IMPORTANT! Files saved to this USB are NOT automatically encrypted. You must use the SecureLock II software interface to secure your files.

SecureLock II™

User Manual



Encryption Application for USB Flash Drives

User Manual Version 1.0.0.4

© 2004-2011 Integral Memory Plc.

Table of Contents

Table of Contents 2
1. Introduction 3
2. System Requirements 4
3. Working with SecureLock II 5
   3.1. Setting up SecureLock II 5
   3.2. Setting up a Password 6
   3.3. Password retries 8
   3.4. Display Settings 8
   3.5. Using Drag & Drop to copy files 9
   3.6. Security settings 12
4. Safely Remove Hardware 13
5. Support 14
6. Important Notice / Disclaimer 15

1. Introduction

Protecting data in transit is essential to ensure no third party has access to data in case a USB Flash Drive is lost, misplaced or stolen.

SecureLock II protects data on the USB with Government-approved 256-bit AES CBC-mode encryption.

With the intuitive Drag & Drop interface, files can be quickly copied to and from the USB for fast, secure and efficient workflow.

SecureLock II is a portable application that does not require any installation process on the host computer. Wherever the USB Flash Drive goes, SecureLock II is saved on the USB and can be used with any compatible Windows PC or Mac.

2. System Requirements

Operating Systems:

- Windows XP (Service Pack 2 is recommended)
- Windows Vista (all Versions)
- Windows 7 (all Versions)
- Mac OS X (10.4+)

- Available USB port

SecureLock II does not require Administrative rights.

3. Working with SecureLock II

3.1. Setting up SecureLock II

To start SecureLock II:

- **On Windows OS**: simply double-click the SecureLock.exe file from the root folder of the USB Flash Drive.
- **On Mac OS**: simply double-click the SecureLock.dmg file from the root folder of the USB Flash Drive.



3.2. Setting up a Password

In order to secure (encrypt) your data, you will need to set up a password. The password must be at least 6 (six) characters long.

For security reasons, it is recommended that you incorporate letters, numbers and symbols into your password.



Enter your password, and then confirm it.

It is recommended that you also set up a password reminder that will help you in case you forget your password.

For security reasons, the password reminder cannot be the same as the password itself.

Click “Next” to proceed.



Click “Finish” to complete the password settings and start using the application.



3.3. Password retries

Each time the application starts, you will be asked, for security reasons, to type in your password.

If your USB is lost or stolen, for your protection the number of password retries is limited to 10. After the password has been entered incorrectly 10 times in a row, SecureLock II will safely erase all encrypted files stored on the USB. The data on the USB cannot be recovered or recreated. It is permanently erased.

3.4. Display Settings

In the toolbar area of SecureLock II there are several options available for customizing the SecureLock II display window.



Swap Panels – to interchange the display of the USB Flash Drive and My Computer panels

Show or Hide My Computer Panel – to display the My Computer Panel

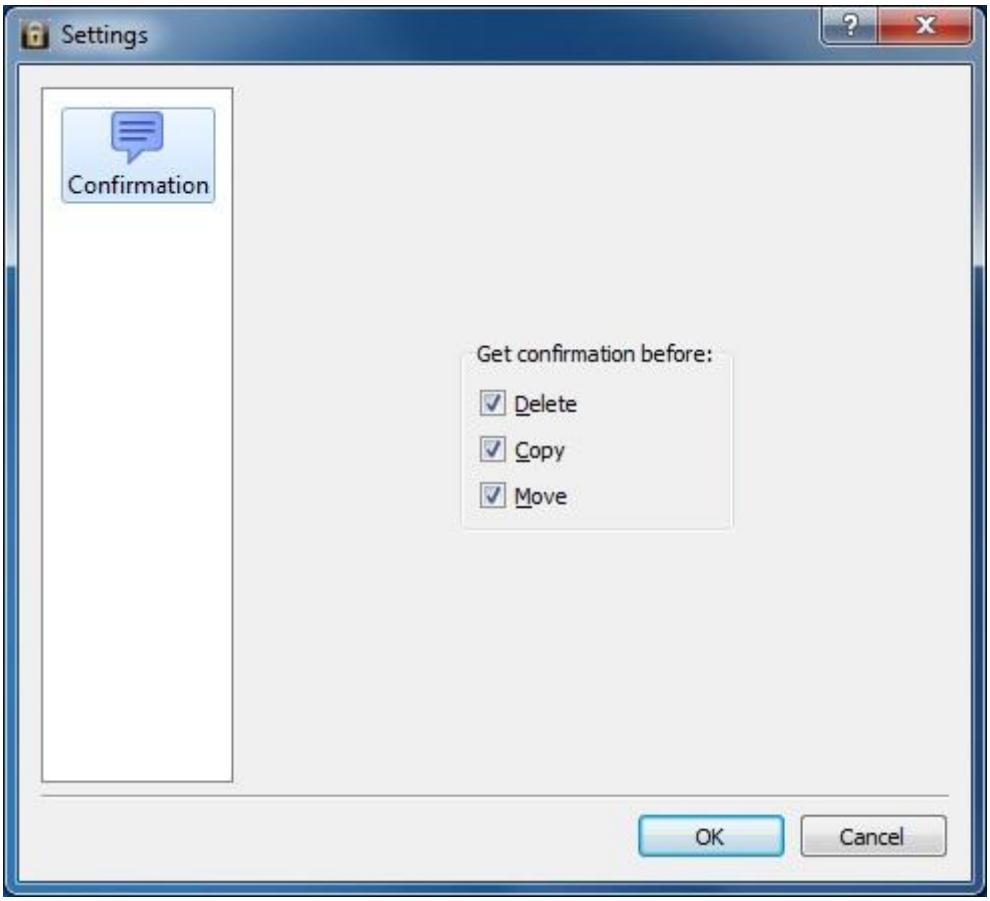
Show Tree View – to display a tree-like structure

Show Detailed View – to show additional information about the files

Show List View – to display the items as a list

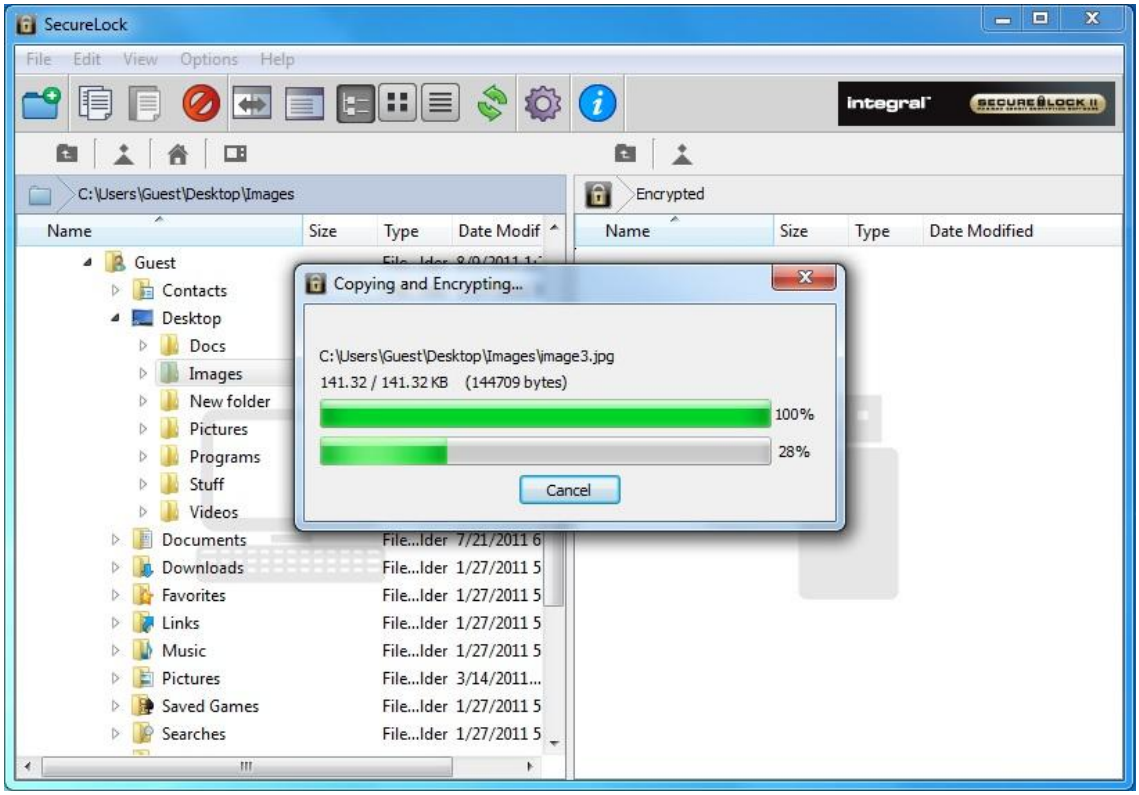
The available options can be selected also directly from the main menu, under the View section.

A new option, Preferences, allows you to select whether you want to have a confirmation message displayed before deleting, copying or moving files.

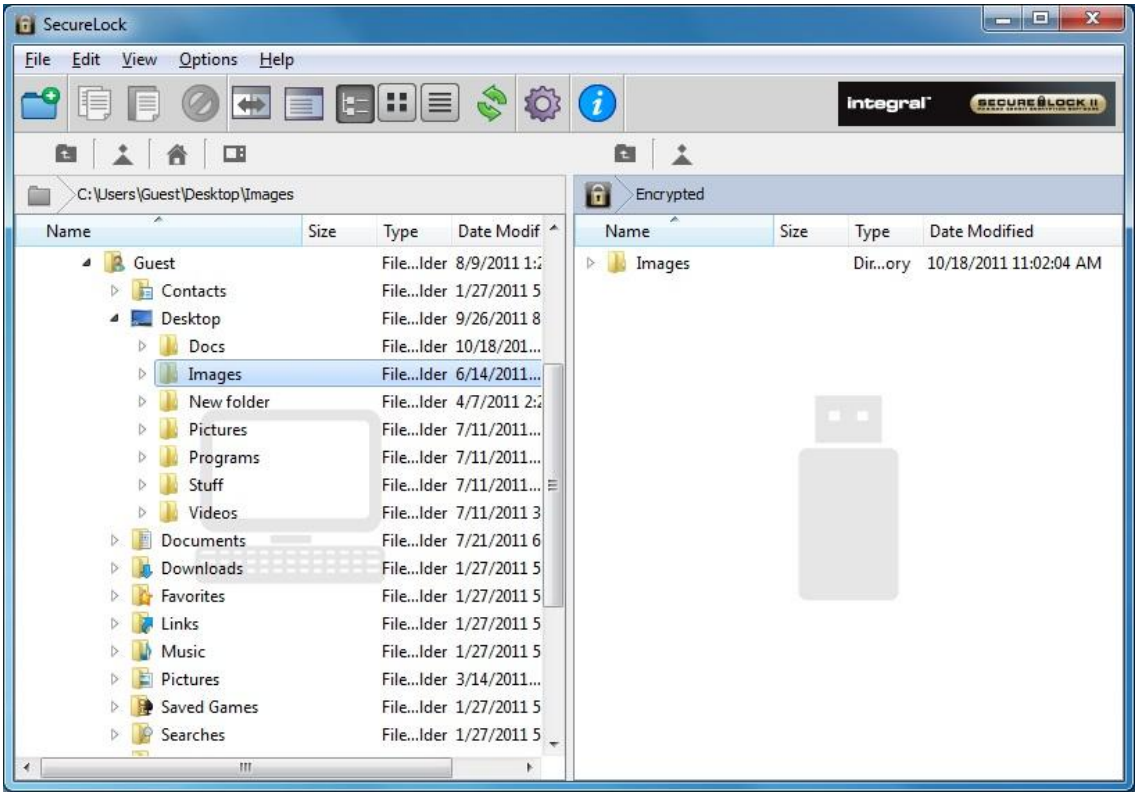


3.5. Using Drag & Drop to copy files

A key feature of SecureLock II is the Drag & Drop functionality which allows you to simply drag the file(s) and/or folder(s) that you want to copy on the computer and drop them onto the window of SecureLock II. These files will be automatically encrypted, ensuring that your data stay safe and private.



The file encryption and transfer status can be seen with the help of the progress bar. When the bar reaches the end, your files have been copied and encrypted.



You can navigate through your encrypted files if you are using Windows Explorer. Clicking on an item with the right mouse button will give you access to options such as “Refresh”, “Copy” and “Delete”.

We recommend using either the Drag & Drop feature or the shortcut keys for copying and pasting, Ctrl+C and Ctrl+V to transfer data to your USB through the SecureLock II interface.

In the toolbar area of SecureLock II you can find additional icons that you can also use to copy and encrypt your files.

Note that the files on your USB are not visible after encryption, unless SecureLock II is running.

To exit SecureLock II, select the File menu and choose Exit, or simply click the “X” button in the upper-right corner of the application window.

3.6. Security settings

The security settings can be modified from within SecureLock II. After logging in, you can modify you password. To do this you need to access the security settings menu. This can be done by either selecting Options->Security Settings from the toolbar area or by pressing the hotkey Ctrl + O.

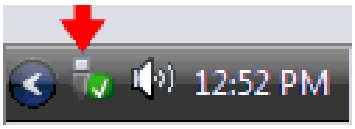


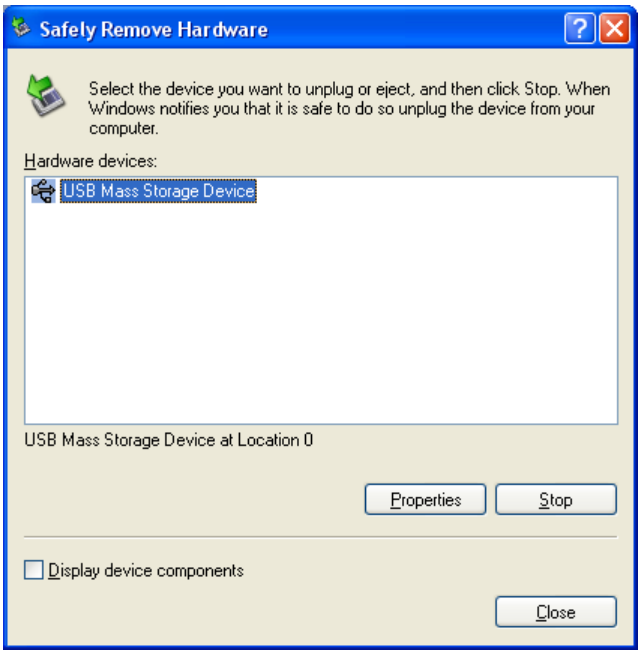
4. Safely Remove Hardware

Before you unplug your USB from the USB port of your computer, you have to use the “Safely Remove Hardware” option from the system tray, otherwise you risk corrupting the data on your USB Flash Drive.

To Safely Remove Hardware, double-click on the system tray icon, then select the USB you want to remove from the list and click on the “Stop” button.







A message will appear indicating that the USB can now be securely removed. If a message saying “The ‘ …’ device cannot be stopped right now” appears, you have to close your Windows Explorer, SecureLock II or any other application that is still accessing the data on the USB Flash Drive.

5. Support

If you require additional help, please visit http://www.integralmemory.com and read the FAQs or email our support team.

6. Important Notice / Disclaimer

Security safeguards, by their nature, are capable of circumvention. Integral Memory cannot, and does not, guarantee that data or devices will not be accessed by unauthorized persons, and Integral Memory disclaims any warranties to that effect to the fullest extent permitted by law.

Copyright Integral Memory Plc.; All rights reserved. All other names and trademarks are property of their respective owners.