

integral™

Crypto Dual

AES 256 Bit Data Encryption

Integral
Advanced Encryption Standard (AES)
256-Bit Security Application Program
Dual Lock

FIPS-197 #1137
IEC60529 IPX8



Type A



Type C



Crypto
Dual

Crypto
Dual+

Security Application Program
Dual Lock

User Manual

Table of Contents

A	Important Notice	3
B	General Description	4
C	Features	5
D	Before Using the Security Application Program - Dual Lock	6
E	Introduction to the Security Application Program - Dual Lock	7
	E2. Language Setup	8
F	USB Flash Drive Usage	13
	F2. Unlocking the Device	14
G	Restoring to Factory Settings	18
H	FAQ - Frequently Asked Questions	20

A. Important Notice

[Important notice to Administrator of Crypto Dual or Crypto Dual +](#)

If a master password is set up on initial use then it must be made clear to the user that the master password exists as a backup option to reset the forgotten user password up to the fifth attempt. The master password must be entered before the sixth password entry attempt.

If the user enters the wrong user password six times or if they reset the USB Flash Drive to factory settings (using the reset option) then both the User Password and Master Password will be reset, allowing the user to set a new master and user password without administrator intervention.

It is the administrator's responsibility to ensure that the user is aware of this.

[Important Notice 2.](#)

Plug in only **ONE** device at a time. **DO NOT** plug in two or more secure devices at the same time when running the security program – Dual Lock.

B. General Description

The Integral Crypto Dual and Dual+ USB Flash Drives feature 256-bit AES hardware encryption security, certified to FIPS 197. The 256-bit AES encryption program has a user interface called “Dual Lock”.

The Crypto Dual and Dual+ have two additional features over and above the original Integral Crypto specification. The Dual and Dual+ support a Dual Password function for straightforward management by the User and Administrator (use of the master password is optional). As a secondary feature, the Crypto Dual and Dual+ work with both Windows® and Mac® operating systems.

The manual refers to “Crypto Dual”. The “Crypto Dual+” is identical in operation (it has the same features but a storage capacity of 64GB and above).

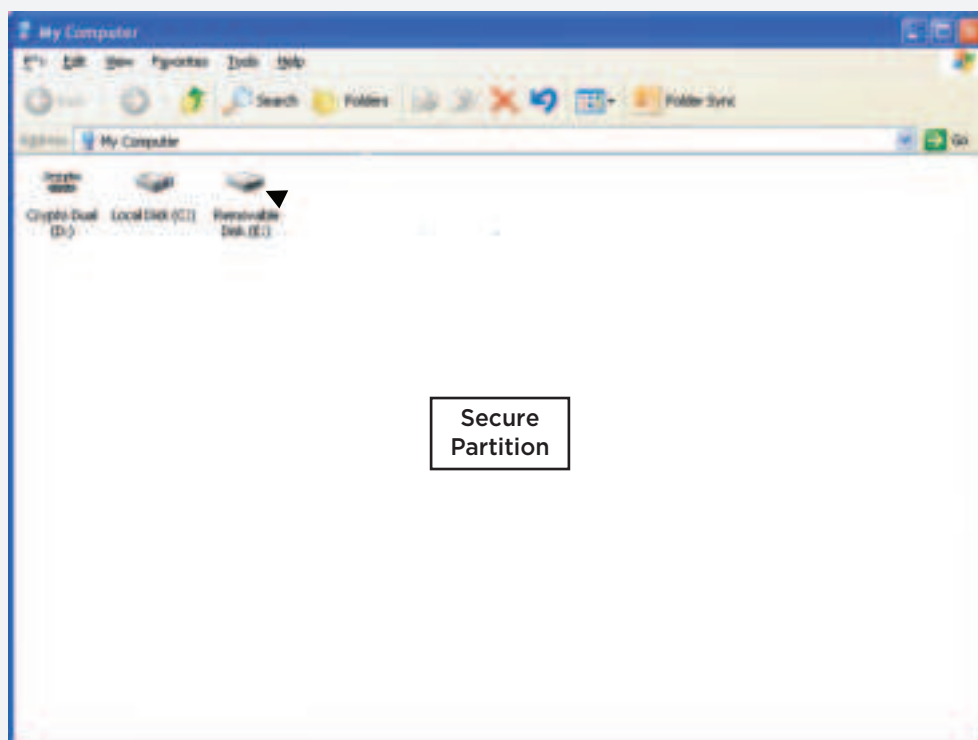
Using the Dual Lock application you can set up a personal private password (with a minimum of 8 - 16 characters set as upper case, lower case letters numbers and special characters).

C. Features

- a. **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, numbers and special characters
- d. **Customized Master Password** - Administrators can now set a master password so the user password can be re-set without the loss of data on the drive
- e. **Fixed Password Retry** - The master & 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
- f. **Friendly Reminder** - there is a password hint function available, in case the master or user forgets his/her password. A password hint message can be setup, with messages up to 32 characters in length
- g. **Multi-lingual Support** - supports 26 languages
- h. **Personal ID Function** - Contact details can be added so that the drive can be returned, whilst confidential data remains secure
- i. **Zero Footprint** - No software installation required

D. Before Using the Security Application Program – Dual Lock

When you plug your Crypto Dual drive into 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 – Dual Lock -- will be stored in the CD--ROM partition with auto--run function, so when you plug in your Crypto Dual to the USB port, the security program will pop up on screen automatically (remember Windows security updates has disabled auto run, so if it is disabled on your system you will need to start the program from My Computer).



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 the Crypto Dual drive. 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 are unable to write or delete data stored in this partition. The security application program – Dual 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.

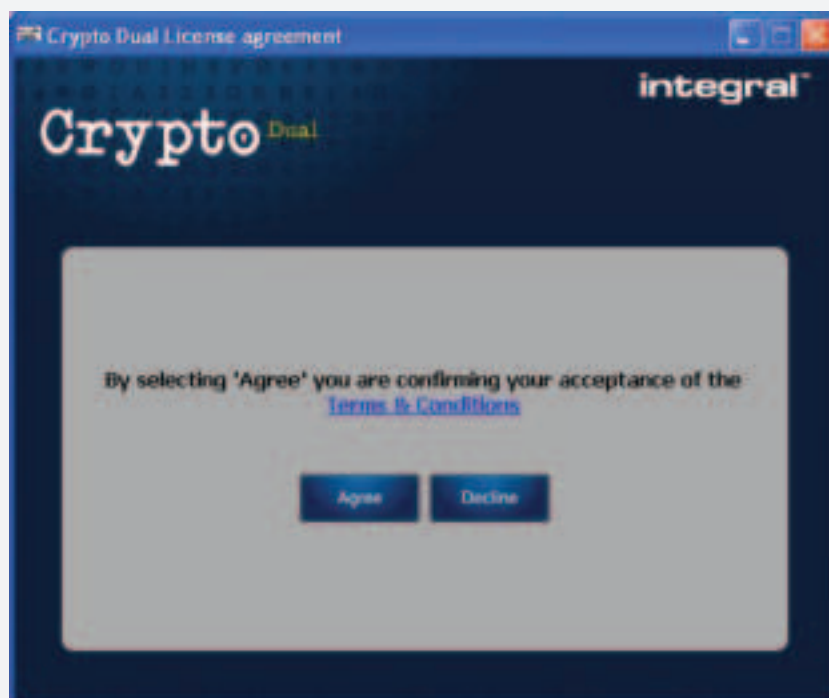
E. Introduction to the Security Application Program – Dual Lock

When you plug your Crypto Dual drive into 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 – Dual Lock -- will be stored in the CD--ROM partition with auto--run function, so when you plug in your Crypto Dual to the USB port, the security program will pop up on screen automatically (remember Windows security updates has disabled auto run, so if it is disabled on your system you will need to start the program from My Computer).

E1. Main Screen



Terms & Conditions



To move forward you will need to hit the 'Agree' button if you hit the 'Decline' button your Crypto Dual drive will close.



E2. Language Setup

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

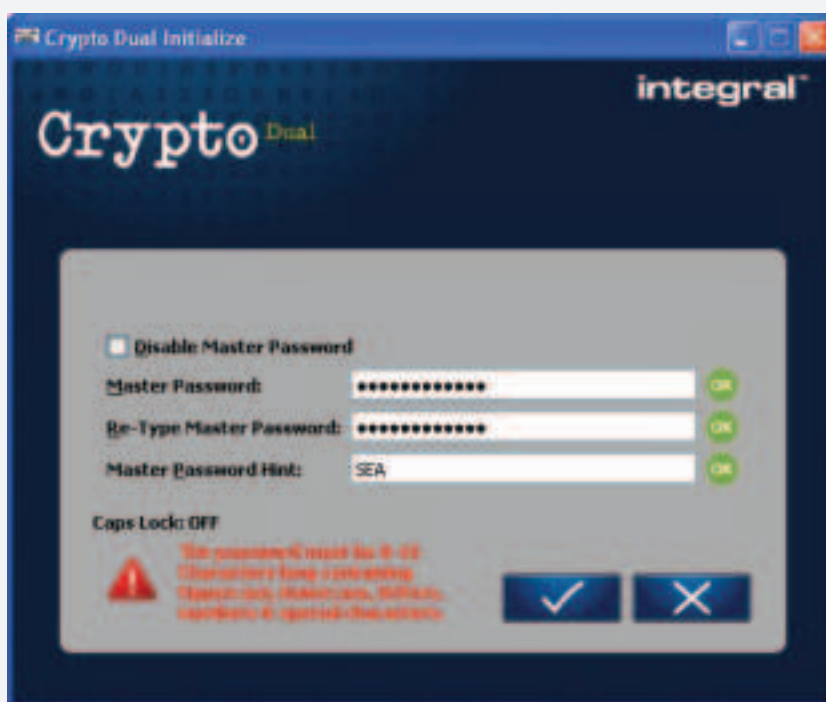
Click  icon.



E3. 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.



E4. Master Password Setup

This screen allows the setup of a complex password for the master or Administrator. The password must consist of between 8 – 16 characters in length and a mixture of uppercase and lowercase letters, numbers and special characters.



E5. User Password Setup


This screen allows the setup of a complex password for the user. The password must consist of between 8 – 16 characters in length and a mixture of uppercase and lowercase letters, numbers and special characters.

E6. Disabling the Master Password

When setting up your Crypto Dual drive you will see a box that will allow you to disable the master password in the password setup, if this box is ticked you will not have to enter a master password and only a user password will be required. (This is not recommended because if the user forgets the password they have set there will be no way to save the data on the drive).



E7. Resetting the Password for the User or Master Password

Sometimes you might want to change your password, this can be done by clicking on the  icon on the top of the main password change screen. You can then change the User password, the Master Password or the User password via the Master password login.

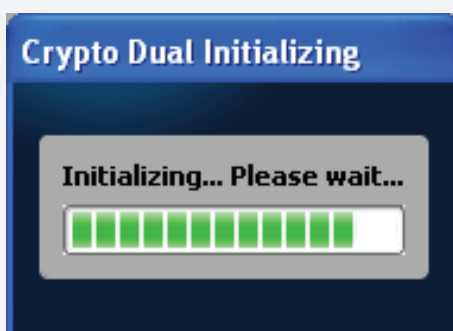


DUAL LOCK

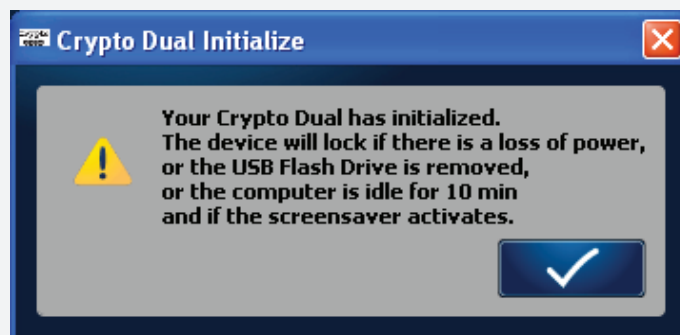
DO NOT FORGET TO ENTER A PASSWORD HINT. THIS SHOULD HELP IF YOU FORGET YOUR PASSWORD.




When you have entered all the details, click  icon. This will initialize the USB Flash Drive by formatting it and setting all parameters that were entered.

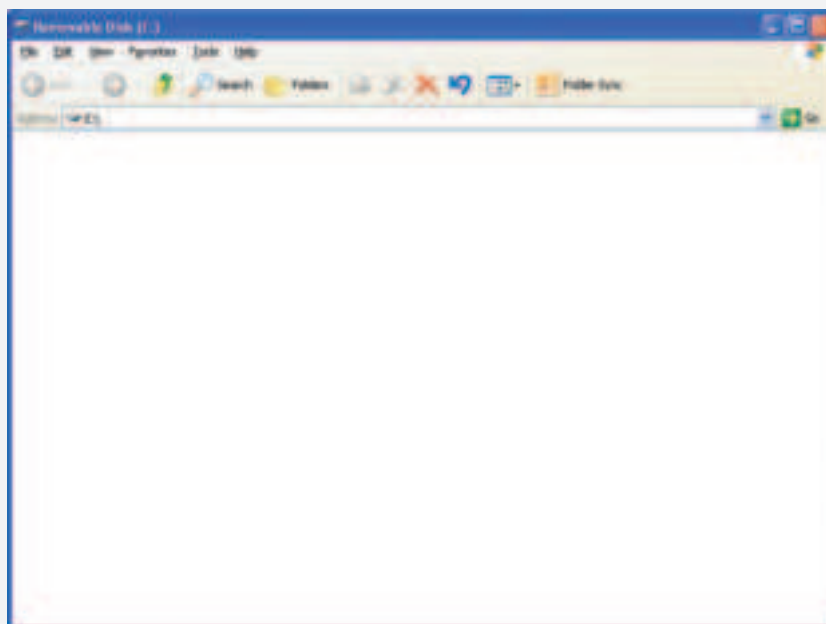


When it has completed you will see the message on screen below:



DUAL LOCK

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




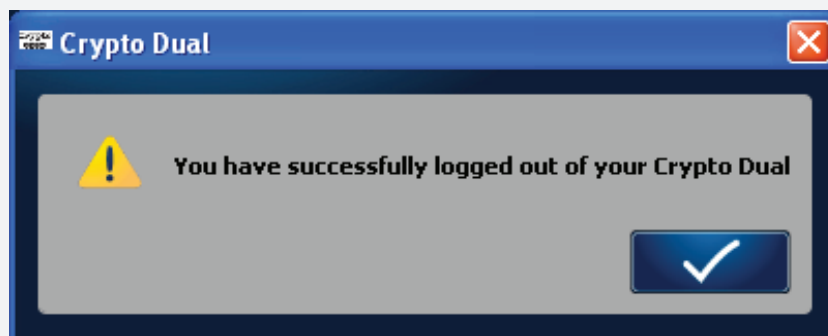
You are now ready to use the Crypto Dual drive. All data that is put in the secure partition will be fully encrypted automatically, or by locking the device via the lock icon or after removing the USB Flash Drive from the socket or if there is a suspension of power. Access to this is only granted with the correct password.

F. USB Flash Drive Usage

F1. Locking the Device

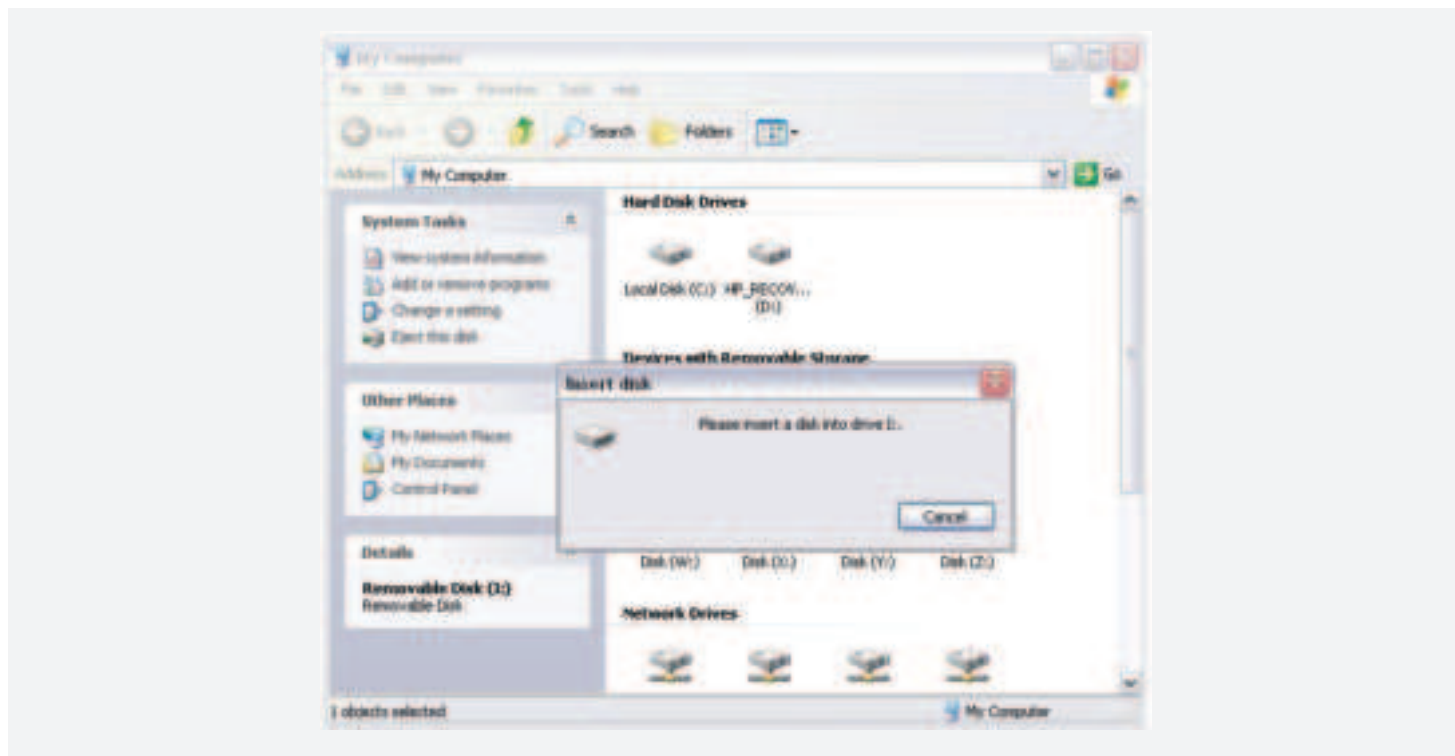


When you have your data on the USB Flash Drive, **click on the**  **icon.**
This will encrypt the data and log you out of the USB Flash Drive.



F2. Unlocking the Device

If you have setup a password, when you remove your Crypto Dual drive from the USB socket (or if there is a suspension in power the screen saver activates, or the computer is idle for 15 min), 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 Dual Lock software.



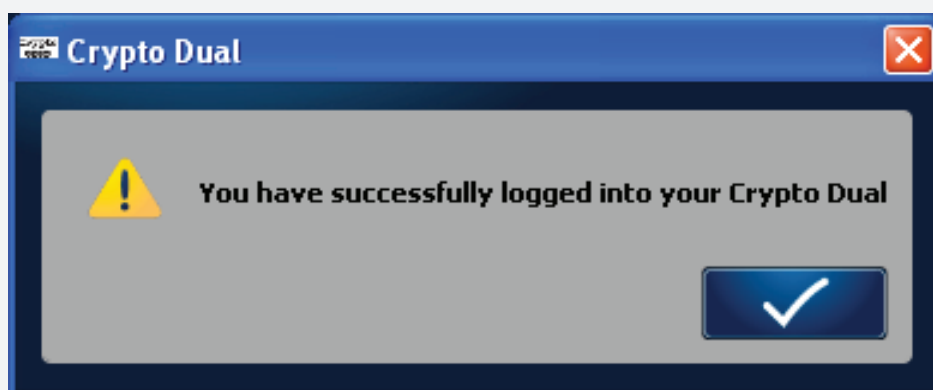
click on the  button.



Input the user or master password depending on who you are. 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.

If the title "Master Password" is highlighted in **Red**, this indicates to the user that a master password has been set.



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.



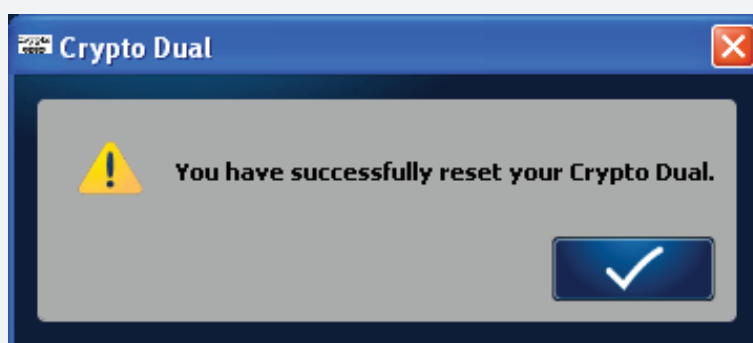
What happens if your Password Hint doesn't help you remember your password or you haven't entered a Password Hint?

The Dual Lock software will allow a maximum of 6 password attempts to be entered before it resets the Crypto Dual. Remember that if a Master Password has been set up you can take your Crypto Dual drive to your administrator and they can reset the user password. If no master password is set, you have the option of resetting the Crypto Dual which will result in the **permanent loss of your data**.

DUAL LOCK



At this point the Crypto Dual drive is not usable until the Dual Lock application has reset. At this stage the drive will be reset back to factory settings and you will see a confirmation message when it is done.



G. Restoring to Factory Settings

G1. Factory Restore

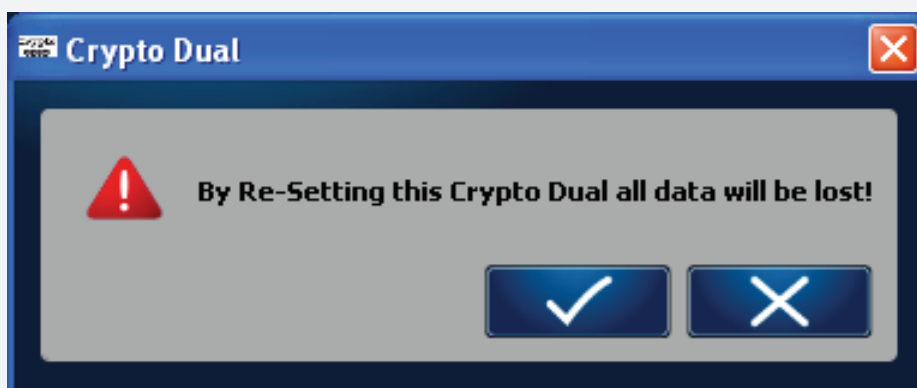
The Dual Lock software allows the user to restore the Crypto Dual drive back to factory settings. For this to be done the USB Flash Drive needs to be in the Locked status.

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

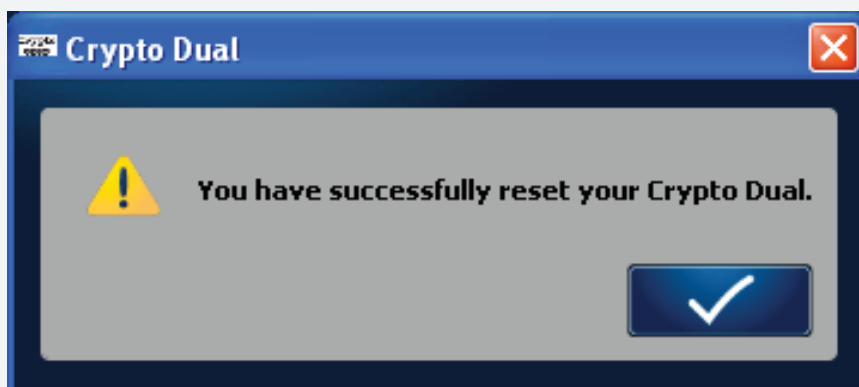


To restore the Crypto Dual back to factory settings, click on the  icon.

Click  icon. You will then see a confirmation message. click  icon again.



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 Dual Lock program, it displayed “Please insert the device or run this utility as privileged user” ?

- **A2** This 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 – Dual Lock requires some security privileges in these Windows operating systems. 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".

Q3 I am having Permission problems with my Integral Crypto Dual 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 sometimes get their permissions striped out, which will make your AES USB Flash Drive fail to initialise. 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™