Quick Start Guide

Welcome to **UltraLock**®, **Version 9.1** software from UltraLock Corporation (www.ultra-lock.com), powered by EncryptX Corporation (www.encryptx.com). UltraLock and is 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 UltraLock.

UltraLock™ - Is a removable drive installed security application that encrypts information on the drive and allows you to create a password to access your encrypted data. UltraLock executes and runs from the removable drive when the user clicks on the RunUltra-Lock.exe program. UltraLock is used to encrypt and decrypt files on the removable drive. Since UltraLock runs from the removable drive, it does not install on the PC, and does not require any special PC administrative rights to run. UltraLock is designed to protect information on drives that are portable – such as those used on multiple PCs. UltraLock 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 UltraLock on the removable drive can also be decrypted by the SecurMedia® application.

UltraLock Supported Operating Systems. **UltraLock 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 any type of file supported by the Microsoft Windows Operating System through the UltraLock software.

SecurMedia® - Is an optional and complimentary application from EncryptX Corporation that works with UltraLock. 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 on PCs and Servers. SecurMedia installs on and runs from the user PC or corporate server and automatically detects any removable drives (e.g. flash drives, removable hard drives, memory sticks, Compact Flash, SD, MicroSD, CDs, DVDs, etc.) 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. A copy of UltraLock is automatically installed on any removable drive that is detected by SecurMedia.

The SecurMedia Quick Start Guide is available at http://www.encryptx.com/downloads/encryptX_SecurMedia_QuickStart_V3.1.pdf.

If you have SecurMedia installed on your PC, simply right mouse button click on the Lock Icon in your Windows System Tray – which is the bar shown at the bottom of your screen, and Select the Quick Start menu item to review the Quick Start guide for SecurMedia.

UltraLock Important Product Use Concepts

1. **Use of the UltraLock software is not mandatory to the use of the drive**. If you do not want to encrypt 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 files on the drive unless you have upgraded to the Enterprise Managed Version**. You will need to remember either your password or your recovery hint question to be able to access your encrypted files. If you are concerned about forgetting your password and recovery hint, you should consider upgrading to the UltraLock Enterprise version. The Enterprise Version of UltraLock 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.   More information about the Enterprise version of UltraLock is available at: http://www.ultra-lock.com and at the end of this Quick Start Guide.

3. <u>**You can open and edit your files from within the UltraLock software and any changes will be automatically saved.**</u>   Any edits you make to files that you have previously encrypted and are opening from within the UltraLock application will be <u>automatically</u> saved and re-encrypted when you SAVE or EXIT your application. If you perform a SAVE AS, the UltraLock application assumes you want to decrypt and save your changes somewhere else other than the drive.

I.   Running the UltraLock Application

The UltraLock software is installed on your removable drive. The first time you run the application you will be asked to establish your password and password recovery hint.

1. In Microsoft Windows, double click on **My Computer** and navigate to the drive letter that corresponds to the removable drive you are working with.

2. At the top level of the removable drive you will see a **RunUltraLock.exe** program. **Double Click** on the **RunUltraLock.exe** program.

3. Review the license in the **UltraLock 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. The **UltraLock User Setup** dialog box will appear if this is the first time you are using the drive with the UltraLock program. In the **UltraLock User Setup** dialog box, enter the password, hint information, and click **OK**.

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

6. The **UltraLock** window that enables the user to perform encryption operations displays. Any folders or files that you drag into the window are automatically encrypted. Any folders or files that you drag out of the UltraLock application window are automatically decrypted. Any files that you have previously encrypted and that you double click in the UltraLock application window will automatically decrypt and the software will launch the application associated with that file type (e.g. a .doc file will launch Microsoft Word).

   Note: **For Enterprise mode setup**, in the **UltraLock 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 Enterprise mode setup and features, please read Section IX of this document.

   Note: The **UltraLock Server Setup** dialog box only displays during Enterprise mode setup.

II.   Encrypting Files and Folders on Your Removable Drive

The left pane of the **UltraLock** main window displays the root drive letter of your removable drive and a navigation tree of any subfolders you have created. You can create new folders and rename folders as you desire. Note: Right-click context menus that Explorer provides are not supported.

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

   – or –

1. In the **UltraLock** window, select the folder location where you want to store the encrypted file or create a New Folder and encrypt files to that location.
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**.

The UltraLock window displays both encrypted files on the drive as well as any files that may have been copied to the drive that are not encrypted. The encryption state of the file is indicated by the "Encrypted" column in the right pane. To encrypt an unencrypted file, simply select the file in the right pane and click the Encrypt button on the toolbar.

III.   Decrypting Files and Folders on Your Removable Drive

When the user decrypts files, the **UltraLock** 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 drive or networked drive as well as to removable storage media.

The user can decrypt files through the **UltraLock** 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 **UltraLock** 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 **UltraLock** window directly on to the associated application. This will automatically decrypt the file and display it within the application.

Decrypt through the UltraLock Decrypt Button

1. In either pane of the **UltraLock** window, select a folder to decrypt.
    – or –
    In the left pane of the **UltraLock** 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 **UltraLock** software adds the modified version to the encrypted file system and supersedes the previous version.

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

– or –

Select the file and click the Open button on the toolbar.

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

The user can delete encrypted files from the removable drive from within the UltraLock application window by selecting them and clicking the Delete icon on the toolbar or by choosing the Delete option from the File Menu.

Files can also be deleted using Windows Explorer or any standard Windows method. If this is done while the UltraLock application window is open, the files may still be displayed in the file list until a user action is taken that causes the file list to be refreshed. In the event that a deleted file is still shown prior to a list refresh, it will be inaccessible nevertheless.

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 **UltraLock Login** dialog box, click **Recover Password**.

– or –

a. Enter anything in the **UltraLock Login** dialog box and click **OK**.

b. In the **UltraLock 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 **UltraLock Login** dialog box displays again.

2.   In the **UltraLock Password Recovery** dialog box, enter the hint answer into the **Response** box and click **OK**.

3.   In the **UltraLock Password Recovered** dialog box, click **OK** after noting the password.

The **UltraLock Login** dialog box displays.

B.   Modify password

1.   In the **UltraLock** 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 **UltraLock** 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.   Enterprise Mode

When the software has been upgraded and is operating in Enterprise mode, the UltraLock Enterprise 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 UltraLock Enterprise Edition software for the first time in Enterprise 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 Enterprise mode

1.   In the **UltraLock** window, click **Upgrade** on the **Tools** menu.

2. In the **UltraLock License Upgrade** dialog box, enter the server connection URL in the **Security 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 UltraLock Enterprise Edition** dialog box displays information about the connection to the corporate server and the policies for offline access to encrypted content on the drive.

VIII.   Copyright and Trademark Information

© 2008, UltraLock Corporation.

All rights reserved.

SecurMedia® and encryptX® are registered trademarks of EncryptX Corporation.

IX.   Contacting UltraLock Corporation

Toll Free Phone	1-800-830-1109
FAX	1-303-413-8255
Email	customersupport@ultra-lock.com
Website	www.ultra-lock.com
Address	917 Front Street, Suite 100, Louisville, CO 80027

X.   Contacting EncryptX Corporation

Toll Free Phone	1-888-431-4550
Email	customersupport@encryptx.com
Website	www.encryptx.com
Address	580 Burbank Street, Suite 110, Broomfield, Colorado 80020
Sales	1-303-464-8564 or sales@encryptx.com