

Quick Start Guide

Welcome to **SecurMedia™, Version 3.0 and SecurFlash™ Version 9.0** software from encryptX Corporation (www.encryptX.com). SecurMedia and SecurFlash are designed to encrypt and protect sensitive information on removable drives such as USB flash drives & removable hard drives. Encryption is designed to prevent unauthorized access to confidential data stored on your removable drives. This Quick Start Guide discusses how to use SecurMedia. Summary information on SecurFlash is provided for informational purposes to understand how the products work together. The SecurFlash QuickStart Guide can be found on any removable device that has been encrypted by SecurMedia.

SecurMedia™ - Is a PC installed security application. SecurMedia is designed for corporations and organizations that want to enforce organizational policies related to protection of sensitive information and protecting against sensitive data leakage. SecurMedia runs from the user PC or corporate server and automatically detects any removable drives connected to the PC or server. When a removable drive is detected, the software asks the user to set a password for the drive. If the user agrees, any data written to the removable drive is automatically and transparently encrypted. The user does not have to change their behavior - they work with files on the encrypted device exactly as if they were in the clear. Any files on the device that the user is opening or modifying are automatically decrypted and re-encrypted when the user is finished making their changes. If the user does not agree to set a password for the drive or if the user does not have the "Don't Encrypt" option installed, then the drive is set to READ ONLY so that no files can be written to the removable device.

Important Note: You must have JAVA Run Time Environment Version 6 or higher installed on your PC in order to use SecurMedia™. If SecurMedia does not run automatically for you check your Windows > Control Panel > Programs to see if Java 6.0 or higher is installed on your PC. If it is not, you can download JAVA 6.0 for free from:

<http://www.java.com/en/download/index.jsp>


SecurFlash™ - Is a removable drive installed security application. A copy of SecurFlash is installed automatically by the SecurMedia application on the removable device that is encrypted. SecurFlash executes and runs from the removable drive when the user clicks on the RunSecurFlash.exe program. SecurFlash is used to encrypt and decrypt files on the removable drive. Since SecurFlash runs from the removable drive, it does not install on the PC, and does not require any special PC administrative rights to run. SecurFlash is designed to protect information on drives that are portable – such as those used on multiple PCs. SecurFlash can also decrypt and open files encrypted on the removable device that have been automatically encrypted by SecurMedia. Any new files that are encrypted with SecurFlash on the removable drive can also be decrypted by the SecurMedia application.

Supported Operating Systems. SecurMedia & SecurFlash are 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 any type of file supported by the Microsoft Windows Operating System through the SecurMedia/SecurFlash software.

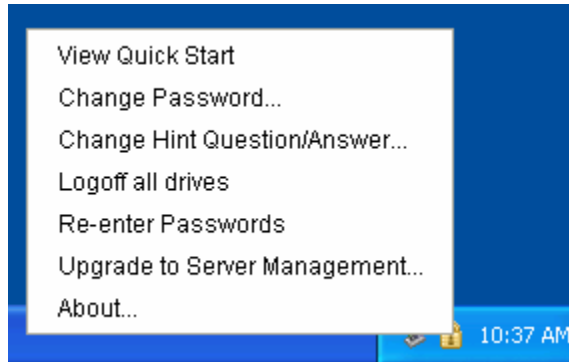
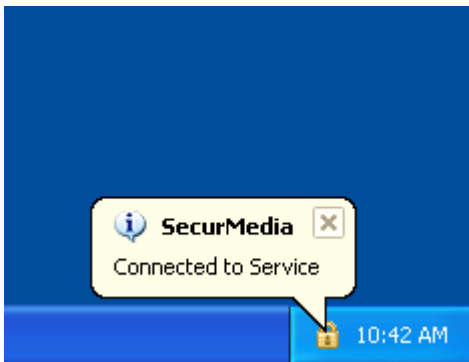
Important Product Use Concepts


1. **When SecurMedia is installed on your PC, data encryption of your removable drives by the SecurMedia software is automatic.** SecurMedia will encrypt any data saved to a removable device by an application, a DOS command window, or by Windows Explorer. Data encryption is completely automatic. If you have permission, you can also choose the “Don’t Encrypt” option for that drive.
2. **If you choose NOT to encrypt data on a device, or choose not to enter the password for a device that is already encrypted, your access to the device may be limited.** When a removable device is connected to your PC, you will be prompted for an encryption password. If you do not have the “Don’t Encrypt” option enabled for your SecurMedia installation, and you decline to provide a password, the device will be made read-only and only unencrypted files will be accessible. This allows you to copy files from your removable drive to your PC, but you will be prevented from writing any data to the removable drive.
3. **If you forget both your password and recovery hint you will not be able to access the encrypted files on the drive, unless you have deployed the optional Security Server software.** You will need to remember either your password or your recovery hint question to be able to access your encrypted files. If you forget both of these values, the optional Security Server software provides remote password recovery capability. Your Security Administrator can recover your password through the Security Server application from encryptX if it has been deployed.
4. **Accessing encrypted data when you are not working on a PC with the SecurMedia software installed must be done through the SecurFlash application on the device.** The encrypted files that have been protected through the SecurMedia software are not directly accessible to applications or the Microsoft Windows Operating System when you are not working on a PC with the SecurMedia software installed. The files appear on the drive, but they are encrypted. The only way to access these files is to run the EncryptX SecurFlash application by double clicking the **Run SecurFlash.exe** located on the device and providing the correct password. The Run SecurFlash.exe will also auto-run on certain operating systems and depending on your user privileges. When SecurFlash.exe is running, you can then open the files and modify them within your applications by double clicking the files that are shown in the SecurFlash application window. You can also encrypt new files to the device using the SecurFlash application.

I. About the SecurMedia Application

Once the SecurMedia software is installed, it will appear as an  icon in your system tray (typically located in the lower right corner of your desktop on the Task bar). The software is automatically started during system startup and therefore should always be available.

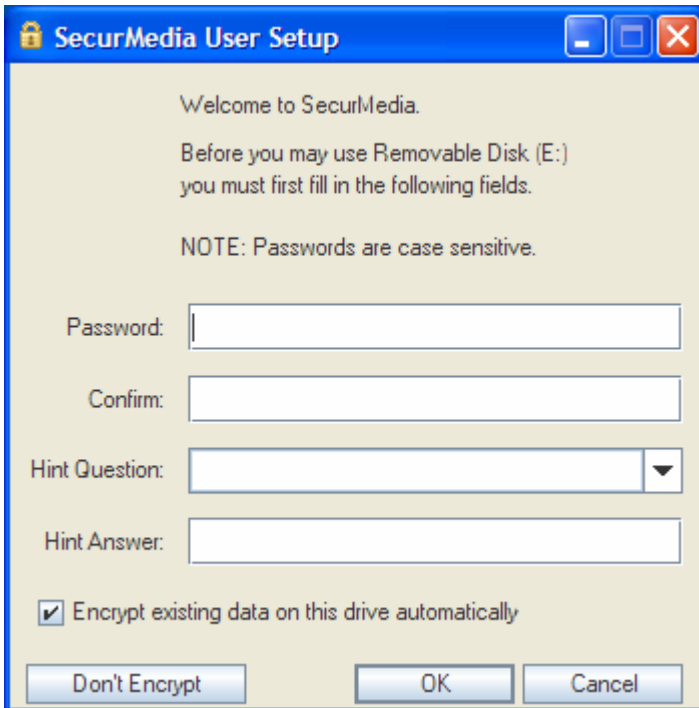
Occasionally, informational messages will be displayed using balloons to provide you with instructions or inform you of events that have been detected. You do not need to click on the balloons to close them, they will disappear by themselves. The “Connected to Service” message indicates that the SecurMedia application has successfully initiated integration with the Windows operating system and is ready to protect removable devices.



Right-clicking on the  icon will display a context menu of the functions available in SecurMedia.

II. Logging On to New Devices

The SecurMedia software will automatically detect any removable drives connected to your PC. If a drive has not already been encrypted, you will be prompted with the User Setup dialog. The User Setup establishes both the encryption password for the drive as well as the password recovery hint question and answer. You may type a unique hint question of your own in the Hint Question text box, or you may select one of the predefined questions. Entering your own question provides greater security. Your Hint Answer will be case sensitive, so don't forget how you type it in. You will need to type it exactly the same if you use it later for password recovery.



Un-checking the “Encrypt existing data on this drive automatically” box will allow you to turn off the automatic encryption of pre-existing, unencrypted files on a device when it is mounted. Any new files written to the device or updates to unencrypted files will be automatically encrypted, regardless. This setting will persist to all future mounts of that particular device.

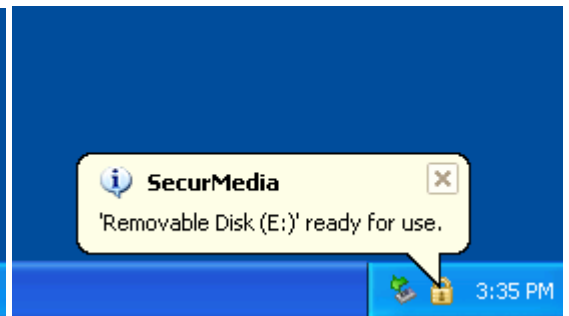
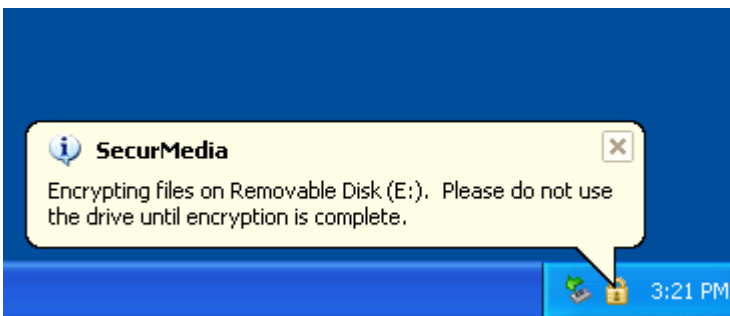
Note: The “Don’t Encrypt” button only appears if it was enabled with your version of the software. Clicking this button will mount the device and allow you to use it without encrypting any data on it.

III. Logging On to Devices Already Encrypted

If SecurMedia detects that a drive has already been encrypted, it will prompt you for the encryption password when the drive is mounted. If you decline to provide a password by clicking on the Cancel button or by closing the dialog box, then the drive will be mounted in read-only mode.



If the drive contains any files that have not yet been encrypted, SecurMedia will immediately encrypt them before the drive is made usable unless the “Should existing data always be encrypted automatically on this drive” setting was turned off when its encryption password was initially set.



Once the drive is ready for use, SecurMedia will intercept all file operations to the drive and encrypt/decrypt automatically as necessary.

Note: Any attempt to access the files on the encrypted device before the encryption password has been entered will result in an error. Typical errors indicate that the file cannot be opened because it does not exist.

IV. Using the SecurMedia Application

Change Password

This option allows you to change the encryption password for any mounted encrypted drives.

Change Hint Question/Answer

This option allows you to change the password recovery Hint Question/Answer for any mounted encrypted drives.

Logoff All Drives

This option will logoff all removable devices from SecurMedia. You will need to either disconnect and reinsert a drive, or select the "Re-enter Passwords" menu option to regain access to the encrypted drives. Attempts to access files when the drives are logged off will result in an error indicating the file is unavailable. Any unencrypted files on the device will be limited to read-only access.

Drives are automatically logged off if they are unplugged or disconnected from the PC.

Re-enter Password

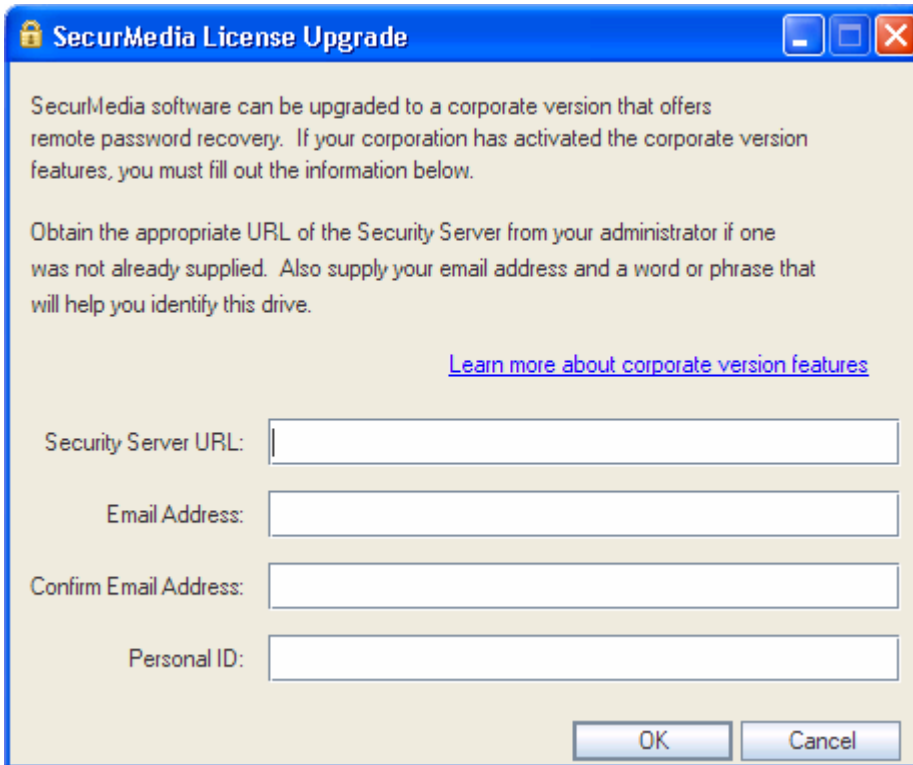
This option prompts for the password of all mounted drives. This option can be used to enter a password for a device that was originally mounted read-only by cancelling or closing the password prompt.

Upgrade to Server Management

This option will upgrade the SecurMedia software to the Corporate Edition, which requires a connection to the corporate Security Server. This provides central management, additional password recovery mechanisms, and enforces corporate policies such as strong passwords, password expiration, offline re-authentication periods, and remote revocation in the event of loss of a device.

About

This option displays information regarding the SecurMedia software version, type of encryption and current drive status of all removable devices.



Security Server URL:

Your security administrator will provide you with the correct Security Server URL to connect to. Do not include the "http://" prefix on the URL. Example: `secureserver.mycompany.com`

Email Address:

Enter your valid email address. This is used to allow the security administrator to assist you in recovering your password if you forget it and/or your recovery hint question/answer. The confirmation text box helps prevent you from accidentally entering a typo in your email address.

Personal ID:

Your security administrator may provide you with corporate guidelines as to what value to enter into the Personal ID field. This field should be unique to each removable device you use. This value assists the security administrator in uniquely identifying each device should you encounter any issues in the future such as a lost device or a compromised password.

V. Accessing Encrypted Data without SecurMedia

If you wish to access protected files that were encrypted with SecurMedia from a PC that does not have SecurMedia installed, you will need to use the **Run SecurFlash.exe** program on the device. This application will allow you to enter your encryption password and use the encrypted files from within the SecurFlash application window. The SecurFlash application does not automatically encrypt new files on your removable device like SecurMedia does, but it provides you with a manual method to encrypt them.

Note: When using a PC that does not have SecurMedia, if you copy files to your device without using the SecurFlash application, they will be written to the device unencrypted and without password protection.

VI. Copyright and Trademark Information

© 1999-2008, encryptX Corporation.

All rights reserved.

SecurFlash & SecurMedia are registered trademarks of encryptX Corporation.

www.encryptx.com

VII. Contacting encryptX Corporation

Toll Free Phone 888-431-4550

Email customersupport@encryptx.com

Website www.encryptx.com

Address 580 Burbank Street, Suite 110, Broomfield, Colorado 80020

Local Phone Number 303-464-8564