automatically. Your backups are encrypted on your PC before they are uploaded, so only you can read them. You can store backups on the GHFS secure backup server, and optionally keep an additional encrypted local copy on an external drive or another folder.

2. How it works (in simple terms)

- You sign in using the account credentials provided by GHFS Hosting.
- You choose which folders you want to protect (you can add multiple folders).
- You set a daily schedule (for example, every day at 02:00).
- A background agent runs on your PC and performs the backup at the scheduled time, even if the app window is closed.
- You can also run a backup manually anytime using Backup Now.
- From the Backups tab you can view snapshots, download an encrypted copy, restore files, or delete old snapshots.

3. System requirements

- Windows 10 or Windows 11 (64-bit).
- Internet connection for server backups.
- A GHFS Backup account (username and password).
- Optional: external drive or a local folder for encrypted local copies.

4. Installation

Install the application using the GHFS Backup Manager setup file:

1. Download the installer from GHFS Hosting.
2. Right-click the installer and select Run as administrator (recommended for first install).
3. Follow the installation wizard. The installer will also install the GHFS Backup Agent (background service).
4. After installation, launch GHFS Backup Manager from the Start Menu or Desktop shortcut.

5. First-time sign-in and setup

5. Open GHFS Backup Manager.
6. Enter your GHFS backup Username and Password (provided after purchase).
7. Create your Personal Security password (second password). This password encrypts your backups. GHFS Hosting cannot recover this password if you lose it.
8. Click Sign In. The app will initialize your repository and verify access.

Important notes:

- Your Personal Security password is required for restore operations. Store it safely.
- If you change PCs, you will need your Personal Security password to restore from existing backups.

6. Choose what to back up (folders)

Go to the Folders & Schedule tab:

- Click Add and select a folder you want to back up.
- Repeat Add to include multiple folders (for example: Documents, Photos, Accounting).
- Select a folder in the list and click Remove if you no longer want to back it up.

7. Choose backup destination

You can back up to:

- Server Backup: Upload encrypted backups to the GHFS backup server.
- Encrypted Local Copy (optional): Save an additional encrypted copy to a folder you choose (for example a USB drive).

If you enable Encrypted Local Copy, the app will ask you to select the destination folder using a Browse dialog.

8. Run a backup now

9. Go to the Folders & Schedule tab.
10. Click Backup Now.
11. Watch the progress indicator: scanning, uploading, and completion status.
12. When complete, your new snapshot will appear in the Backups tab.

9. Set or change the schedule

Set a daily backup time in the schedule field (HH:mm) and click Apply Schedule. If you change the time later, the background schedule is updated automatically (old schedule is replaced).

To set schedule only (without running a backup immediately), use the Set Schedule Only option.

After you apply the schedule, you should see a confirmation message showing:

- The selected folders.
- The schedule time.
- Whether a local encrypted copy is enabled and where it will be saved.

10. Backups tab: view, download, restore, delete

10.1 Refresh

The Backups tab refreshes automatically when you open it, and you can also click Refresh anytime.

10.2 Snapshot list

Each snapshot shows the date, snapshot ID, size, number of files, and any note/tags.

10.3 Download (encrypted export)

Download creates an encrypted archive of the selected snapshot to a folder you choose. This export remains encrypted and still requires your Personal Security password to read.

10.4 Restore

Restore lets you restore a snapshot to a folder you choose. If Windows blocks writing file timestamps/attributes (Access Denied), the restore still completes and your files are safe.

10.5 Delete selected

Select one or more snapshots and click Delete selected to remove them from your account.

11. Troubleshooting

11.1 Backup fails with VSS / Access Denied

- If you see a VSS privilege error, try running the app once as Administrator.
- Some locked files may be skipped if VSS is not available; your other files will still be backed up.

11.2 Cannot connect / 401 Unauthorized

- Double-check your Username and Password (case sensitive).
- If your account is suspended, login and backup operations will be blocked until renewed.

11.3 HTTPS/Certificate issues (Windows curl)

- Some systems may block certificate checks due to missing revocation access. Your app uses standard Windows TLS.
- If your network blocks certificate checks, try a different network or contact your IT admin.

11.4 Scheduled backups do not run

- Make sure GHFS Backup Agent service is installed and running (it is installed by the setup).
- If you recently changed the schedule, click Apply Schedule again and verify it saved successfully.

12. Security and privacy

- Backups are encrypted on your device before upload using your Personal Security password.
- GHFS Hosting cannot view or recover your encrypted data.
- Keep your GHFS account password and Personal Security password safe.
- For best security, use a strong Personal Security password and do not share it.

13. Help and support

For step-by-step help, common questions, and troubleshooting, visit the GHFS Backup Manager Knowledge Base category:

<https://ghfshosting.com/knowledgebase/8/GHFS-BACKUP-MANAGER>

If you need assistance, contact GHFS Hosting via the support portal.

14. About GHFS Hosting

GHFS Hosting provides secure hosting and backup services. Learn more about us here:

<https://gh-fs.com/index.php/about/>