

integral™

Crypto

Security Application Program
'Total Lock' PC & Mac

User Manual

FIPS-197 Certificate Number #1137
Waterproof Standard:
IEC60529 IPX8



Table of Contents

A	Introduction	3
B	General Description	3
C	Features	4
D	Before using the Security Application Program - TOTAL LOCK	5
E	Introduction to the Security Application Program - TOTAL LOCK	6
	E1. Terms & Conditions	6
	E2. Language Setup	7
	E3. Personal Information	7
	E4. Password Setup	8-9-10
F	USB Flash Drive Usage	11
	F1. Locking the Device	11
	F2. Unlocking the Device	12-13
	F3. Forgotten Password	14
G	Restoring to Factory Settings	15
	G1. Factory Restore	15-16
H	FAQ - Frequently Asked Questions	17

A. Introduction

- Plug in only **ONE** device at a time. **DO NOT** plug in two or more secure devices at the same time when running this security application program – Total Lock.
- The security application program - Total Lock - is designed for Windows® XP, Vista, 7, 8 and Mac® OS X (10.x) based operating systems

B. General Description

Integral AES 256-bit USB Flash Drives are removable storage devices that encrypt data transferred onto them. Available in capacities of 2GB, 4GB, 8GB, 16GB, 32GB. The device implements AES, SHA, and ANSI X9.31 RNG in FIPS Approved Mode.

The device works by creating two partitions when attached to either a Microsoft Windows® based PC or to an Apple Mac® computer. The first partition appears as a CD drive which runs a program (called Total Lock) directly from the device. The second partition is the password protected data drive onto which files can be transferred. Data can only be accessed on this drive once the correct password is entered via the Total Lock program. The CD drive is read only and no files can be transferred to this partition. Integral AES 256-bit USB Flash Drives have zero footprints, with no software installation required and a people friendly interface that makes using the drive simple and easy but does not compromise security.

Integral's AES 256-bit USB drives also have an optional function to add unencrypted contact information to the device whilst keeping all other data secure. This allows lost devices to be returned to the correct owner. The contact information can only be changed during the setup or factory reset of the device; at which point any sensitive data being stored will automatically be destroyed.

The AES 256-bit USB drives have mandatory encryption for any data transferred onto it. The encryption is carried out using AES (256-bit in CBC mode). It also supports identity based authentication with a strong user password of at least 8 and a maximum of 16 characters.

The password must contain both upper and lower case letters, and include at least one numeric and special character. For further protection, the AES 256-bit drives allow only 6 incorrect password attempts before destroying all data on the device. This protects against brute force attacks on the drive.

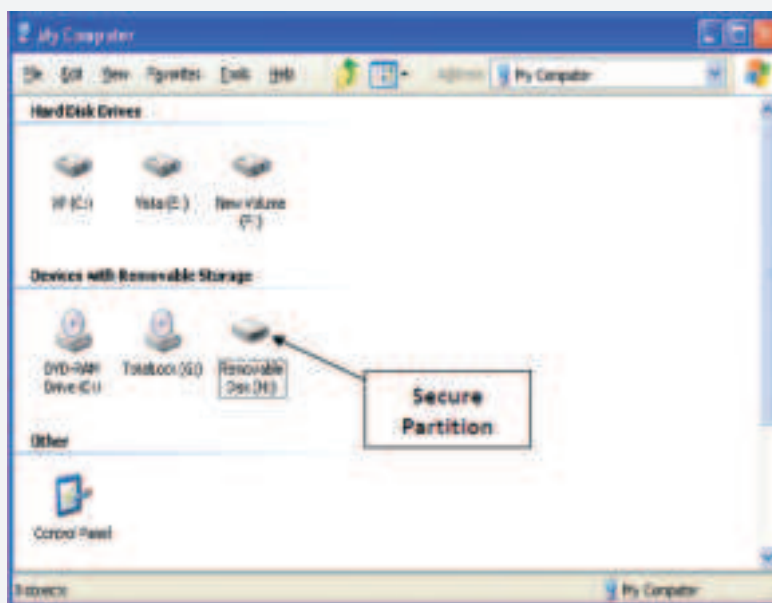
The AES 256-bit USB drives have a multilingual interface in 26 languages.

C. Features

- a. **Military Level Security** – AES 256 bit hardware encryption. Mandatory encryption of all files (100% privacy).
- b. **Easy to Operate** – program is pictorial with easy to understand icons and friendly descriptions.
- c. **Customized Password** – users can choose a password of their own from 8 to 16 characters long of upper and lower case letters and numbers.
- d. **Fixed Password Retry** – users are only allowed to type in the password 6 times, when typing in the wrong password for the sixth time; the drive will be formatted to protect the data from being exposed to others.
- e. **Friendly Reminder** – there is a password hint function available, in case user forgets his/her password. A password hint message can be setup, with messages up to 32 characters in length.
- f. **Multi Lingual Support** – supports 22 languages
- g. **Personal ID Function** – Contact details can be added so that the drive can be returned, whilst confidential data remains secure.
- h. **Zero Footprint** – No software installation required.

D. Before Using the Security Application Program - TOTAL LOCK

- a. When you plug in your Integral AES 256-bit Drive to a USB port, the Windows® or Mac® operating system should recognise the device and show an extra “CD-ROM” and a “Removable Disk” icon. The security application program – Total Lock - will be stored in the CD-ROM partition with auto-run function, you must have auto run enabled for this to work or you will have to go to my Computer and run the TotalLock.exe and then the security program will pop up on screen automatically.



Partition 1 – Secure Area

This secure area is protected by password and can only be accessed by typing in the correct password. There is no PUBLIC partition on this. All data will be protected.

Partition 2 – CD-ROM Area

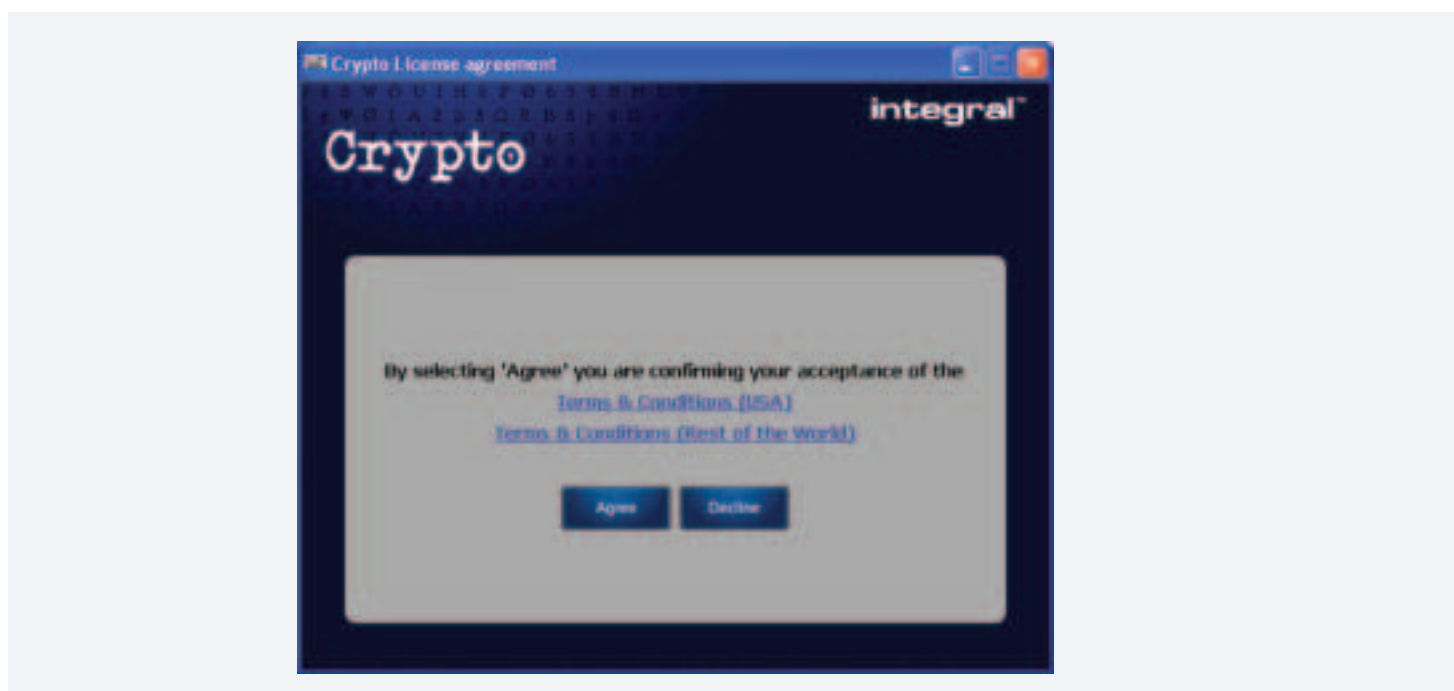
This area is a “Read-Only” area. Users can read data from this partition, but is unable to write or delete data stored in this partition. The security application program – Total Lock will be stored in this partition with auto-run function. Password security will only apply to the secure partition and will not affect this partition.

E. Introduction to the Security Application Program – Total Lock

E1. Main Screen



E2. Terms & Conditions.



After the splash screen shows up you will be asked to accept the terms and conditions once you have agreed you will be then passed on to the language setup screen.

E3. Language Setup


There are 26 different languages to choose from. Select the language you require from the drop-down menu.

Click  icon.



E4. Personal Information



On the next screen you can chose to enter your personal contact information and then Click  icon. Adding your name and address details is optional.

E5. Password Setup

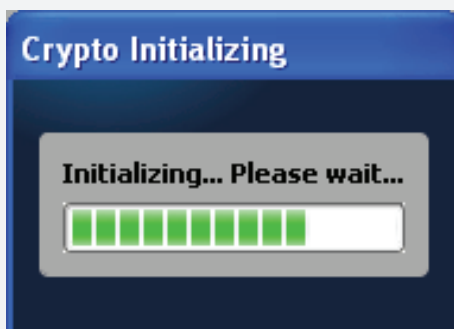
This screen allows the setup of a complex password. The password must consist of between 8 – 16 characters in length and a mixture of uppercase and lowercase letters, numbers and special characters. If you meet the password requirements you will see a green OK if you do not meet the password requirements there will be a red X till you do. The program will not let you go forward till you have met all password requirements.

DO NOT FORGET TO ENTER A PASSWORD HINT.
THIS SHOULD HELP IF YOU FORGET YOUR PASSWORD.

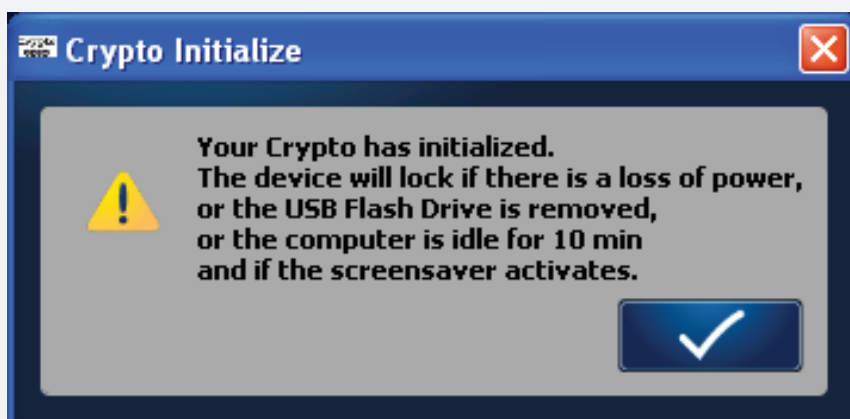



When you have entered all the details, Click  icon.

This will initialize the USB Flash Drive by reformatting it and setting all parameters that were entered.

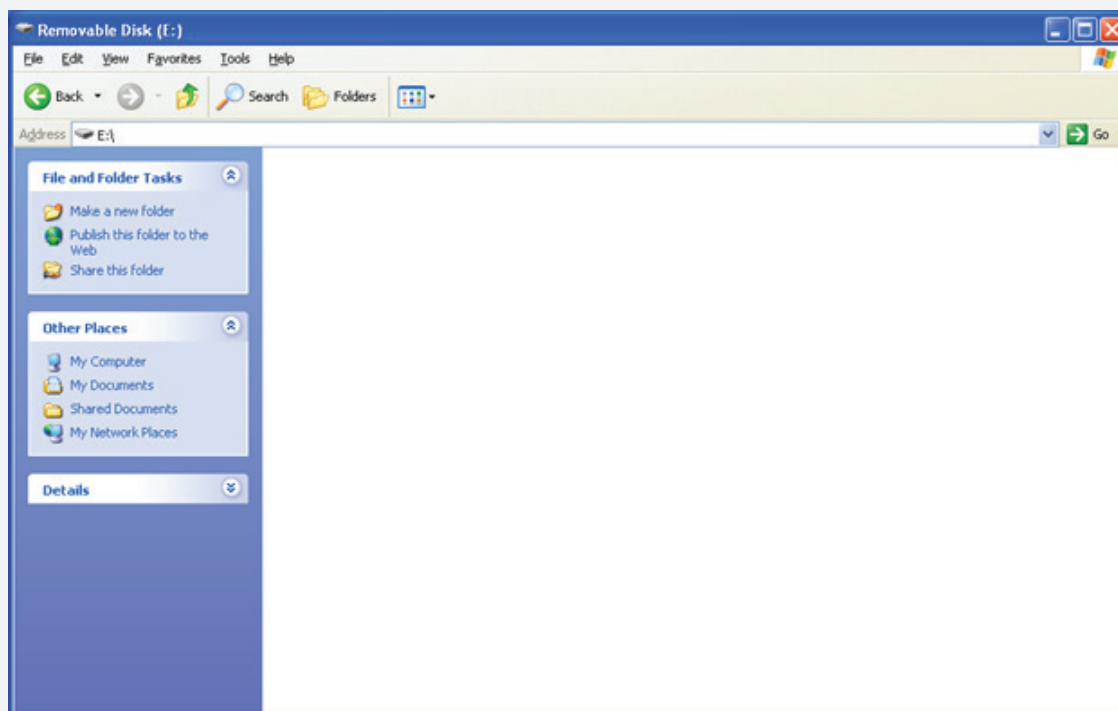


When it has completed you will see the message on screen below:



When you have **Click on the**  **icon.** this will launch the secure partition of the USB Flash Drive and the program interface will change. You will see the information about the security applied to the USB Flash Drive (i.e. Password and Device Status).






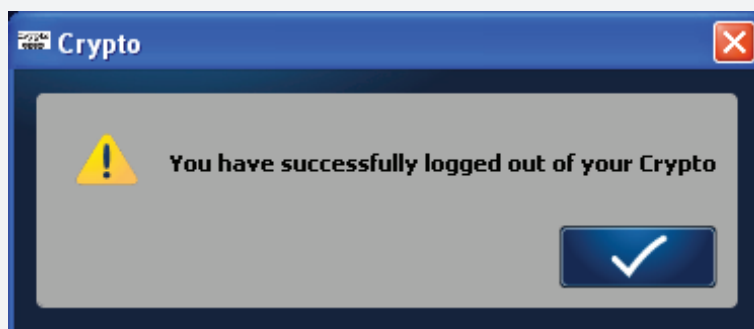
You are now ready to use the Integral AES 256-bit USB Drive. All data that is put in the secure partition will be fully encrypted automatically as soon as you remove the USB Flash Drive from the socket or if there is a suspension of power. Access to this is only granted with the correct password.

F. USB Flash Drive Usage

F1. Locking the Device

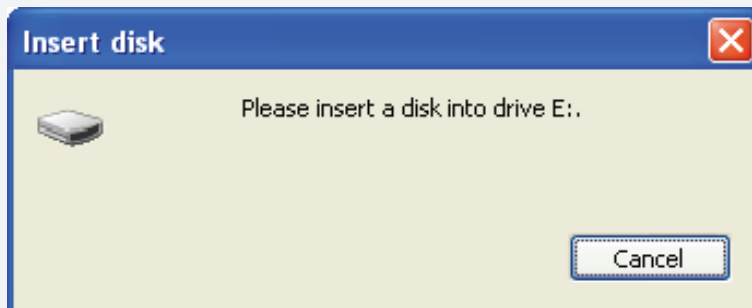


When you have your data on the USB Flash Drive, [click on the](#)  [button](#). This will encrypt the data and log you out of the USB Flash Drive.



F2. Unlocking the Device

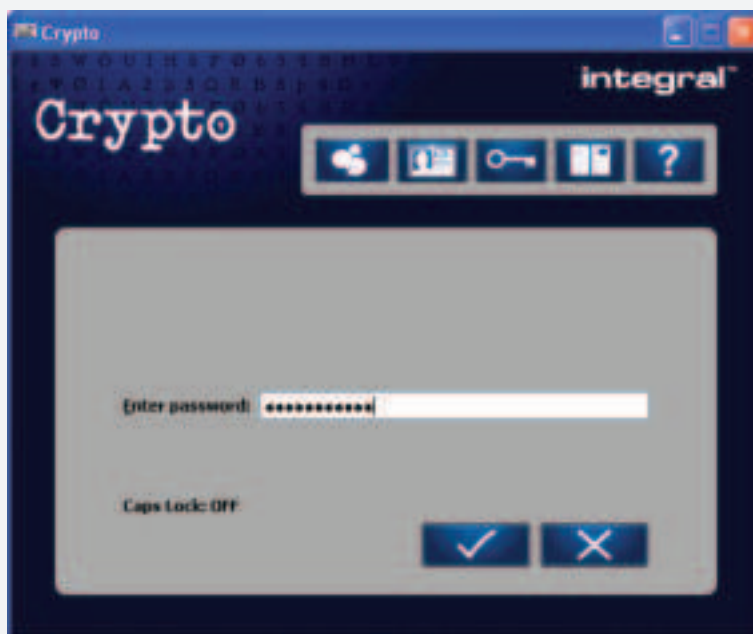
If you have setup a password, when you remove your Integral AES 256-bit USB Drive from the USB socket (or if there is a suspension in power), the secure partition of your Drive will be locked automatically. You will not be able to access this partition, nor read or write data to this partition.





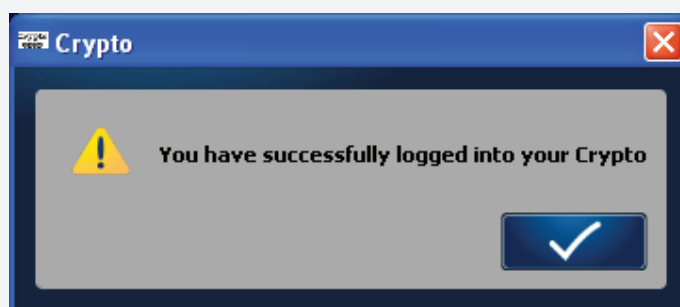
To get back into the secure partition you will need to launch the Total Lock program.




Click on the  button.



Input the password that was used to set up the Crypto Drive. If you have forgotten your password, click on the  icon. This will display your Password Hint (providing you have entered one). When you have completed this, click the  icon. This now unlocks the secure partition. You now have access to your data.

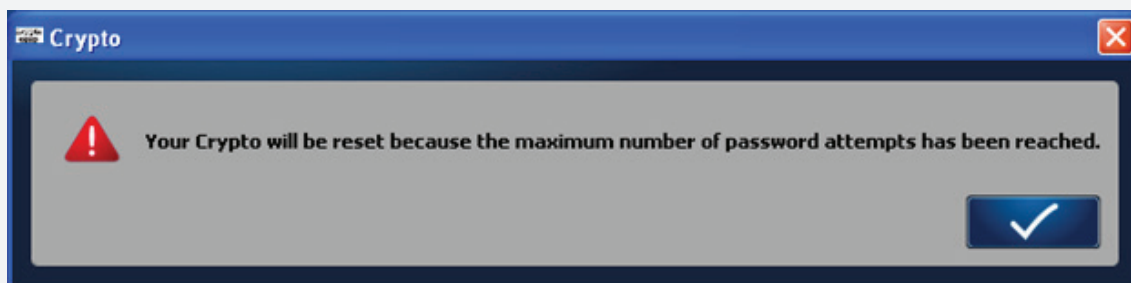
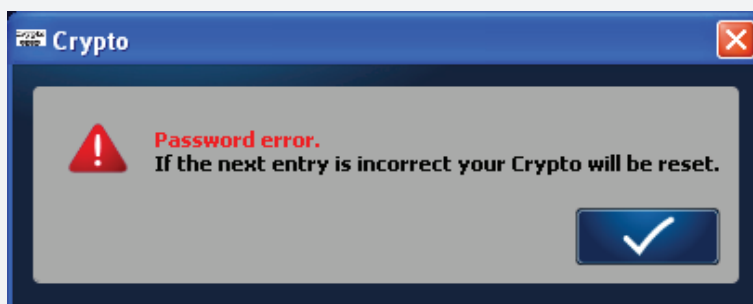
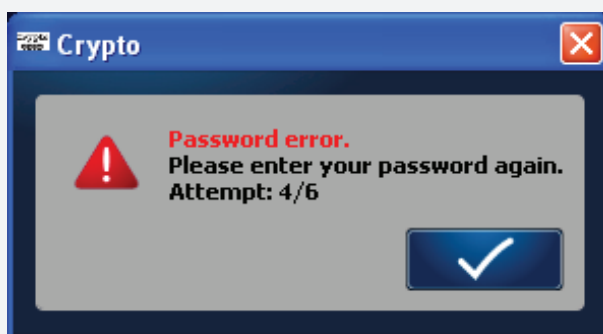
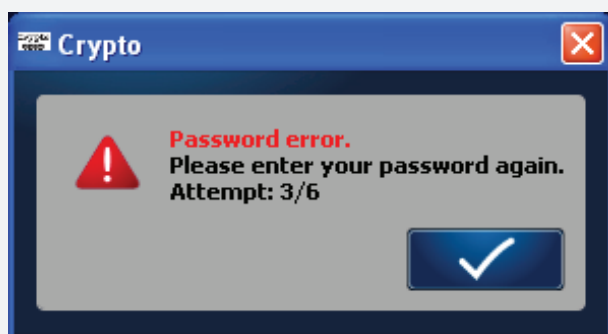
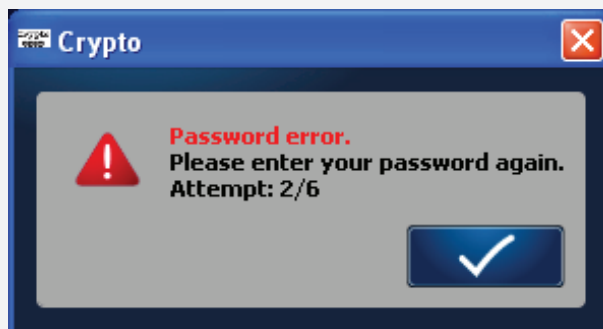
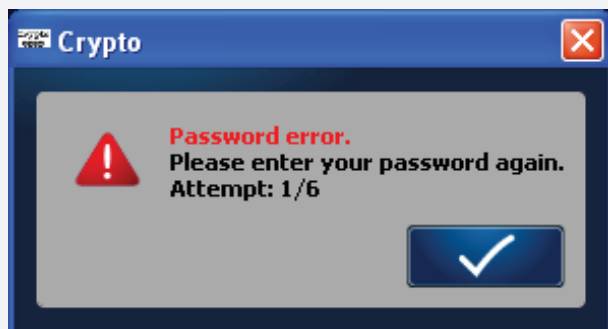


F3. Forgotten password

What happens if you forget your password? Hopefully, you would have entered a Password Hint, which will help you remember the password. Click on the  icon to display your Password Hint.

What happens if your Password Hint doesn't help you remember your password or you haven't entered a Password Hint?

The Total Lock program will allow a maximum of 6 password attempts to be entered before it formats the Integral AES 256-bit USB Drive resulting in the permanent loss of your data.



At this point the Integral AES 256-bit USB Drive is not usable until the Total Lock application has formatted it. At this stage the Drive will be set back to factory settings.

G. Restoring to Factory Settings

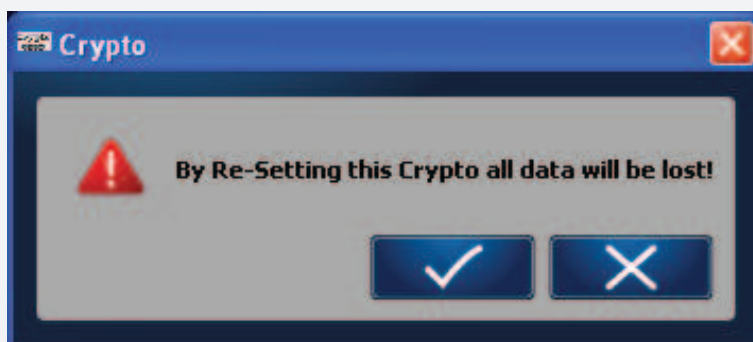
G1. Factory Restore

The Total Lock program allows the user to restore the Crypto Drive back to factory settings. For this to be done the USB Flash Drive needs to be in the Locked status.

By restoring the Crypto Drive back to factory settings, this will format the device; data will be lost permanently and the Drive reset.

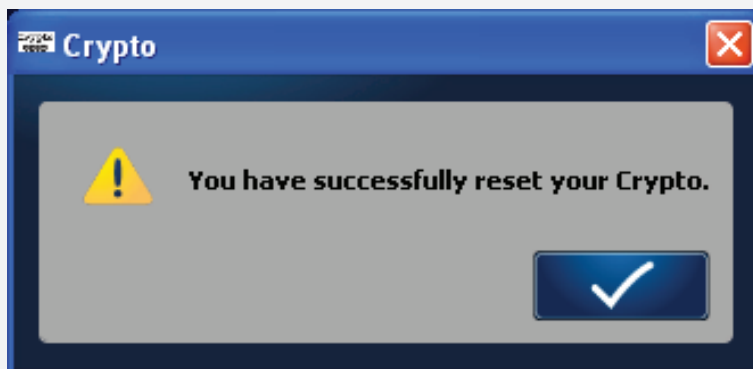


To restore the Crypto Drive back to factory settings, click on the  icon.



click on the  icon. You will then see a confirmation message. click on the  icon.

After restoring to factory settings has been successfully completed, you will see the confirmation message.



Your USB Flash Drive is now ready to be used again.

H. FAQ – Frequently Asked Questions

Q1 My Windows XP computer cannot detect my device, what can I do?

- **A1** Since there is no driver required for these operating systems, the device uses the built-in driver (USB Mass Storage Class Driver) from these operating systems. If your operating system cannot find the device, then it is very likely that the built-in driver files were missing or corrupted; please try to recover these files from other computer or from the original Windows operating system CD.

Q2 When I run the LOCK program it displayed “Please insert the device or run this utility as privileged user”, what is wrong?

A2 The problem may occur in Windows XP, under the following two situations:

Situation 1 : You have forgotten to insert your device.

Situation 2 : The security application program – Total Lock requires some security privileges in this Windows operating system. If you are not the administrator of the computer, these privileges may be restricted by administrator. Please check with your MIS or administrator of the computer to open up the privileges for you. (See following method)

When logged into the account affected, run GPEDIT.MSC from the run menu (If there is not enough access use the 'Run As' option). We now need to find the security policy "Devices: Allowed to eject removable NTFS media". It is located in Local Computer Policy >> Computer Configuration >> Windows Settings >> Security Settings >> Local Policy >> Security Options. You need to change the access from "Administrators and Power Users" over to "Administrators and Inter Active Users". You need to change the access from "Administrators and Power Users" over to "Administrators and Inter Active Users".

Q3 I am having Permission problems with my Integral Crypto Drive is there a fix for this?

A3 There can be several reasons for this to be happening:

- 1 :** Your system is not patched
- 2 :** Your User Permissions level
- 3 :** Your Registry

Windows XP Service Pack 3 should be installed and the system then fully updated.

If you are still using Windows XP Service Pack 2, the following hot fix will also need to be installed.

<http://support.microsoft.com/kb/297694/>

When computers are imaged they sometime get there permissions striped out which will make your AES Drive to fail. The following registry entrees need to be set to

Domain User Read:

HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices HKEY_LOCAL_MACHINE\SYSTEM

CurrentControlSet\Services\Disk

integral™