SecureAge® MySecureDrive

User Guide

Version 3.0

October 2008

Table of Content

1 MySecureDrive

MySecureDrive is a software tool to protect your files in removable drives such as USB thumb drive, CD, external hard drive or local non-system drive. It provides 256 bits AES encryption to protect sensitive files in your removable drives. Ideally, you should copy *MySecureDrive* to the removable drive and run it from that location. In the basic transparent mode, it provides automatic encryption / decryption to the files and requires no modification to desktop applications. It also provides manual file encrypt / decrypt using Drag & Drop from Explorer, so that you can protect certain files in your local drive or network drive.

For a new machine, MySecureDrive will add registry keys to allow transparent file encryption and shell icon integration. Admin privilege is required and it will prompt you to allow its setup program (MSDSetup.exe) to continue in Windows Vista. The next time onwards it will run with limited user privilege.

2 Unique Features in *MySecureDrive* Version 3.0

This version of *MySecureDrive* has some exciting features, including:

- Protect sensitive data in removable drive using AES 256-bit encryption
- Able to use different passwords to encrypt different sets of files
- No change in filename when a file is encrypted, thus allow file search based on filename, and retain the same icon as the plain file
- Explorer integration to visually distinguish encrypted files with custom icons
- Allow limited user to use the tool, except running it the first time which required administrator privilege
- No installation required, small footprint, single executable
- Two modes of operation: Basic and Manual

Basic transparent mode:

- Transparently encrypt files when copy to removable drive from any location
- Transparently decrypt files when copy from removable drive to local hard drives
- Open encrypted files in removable drive, including CD/DVD, content will be decrypted on-the-fly
- Edit encrypted files in removable drive, updated content will be automatically encrypted on-the-fly
- Optionally support local data drive (exclude operating system drive) to protect user files
- No change in existing applications such as Microsoft Office, they can read/write encrypted content in the removable drive
- No compromise in performance in transparent mode

Manual mode:

- Support Drag & Drop operations from Explorer
- Support temporary password to share secret files among friends
- Support encrypt / decrypt multiple files or directories in any drive including local, removable and network drives
- Support whole directory (including all files in sub-directories) encryption / decryption
- Display encryption status of files and directories
- Display completed status of files and directories in real time
- Display processing time of each file and directory

3 System Requirement

MySecureDrive can run in the following Windows operating systems:

- Windows 2000 with Service Pack 4 and Update Rollup Pack
- Windows XP with Service Pack 2 and above
- Windows XP Media Center Edition 2005 with Service Pack 2 and above
- Windows Server 2003 with Service Pack 1 and above
- Windows Vista

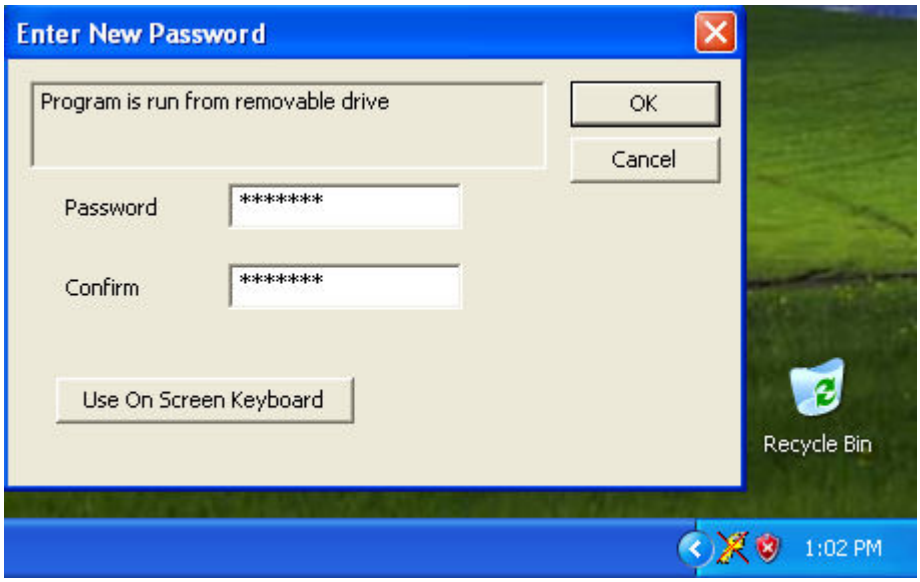
4 Upgrade from older version (version 2.3 and below)

Due to security enhancement in the version 3.0, the encryption format is **changed** and **not compatible** with the old version of *MySecureDrive*. The format of the **.hash** file also changed and not compatible, it will be regenerated to the new format. If you use *MySecureDrive* version 2.3 previously, please follow the step listed below to migrate to the new format:

- Decrypt all the files in your removable drive using the older version of *MySecureDrive*. You can download older versions of *MySecureDrive* from http://www.mysecuredrive.com/archive/MySecureDrive_V2.3.zip In Manual Encrypt / Decrypt mode, drag the whole drive from Windows Explorer to the dialog box and press Decrypt button.

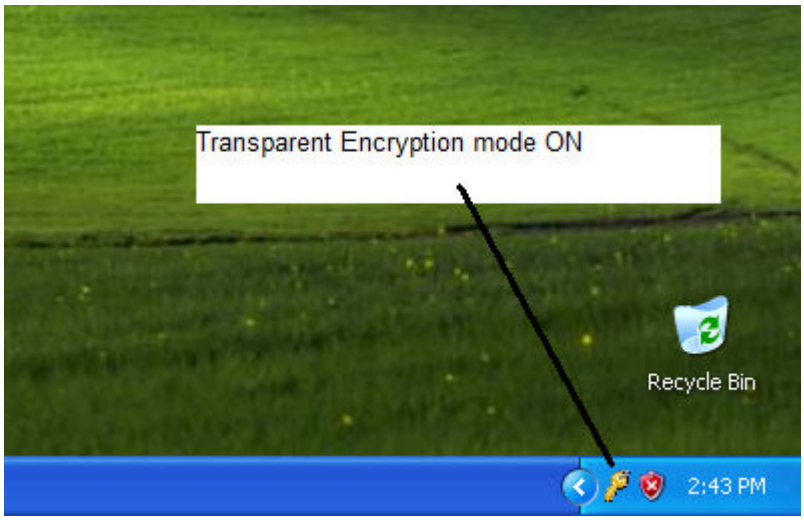
5 Basic Transparent Mode

When you start *MySecureDrive*, it will ask for a password which is used for the whole session. For better security, use 'On Screen Keyboard' to input the password. The 'On Screen Keyboard' can also be used for typing passwords with non-standard characters in them or typing passwords in a foreign language.



When the Transparent Encryption Mode is OFF, a red X mark will appear as shown above. This means that no automatic encryption will be performed on any files created / copied to the removable drive.

After you enter a new password, the program will turn ON the Transparent Encryption mode as shown below.

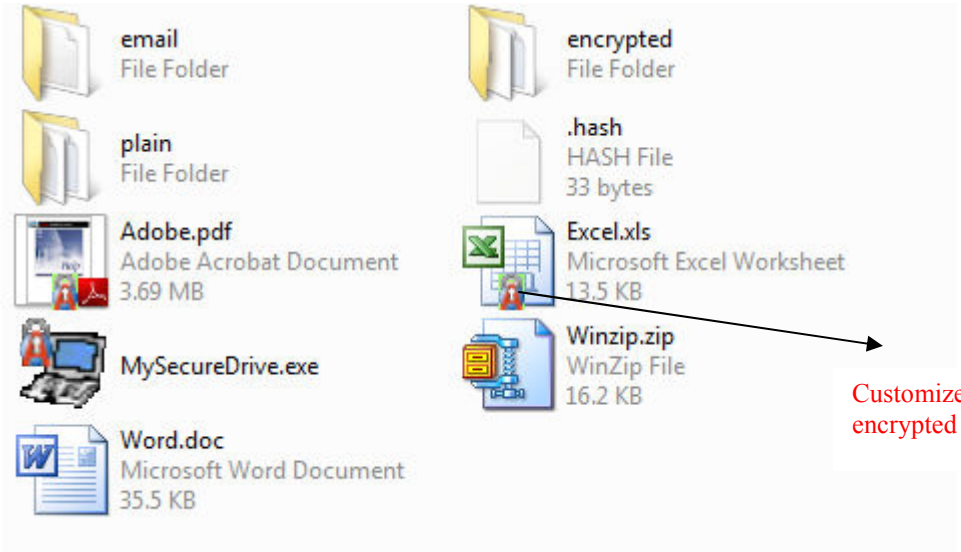


Remember this password or store it in a safe place. The password is required the next time you want to open the encrypted files. There is a built-in password verification process when you run *MySecureDrive* from a removable drive. If the password is not found, it will prompt the user to add the new password hash in the verification process or cancel the operation. No password verification is performed when you run the *MySecureDrive* from a local drive.

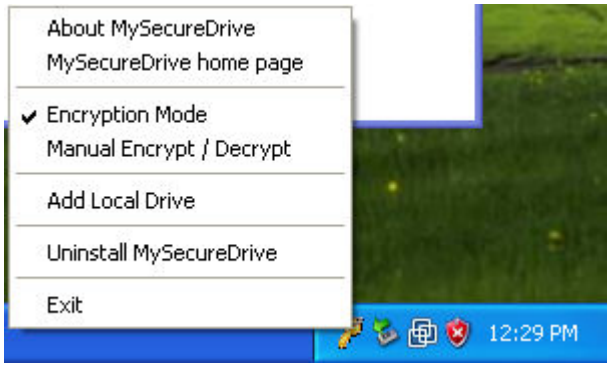
MySecureDrive supports multiple passwords. This allows you to encrypt a set of files using one password and another set of files using another password. **It is your responsibility to remember these passwords; without the passwords, there is no way to RECOVER your files.**

With Transparent Encryption mode, you can copy any file to your removable drive and *MySecureDrive* will automatically encrypt it for you. The file will appear as if it is a plain file. You can edit the file as per normal and new content will be encrypted as well. For existing file which is plain, you can still open or edit the file, but the modified content may then be encrypted; this encryption behavior depends on your application that opens your file.

All encrypted files have customized icons, which overlays a small lock on the existing icon as shown below:



Right-click on the icon at the taskbar will display the following menu. The Encryption Mode is ticked to indicate Transparent Encryption mode is ON.



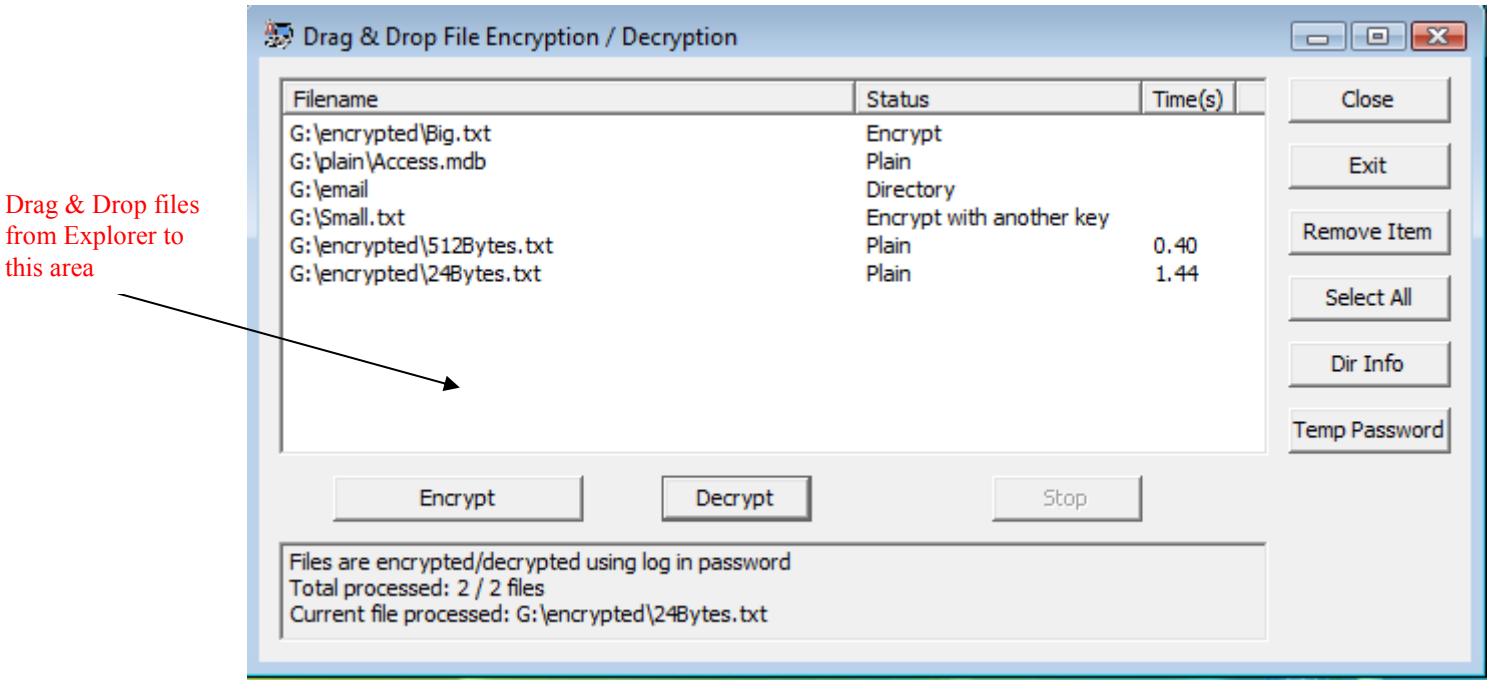
MySecureDrive also optionally support transparent encryption / decryption on local data drives. To enable this option, you can select 'Add Local Drive' option as shown in the above figure. Please note that operating system drive such as Drive C is not supported. Whatever files you copied to the local drive will be encrypted automatically using the log in password.

To disable Transparent Encryption mode, just unselect the 'Encryption Mode' menu item. In this mode, all files copied to removable drive will be plain. This mode is required if you would like to send files in your removable drive as encrypted to third party using email or file transfer application. If you want to copy encrypted files from your removable drive to a local drive and the new file remains encrypted, you should also disable Transparent Encryption mode.

You can also manual encrypt/decrypt files by selecting the item "Manual Encrypt / Decrypt' as shown above, or click on the *MySecureDrive* taskbar icon.

6 Manual Mode

You can selectively encrypt / decrypt files or directories on your removable drive, local hard drives or network drive as shown below:



Drag any files using the mouse to the dialog box and it will show your file encryption status. You can choose to decrypt / encrypt a file, multiple files and directories. The 'Dir Info' button can be used to display status of the files in one directory. To sort the files based on filename or status, click on 'Filename' or 'Status' bar respectively. If a file is encrypted manually, it will be transparently decrypted when you open the file in Transparent Encryption mode; however, this is only applicable to the file resides in removable drives.

If you want to share an encrypted file with friends using a shared password, you can choose 'Temp Password' option. This allows you to manual encrypt / decrypt files using this temporary password. To remove temporary password, click 'Temp Password' button again and don't input any password. You can find out whether current files are encrypted using temporary password or log in password from Information text area.

If the encrypted file is stored in removable drive, you should disable the Transparent Encryption mode to prevent auto-decryption when copy out the file. Now you can copy the file to your network drive or send it using email, web upload or FTP program and the transmitted file will remain encrypted.

During manual encrypt / decrypt file operation, you can cancel the operation by clicking 'Stop' button. The operation will stop once the current file encryption / decryption process finishes. If you click 'Close' button, it is the same as cancel operation but the dialog box will be closed.

7 UDF Support in Windows Vista

Windows Vista supports UDF file system to treat DVDRW disc as if it is a removable media, no CD/DVD burning software is required. To enable this feature, you should format the disc using Explorer to UDF file system. Then you will be able to copy files to the disc and edit them as per normal. The same disc can be read in Windows XP, but the disc is treated as read-only in Windows XP. In *MySecureDrive* version 2.1 and

above, it can support both transparent and manual modes for UDF file system in Windows Vista. This is useful if you want to back up your personal files to DVDRW media in Windows Vista and they are protected.

8 Uninstall MySecureDrive

To remove registry settings that was added by *MySecureDrive*, you can right-click *MySecureDrive* icon and choose 'Uninstall *MySecureDrive'* option. The uninstall option requires admin privilege and it will automatically prompt you if the current user belongs to limited user account.

9 Contact Us

For more information, please feel free to contact us at: contactus@secureage.com.