U.S. Patent Pending

Chameleon Pro

User Device Manual

Marathon

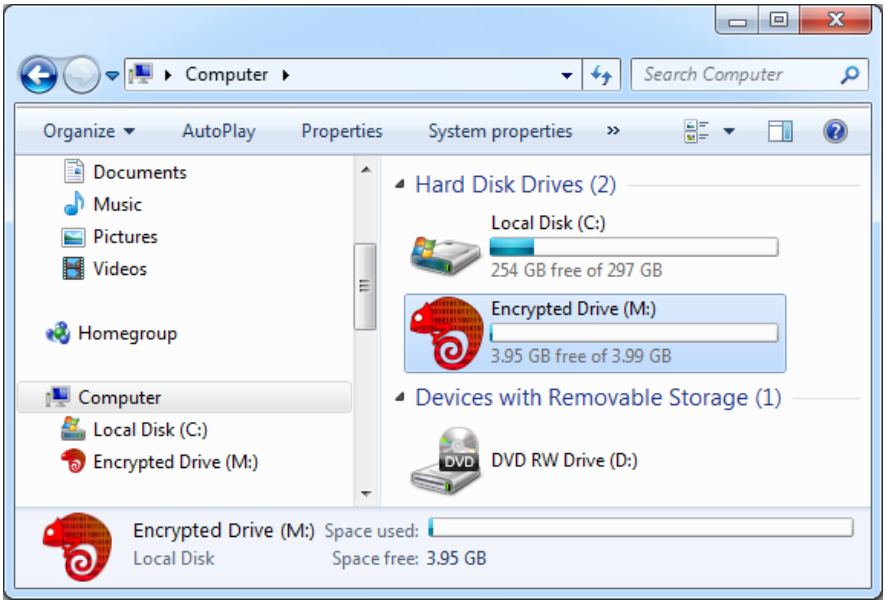
Contents

1 Introduction 2
2 Chameleon Pro User Installation 2
2.1 Uninstalling 4
3 Chameleon Encrypted Drives: Protecting Your Data 4
4 Encrypting Individual Files and Folders 7
4.1 Encrypting Individual Files and Folders 7
4.2 Decrypting Files 10
4.3 Migrating Encrypted Files 13
4.4 View Encrypted File Details 14
5 Password Protection 15
5.1 Password Modification 16
6 Adding, Deleting, and Resizing Encrypted Drives 17
7 PC Lock 19
8 AutoLogin 20
9 Additional Functions and Limitations 23
9.1 Display User Device Programming 23
9.2 Windows Paging File 24
9.3 Lost Chameleon Devices 25
9.4 Safe Removal 25
9.5 Backing up Data 26
9.6 Using the Chameleon Device with Multiple Computers 27
9.7 Using Multiple Devices with the Same Computer 27
10 Limited Warranty and Legal Notices 27

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

1 Introduction

Chameleon Pro protects the files on your PC with AES-256 encryption. Chamelon Pro differs from other USB encryption devices by protecting the files on your hard disk rather than transferring them to a USB device. Chameleon Pro creates an encrypted drive using the free space in your hard disk. Files and applications stored in this encrypted drive are protected and can only be accessed when the Chameleon device is plugged in. Like the key for your car, the device acts like a physical key for your hard disk.



Chameleon Pro includes two types of devices: Masters and Users. User devices provide all of the core Chameleon security features (encrypted drives, individual file encryption, etc.). Master devices offer the same features in addition to being able to manage Users.

A Master can access, create, duplicate, set policies for, and lock out Users. While Users cannot access data protected by other Users, the Master can access data protected by any User associated with it. A Master can also manage its own independent, encrypted data.

The Chameleon Pro works with Windows XP, Vista, and Win7 based PCs.

2 Chameleon Pro User Installation

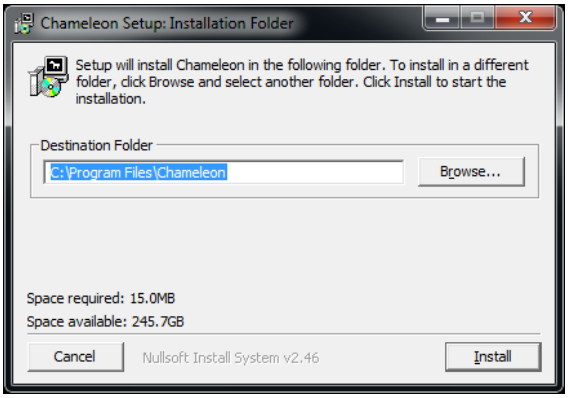
The User device must be initialized by a Master before it is operational.

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

1. Before installing the Chameleon software, make sure any previous versions of the software are uninstalled. Uninstalling does not delete existing encrypted drives.

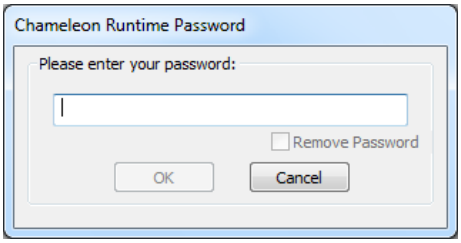
2. **Insert the installation CD** that and **run the Setup** program.[1] (You can also download the setup program from http://www.marathon6.com/chameleon.)

3. **Click on the "Install" button** to load the software.

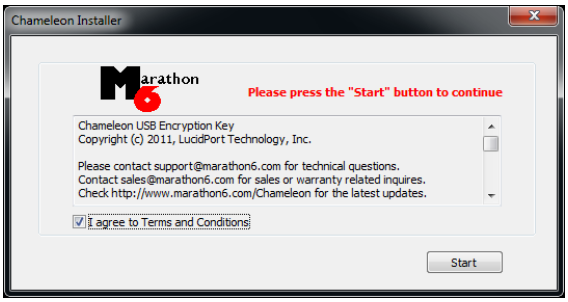


4. **Insert your User device**.

5. If your IT administrator requires a password on your device, you will be prompted to enter it. Contact your IT administrator for the temporary password

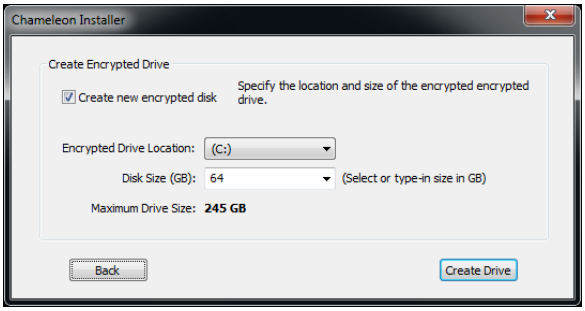


6. **Press "Start"** to launch the installation wizard.



[1] On some Windows7 computers, you may get a User Account Control warning that a program is trying to make changes to the computer. Select "Yes" or "Install" if this occurs.

7. **Choose** the encrypted drive location and size.



8. **Press "Create Disk"**.

All content copied to the encrypted drive is automatically protected. It is accessible when the device is inserted, and disappears when the device is removed.

2.1 Uninstalling

You can uninstall the Chameleon software by locating "Chameleon" from the Windows start menu and selecting "Uninstall" (Start > All Programs > Chameleon > Uninstall). Uninstalling does not remove your encrypted drives. To remove the encrypted drives, delete the directory ChameleonDrives from your hard disk's top level directory (ex. C:\ ChameleonDrives\). The ChameleonDrives directory can only be deleted when the Chameleon device is unconnected.

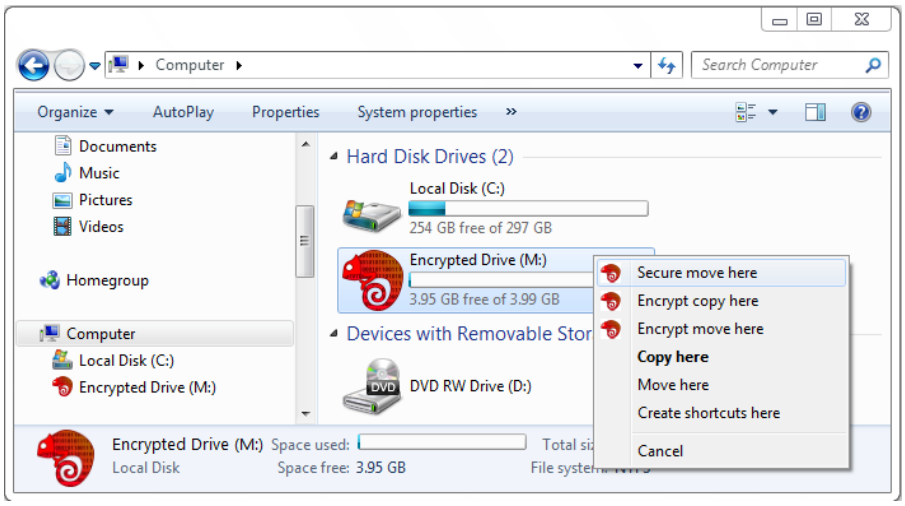
3 Chameleon Encrypted Drives: Protecting Your Data

Plug in your Chameleon device to access the encrypted drive. The encrypted drive appears like any other hard disk in your system. You can store files in it, open files from it, install and run programs from it, move files from one directory to another, and direct applications to use the encrypted drive. Once the Chameleon device is removed, the encrypted drive disappears from Windows. A forensic examination of your hard disk will reveal only encrypted, apparently random, data.

Only files that are stored on the Chameleon drive are encrypted. Any files copied or read from the encrypted drive are automatically decrypted. For instance, if a user were to attach a file from an encrypted drive to an email, that file would be attached decrypted. For securing email attachments and cloud storage, see section "4 `Encrypting Individual Files and Folders`".

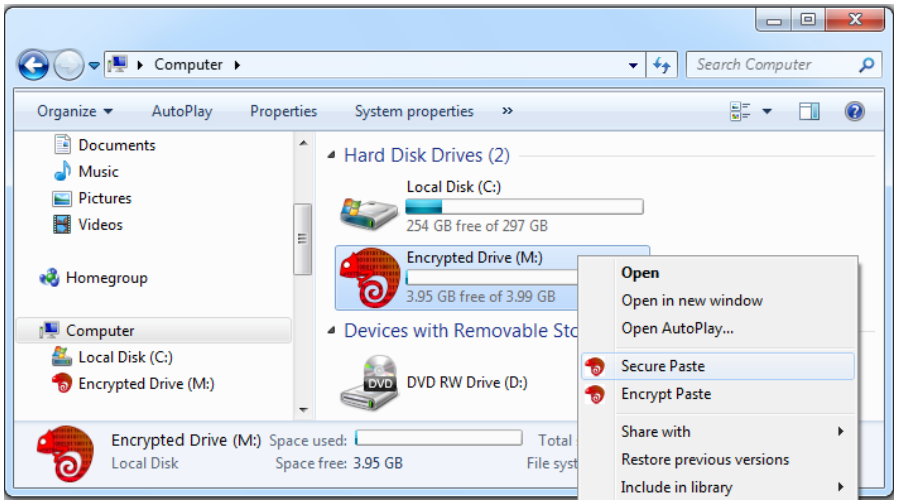
You can copy files to the encrypted drive simply by dragging and dropping them there. However, this retains the original unencrypted file at its original location. A more secure method is to right-click drag and drop. Hold down the right mouse button, then drag the selected file to the encrypted drive. A dialog appears showing "Copy", "Move", and "Secure move". The secure move option moves the file into the encrypted drive, then scrubs away any traces of that

file from its original location.[2] If a significant amount of data is involved, this may take some time.



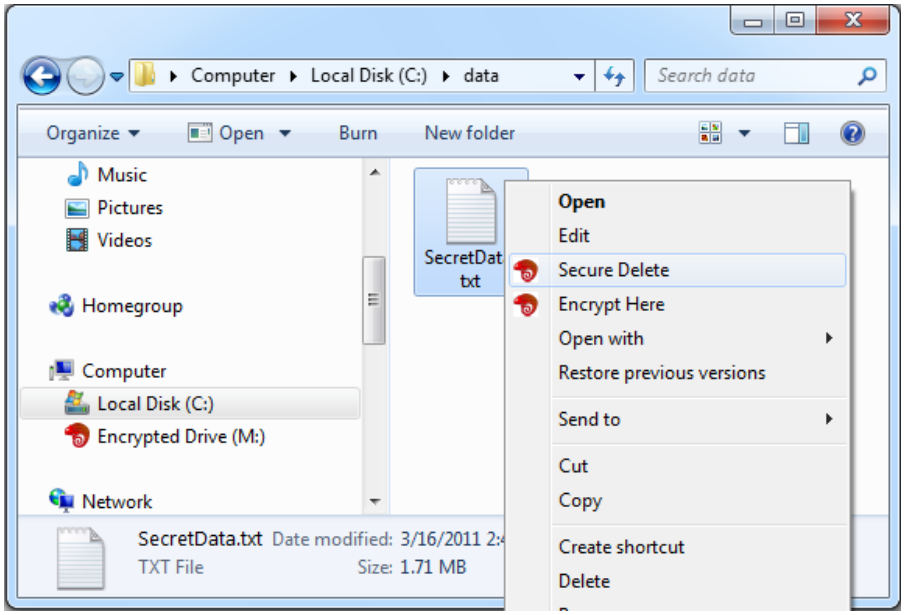
You can also securely move a file to the encrypted drive by using the secure paste option. Right click on the file or folder you want to move, then select "Cut". Next, right click on a encrypted drive or sub-directory, then select "Secure Paste". Like the secure move option, the secure paste command cleans away all traces of the unencrypted files from the hard disk.

Secure commands are only available when the Chameleon device is plugged in.



[2] The standard Windows move command copies the file, then marks the original file as deleted. The deleted file may be recoverable with specialized tools. The secure move option prevents recovery by overwriting the deleted file.

The Chameleon software also adds a secure delete command. Right click on any file or folder then select "Secure Delete". This is more secure than deleting the file then deleting it again from the Windows' Recycle Bin. Since secure delete overwrites every bit of the file from the hard disk, this may take some time if a significant amount of data is involved. The normal Windows cut, paste, and delete commands are still available.

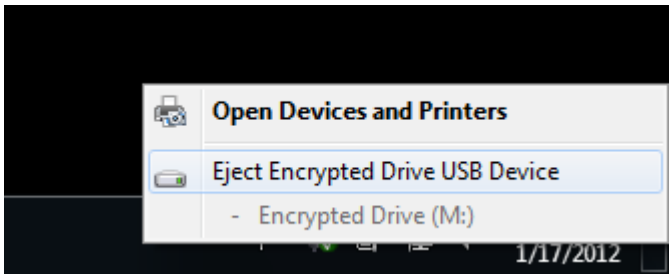


Deleting a file stored in an encrypted drive places it in the Windows' Recycle Bin. You can recover the file from the Recycle Bin as long as the Chameleon device is still inserted. Deleted files disappear from the Recycle Bin when the device is removed. They reappear in the Recycle Bin when the device is reinserted. There is no need to secure delete any files located in the encrypted drive.

Any files you create directly on the encrypted drive are automatically protected. However, some applications store temporary information to your unencrypted drive. This information may be recoverable with specialized tools. You should direct your applications to store their temporary files in the encrypted drive. This can usually be accomplished by installing your applications directly in the encrypted drive.

You can plug or unplug the Chameleon device at any time. Your computer is still fully functional without the Chameleon device. Only the encrypted drive (and any programs and data in it) will be unavailable. Be aware that unplugging the device while writing data to the encrypted drive may result in data corruption. This is similar to removing an external hard disk in the middle of a write to it. To be absolutely sure that no writes are occurring, use the Windows Safe Remove function before unplugging the device.

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com



If an application is open with an encrypted file, that application and file may still be accessible even after you unplug the Chameleon device. For example, let's say you are editing a protected file in Microsoft Word. If you unplug the device, a copy of this file is still open in Word. You cannot save this file to the encrypted drive until you re-insert the device. However, you are still able to view and edit the parts of the file cached in working memory.

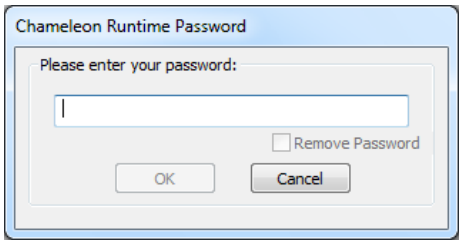
4 Encrypting Individual Files and Folders

The Chameleon device automatically encrypts all data placed in the encrypted drive and automatically decrypts all data taken out of the encrypted drive. While convenient and secure, this does not protect information you email or store online. For these situations, the Chameleon device can encrypt and decrypt individual files and folders.

4.1 Encrypting Individual Files and Folders

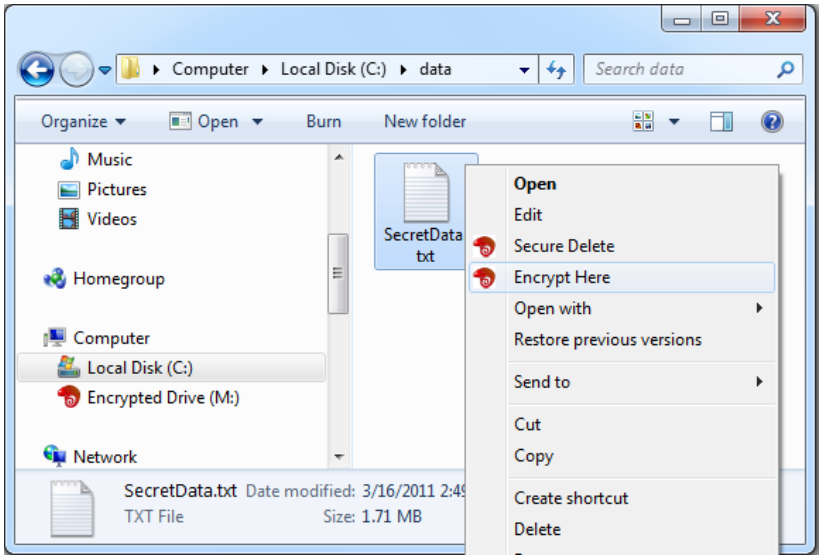
You can encrypt a single file, a group of files, or whole directories (but not shortcuts or special icons like the Windows Recycle Bin). Files encrypted by a Chameleon device can only be decrypted using the same device (or by its Master).

1. **Plug in the device**
2. **Enter your password (if enabled)**



3. **Right click on the file** or folder you want to protect.

4. **Select "Encrypt here"** to create an encrypted version of the selected file

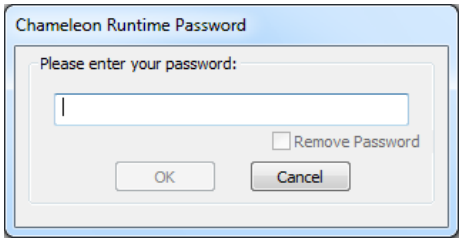


The encrypted file appears as a file in the same folder with the same file name but with the extension ".cge". If desired, you can change the file name, but not the extension. This file is encrypted using device's AES-256 hardware. Unlike the encrypted drive, the encrypted file is still visible when the device is removed. It can be attached to an email, copied to a thumb drive, stored on the network, or synced to a cloud service.

You can also encrypt individual files and folders with right click drag and drop.

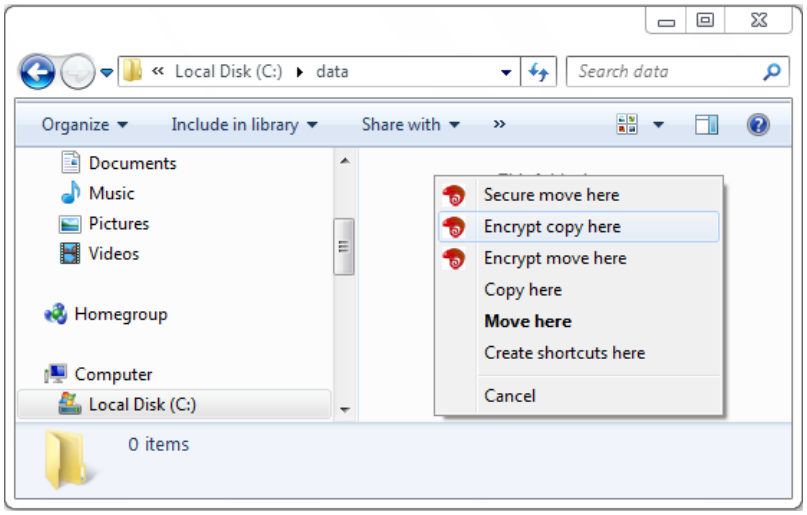
1. **Plug in the device**

2. **Enter your password (if enabled)**



3. **Click and hold down the right mouse button on the file** or folder you want to protect.

4. **Drag the mouse pointer** to the target folder and release the right mouse button. The encrypted file will be created in this folder.



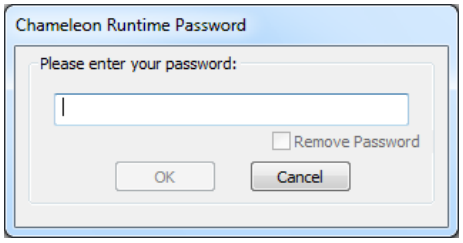
5. **Select "Encrypt move here" or "Encrypt copy here"**.
   "Encrypt move here" places the encrypted file at the destination while securely deleting the source file.

   "Encrypt copy here" does the same without deleting the source file.

You can also encrypt a file or folder by using the encrypted paste option:

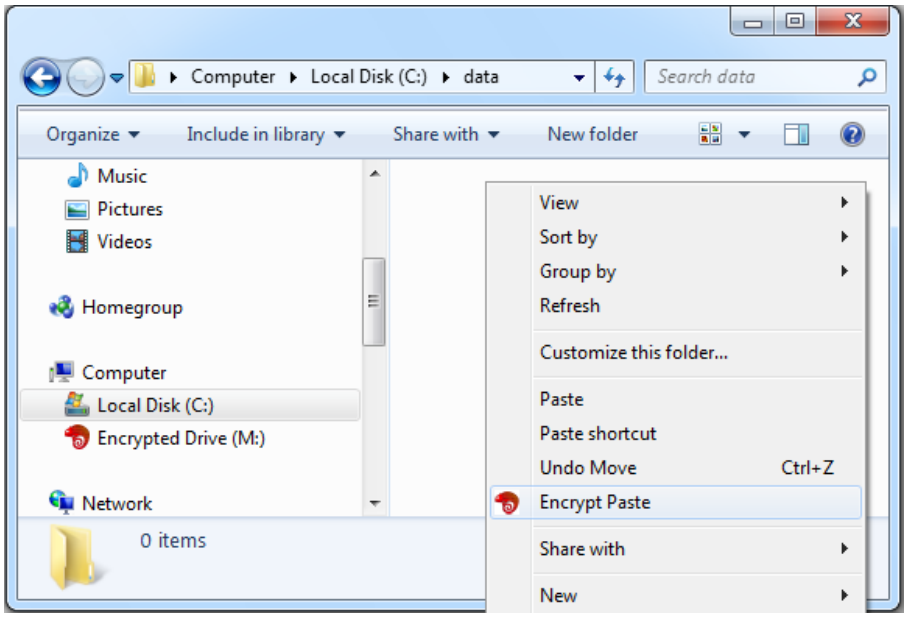
1. **Plug in the device**

2. **Enter your password (if enabled)**



3. **Right click on the file** or folder you want to encrypt, then **select "Cut" or "Copy"**. You can also use the Cut (CTRL+x) or Copy (CTRL+c) keyboard shortcuts.

4. **Right click on the destination drive or directory.**



5. **Select "Encrypt Paste"**

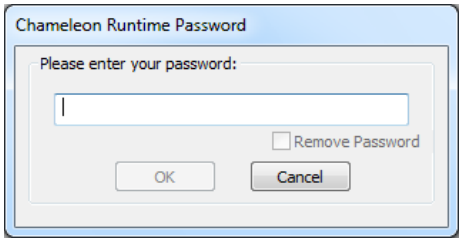
This places the encrypted file at the destination. If you selected "Cut", the source file will be securely deleted after the encryption completes.

4.2 Decrypting Files

To decrypt a .cge file:

1. **Plug in the device**

2. **Enter your password (if enabled)**



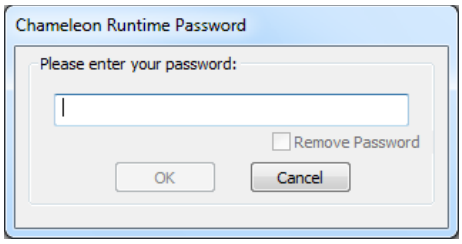
3. **Double click the .cge file**.
   The decryption process will begin immediately.

Note: if you open the .cge file from an application (e.g. a web browser) using (for example) "Open With", then the file will be downloaded and decrypted in a temporary folder of the application's choosing. This will place the decrypted contents of the .cge file in an unintended folder. Instead of opening the .cge directly from the application, save the .cge file to a folder of your choice (using "Save As"), and then decrypt the file.

The other methods for decrypting .cge files are essentially identical to encrypting:

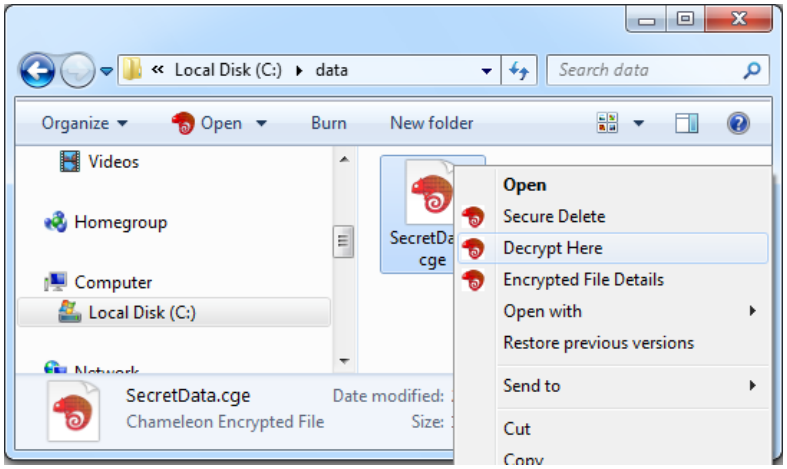
1. **Plug in the device**

2. **Enter your password (if enabled)**



3. **Right click on the .cge file** to be decrypted.

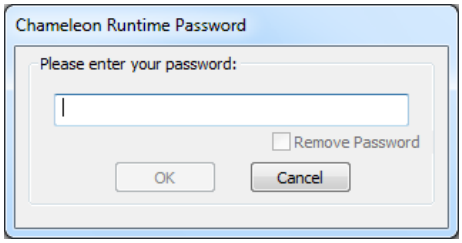
4. **Select "Decrypt here"** to create a copy of the decrypted file(s) or folder(s) contained within the .cge file



Likewise, you can decrypt .cge files using the right-click/drag and drop method. Use this method when the .cge file is located in unsecure storage. It is more secure because it avoids having your unencrypted data reside (temporarily) in the unsecured storage. For instance, you may have a .cge file stored on a network drive. Instead of double-clicking the file to decrypt it on the network folder, you could use the following method to decrypt the file onto your local hard drive.

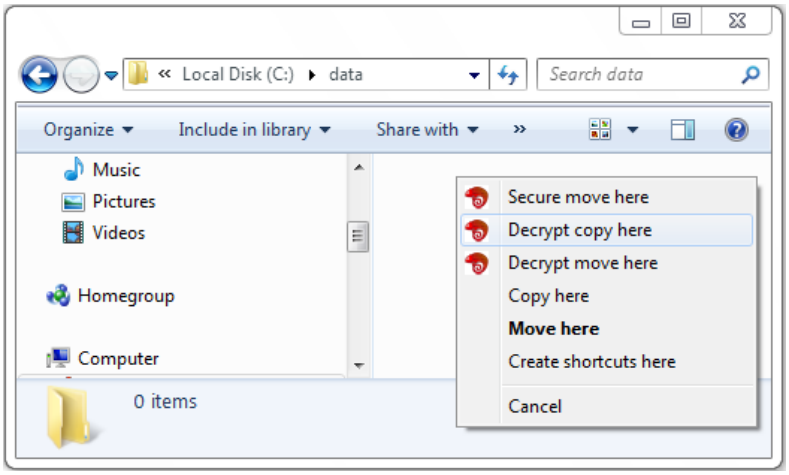
1. **Plug in the device**

2. **Enter your password (if enabled)**



3. **Click and hold down the right mouse button on the .cge file**.

4. **Drag the mouse pointer** to the target folder and release the right mouse button. The decrypted contents will be created in this folder.



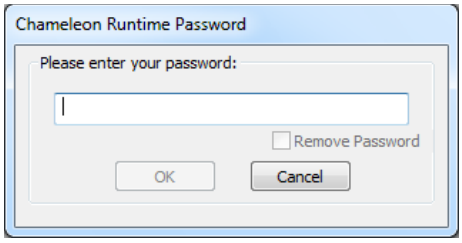
5. **Select "Decrypt move here" or "Decrypt copy here"**.
   "Decrypt move here" places the decrypted contents at the destination while securely deleting the .cge file. You may want to use this method to avoid having your unencrypted data reside (temporarily) in remote or unsecured storage.

   "Decrypt copy here" does the same without deleting the source file.

The Decrypt Paste option is also available:

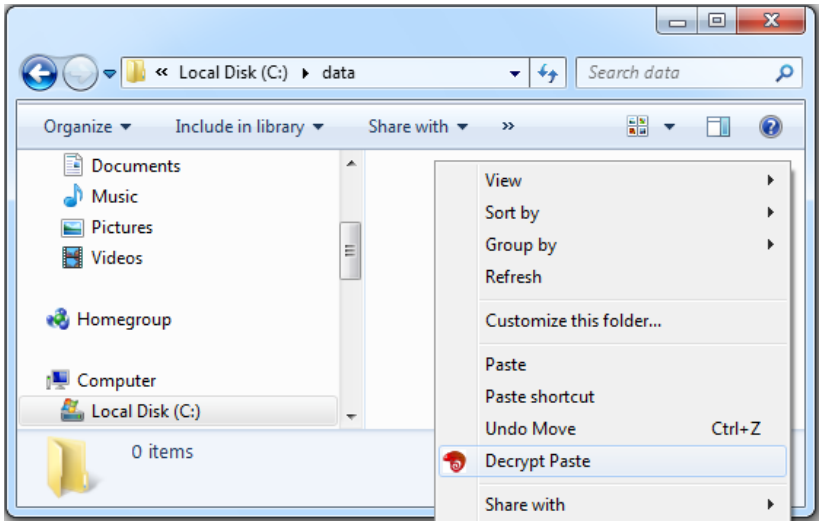
1. **Plug in the device**

2. **Enter your password (if enabled)**



3. **Right click on the .cge file** to be decrypted, then **select "Cut" or "Copy"**. You can also use the Cut (CTRL+x) or Copy (CTRL+c) keyboard shortcuts.

4. **Right click on the destination drive or directory.**



5. **Select "Decrypt Paste"**

This places the decrypted contents at the destination. If you selected "Cut", the source file will be securely deleted after the decryption completes.

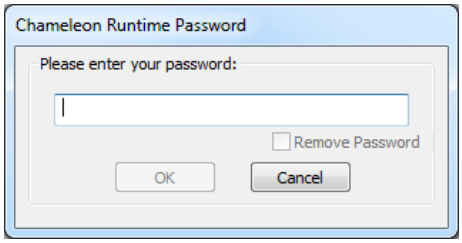
4.3 Migrating Encrypted Files

There are some scenarios in which it is necessary to migrate .cge files:

- The Master device has been replaced: In this case, an IT administrator will provide an updated User device. The user will need to migrate .cge files encrypted with the original key to the updated Master.
- A User is being retired: a User ID may need to be retired if a User device has been lost or a user is leaving the company. A migration-enabled User device can transfer ownership of a .cge file from the retired User ID to your User ID.

1. **Plug in the device**
   (Updated User device or migration-enabled User device)

2. **Enter your password** (if enabled)



3. **Start the "Encrypted File Migrator"**

Click on Windows "Start" >
All Programs >
Chameleon >

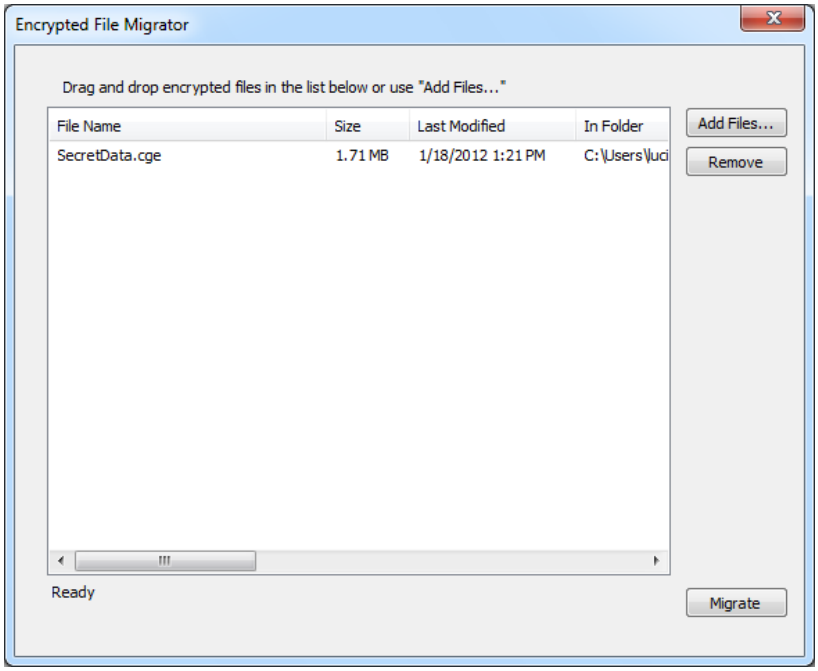
Encrypted File Migrator

4. **Select the .cge files to be migrated.**

   Drag them directly into the Chameleon Migrator file list.

   or

   Click on "Add Files", navigate to and select the files.



5. **Close all open files residing in the encrypted drive.**

   Before the migration process begins the encrypted drives will be detached. If a file is open, the Migrator will prompt the user to close it.

6. **Click on the "Migrate" button**

Once the migration process is complete, the old user will not be able to access the encrypted file.

The hard disk containing the .cge files must have enough free space to contain a copy of the largest file in the list. Depending on the volume of encrypted data, this process may take some time.

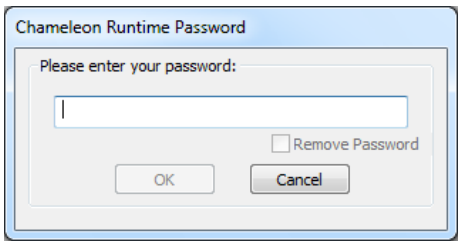
Your encrypted drives will be reattached when the migration process is complete.

4.4 View Encrypted File Details

To view the details of an encrypted file:

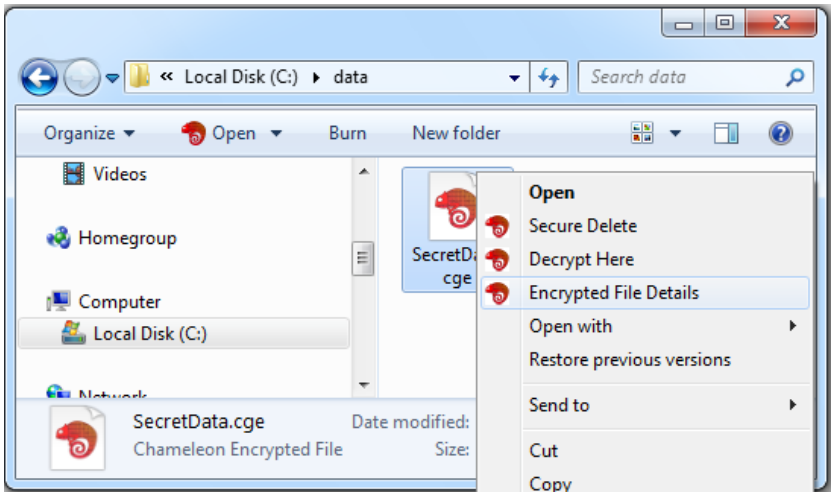
1. **Plug in the device**

2. **Enter your password** (if enabled)

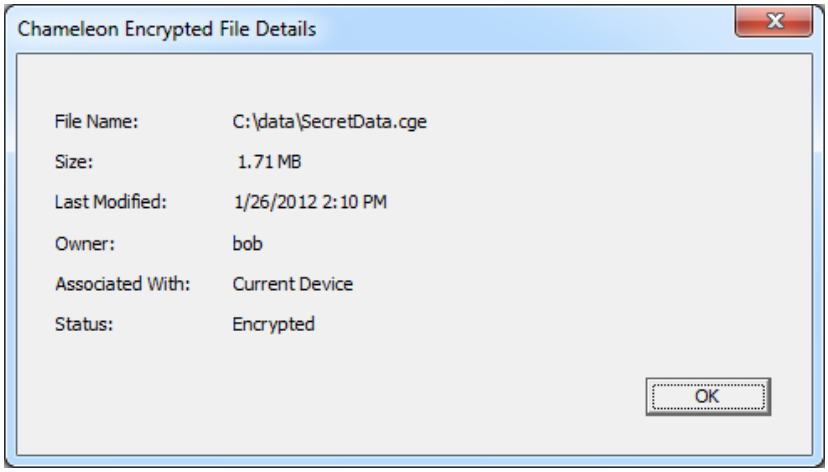


3. **Right click on the .cge file**

4. **Select "Encrypted File Details"**

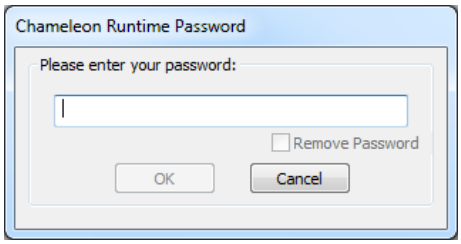


5. The file details are displayed in a new window



5 Password Protection

By default, no passwords are required for User devices. However, you may enable a password or your IT administrator may require password protection to secure your data in the event that you lose your device along with your PC. When enabled, the Chameleon software requests the password whenever it is plugged in or when the computer is restarted or wakes from sleep.

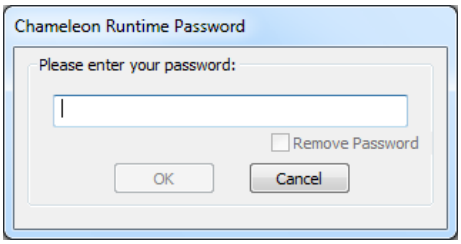


5.1 Password Modification

If allowed by your IT administrator, you can add, change, or remove Chameleon password protection. A password does not lock out access by the Master, or by duplicate User devices with the same User ID. The password only prevents unauthorized people from using your particular device.

To modify password options:

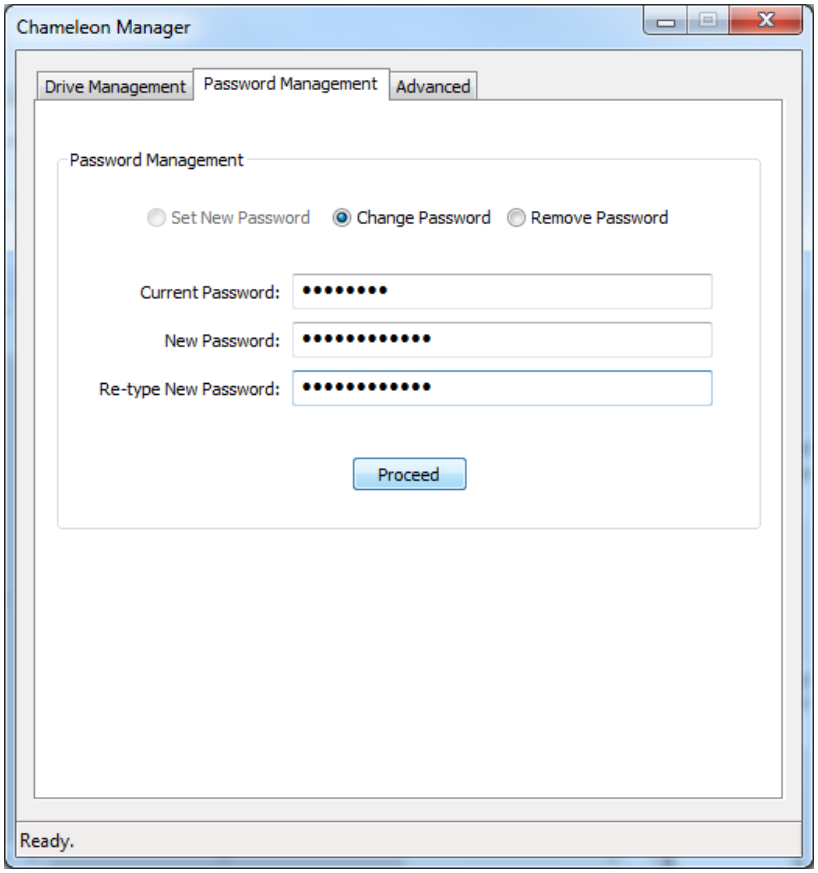
1. **Plug in the device**
2. **Enter your password (if already enabled)**



3. **Start the Chameleon Manager**

Click on Windows "Start" >
All Programs >
Chameleon >
Chameleon Manager

4. **Select the "Password Management" tab.**



- To add a password, select "Set New Password" then enter the new password and click the "Proceed" button.

- To change your password: Select "Change Password". Enter your existing password. Enter the new password and verify it. Click the "Proceed" button. If your IT administrator has enabled password complexity, your password must be at least 6 characters long and include at least one number and one letter.

- To remove the password, select "Remove Password" then enter your existing password and click the "Proceed" button.

You can change the password as many times as you want.

6 Adding, Deleting, and Resizing Encrypted Drives

You can add, delete, or resize encrypted drives at any time. As long as there is sufficient disk space, there is no limit to the number of encrypted drives you can have associated with a single

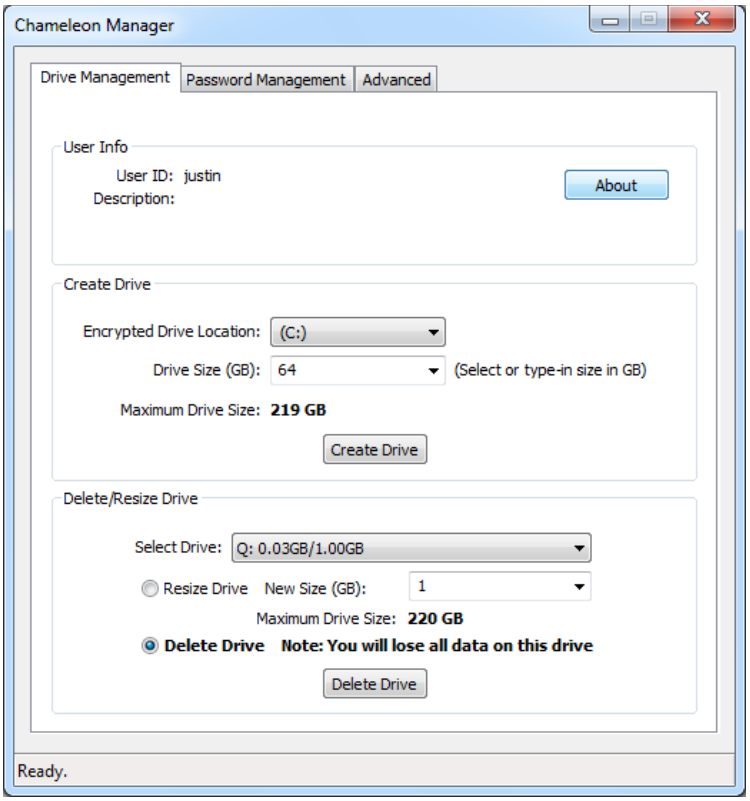
Chameleon device. Encrypted drives can be created on your internal hard disk as well as external USB drives.

1. **Plug in your device.**

2. **Start the Chameleon Manager**

   Click on Windows "Start" >
   All Programs >
   Chameleon >
   Chameleon Manager

3. **Select the "Drive Management" tab.**



- To add a drive, specify the size and location of the encrypted drive, then click the "Create Drive" button.

- To delete a drive, select the existing drive from the drop down menu, then select "Delete Drive". Click on the "Delete Drive" button. You will be prompted to type in a confirmation.

- To resize a drive, select your drive from the drop down menu, then select "Resize Drive". Enter the desired size, then click the "Resize Drive" button. When reducing drive size, your hard disk (C:\) must have enough free space to temporary hold all the contents of the

encrypted drive.

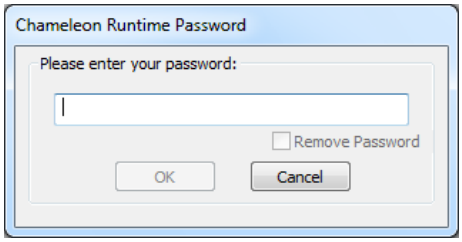
7 PC Lock

Unplugging the Chameleon device protects your sensitive data, but open documents, network connections, and email may still be vulnerable. PC Lock automatically locks the Windows session whenever the device is removed.

To enable PC Lock:

1. **Plug in the device**

2. **Enter your password** (if enabled)



3. **Start the Chameleon Manager**

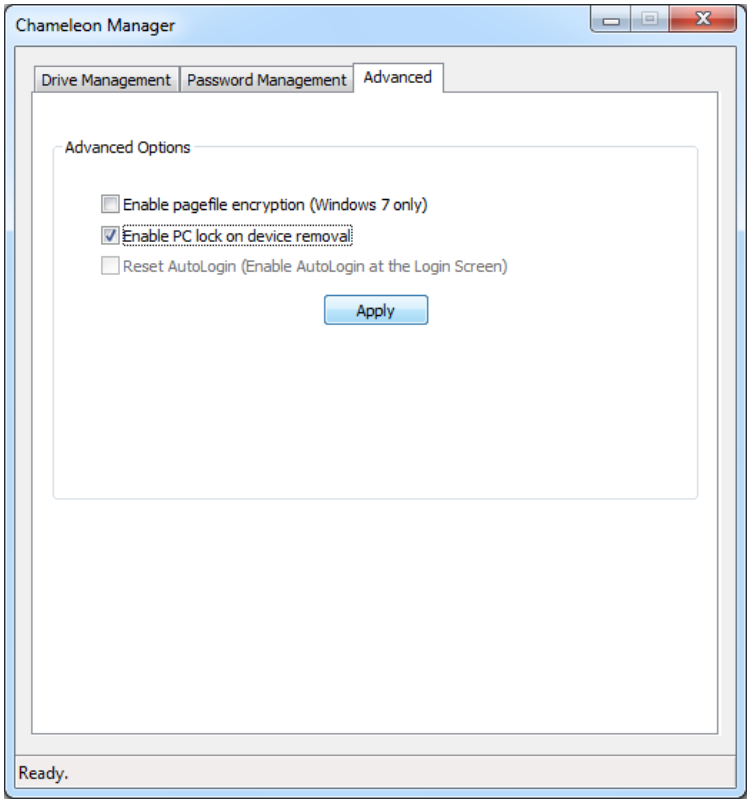
Click on Windows "Start" >
All Programs >
Chameleon >
Chameleon Manager

4. **Select the "Advanced" tab**.

5. **Select "Enable PC Lock on device removal"**

6. **Click on "Apply"**.

You cannot disable PC Lock if it is required by your IT administrator.



8 AutoLogin

Chameleon Autologin is the opposite of PC Lock: if enabled, you can log-in to Windows simply by plugging in the Chameleon device. AutoLogin is only supported on Windows Vista and Windows 7.

Autologin is not supported on devices with a password enabled.

Masters have the option of forbidding their Users from using AutoLogin.

To enable AutoLogin:

1. **Goto the Windows Login Screen.**

2. **Plug in your User device.**

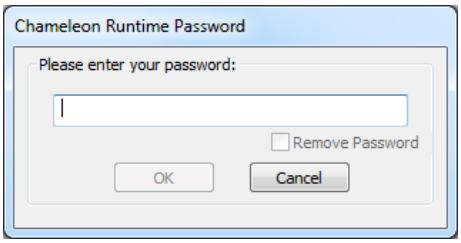
3. **Enter** your **Windows login information**.

The login information will be verified with the operating system. If login is successful, the login information is encrypted and saved. The next time the Chameleon is plugged in at the login screen, Windows will log-in automatically.

To disable AutoLogin:

1. **Plug in the device**

2. **Enter your password** (if enabled)



3. **Start the Chameleon Manager**

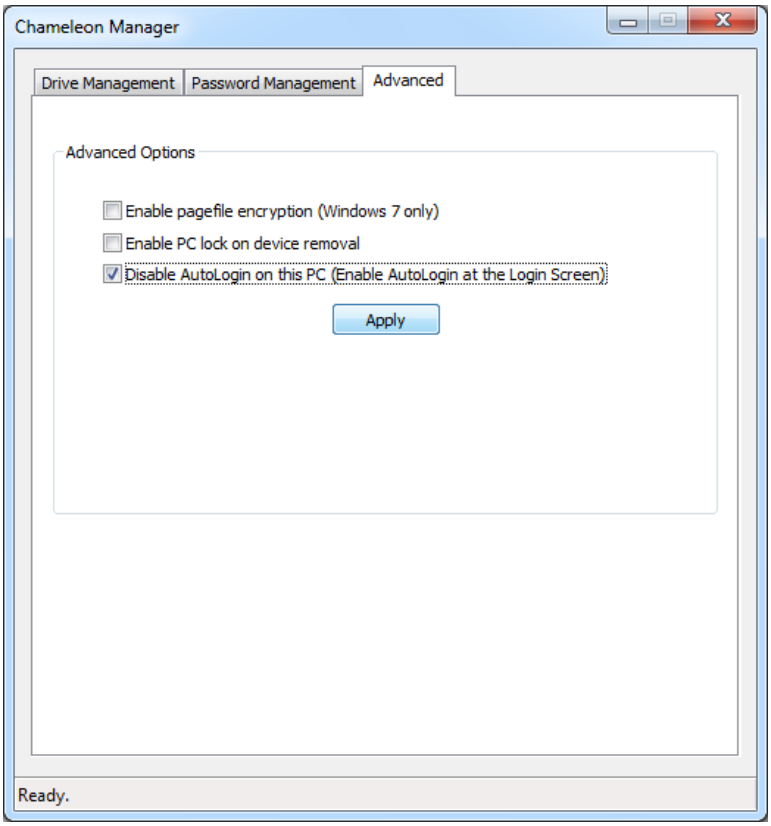
Click on Windows "Start" >
All Programs >
Chameleon >
Chameleon Manager

4. **Select the "Advanced" tab**.

5. **Select "Disable AutoLogin on this PC"**

6. **Click on "Apply"**.

This disables AutoLogin only on the current PC. It does not disable AutoLogin on the device.



9 Additional Functions and Limitations

9.1 Display User Device Programming

To review a User device's programming:

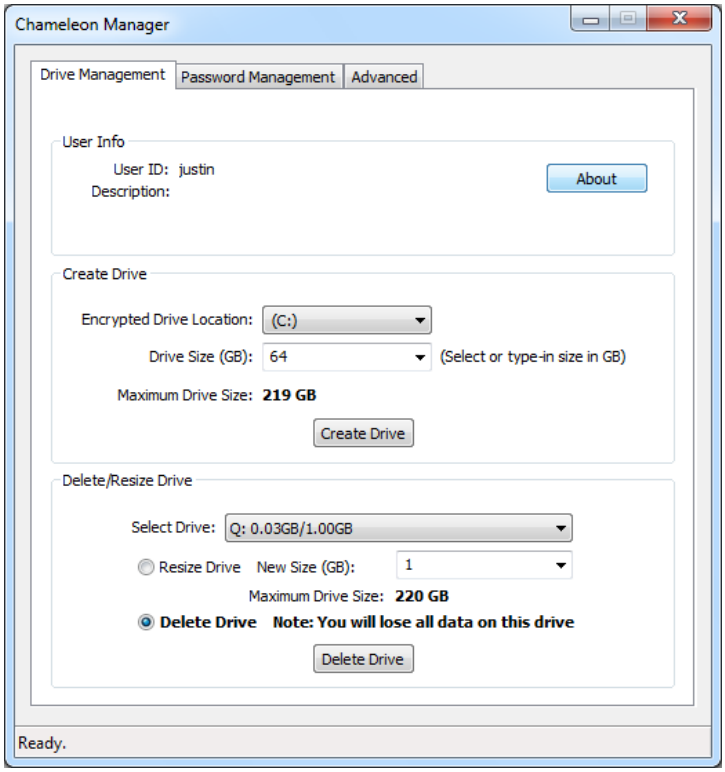
1. **Plug in the User device.**

2. **Start the Chameleon Manager**

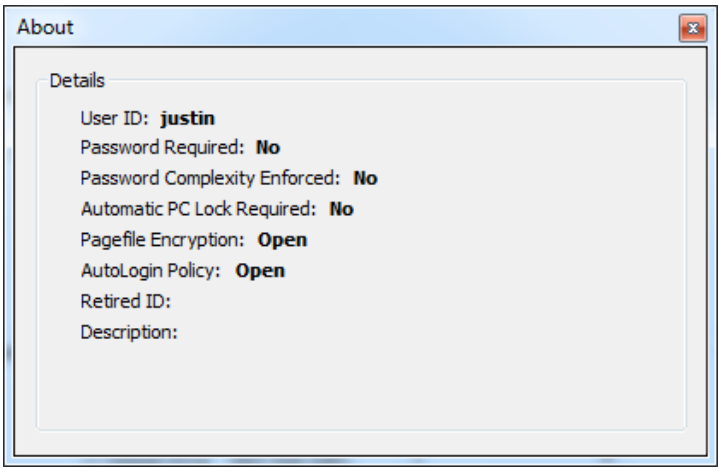
   Click on Windows "Start" >
   All Programs >
   Chameleon >
   Chameleon Manager

3. **Select the "Drive Management" tab.**

4. **Press the "About" button**



5. The About box displays the User's configuration.



9.2 Windows Paging File

Windows may store temporary data in its paging file (virtual memory). This file is usually unencrypted and is updated continuously. Enable pagefile encryption to direct Windows to encrypt its paging file. Your IT administrator may require paging file encryption.

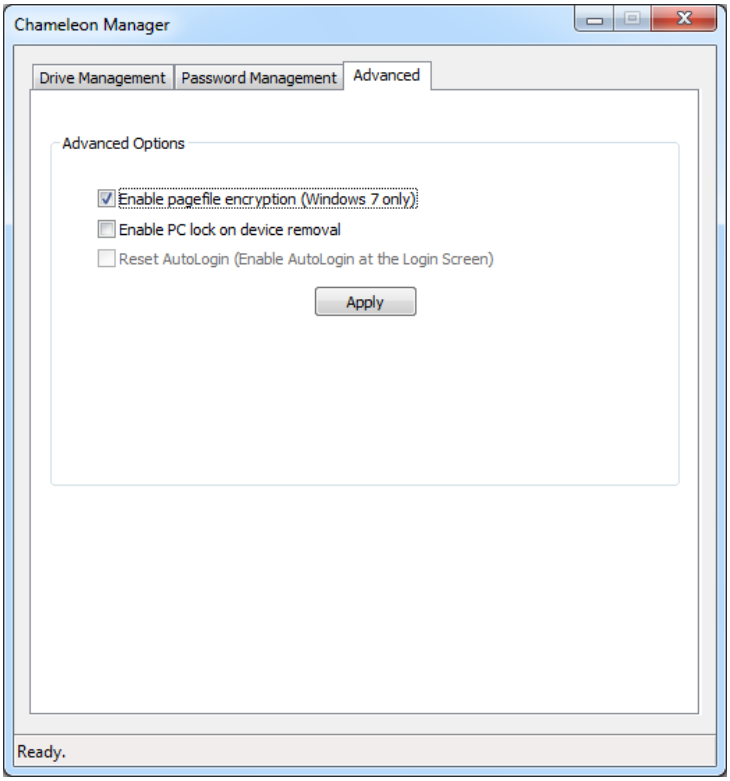
To enable page file encryption:

1. **Plug in the device.**

2. **Start the Chameleon Manager** Click on Windows "Start" > All Programs > Chameleon > Chameleon Manager

3. **Select the "Advanced" tab.**

4. **Select "Enable pagefile encryption"** then **click on "Apply"**



Encrypting the paging file eliminates a potential security hole, but slows the computer down slightly. Only Windows 7 supports page file encryption (ignored for other operating systems).

9.3 Lost Chameleon Devices

If you lose or break your Chameleon device, contact your IT administrator immediately. The data in the encrypted drive can be recovered using a duplicate User device. A migration-enabled User device can also re-encrypt you data, preventing a lost device from accessing your data.

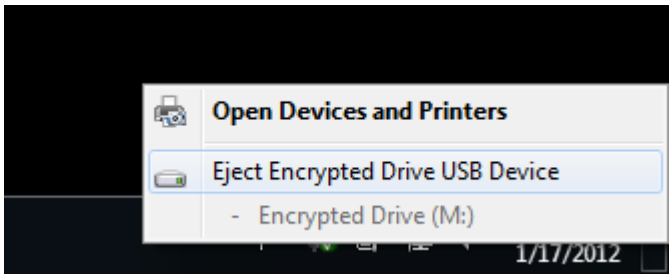
9.3.1 User Migration

When a Chameleon device is lost or a user is leaving the company, the IT administrator may provide you with a migration-enabled User device. This device will allow you to migrate the retired User's data to your User ID. To migrate the encrypted drives, simply plug in the device and open the Chameleon Manager. To migrate .cge files, see "4.3 Migrating Encrypted Files".

9.4 Safe Removal

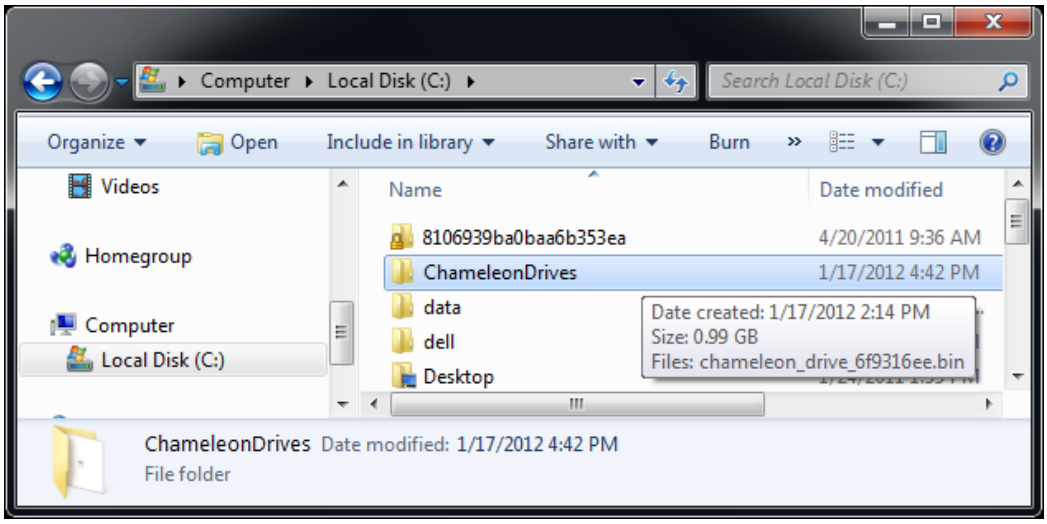
Unplugging the Chameleon device while writing data to the encrypted drive may result in data corruption. This is similar to removing an external hard disk in the middle of a write to it. To be

absolutely sure that no writes are occurring, use the Windows Safe Remove function before unplugging the device.



9.5 Backing up Data

Backup encrypted drives by copying the ChameleonDrives directory to another location. This directory is located at the top level of your hard disk (ex. C:\ChameleonDrives\). Since encrypted drives are always encrypted, backups are still protected. You should not plug in the Chameleon device when backing up your data.



You can add the ChameleonDrives directory to your list of scheduled backups.

WARNING: Do not copy the backup ChameleonDrives directory to the top level (root) of a drive (e.g. D:\ChameleonDrives). The Chameleon software cannot distinguish between the original and the copy. If identical drives are detected in the top level, the Chameleon software will not activate either drive. Any subdirectory or network location will work (e.g. D:\backup\ChameleonDrives).

9.6 Using the Chameleon Device with Multiple Computers

A User device can be used with multiple computers. If the Chameleon software has already been installed on the new computer, there is no need to reinstall it. If the Chameleon software is not installed, insert the Chameleon Installation CD and run the installer on the new computer.

9.7 Using Multiple Devices with the Same Computer

You can have multiple encrypted drives associated with different User devices on the same computer and hard disk. Additional software installation is unnecessary.

Plug in the device and use the Chameleon Manager to make encrypted drives associated with it.

Should you no longer want to use a given Chameleon device on a particular PC, delete its encrypted drive from the Chameleon Manager instead of uninstalling the Chameleon software. Uninstalling the Chameleon software does not delete the encrypted drives.

The Chameleon software does not support plugging in more than one device at a time.

10 Limited Warranty and Legal Notices

Chameleon

485 E. Evelyn Ave
Sunnyvale, CA 94086
Tel: (408) 720-8800
Fax: (408) 720-8900

Please contact support@marathon6.com for technical questions.
Contact sales@marathon6.com for sales or warranty related inquires.
Check http://www.marathon6.com/chameleon for the latest updates.

LucidPort Technology, Inc. warrants to you that the Chameleon will be free from defects in materials and workmanship under normal use for the 90 day warranty period starting on your date of purchase. Your dated sales or delivery receipt is your proof of purchase date. You may be required to provide proof of purchase as a condition of receiving warranty service.

If LucidPort Technology, Inc. receives, during the warranty period, notice of a defect in the Chameleon, LucidPort Technology, Inc. will repair or replace the product, at LucidPort Technology, Inc.'s option. LucidPort Technology, Inc. shall have no obligation to repair, replace, or refund until you return the defective product to LucidPort Technology, Inc.. If your Chameleon has recurring failures, at LucidPort Technology, Inc.'s option, LucidPort Technology, Inc. may provide you a replacement of LucidPort Technology, Inc.'s choosing that

is the same or equivalent in performance or a refund of your purchase price instead of a replacement.

To the extent permitted by local law, LucidPort Technology, Inc., and any replacement products or parts, may contain new and used materials equivalent to new in performance and reliability. Any replacement product or part will also have functionality at least equal to that of the product or part being replaced. Replacement products and parts are warranted to be free from defect in material or workmanship for 90 days.

LucidPort Technology, Inc., at its sole discretion, may subcontract to or engage a third party to provide the warranty services.

DATA LOSS IS A FREQUENT CONSEQUENCE OF REPAIR. DATA STORED WITH THE CHAMELEON IS NEVER COVERED BY WARRANTY.

This Limited Warranty does not apply to expendable or consumable parts or to any product in which the chassis has been opened or if damaged or defective (a) due to accident, misuse, abuse, contamination, virus infection, improper or inadequate maintenance or calibration or other external causes; (b) by software, interfacing, parts or supplies not supplied by LucidPort Technology, Inc.; (c) improper site preparation or maintenance; (d) loss or damage in transit; or (f) modification or service by other than LucidPort Technology, Inc. or a LucidPort Technology, Inc. authorized service provider.

TO THE EXTENT ALLOWED BY LOCAL LAW, IN NO EVENT SHALL LUCIDPORT TECHNOLOGY, INC. BE LIABLE FOR ANY DAMAGES CAUSED BY THE PRODUCT OR THE FAILURE OF THE PRODUCT TO PERFORM, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY KIND, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), OR ANY OTHER LEGAL THEORY AND WHETHER ADVISED OF THE POSSIBILITIES OF SUCH DAMAGES. LUCIDPORT TECHNOLOGY, INC. IS NOT LIABLE FOR ANY CLAIM MADE BY A THIRD PARTY OR MADE BY YOU FOR A THIRD PARTY.

The AES encryption technology in the Chameleon is classified by the United States government as an ECCN 5A002 item and can be exported under License Exception ENC, Sec. 740.17 (b)(3) of the Export Administration Regulations ("EAR"). The Chameleon may not be used or otherwise exported or re-exported into (or to a national or resident of) Cuba, Iran, North Korea, Sudan, or Syria. No further approvals or authorizations from the US government are required.

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com