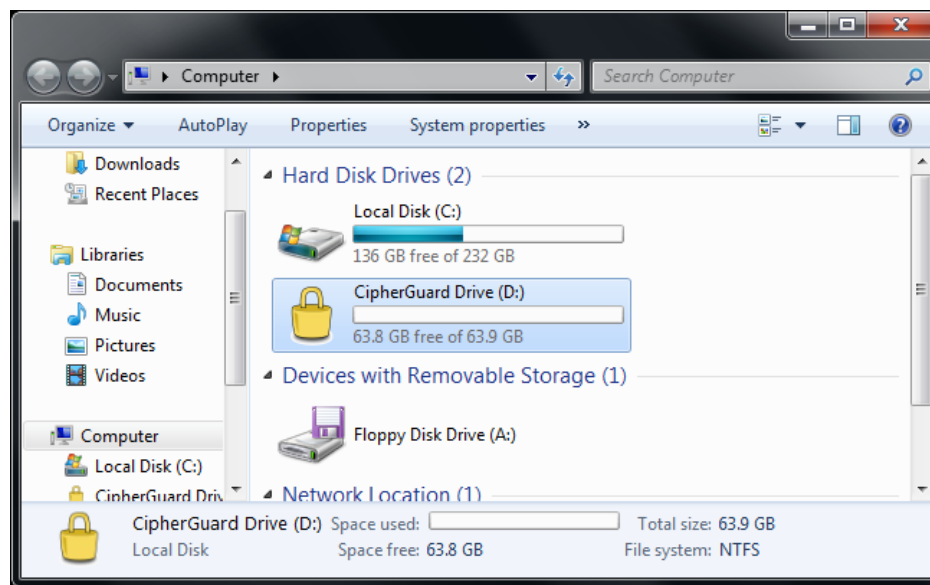


1 Introduction

Congratulations on your purchase of the CipherGuard. The CipherGuard protects the files on your PC with AES-256 encryption. Since 2002, AES has been the encryption standard used by the United States Government. There is no known technique to break AES encryption. A brute force attack is expected to take longer than the lifetime of the universe.¹

The CipherGuard differs from other USB encryption devices by protecting the files on your hard disk rather than transferring them to a USB device. The CipherGuard 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 CipherGuard is plugged in. Like the key for your car, the CipherGuard acts like a physical key for your hard disk.



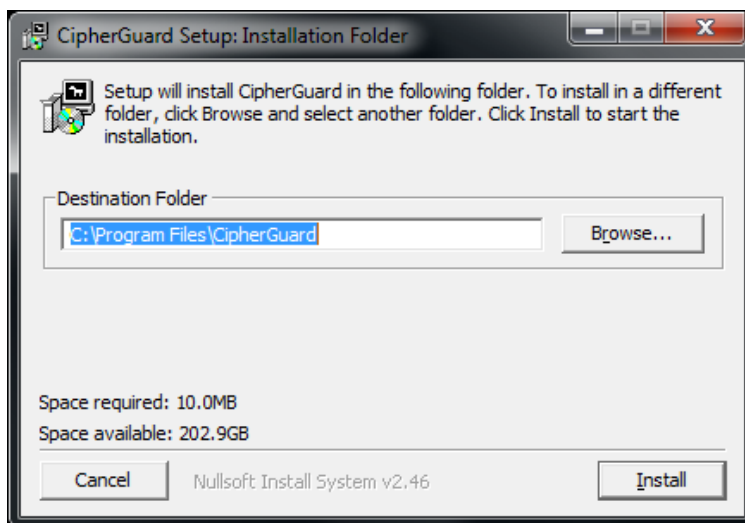
The CipherGuard works with Windows XP, Vista, and Win7 based PCs.

2 Installation and Setup

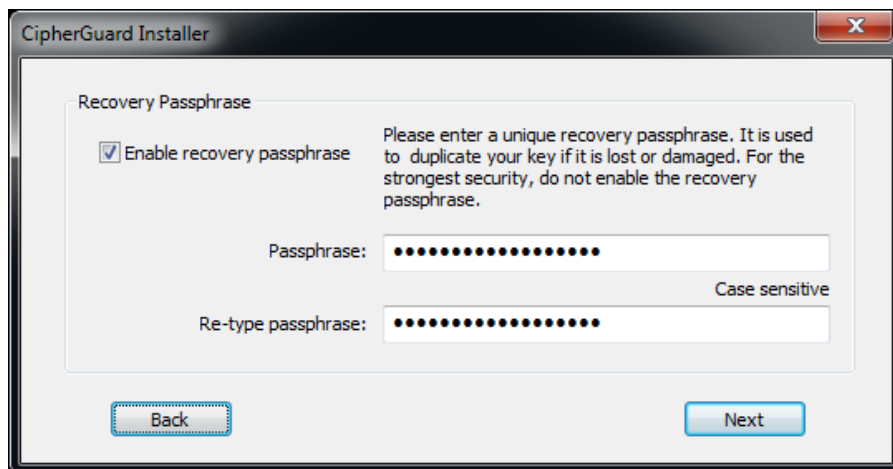
Before installing the CipherGuard, make sure any previous versions of the CipherGuard are uninstalled. Uninstalling does not delete your CipherGuard drives.

¹ In order to simply scan through the possible values for a 256-bit symmetric key (ignoring doing the actual computing to check it) requires $2^{256} - 1$ bit flips. http://en.wikipedia.org/wiki/Brute_force_attack

Insert the CD that comes with the CipherGuard and run the Setup program.² (You can also download the setup program from <http://www.marathon6.com/cipherguard>.) Click on the "Install" button to load the CipherGuard software.



Plug in the CipherGuard then press "Start" to launch the installation wizard. It prompts for a Recovery Passphrase. This passphrase is only used for making duplicate copies of your CipherGuard (in case you lose it) and not used in normal operation. You can think of the Recovery Passphrase as a password stored on the CipherGuard device itself.



Select a unique passphrase. Another CipherGuard with the same passphrase may be able to access your data. Once programmed, the Recovery Passphrase can never be changed.

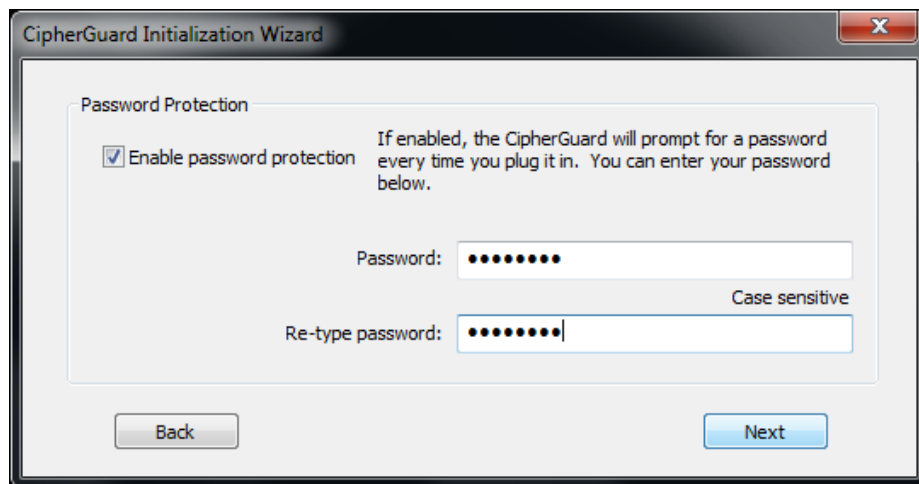
A good passphrase is at least 8 characters long and includes random letters (upper and lower case), numbers, and special symbols. Protect your passphrase as you would protect a password.

² 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.

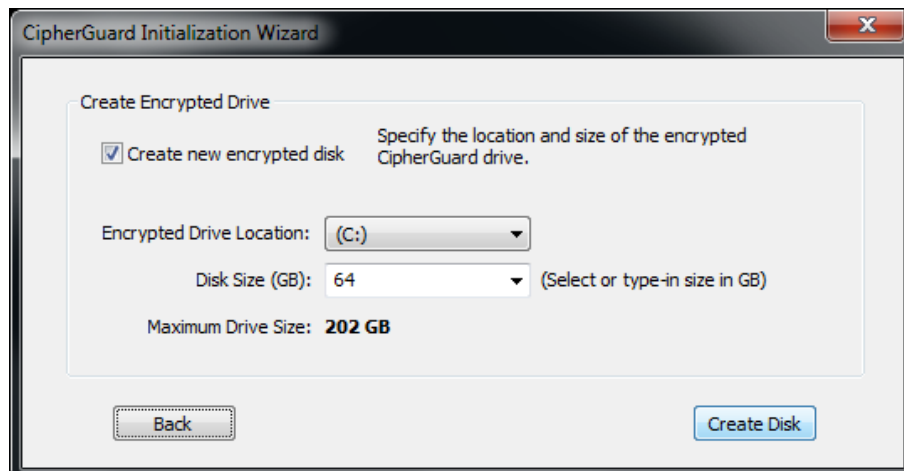
An attacker who learns your passphrase can use it to make a duplicate CipherGuard. There is no way to duplicate a CipherGuard without your Recovery Passphrase.

For the strongest security, disable the Recovery Passphrase. This instructs the CipherGuard to generate its own random encryption key. However, this means that you will not be able to duplicate the CipherGuard if it is lost or broken. As an alternative, you can use a random sequence of numbers and letters as the passphrase. Make several CipherGuards with this sequence (as backups), then erase the random number. (See Duplicating a Lost CipherGuard)

The installation wizard prompts for a password in the next screen. When enabled, the CipherGuard asks for this password whenever it is plugged in. A password is not required and may be added or changed at any time with the CipherGuard Manager software (Start > All Programs > CipherGuard > CipherGuard Manager). The password protects your CipherGuard from unauthorized users.



Create a CipherGuard drive by specifying the size and location of the drive. The installer creates the encrypted drive using the free space at that location. It can reside on your local hard disk or on external USB drives. It can be resized later using the CipherGuard Manager software (Start > All Programs > CipherGuard > CipherGuard Manager).



The CipherGuard protects all content in the encrypted drive. It is accessible when the CipherGuard is inserted and disappears when the CipherGuard is removed.

2.1 Uninstalling

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

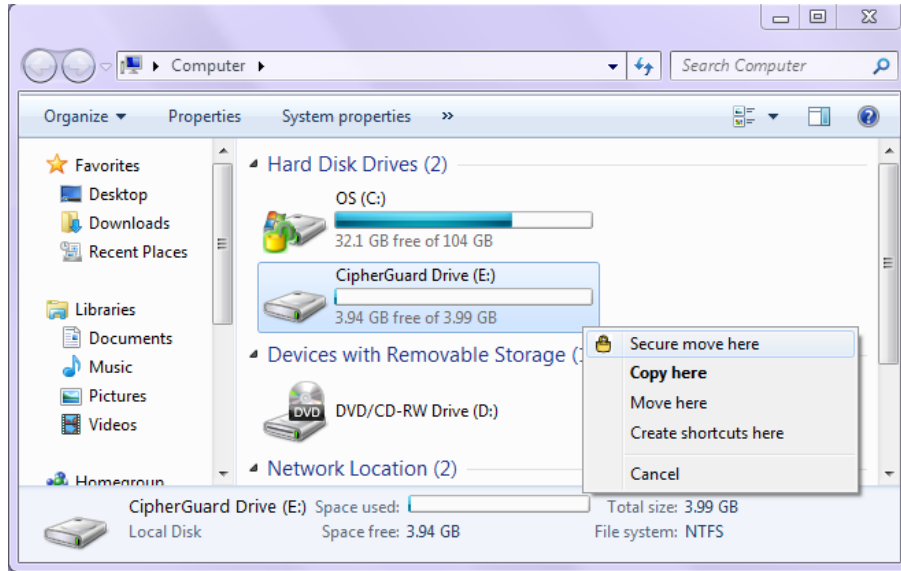
3 Protecting Your Data

Plug in your CipherGuard to access the CipherGuard drive. Once installed, there is no software to run or passwords to enter (unless enabled). The CipherGuard 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 CipherGuard drive. Once the CipherGuard is removed, the 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 CipherGuard drive are encrypted. Any files copied or read from the CipherGuard drive are automatically decrypted. For instance, if a user were to attach a file from a CipherGuard drive to an email, that file would be attached decrypted.

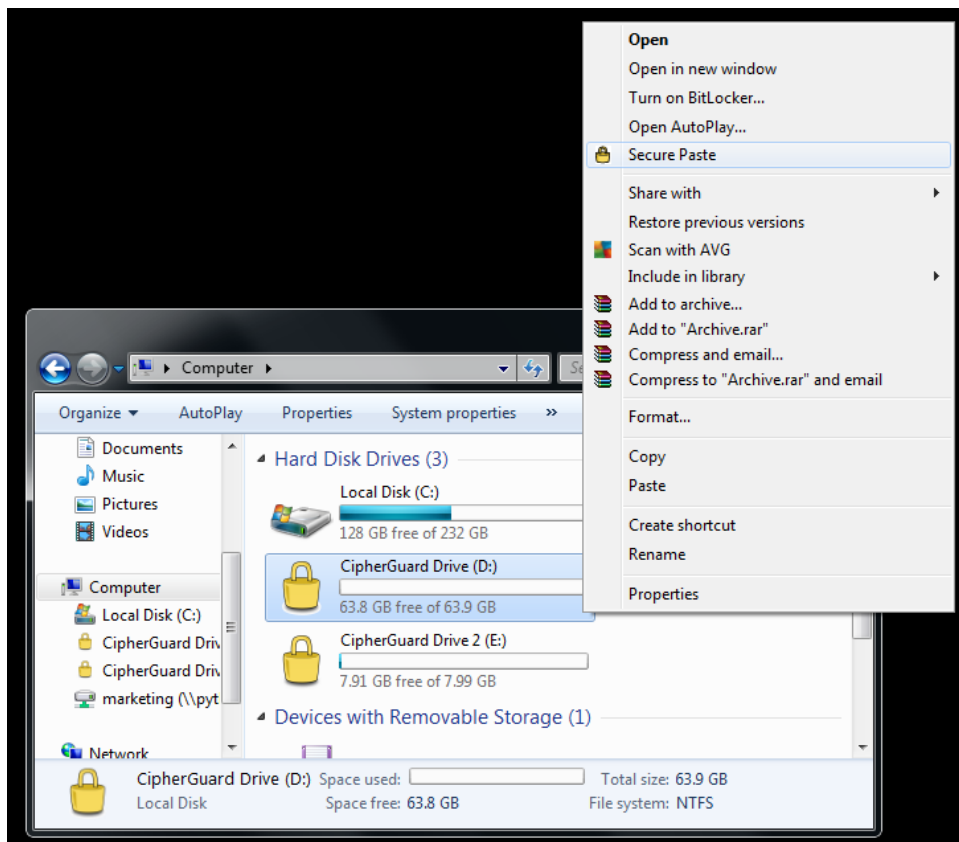
You can copy files to the CipherGuard drive simply by dragging and dropping them there. However, this retains the original unencrypted file at its original location. A more secure method is to right-click drag and drop. Hold down the right mouse button, then drag the selected file to the CipherGuard drive. A dialog appears showing “Copy”, “Move”, and “Secure move”. The secure move option moves the file into the CipherGuard drive, then scrubs away any traces of that file from its original location.³ If a significant amount of data is involved, this may take some time.

³ The standard Windows move command copies the file, then marks the original file as deleted. The deleted file may be recoverable with specialized tools. CipherGuard’s secure move command prevents recovery by overwriting the deleted file.

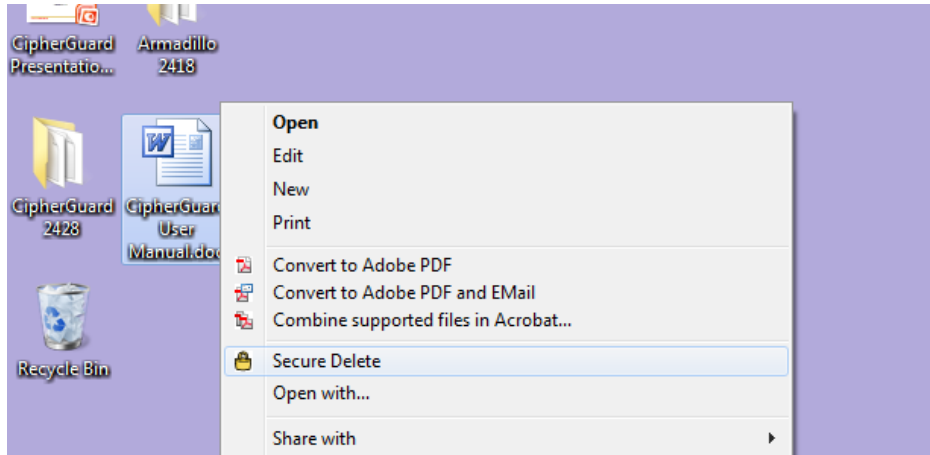


You can also securely move a file to the CipherGuard drive by using the secure paste option. Right click on the file or folder you want to move, then select “Cut”. Next, right click on a CipherGuard drive or sub-directory, then select “Secure Paste”. Like the secure move option, the secure paste command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

Secure commands are only available when the CipherGuard is plugged in.



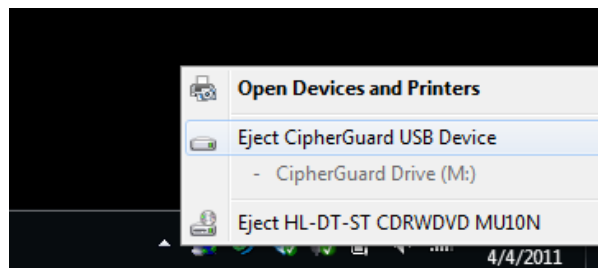
The CipherGuard also adds a secure delete command. Right click on any file or folder then select “Secure Delete”. This is more secure than deleting the file then deleting it again from the Windows’ Recycle Bin. Since secure delete overwrites every bit of your file from the hard disk, this will take some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



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

Any files you create directly on the CipherGuard 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 CipherGuard drive. This can usually be accomplished by installing your applications directly in the CipherGuard drive.

You can plug or unplug the CipherGuard at any time. Your computer is still fully useable without the CipherGuard. Only the CipherGuard drive (and any programs and data in it) will be missing. Be aware that unplugging the CipherGuard while writing data to the CipherGuard 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 CipherGuard.



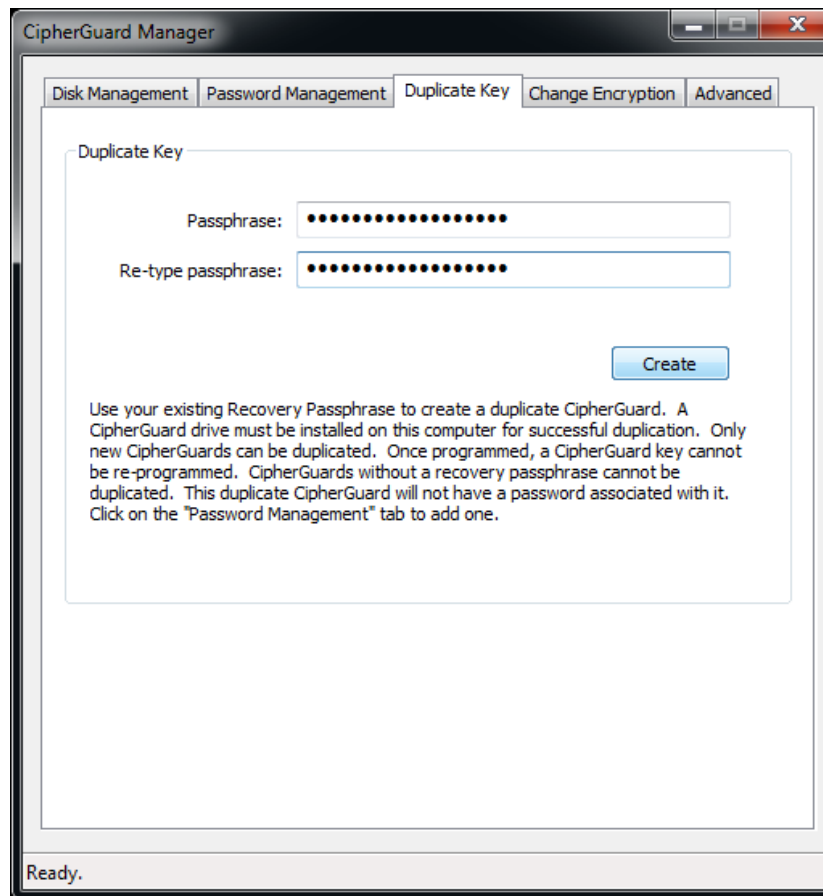
If an application is open with a protected file, that application and file may still be accessible even after you unplug the CipherGuard. For example, you are editing a protected file in Microsoft Word. If you unplug the CipherGuard, a copy of this file is still open in Word. You cannot save this file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

4 Duplicating a Lost CipherGuard

If you lose or break your CipherGuard, the data in the CipherGuard drive can be recovered using a new CipherGuard and the Recovery Passphrase you specified during installation. This process can also be used to create duplicate CipherGuards. CipherGuards without a Recovery Passphrase cannot be duplicated.

Insert a new CipherGuard in the PC. There is no need to reinstall the software. Start the CipherGuard Manager then select the “Duplicate Key” tab. Enter your Recovery Passphrase then click “Create”. This new CipherGuard will not have a password associated with it. Click on the “Password Management” tab to add one.

You do not need the original CipherGuard to make a duplicate. But as a precaution, a CipherGuard drive must be present for successful duplication.



5 Disabling Lost CipherGuards

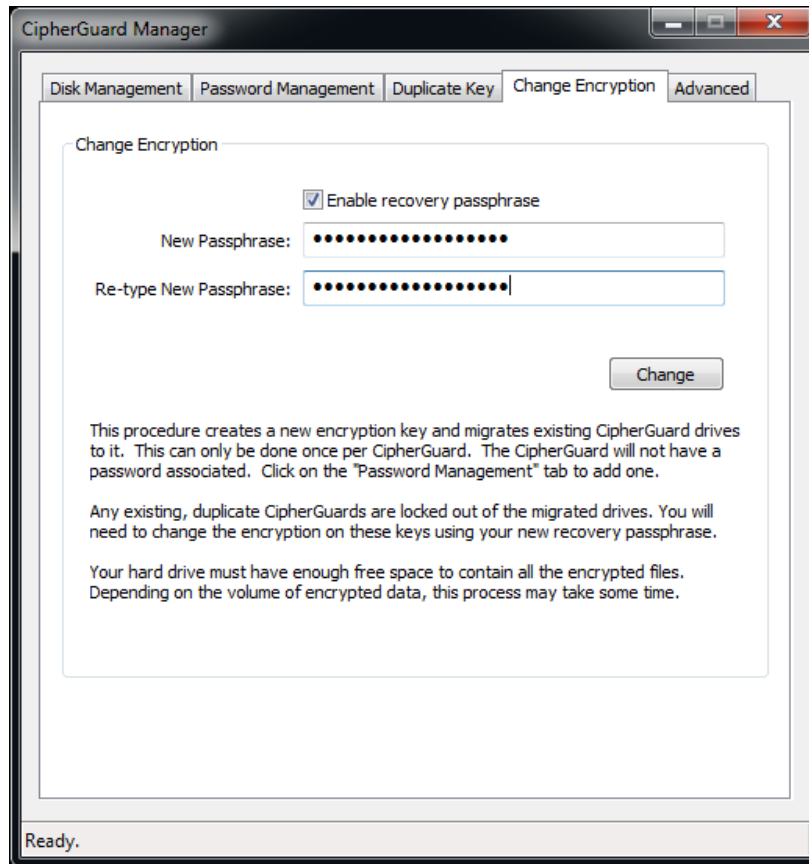
You can lock out a lost CipherGuard by updating the CipherGuard's Recovery Passphrase and migrating all your CipherGuard drives⁴ to the new CipherGuard. Each CipherGuard can only be updated once. To repeat this procedure, you will need a new CipherGuard device. As a precaution, a CipherGuard drive must be present for successful migration.

You will need a CipherGuard programmed with the original Recovery Passphrase that you specified during installation. If your CipherGuard has been lost, you will need to prepare a replacement CipherGuard (see Duplicating a Lost CipherGuard). Your hard disk (C:\) must have enough free space to contain all the encrypted files. Depending on the volume of encrypted data, this process may take some time. Any unconnected CipherGuard drives (and backups) will still be accessible by the original CipherGuard. You will be prompted to migrate them when they are later connected.

Insert your CipherGuard in the PC. Enter the password if enabled. Start the CipherGuard Manager then select the "Change Encryption" tab. Enter your new Recovery Passphrase. This procedure creates replacement CipherGuard drives using the new Recovery Passphrase with all your encrypted files in it. The updated CipherGuard device will not have a password associated with it. Click on the "Password Management" tab to add one.

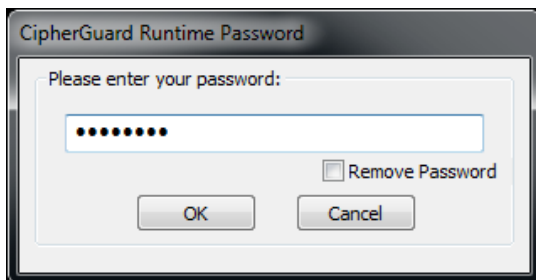
Unmigrated CipherGuard drives are still accessible with the new CipherGuard device.

⁴ Including backups



6 Password Protection

The CipherGuard drive cannot be accessed without the CipherGuard device, no passwords are required. Adding password protection secures your data in the event that you lose your CipherGuard along with your PC. When enabled, the CipherGuard requests the password whenever it is plugged in or when the computer is restarted (or wakes from sleep).



The password is different from the CipherGuard's Recovery Passphrase. The Recovery Passphrase is only entered during initialization or duplication. The password needs to be entered every time the CipherGuard is plugged in. It is used to prevent unauthorized access to your CipherGuard, not to protect your data. CipherGuard devices with the same Recovery Passphrase, but different passwords can access the same CipherGuard drive.

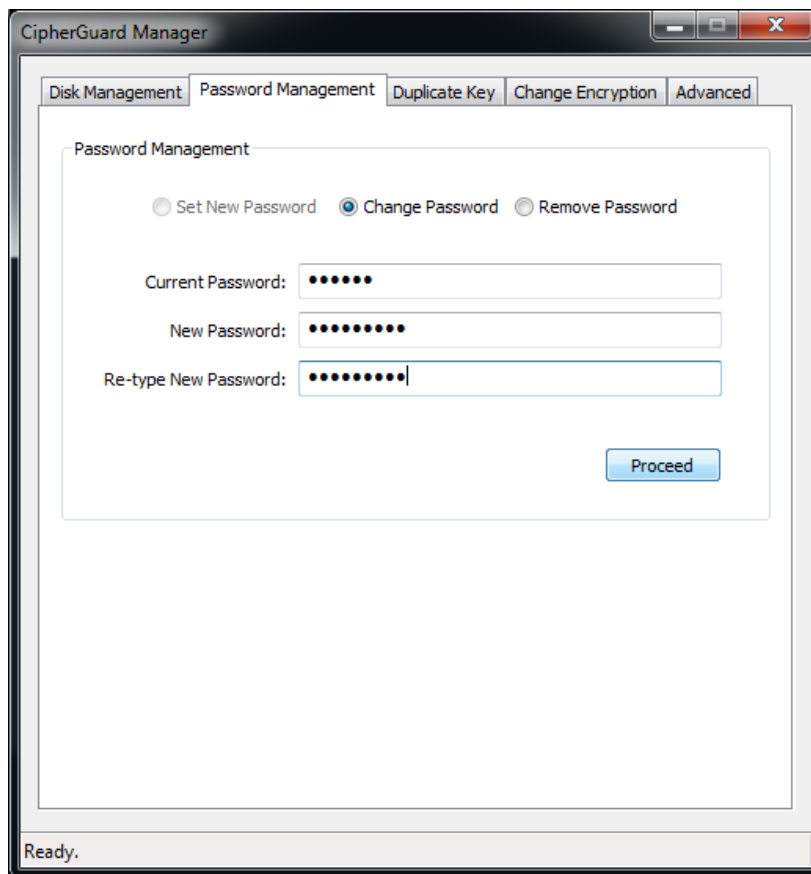
If you forget your password, remove password protection by entering your Recovery Passphrase at the password prompt.

6.1 Password Modification

You can add, change, or remove CipherGuard password protection as many times as you want. It is possible to have duplicate CipherGuards with different passwords (or no passwords at all). Be aware that a CipherGuard without password protection can access the data protected by a different CipherGuard with password protection as long as they have the same Recovery Passphrase.

Insert your existing CipherGuard in the PC and enter your password (if enabled). Start the CipherGuard Manager then select the “Password Management” tab.

- To add a CipherGuard password, select “Set New Password” then enter the new password and click the “Proceed” button.
- To change your CipherGuard password, select “Change Password” then enter both your existing password and the new password, and click the “Proceed” button.
- To remove the CipherGuard password, select “Remove Password” then enter your existing password and click the “Proceed” button.

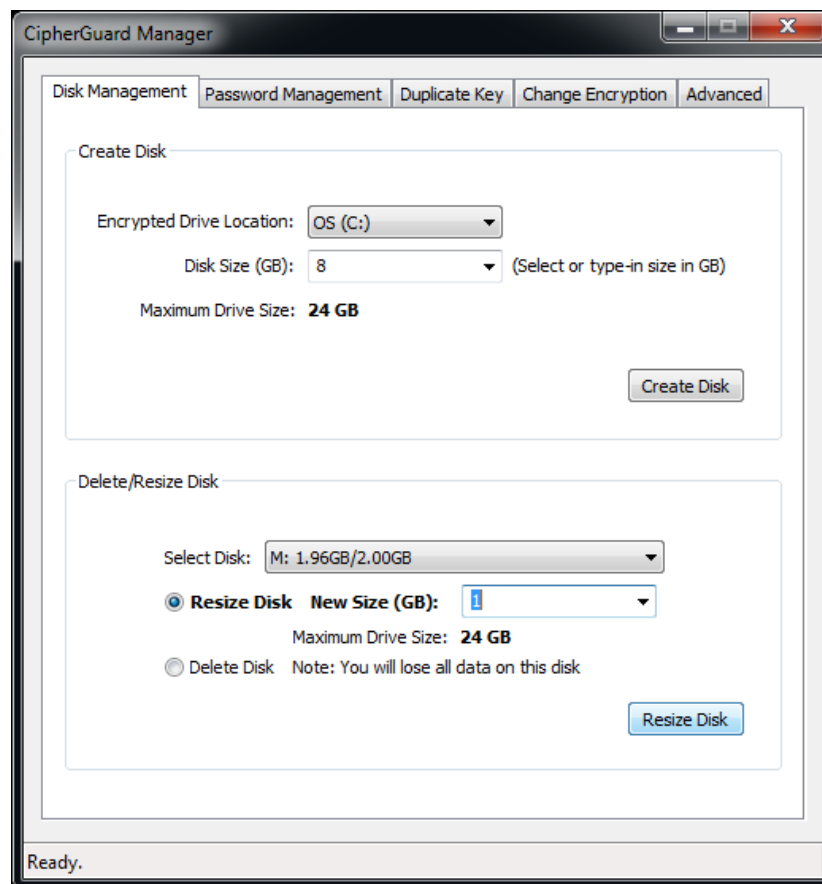


7 Adding, Deleting, and Resizing CipherGuard Drives

You can add, delete, or resize CipherGuard drives at any time. As long as there is sufficient disk space, there is no limit to the number of CipherGuard drives you can have associated with a single CipherGuard device. CipherGuard drives can be created on your internal hard disk as well as external USB drives.

Insert your CipherGuard in the PC and enter your password (if enabled). Start the CipherGuard Manager then select the “Disk Management” tab.

- To add a drive, specify the size and location of the CipherGuard drive, then click the “Create Disk” button.
- To delete a drive, select the existing drive from the drop down menu, then select “Delete Disk”. Click on the “Delete Disk” 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 Disk”. Enter the desired size, then click the “Resize Disk” button. When reducing drive size, your hard disk must have enough free space to temporary hold all the contents of the CipherGuard drive.



8 Additional Functions and Limitations

8.1 Using the CipherGuard with Multiple Computers

A single CipherGuard device can be used with multiple computers. Plug your programmed CipherGuard into the new computer. Insert the CipherGuard CD and run the CipherGuard installer on this new computer. The installer will prompt you to make a CipherGuard drive on the new computer.

8.2 Using Multiple CipherGuards with the Same Computer

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

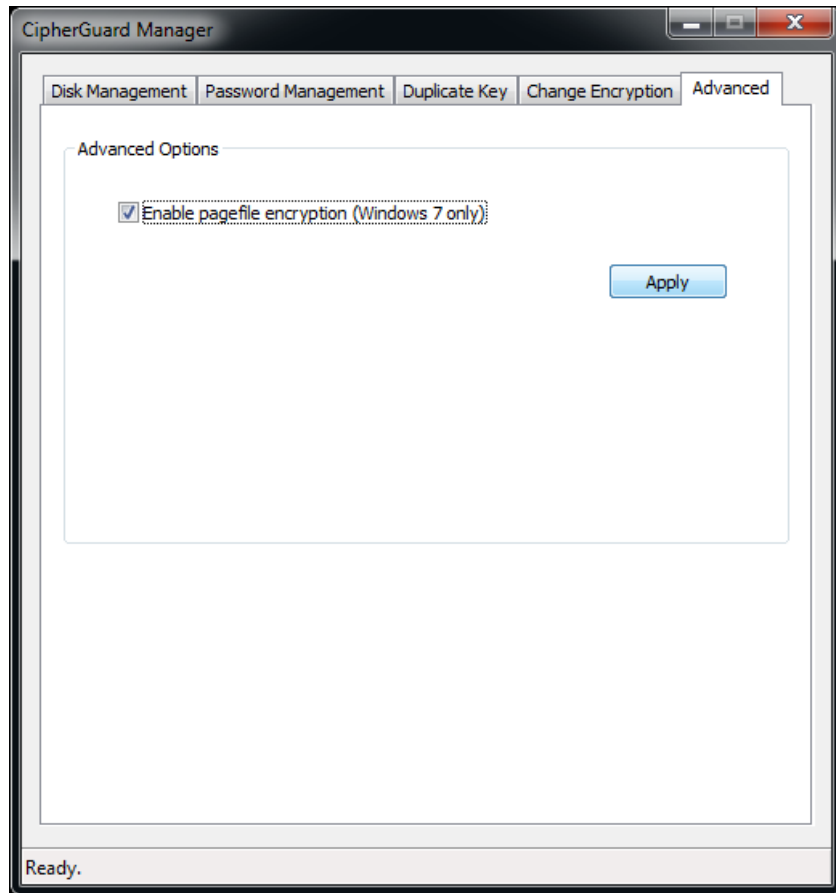
Plug in the second CipherGuard and use the CipherGuard Manager to make CipherGuard drives associated with it. Unless they are duplicates, the second CipherGuard can only access its own drives – and not the drives associated with the first CipherGuard.

Should you no longer want to use the second CipherGuard, delete its CipherGuard drive from the CipherGuard Manager instead of uninstalling the CipherGuard software. Uninstalling the CipherGuard software does not delete the CipherGuard drive while also disabling access by the first CipherGuard.

The CipherGuard does not support more than one CipherGuard device being inserted at a time.

8.3 Windows Paging File

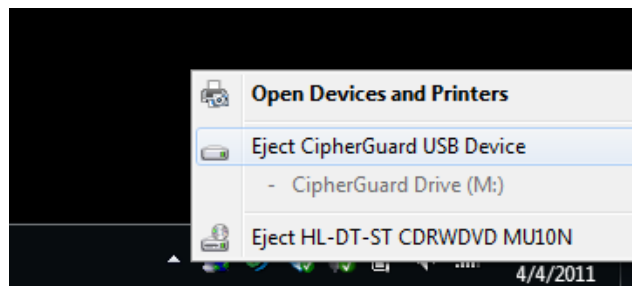
Windows may store temporary data in its paging file (virtual memory). This file is usually unencrypted, appearing as a jumble of characters, and is updated continuously. Enable pagefile encryption to direct Windows to encrypt its paging file.



Enable pagefile encryption by starting the CipherGuard Manager and selecting the “Advanced” tab. 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).

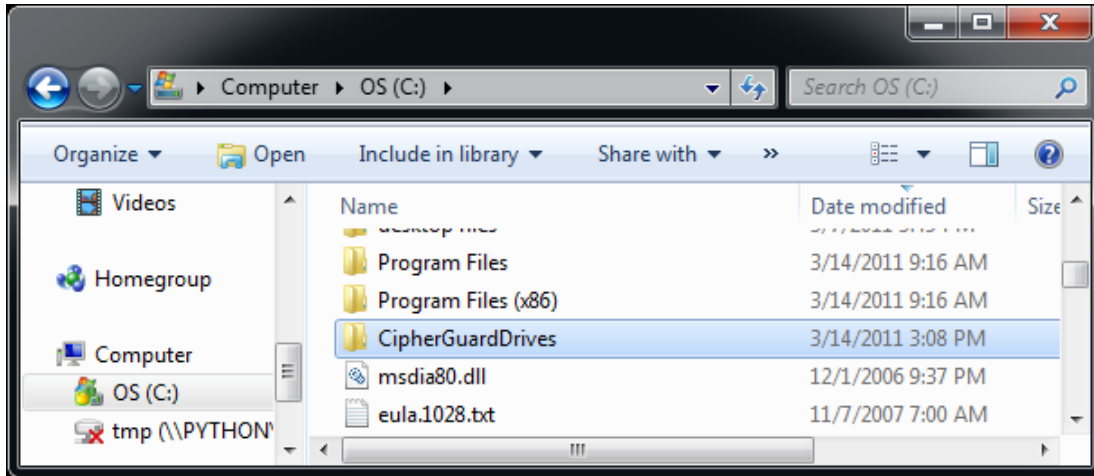
8.4 Safe Removal

Unplugging the CipherGuard while writing data to the CipherGuard 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 CipherGuard.



8.5 Backing up your Data

Backup CipherGuard drives by copying the CipherGuardDrives directory to another location. This directory is located at the top level of your hard disk (ex. C:\CipherGuardDrives\). Since CipherGuard drives are always encrypted, backups are still protected. You do not need to plug in the CipherGuard to back up your data.



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

WARNING: Do not copy the backup CipherGuardDrives directory to the top level (root) of a drive. Any subdirectory or network location will work. Since the CipherGuard cannot distinguish between the original and the copy, if identical drives are detected, the CipherGuard will not activate either drive.

9 Limited Warranty and Legal Notices

CipherGuard

Copyright (c) 2011, LucidPort Technology, Inc.

Please contact support@marathon6.com for technical questions.

Contact sales@marathon6.com for sales or warranty related inquiries.

Check <http://www.marathon6.com/cipherguard> for the latest updates.

Marathon6 warrants to you that the CipherGuard 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 Marathon6 receives, during the warranty period, notice of a defect in the CipherGuard, Marathon6 will repair or replace the product, at Marathon6's option. Marathon6 shall have no obligation to repair, replace, or refund until you return the defective product to Marathon6. If your CipherGuard has recurring failures, at Marathon6's option, Marathon6 may provide you a replacement of Marathon6'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, Marathon6, 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.

Marathon6, 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 CIPHERGUARD 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 Marathon6; (c) improper site preparation or maintenance; (d) loss or damage in transit; or (f) modification or service by other than Marathon6 or an Marathon6 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 CipherGuard 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 CipherGuard 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.