Quick Start Guide

Welcome to **SecurFlash**™, **Version 8.2** software from encryptX Corporation (www.encryptX.com) . The SecurFlash software encrypts and hides sensitive information on removable drives such as USB flash drives, removable hard drives, and also works to encrypt and hide files on your local PC hard drive. Encryption is designed to prevent unauthorized access to confidential data, such as files for corporate projects, personal finances, entertainment (e.g. video and audio files) or can be used as a repository to store all your other usernames and passwords in a central and hidden location. When you encrypt files through the SecurFlash application, they are also hidden on the drive from the PC Operating System so that they can only be seen and opened by first running the SecurFlash application and providing the password.

Supported Operating Systems. The software is supported on Microsoft Windows 2000, XP Home, XP Pro, and Vista. The software is not supported on Windows 95, Windows 98, Windows Me, Linux, or any of the Macintosh operating systems. You can encrypt and hide any type of file supported by the Microsoft Windows Operating System through the SecurFlash software.

Important Product Use Concepts

1. **Use of the SecurFlash software is not mandatory to the use of the drive**. If you do not want to encrypt and hide files on the drive that the software is installed on you can simply drag and drop or save files to the drive within your application or copy files using Windows Explorer.
2. **If you forget both your password and recovery hint you will not be able to access the encrypted and hidden files on the drive unless you have upgraded**. You will need to remember either your password or your recovery hint question to be able to access your encrypted and hidden files. If you are concerned about forgetting your password and recovery hint, you should consider upgrading to the "Corporate Version" of the SecurFlash software by running the selecting the **Tools > Upgrade** menu selection from within the SecurFlash application. You do not have to reinstall or download new software. You will have to pay a small fee to upgrade – which is explained in the "Learn more about Corporate Features" dialog box when you select **Tools > Upgrade** from within the SecurFlash application. The Corporate Version of the software integrates with a web accessible server application that provides Administrator password recovery for users that forget their password and recovery hint, provides audit tracking of encrypted file system content, provides dynamic revocation of authorized password access to encrypted file system content if the drive is lost/stolen and the password is compromised, and provides optional enforcement of strong passwords and periodic password changes.
3. **It is very important to understand that when you encrypt files using the SecurFlash software they are stored in a hidden and encrypted file system on the drive.** The encrypted files and folders that you have protected through the SecurFlash software are not visible to applications or the Microsoft Windows Operating System. You cannot launch these files directly from the drive from within the Operating System or from within other applications, such as Microsoft Office. The only way to access these files is to run the EncryptX SecurFlash application by double clicking the **Run SecurFlash.exe** from the drive where it is installed and providing the correct password. Only then will you be able to see the hidden and encrypted files and folders that you have previously stored in the encrypted file system on your drive. You can then open the files and modify them within your applications by double clicking the files that are shown to you in the SecurFlash encrypted and hidden file system.
4. **You can open and edit your files from within the SecurFlash software and any changes will be automatically saved.** Any edits you make to files that you have previously encrypted and are opening from within the SecurFlash application will be automatically saved back in to the hidden and encrypted file system on the drive, when you SAVE or EXIT your application. If you perform a SAVE AS, the SecurFlash application assumes you want to save your changes outside of the encrypted file system on the drive.

I. Running the SecurFlash Application

The SecurFlash software may have been pre-installed on your drive. The first time you run the application you will be asked to accept a license agreement and to establish your password and password recovery hint.

1. If the **Run SecurFlash.exe** file is not already present on your drive:
   a. Download the SecurFlash installation file from the encryptX website (www.encryptx.com) in the download directory.
   b. Connect the removable drive to a PC.
   c. Double-click the installation file to install the **Run SecurFlash.exe** file to the drive.
2. If the Run SecurFlash.exe is already present on your drive, then Double-click the **Run SecurFlash.exe** file.
3. Review the license in the **EncryptX SecurFlash End User License Agreement** dialog box.
4. To accept the license agreement, click **I Accept**. (If the user does not accept it, they cannot use the software.)
5. For Corporate mode setup, in the **SecurFlash Server Setup** dialog box, enter the server connection URL in the **Security Server URL** box if the URL is not already displayed and enter your email address. You will also be required to verify your email address by entering it a second time. Then click **OK**.

   – or –

   If the server connection URL is displayed, click **OK**. If you want to learn more about Corporate mode setup and features, please read Section IX of this document.

   Note: The **SecurFlash Server Setup** dialog box only displays during Corporate mode setup.
6. In the **SecurFlash User Setup** dialog box, enter the password, hint information, and click **OK**. The **EncryptX SecurFlash** window that enables the user to perform encryption operations displays.

   Note: The password is case-sensitive and the hint answer must be eight characters or longer.

II. Encrypting

The left pane of the **SecurFlash** main window contains a **My Files** folder which is a default folder provided in the application to organize your encrypted files. It functions similar to the **My Documents** folder on your PC. You can also create new folders at the same level as **My Files** or subordinate folders under **My Files** and rename folders based on your personal preferences.

There are several methods for encrypting files and folders: dragging-and-dropping files and/or folders into the Left or Right Pane of the SecurFlash main window, clicking on the Encrypt button in the toolbar, or selecting Encrypt from the File Menu in the SecurFlash Application.

1. To add folders and/or files through dragging-and-dropping, open Windows Explorer, if it is not already open.
2. In Windows Explorer, select one or more files and/or folders.
3. Drag-and-drop the selected items onto a location in the **SecurFlash** window.

   – or –

1. In the **SecurFlash** window, select the folder location where you want to store the encrypted file or create a New Folder and encrypt files to that location. **NOTE**: These folders are hidden from view on the drive when you are not using the SecurFlash application.
2. Click the toolbar button for adding files.
3. In the **Select Files for Encryption** dialog box, select one or more files to encrypt and click **Open**.

III. Decrypting

When the user decrypts files, the SecurFlash software decrypts the files to the user specified location. A copy of the original encrypted files will remain in the encrypted file system until deleted.

After the decryption of a file or folder, the decrypted item is not protected and can be freely used. The user can choose to decrypt files to a hard or networked drive as well as to removable storage media.

The user can decrypt files through the **SecurFlash** window interface or by selecting the files in this window and dropping them onto a location in Windows Explorer.

Decrypt through dragging-and-dropping

1. In the left pane of the **SecurFlash** window, select the folder that contains the file (s) to decrypt and select the file (s) in the right pane.
   a. Drag-and-drop the selected items onto a folder displayed in Windows Explorer – or directly to the desktop.
   b. If you have your application open (e.g. Microsoft Word, Excel, Powerpoint, Media Player, etc.) You can also decrypt by dragging and dropping the file from the SecurFlash window directly on to the associated application. This will automatically decrypt the file and display it within the application.

Decrypt through the SecurFlash Decrypt Button

1. In either pane of the **SecurFlash** window, select a folder to decrypt.
   – or –
   In the left pane of the **SecurFlash** window, select the folder that contains the file (s) to decrypt and select the file (s) in the right pane.
2. Click the toolbar button for decrypting files.
3. To decrypt a folder or multiple files, in the **Browse for Folder** dialog box, select the location for the decrypted content and click **OK**.
   – or –
   To decrypt a single file, in the file saving dialog box, select the location for the data and click **Save**.

IV. Opening and Updating Encrypted Files

If the user opens an encrypted file, modifies the file and saves it, the SecurFlash software adds the modified version to the encrypted file system and hides the previous version.

To open a file, double-click the file shown in the **SecurFlash** window.

– or –

Select the file and click the toolbar button for opening files.

As long as there is an application associated with the file type installed on the PC, the file immediately opens in the application.

Note: To add the modified version of an opened file to the encrypted file system, the user can save the changes before closing the file and application.

V. Deleting Files

To increase the available space on the removable drive, the user can delete files from the encrypted file system. There are several ways to delete encrypted files, each having different consequences.

Encrypted files can be marked for deletion so that they no longer appear in the user interface but are still in the encrypted files. To permanently delete the files, the user can **Empty** the files and folders from the encrypted file system.

A. Mark Files and Folders for Deletion

When files and folders are marked for deletion, the encrypted file system size does not diminish initially because they have not yet been emptied from the file system. To permanently delete the files are recover space on the drive you must also **Empty** the files/folders that you marked for deletion. Files can be marked for deletion first and their space recovered later.

1. In the **SecurFlash** window, select one or more files to mark for deletion.
2. Click the **Delete** toolbar button for hiding and marking files for deletion.
3. In the confirmation box, click **Yes**.

B. Empty encrypted files and folders from the removable drive

The user can empty previously encrypted files and folders from the drive by selecting the **Empty** button from the SecurFlash toolbar. Two options are provided by selecting the down arrow next to the **Empty** button - **Empty** and **Empty All**. If you select **Empty** only files and folders that you previously marked for deletion will be removed from the drive. **If you select Empty All all files and folders in the encrypted file system will be removed.** When the encrypted container is emptied, the encrypted container auditing information is also deleted.

1. In the **SecurFlash** window, click the **Empty** option of the toolbar button to remove previously marked files and folders for deletion.
2. In the **Confirm Empty Encrypted container** confirmation box, click **Empty Now**.
3. Or select **Empty All**. This will empty **ALL** encrypted files and folders stored on the drive.

VI. Password Management

The password recovery feature enables recovering the encrypted file system password if it has been forgotten. After unsuccessfully trying to log in, the user can use the hint answer that they previously entered when setting up the encrypted container to recover their password. Also, the user can modify their password and/or hint question and answer at any time from within the application

A. Recover password

1. When trying to access the encrypted container:
   In the **SecurFlash Login** dialog box, click **Recover Password**.
   – or –
   a. Enter anything in the **SecurFlash Login** dialog box and click **OK**.
   b. In the **SecurFlash Login Failure** dialog box, select **Attempt password recovery** and click **OK**.

   Note: Instead of going through the password recovery process, the user can re-attempt to log in by selecting **Enter new password** and clicking **OK**. The **SecurFlash Login** dialog box displays again.
2. In the **SecurFlash Password Recovery** dialog box, enter the hint answer into the **Response** box and click **OK**.
3. In the **SecurFlash Password Recovered** dialog box, click **OK** after noting the password.
   The **SecurFlash Login** dialog box displays.

B. Modify password

1. In the **SecurFlash** window, click **Password** on the **Tools** menu.
2. In the **Change Password** dialog box, enter the existing password in the **Old Password** box.
3. Enter a new password in the **New Password** box, confirm it, and click **OK**.

C. Modify hint question and answer

1. In the **SecurFlash** window, click **Hint** on the **Tools** menu.

2. In the **Change Password Hint** dialog box, enter a new hint question and answer and click **OK**.

VII. Auditing

The SecurFlash software tracks files that have been encrypted and stored in the encrypted and hidden file system on the drive.

1. Click the **Audit** toolbar button.
   The **Audit History** dialog box that lists encrypted files/folders and user actions is displayed.
2. You may optionally decrypt a file or folder from the audit report by selecting a file in the displayed item list, and clicking the **Decrypt** button in the dialog box.
3. After auditing, click **Close** to close the **Audit History** dialog box.

VIII. Product Version Upgrades

SecurFlash versions prior to 8.1 used 128-bit encryption. Versions beginning with 8.1 and later use 256-bit encryption. When upgrading from versions prior to 8.1 to a later version, you will continue to use 128-bit encryption. If you wish to strengthen your encryption to 256-bit, you will need to follow these steps:

1. Copy all non-encrypted files from your USB drive to your PC Hard Drive
2. Decrypt all of your encrypted files to your PC Hard Drive
3. If you are sure you have backed up all your files to your PC Hard Drive, then Quick Format your USB drive
4. Re-install the current version of SecurFlash on your USB drive
5. Run SecurFlash on your USB drive
6. Re-encrypt your files by dragging and dropping your files into the SecurFlash main window
7. Restore your non-encrypted files from your PC Hard Drive to your USB drive

IX. Corporate Mode

When the software has been upgraded and is operating in Corporate mode, the SecurFlash Corporate Edition software communicates with a web accessible Security Manager application that provides advanced administrative features including remote password administration and recovery, drive auditing features, and the ability to dynamically revoke access to the encrypted files on the drive it if is lost or stolen, or the password is compromised. The user must be online and connected to the Security Manager Application Server through either a corporate network or the Internet to use the SecurFlash Corporate Edition software for the first time in Corporate mode. The user may also be required to be online with the Security Server on a periodic basis to ensure the audit trail is kept up to date and to communicate the need for the user to make password changes.

A. Upgrade to Corporate mode

1. In the **SecurFlash** window, click **Upgrade** on the **Tools** menu.
2. In the **SecurFlash License Upgrade** dialog box, enter the server connection URL in the **Securit Serve**r URL box if the URL is not already displayed.
3. Enter your email address and verify it by typing it in twice in the provided fields.
4. Click **OK**.

B. View server connection information

The **About SecurFlash Corporate Edition** dialog box displays information about the connection to the corporate server and the policies for offline access to encrypted content on the drive.

X. Copyright and Trademark Information

© 1999-2007, encryptX Corporation.

All rights reserved.

SecurFlash is a registered trademark of encryptX Corporation.