“Digital Scapegoat” Data Resource Protection System

User Manual（windows）-v2.1.11

2025.1.17

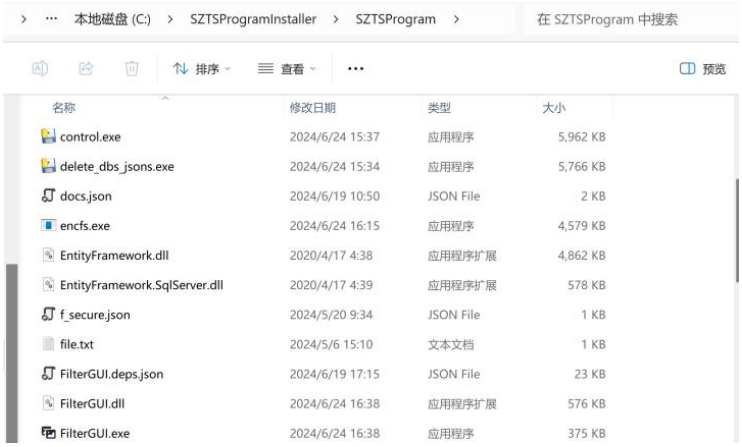
I. Installation and Configuration

1.1 Configuration Requirements

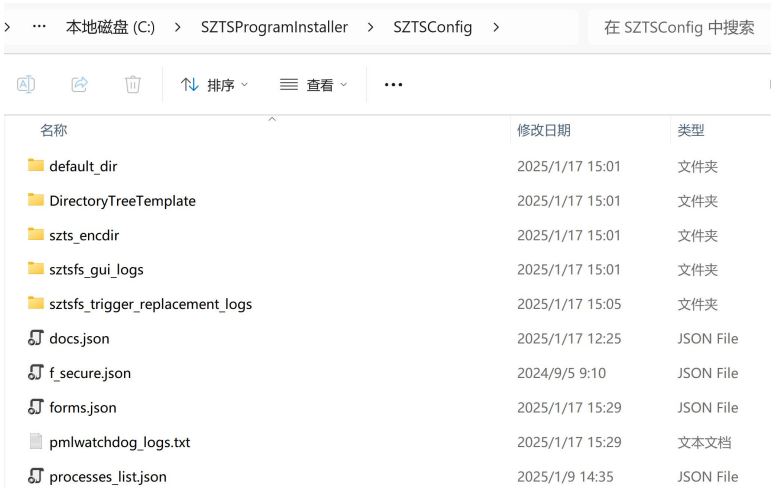
The software supports Windows 8.1/10/11, compatible with both 64-bit systems.

1.2 Installation

Run the DAIDepProgramEngInstaller.exe installer. The default installation path is C:\SZTSProgramInstaller\SZTSProgram (modification of the installation path is currently not supported). During the installation process, click "Allow" on all prompts. Once installed, a shortcut to the "Digital Clone" resource protection program will appear on the desktop. Program and data files will be stored in C:\SZTSProgramInstaller\SZTSProgram.



The installer will automatically create the directory C:\SZTSProgramInstaller\SZTSConfig to store system configuration files, log files, and sample encrypted files.



II. Getting Started

2.1 Interface Overview

Including visual guides would be more effective for this section.

2.2 Basic Usage

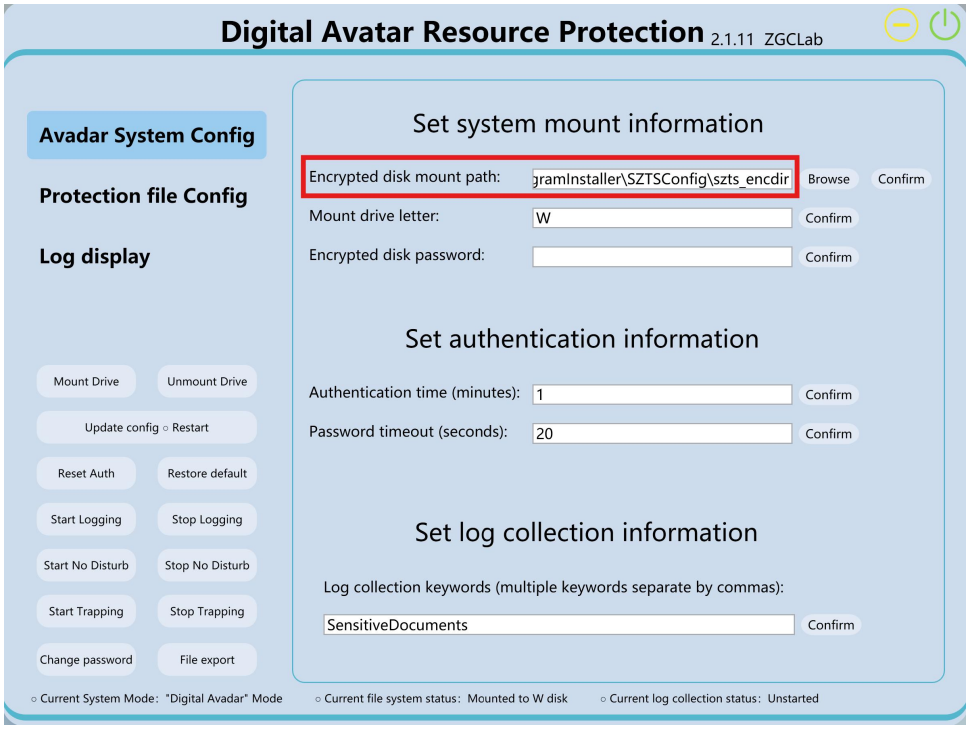
(1) Mounting and Unmounting the File System

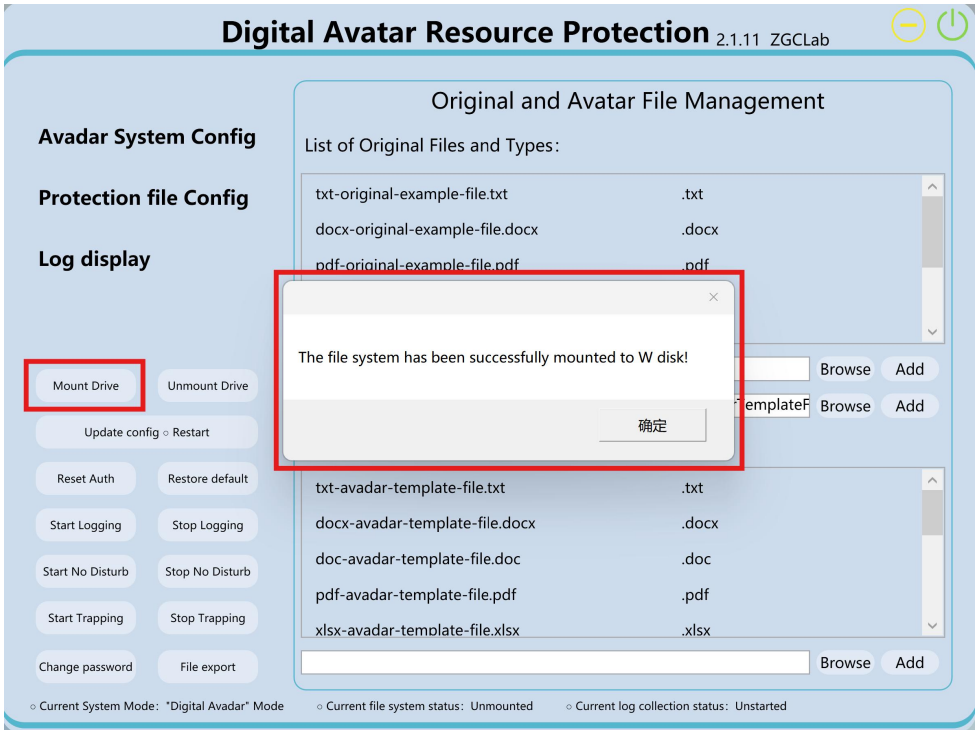
After launching the "Digital Avadar" resource protection program, click "Mount Drive" The program will use the default configuration to decrypt and mount the sample encrypted file directory created during installation (C:/SZTSProgramInstaller/SZTSConfig/szts_encdir). A new W: drive will appear in the Windows File Explorer (if the new drive does not appear, refresh the directory list). Click "Unmount Drive" and after refreshing, the W: drive will disappear.

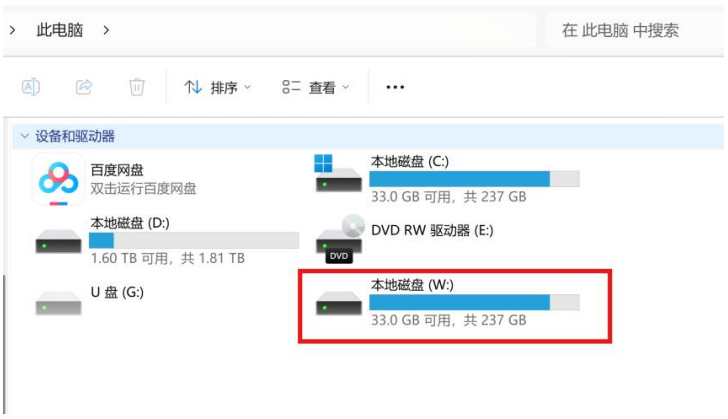
In Windows File Explorer, the size, used space, and available space of the W:`drive are consistent with the corresponding information for the disk where the encrypted file directory is located (by default, the encrypted file directory is on the C: drive, so the size and available space of the W: drive match the C: drive). Files stored on the W: drive also consume storage space on the corresponding disk.

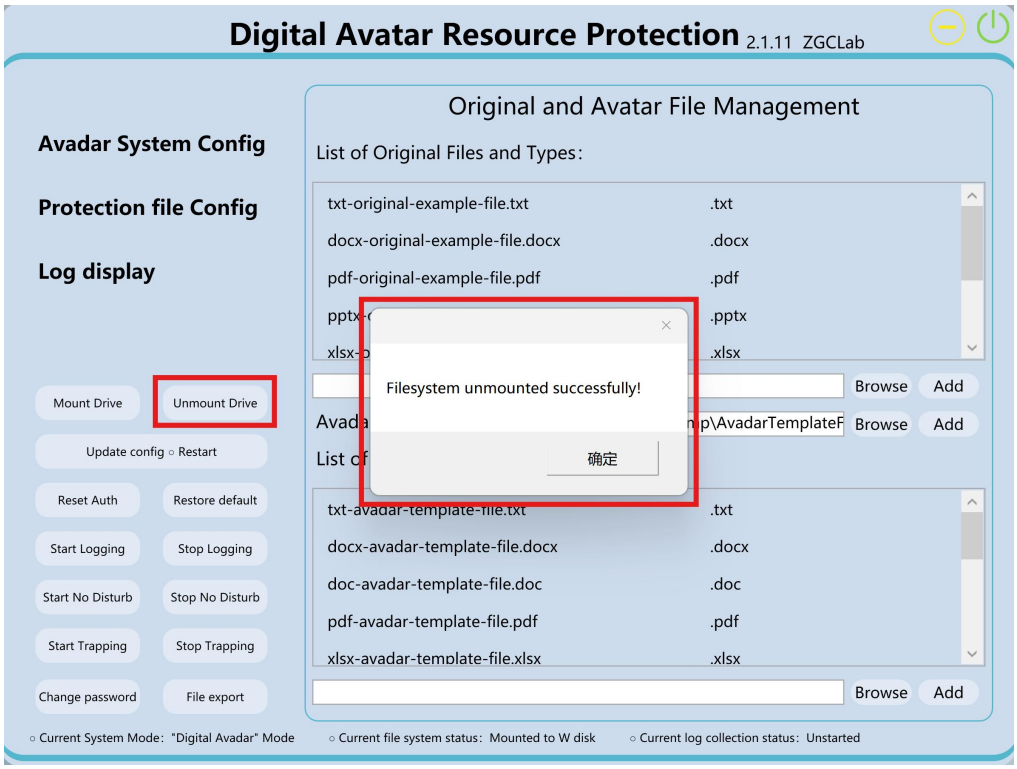
After a device restart, the GUI program will automatically launch and minimize to the system tray. The file system will be automatically mounted.

To unmount the file system, click "Unmount Drive" A prompt will appear, and after refreshing, the new drive letter will disappear.


Digital Avatar Resource Protection 2.1.11 ZGCLab
Avadar System Config
Protection file Config
Log display
Set system mount information
Encrypted disk mount path:
gramInstaller\SZTSConfig\szts_encdir
Browse
Confirm
Mount drive letter:
W
Confirm
Encrypted disk password:
Confirm
Set authentication information
Authentication time (minutes):
1
Confirm
Password timeout (seconds):
20
Confirm
Set log collection information
Log collection keywords (multiple keywords separate by commas):
SensitiveDocuments
Confirm
Mount Drive
Unmount Drive
Update config ○ Restart
Reset Auth
Restore default
Start Logging
Stop Logging
Start No Disturb
Stop No Disturb
Start Trapping
Stop Trapping
Change password
File export
○ Current System Mode: "Digital Avadar" Mode
○ Current file system status: Mounted to W disk
○ Current log collection status: Unstarted


Digital Avatar Resource Protection 2.1.11 ZGCLab
Avadar System Config
Protection file Config
Log display
Original and Avatar File Management
List of Original Files and Types:
txt-original-example-file.txt .txt
docx-original-example-file.docx .docx
pdf-original-example-file.pdf .pdf
The file system has been successfully mounted to W disk!
确定
Browse
Add
emplateF
Browse
Add
txt-avadar-template-file.txt .txt
docx-avadar-template-file.docx .docx
doc-avadar-template-file.doc .doc
pdf-avadar-template-file.pdf .pdf
xlsx-avadar-template-file.xlsx .xlsx
Browse
Add
Mount Drive
Unmount Drive
Update config ○ Restart
Reset Auth
Restore default
Start Logging
Stop Logging
Start No Disturb
Stop No Disturb
Start Trapping
Stop Trapping
Change password
File export
○ Current System Mode: "Digital Avadar" Mode
○ Current file system status: Unmounted
○ Current log collection status: Unstarted

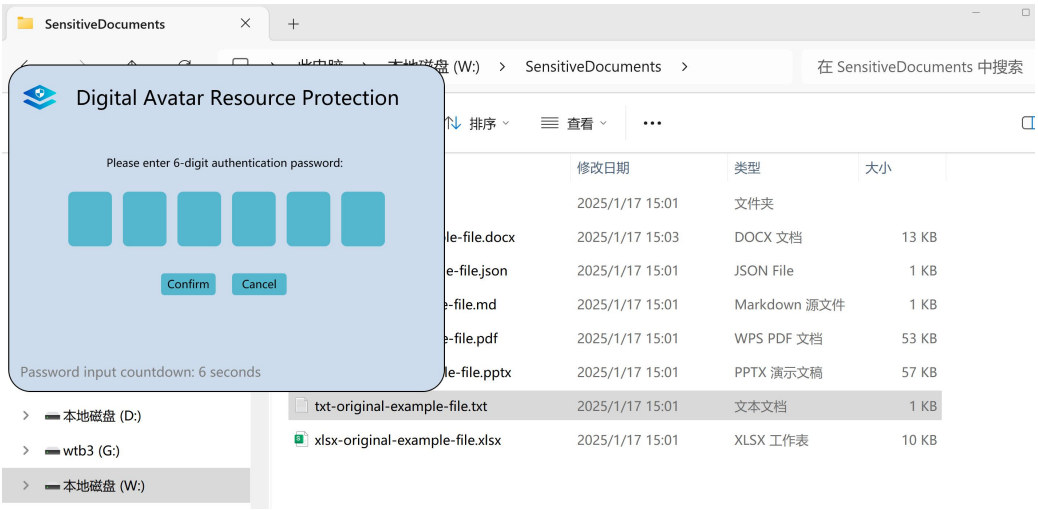




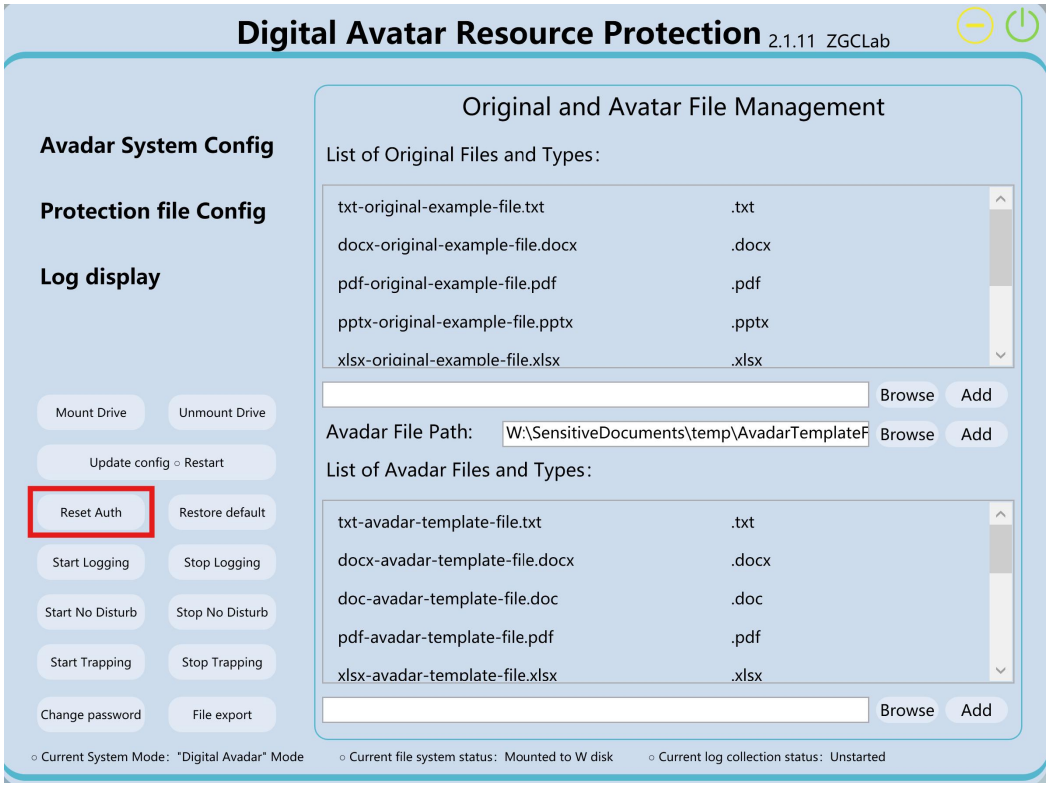
(2) Accessing Original Files

When opening an original file using an application, the program will display a pop-up window prompting the user to enter a password. If the password is correct, the file's correct content will be opened. For subsequent accesses to the original file on the same day, no further password input is required. If the password is incorrect, not entered within the timeout period (default is 20 seconds), or the user cancels input, the content of a avadar file will be opened instead. Subsequent access by the same application will continue to prompt for password verification.

Upon successful authentication, modifications will be written to the original file. Otherwise, modifications will be written to the avadar file.

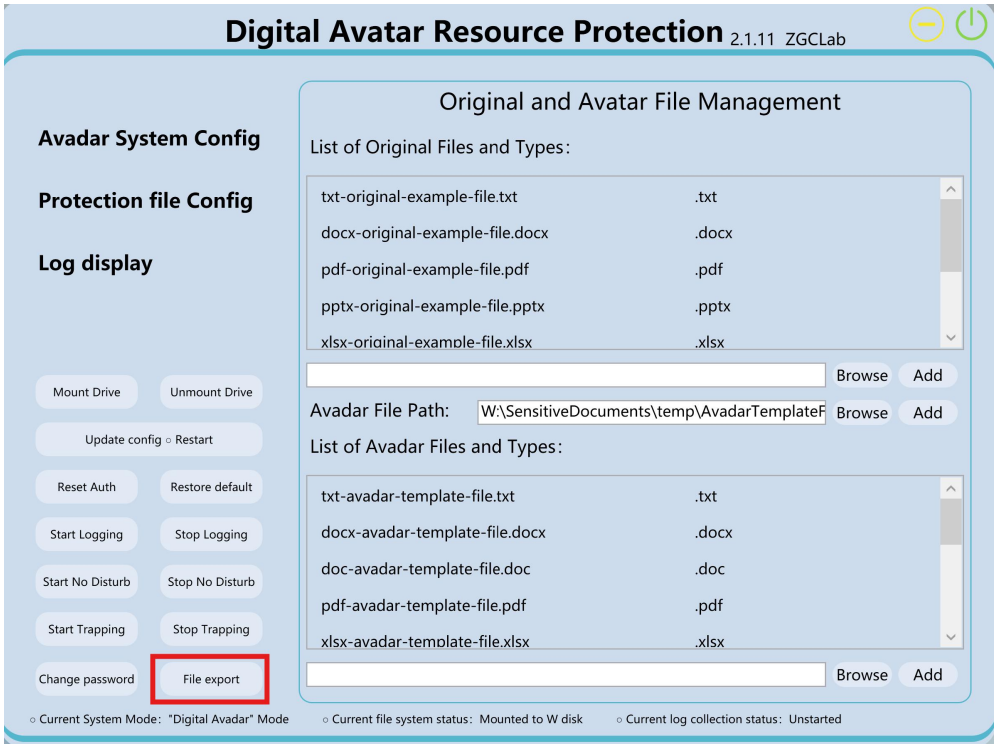


❖ **Note:** After successful authentication, subsequent authentications by the application will be completed in the background via private key signature verification. If authentication fails, the application will only be able to access decoy template files within the authentication validity period (default is 1 minute). Users can click the "Reset Auth" button to remount the file system and re-enter the password when accessing the original file again.



To export files from the W: drive to an external path, use the "File Export" function in the software GUI.

❖ **Note:** If a user directly copies a file from the W: drive to another path on the device, the copied file will not open correctly (e.g., showing as an empty file or with an invalid format).

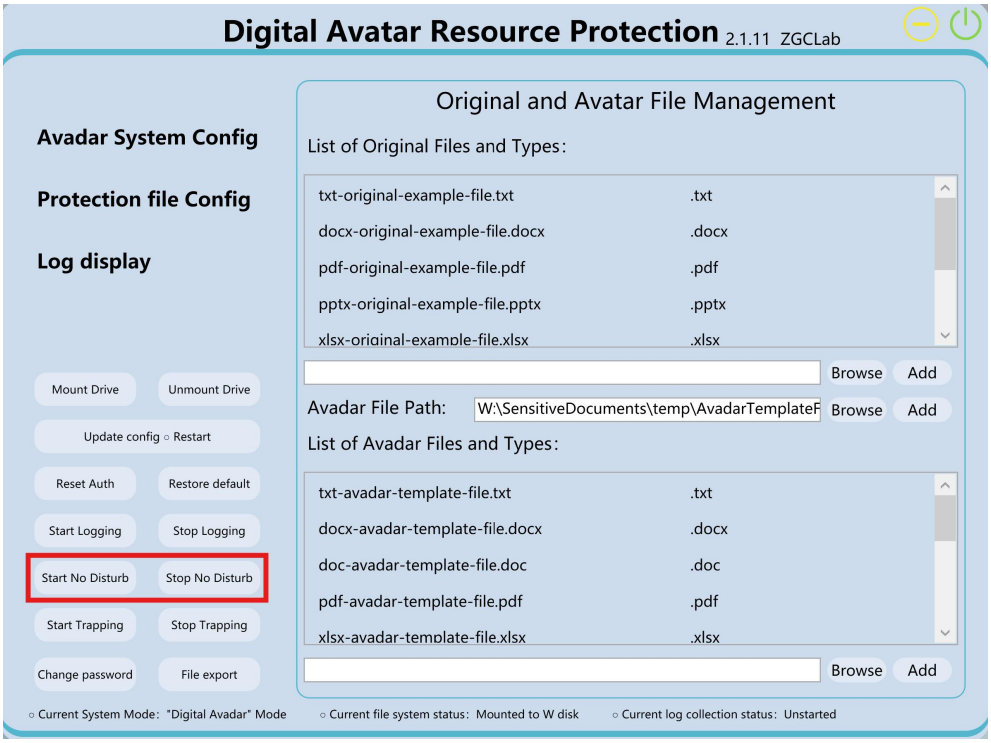


(3) Trap Mode and Do Not Disturb Mode

➢ **No Disturb Mode:**

When the user fully trusts the current device's operating environment, they can click the "Start No Disturb" button. After successful identity verification with the correct password, the program will remount the disk in No Disturb Mode. In this mode, all processes can open and modify original files without requiring verification.

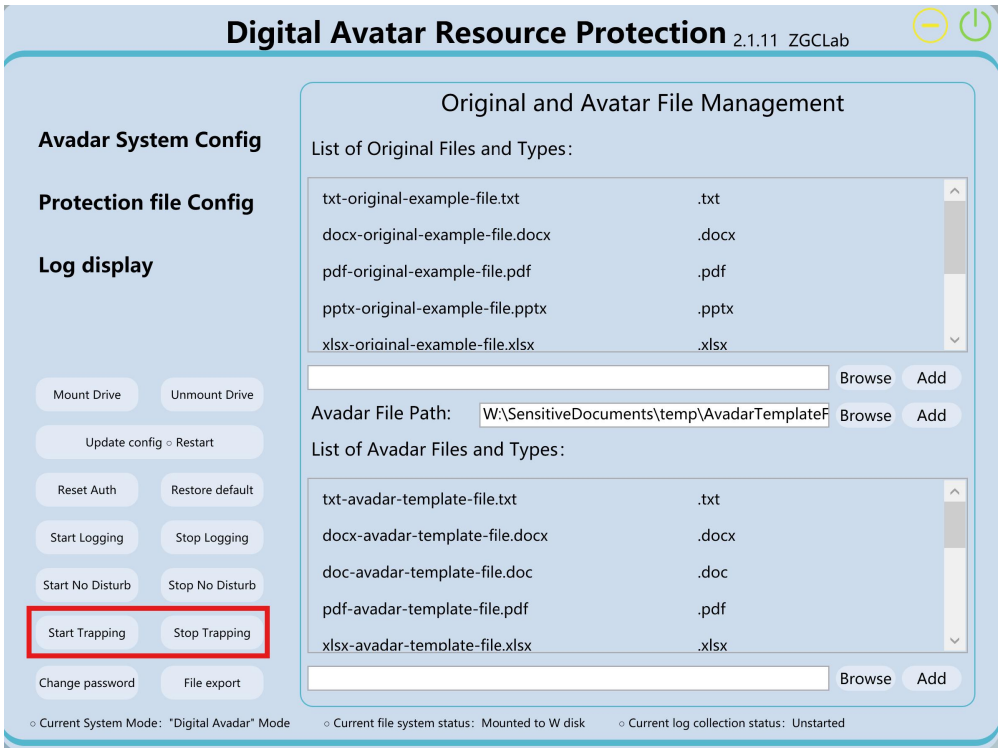
To exit this mode, click "Stop No Disturb" and the normal identity verification mechanism for accessing original files will be restored.



➢ **Trapping Mode:**

When the user temporarily leaves the device or does not need to operate on protected files, they can click the "Start Trapping" button. This remounts the disk in trapping mode, redirecting all attempts to open or modify original files to avadar template files.

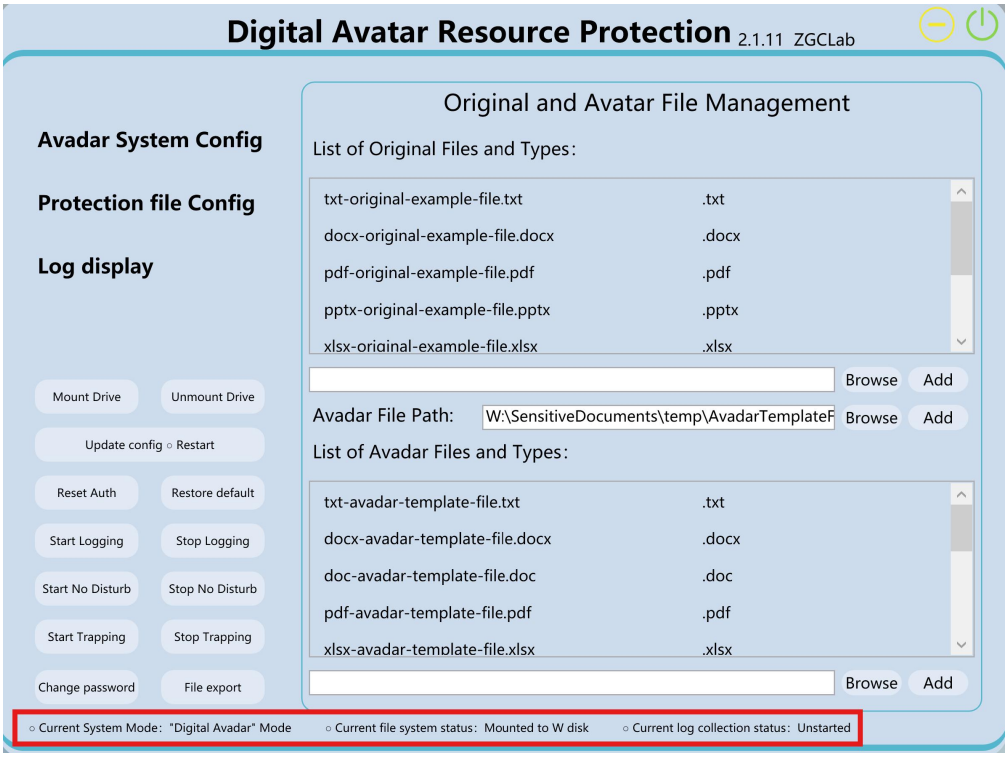
To exit this mode, click "Stop Trapping" and the normal identity verification mechanism for accessing original files will be restored.



(4) Viewing System Status

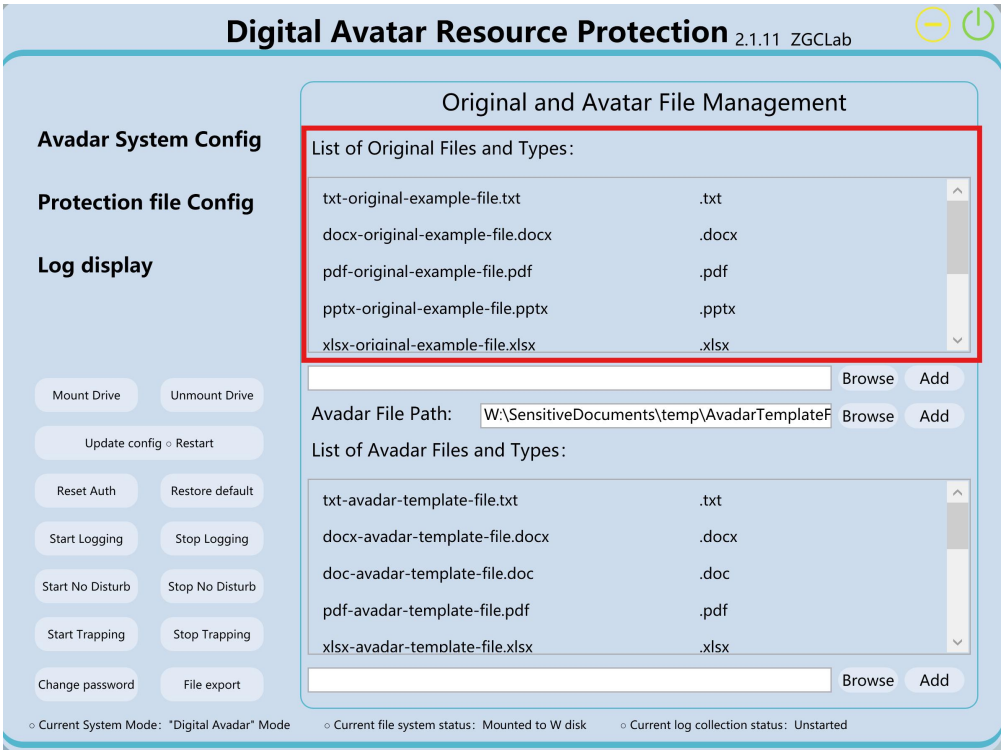
The bottom of the GUI interface of the "Digital Avadar" data resource protection software displays three groups of real-time system status information:

- Current System Mode: “Digital Avadar” Mode / No Disturb Mode / Trapping Mode.
- Current File System Status: Mounted to W disk / Unmounted.
- Current Log Collection Status: Started / UnStarted.



(5) Updating Original File List and Avadar Template List

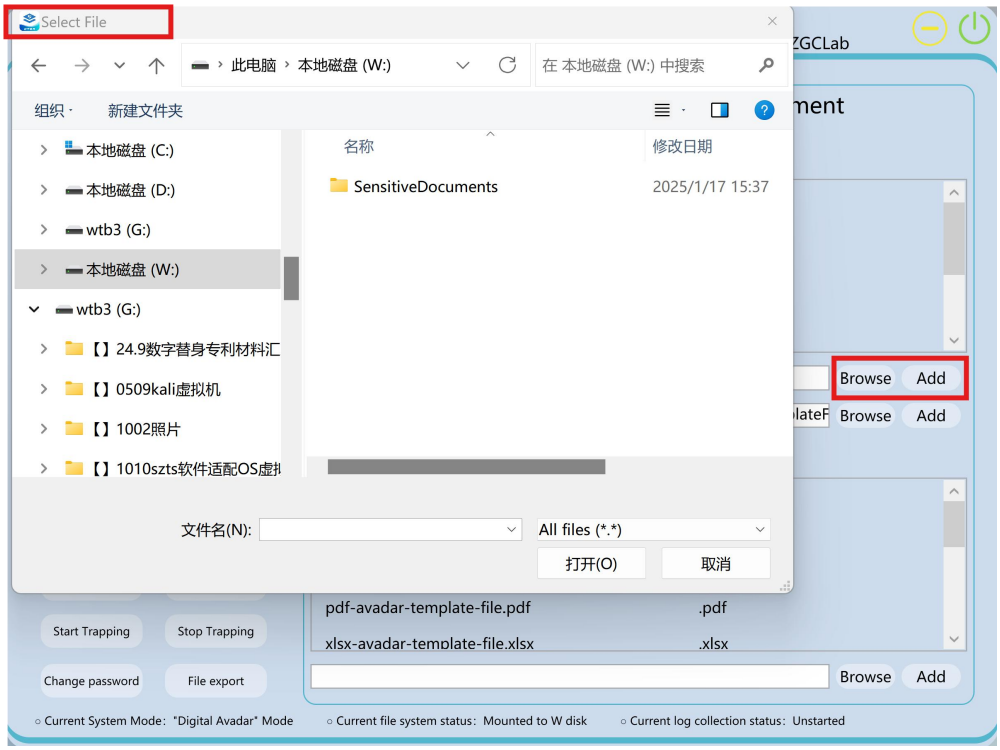
The “Protected File List Config” -> "List of Original Filesand Types" window displays 7 default protected original files.

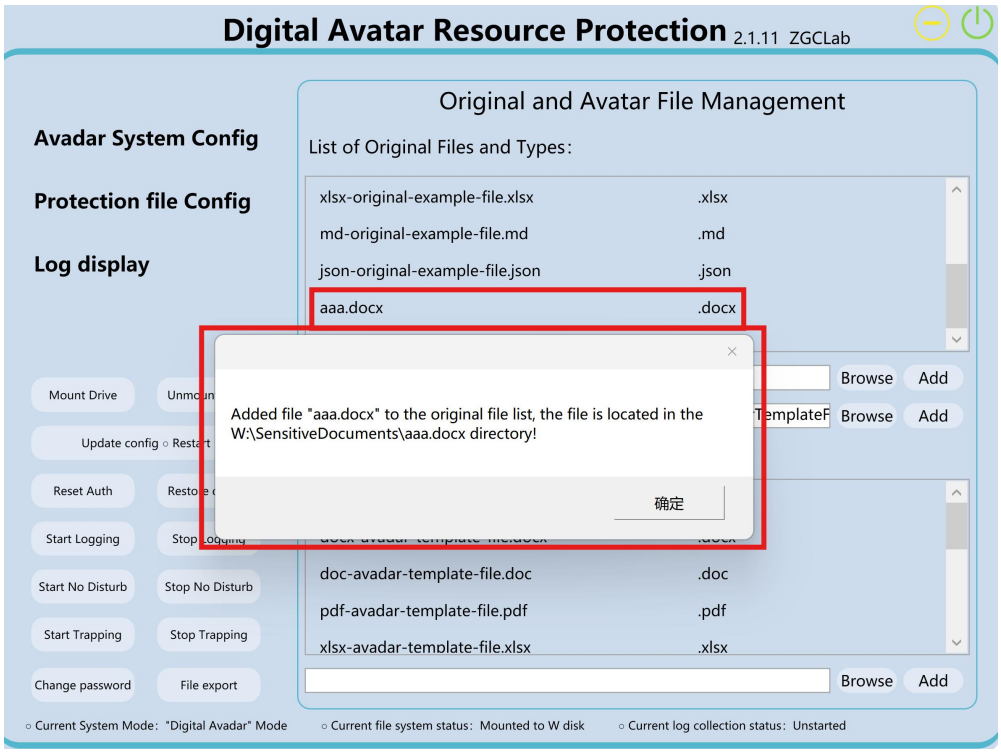


- **Adding Original Files:**

Click the "Browse" button on the right of the text box, select the target file, and click "Add." The system will automatically recognize the file extension type and add it to the configuration file.

If the selected file already exists in the W: drive or if it was created within the W: drive, no copying or overwriting will occur.



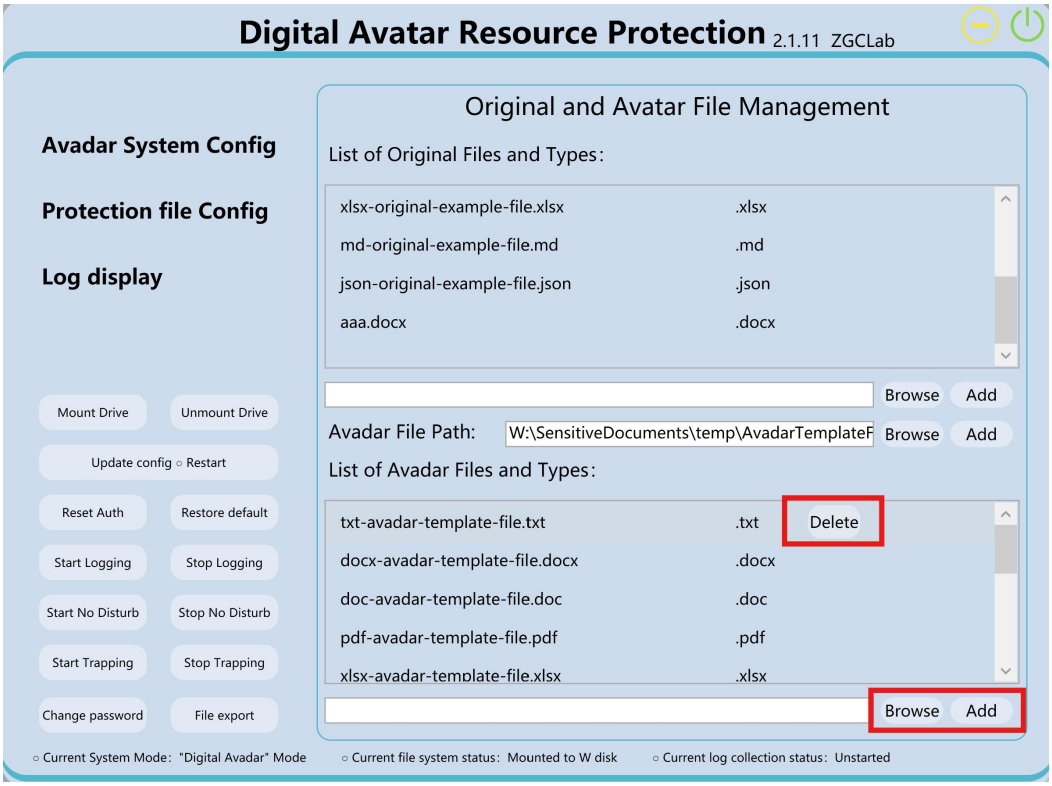


➢ **Deleting Files:**

Removing a file from the list only updates the configuration for protected file names. It does not delete the actual file from the virtual drive (e.g., W:).

➢ **Updating Avadar Templates:**

To update a specific file type's avadar template, delete the current decoy template in the list. Then, use the "Browse" button to select a new template and click "Add." After configuration, click "Update System Config · Restart" for the changes to take effect.

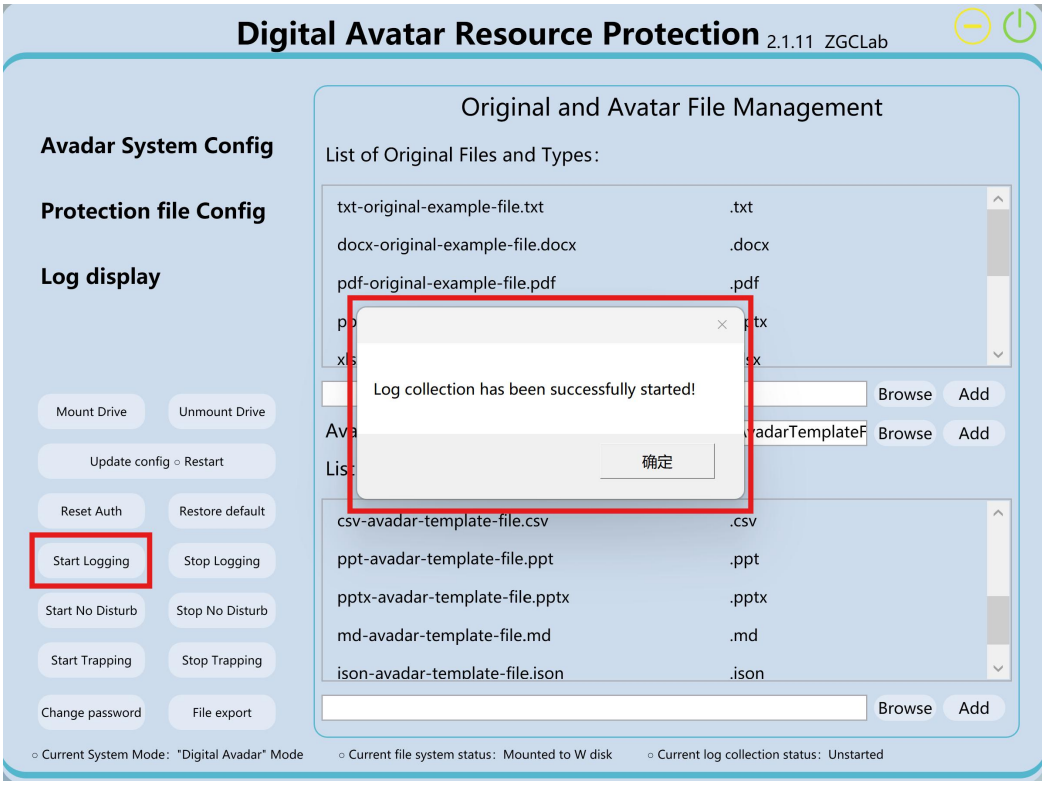


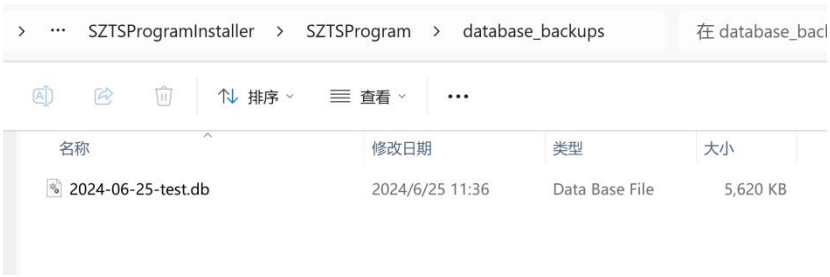
(6) Log Collection

➢ **Starting Log Collection:**

Click "Start Logging" to enable the program to record file system operations on the virtual disk.

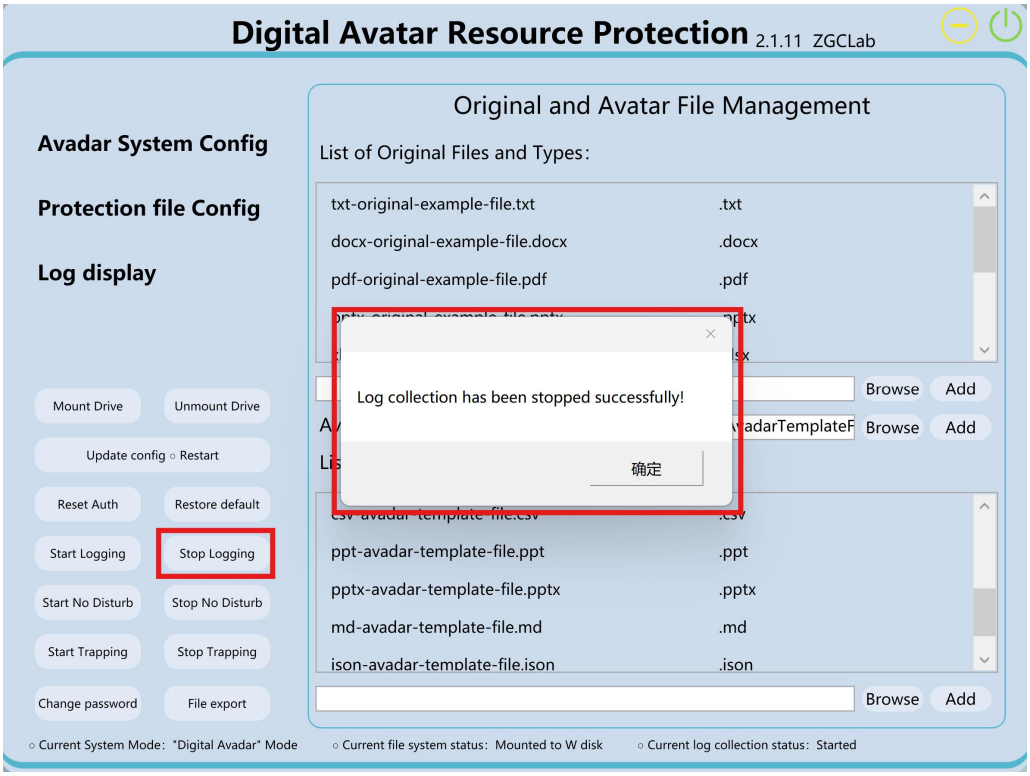
Collected log data is parsed and stored in the database file C:\SZTSProgramInstaller\SZTSProgram\test.db. Backup files are automatically created daily at 8:00 AM and stored in C:\SZTSProgramInstaller\SZTSConfig\database_backups.





➢ **Stopping Log Collection:**

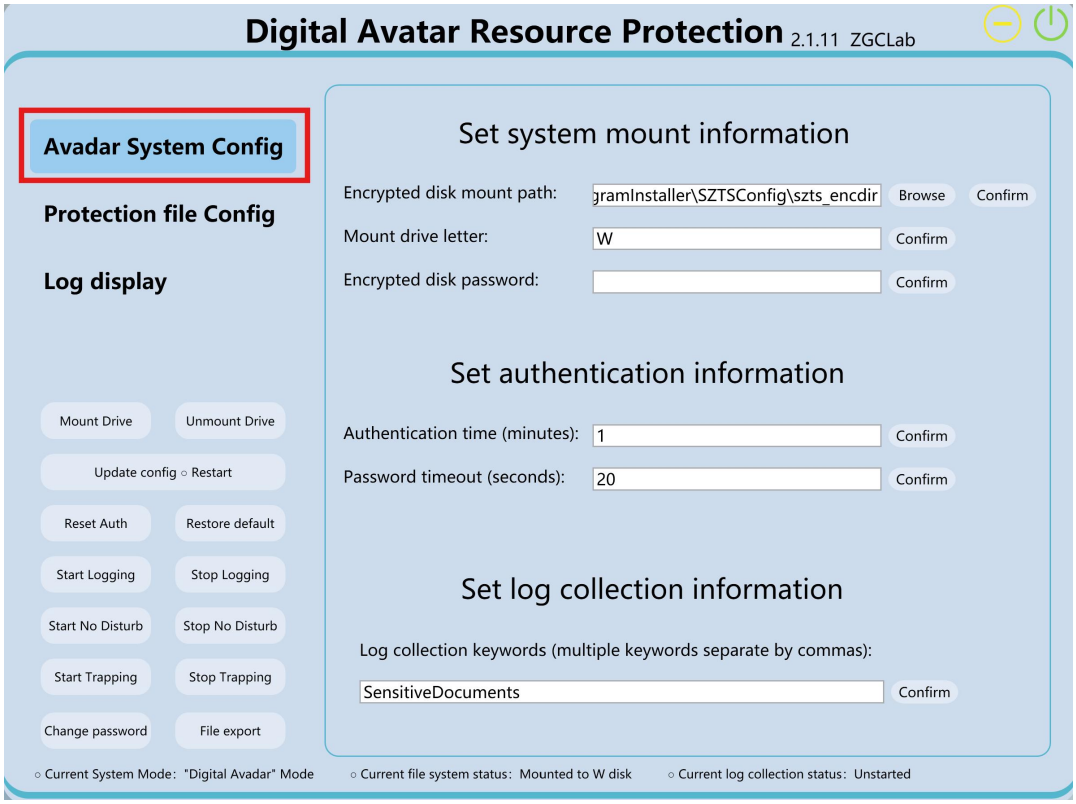
Click "Stop Logging" to terminate the logging process.



(7) System Configuration

Users can customize the following settings:

- Mount Path: Specify the path for the encrypted file directory.
- Authentication Settings: Configure password authentication options, including the timeout period (default: 20 seconds) and the password (default: "123456").
- Log Keywords: Define keywords for log filtering, separated by commas (default: "SensitiveDocuments").


Digital Avatar Resource Protection 2.1.11 ZGCLab
Avadar System Config
Protection file Config
Log display
Mount Drive
Unmount Drive
Update config ○ Restart
Reset Auth
Restore default
Start Logging
Stop Logging
Start No Disturb
Stop No Disturb
Start Trapping
Stop Trapping
Change password
File export
Set system mount information
Encrypted disk mount path:
gramInstaller\SZTSConfig\szts_encdir
Browse
Confirm
Mount drive letter:
W
Confirm
Encrypted disk password:
Confirm
Set authentication information
Authentication time (minutes):
1
Confirm
Password timeout (seconds):
20
Confirm
Set log collection information
Log collection keywords (multiple keywords separate by commas):
SensitiveDocuments
Confirm
○ Current System Mode: "Digital Avadar" Mode
○ Current file system status: Mounted to W disk
○ Current log collection status: Unstarted