COMODO
Creating Trust Online®

Comodo
Disk Encryption

Software Version 2.0

User Guide

Guide Version 2.0.092611

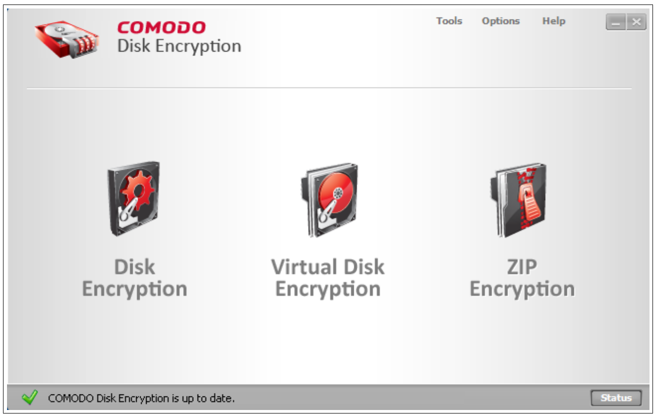
Comodo Security Solutions
525 Washington Blvd.
Jersey City, NJ 07310

Table of Contents

1. Comodo Disk Encryption - Introduction

What is Comodo Disk Encryption?

Comodo Disk Encryption (CDE) protects your sensitive information by enabling you to encrypt any disk on your system with the strongest algorithms available, even root disks. You can also mount encrypted virtual disks in your hard drive and save your information in them securely or encrypt specific files/folders in a single encrypted ZIP file.



COMODO Disk Encryption is up to date.

Comodo Disk Encryption Offers Three Varieties of Data Protection:

- **Disk Encryption** - You can encrypt any physical disk that contains information to be secured, with different encryption algorithms. Even the physical disks which contain Operating Systems, can be encrypted.
- **Virtual Disk Encryption** - You can also create encrypted virtual disks in your hard drive and save your information in them securely. This functionality will use (create/open) a file to emulate a physical disk.
- **ZIP Encryption** - You can also create encrypted ZIP containers where you can save several files and folders. Physical disk encryption can be carried out with different authentication types, increasing the security.

An additional layer of security can be added if you choose to implement user authentication before a drive can be decrypted. CDE offers the following authentication types:

- **Password Authentication** - Set a password of your choice as authentication key to encrypt and decrypt the required disks. The password must be entered whenever the system is started to successfully access the encrypted disks.
- **USB Memory Key Authentication** - Configure a USB memory as authentication key to encrypt the required disks. This key must be plugged-in to the system whenever the system is started to successfully access the encrypted disks.
- **Authentication with both Password and USB memory key** - Combination of both password and USB keys for authentication. This is a highly secure practice that meets the classic two factor authentication criteria of 'something you own' plus 'something you know'.

Once the user is authenticated and the disk has been decrypted, the disk will behave 'as normal'. Users can save, view and modify files on the disks as before. All encryption/decryption processes are performed on the fly with no reboot needed.

Why do you need Comodo Disk Encryption?

- Keep data totally protected from hackers, thieves, and all unauthorized viewing;
- You don't want private data to be accessed when you're away from your computer;
- If your desktop or laptop is stolen, the thieves will not have access to personal data;
- Share your computer with other people knowing that they can't view your personal files;
- To be the only person that is able to start a specific computer.

Guide Structure

This guide is intended to take the user through the installation, configuration and use of Comodo Disk Encryption.

1.1. System Requirements

Comodo Disk Encryption System Requirements	
Operating Systems - 32 bit	**Operating Systems - 64 bit**
Windows Vista Windows XP Windows 2000	Windows Vista Windows XP Windows Server 2003

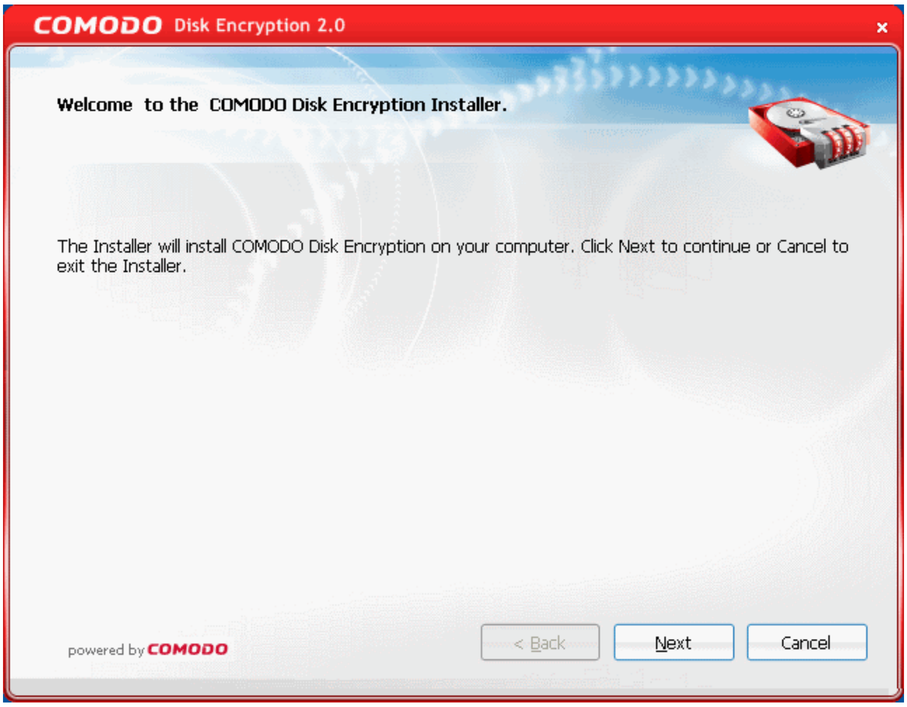
Comodo Disk Encryption System Requirements	
Windows Server 2003 32 MB RAM 6 MB Hard Disk Space	32 MB RAM 6 MB Hard Disk Space

1.2. Installing Comodo Disk Encryption

Before you install Comodo Disk Encryption, please make sure to quit all other Windows programs. You must also have local Administrator privileges to run this installer. After downloading the setup file to your local hard drive, double click on Setup.exe to start the installation wizard.

Step 1

A Welcome screen appears. Click **'Next'**.

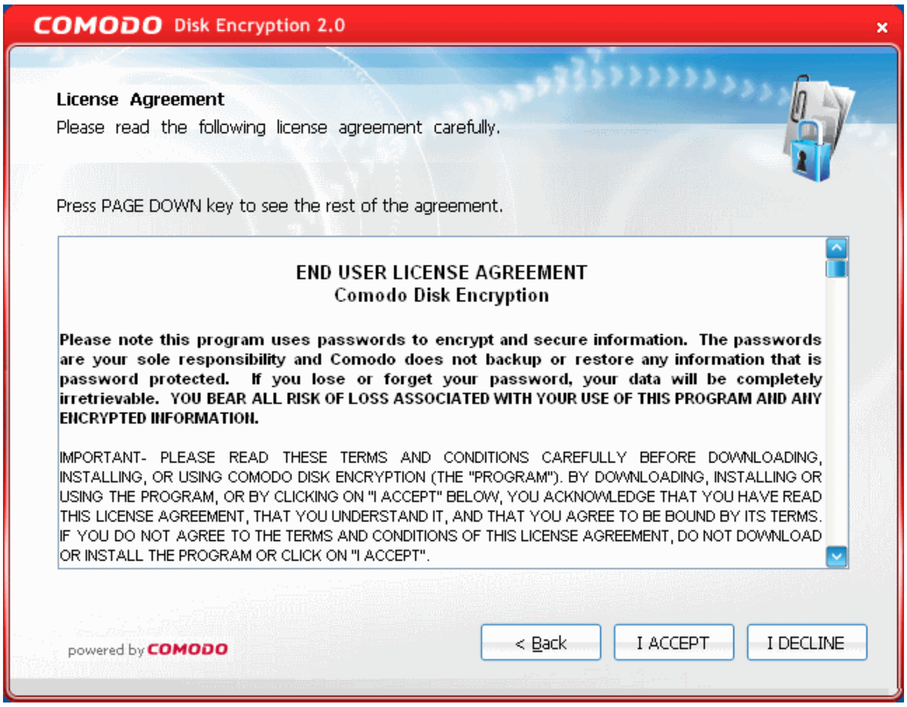


Welcome to the COMODO Disk Encryption Installer.

The Installer will install COMODO Disk Encryption on your computer. Click Next to continue or Cancel to exit the Installer.

Step 2

End User License Agreement - In order to finalize installation, you must first read and accept the license agreement:



License Agreement

Please read the following license agreement carefully.

Press PAGE DOWN key to see the rest of the agreement.

END USER LICENSE AGREEMENT
Comodo Disk Encryption

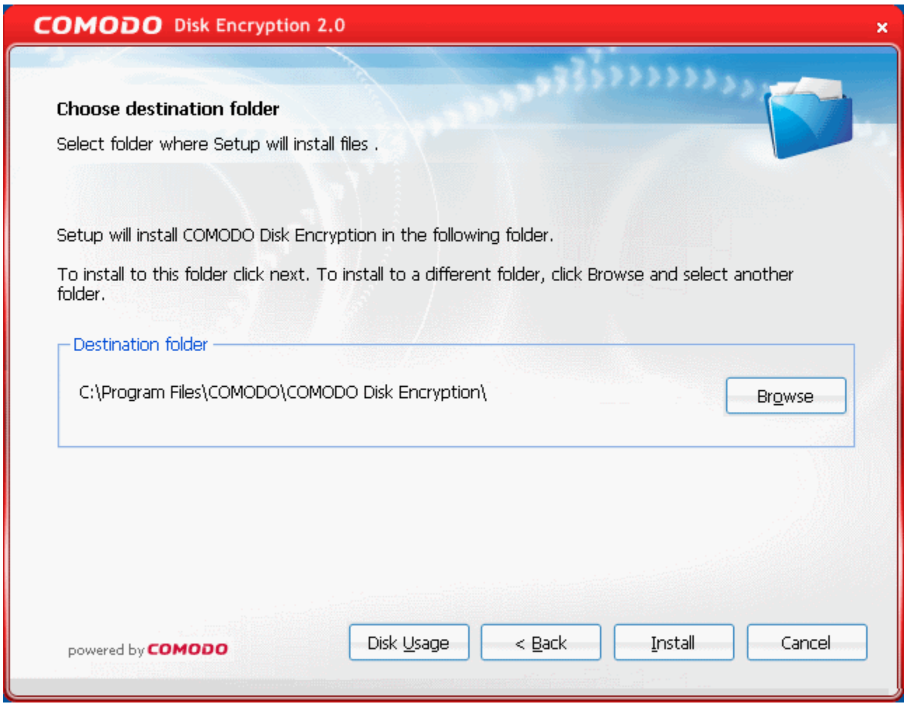
Please note this program uses passwords to encrypt and secure information. The passwords are your sole responsibility and Comodo does not backup or restore any information that is password protected. If you lose or forget your password, your data will be completely irretrievable. YOU BEAR ALL RISK OF LOSS ASSOCIATED WITH YOUR USE OF THIS PROGRAM AND ANY ENCRYPTED INFORMATION.

IMPORTANT- PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING, INSTALLING, OR USING COMODO DISK ENCRYPTION (THE "PROGRAM"). BY DOWNLOADING, INSTALLING OR USING THE PROGRAM, OR BY CLICKING ON "I ACCEPT" BELOW, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO BE BOUND BY ITS TERMS. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT, DO NOT DOWNLOAD OR INSTALL THE PROGRAM OR CLICK ON "I ACCEPT".

Click on '**I ACCEPT**' button if you agree with EULA terms . If you don't want to continue the installation, click on '**I DECLINE**' button and exit from the setup.

Step 3

Choose destination folder - By default, Comodo Disk Encryption will be installed in C:\Program Files\Comodo\Comodo Disk Encryption.



Choose destination folder

Select folder where Setup will install files .

Setup will install COMODO Disk Encryption in the following folder.

To install to this folder click next. To install to a different folder, click Browse and select another folder.

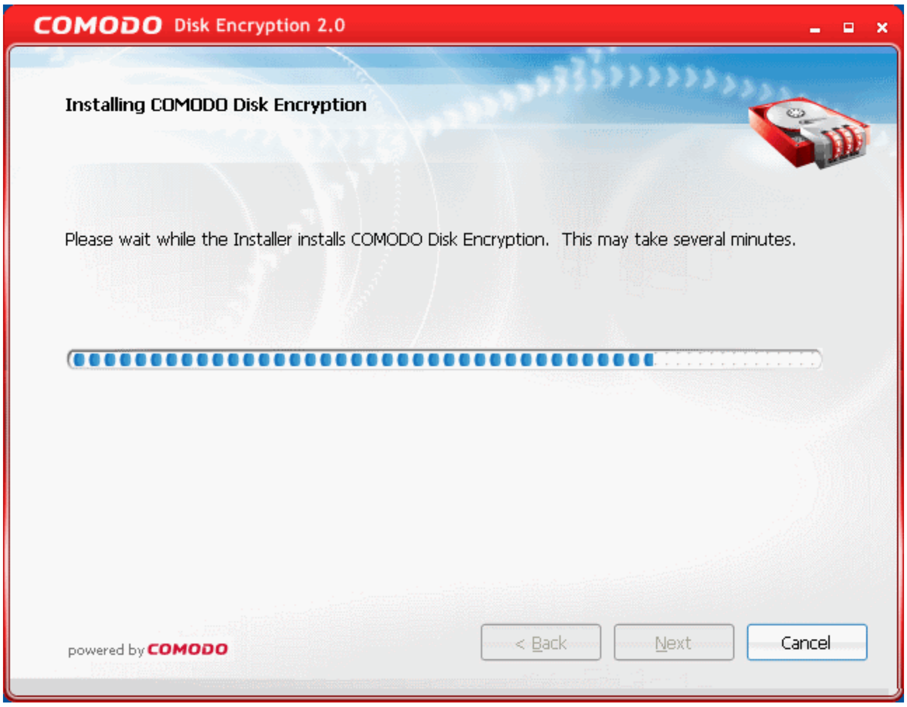
Destination folder

C:\Program Files\COMODO\COMODO Disk Encryption\

If you want to install the application in the default folder, click **'Next'**. If you want to install the application in a different folder, click **'Browse'**, navigate to your desired folder and click **'Next'**.

Step 4

Setup progress - You will see a progress bar indicating the status of your installation.



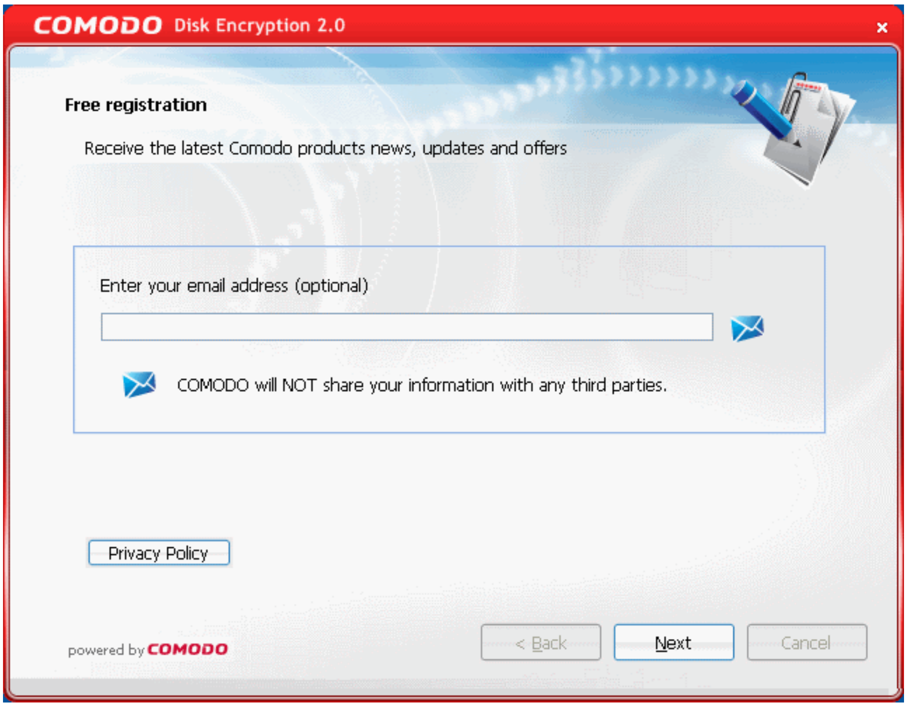
COMODO Disk Encryption 2.0

Installing COMODO Disk Encryption

Please wait while the Installer installs COMODO Disk Encryption. This may take several minutes.

Step 5

Product Activation - The product Activation dialog is displayed. Comodo Disk Encryption is activated at free of cost for lifetime usage. If you wish to sign up for news about Comodo products, then enter your email address in the space provided (this is optional) and click **'Next'**.



COMODO Disk Encryption 2.0

Free registration

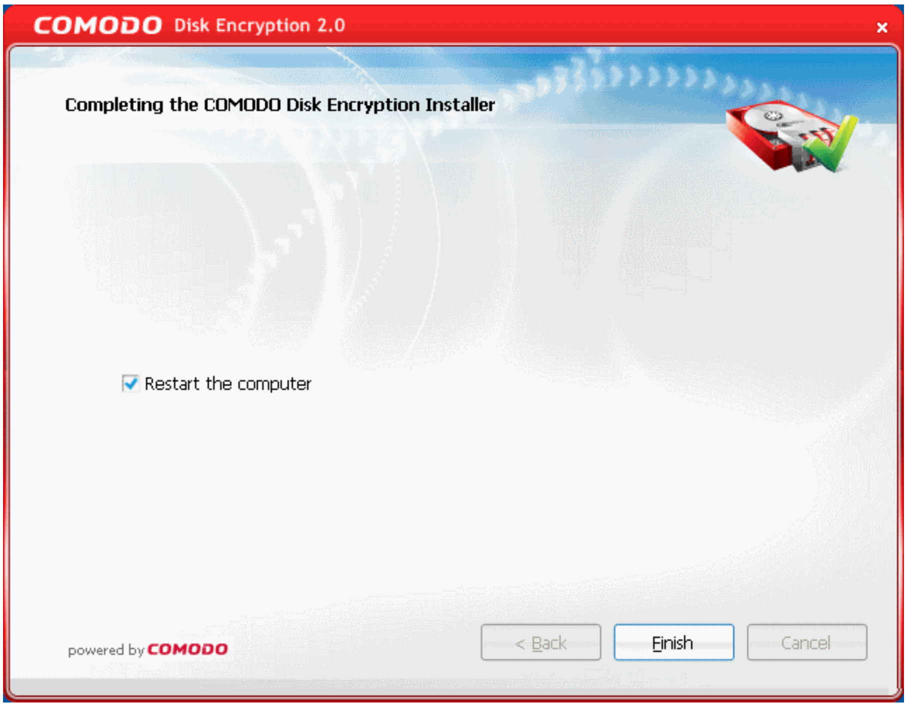
Receive the latest Comodo products news, updates and offers

Enter your email address (optional)

COMODO will NOT share your information with any third parties.

Step 6

Finish - The Finish dialog is displayed indicating the successful completion of installation. For the installation to take effect, the system has to be restarted. Please save any unsaved data and click **'Finish'** to restart the system. If you want to restart the system at a later time, uncheck **Restart the computer** box and click **'Finish'**.


COMODO Disk Encryption 2.0
Completing the COMODO Disk Encryption Installer
☑ Restart the computer
powered by COMODO
< Back
Finish
Cancel

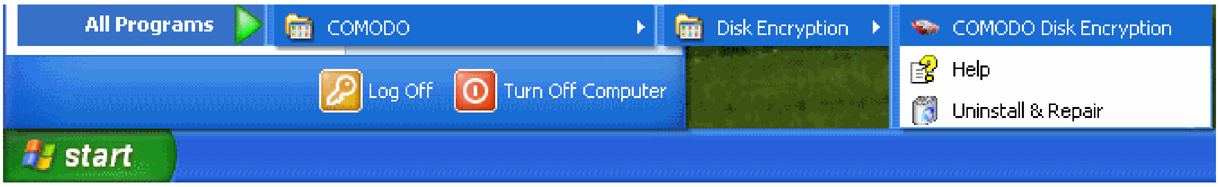
Note: The installation will take effect only on the next restart of the computer.

1.3. Starting Comodo Disk Encryption

You can access Comodo Disk Encryption through the Windows Start Menu or through the desktop shortcut.

1. Start Menu

After downloading and installing a Comodo Disk Encryption, the setup procedure creates an entry in the 'Programs' section of Windows Start Menu. You can start Comodo Disk Encryption by hitting the 'Start' button and navigating to: Start > All Programs > Comodo > Disk Encryption.



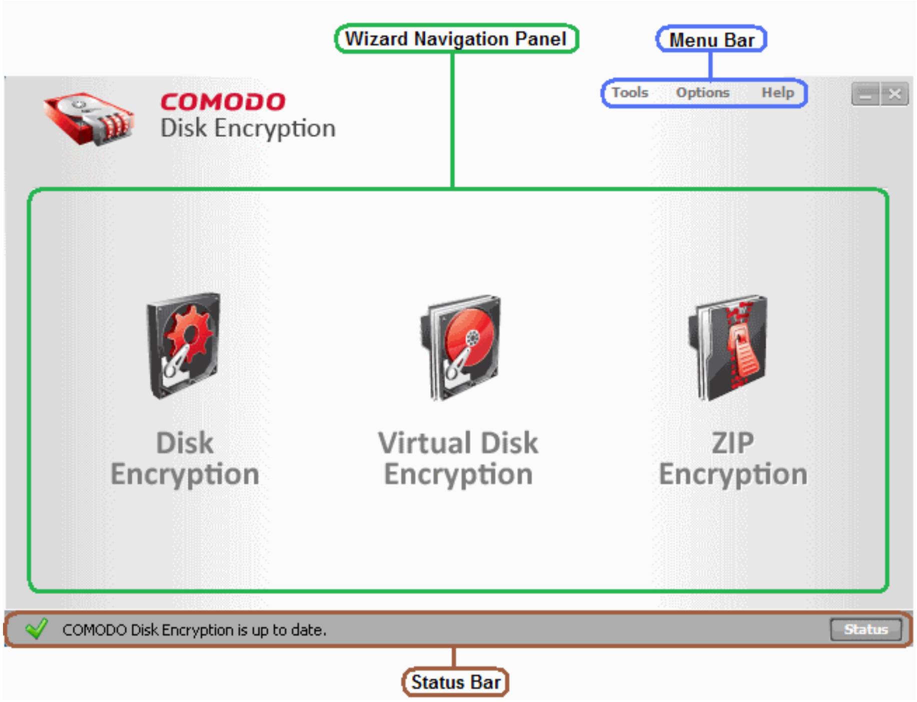
2. Desktop Shortcut

Users can also start Comodo Disk Encryption by double-clicking on the desktop shortcut created during installation:

1.4. The Main Interface

The main interface of Comodo Disk Encryption has three main function areas:

- **Menu Bar**
- **Wizard Navigation Panel**
- **Status Bar**



COMODO Disk Encryption is up to date.

Disk Encryption Menu Bar

The Menu bar provides access to 'Tools', 'Options', 'Help**'** menus of Comodo Disk Encryption.

Disk Encryption Wizard Navigation Panel

The Wizard Navigation Panel displays the icons for starting various tasks in Comodo Disk Encryption.

Disk Encryption Status Bar

This area shows any status messages regarding the Disk Encryption application. Any program errors will be shown in this area. If the program is running smoothly, then the standard message is **'Comodo Disk Encryption is up to date'**.

1.5. Understanding Authentication

Once encrypted, a drive can only be accessed if the user presents up to two authentication factors. These include:

- **Password Authentication** - You can use a password of your choice as authentication key to encrypt the required drive. This password is necessary to access the drive, decrypt the drive, change the encryption settings, etc. The password must be entered whenever Windows is started to enable access to the encrypted drives.
- **USB memory key Authentication** - You can use a USB memory as a key to encrypt the required drive. This key is necessary to access the drive, decrypt the drive, change the encryption settings, etc. This key must be plugged-in in the system whenever Windows is started to enable access to the encrypted drives.

Note: The USB memory will be configured as a key for encrypting the drives in your system. This USB should not contain any information you wish to keep. Once it has been used to store encryption settings it will have no other function that to act as a key for your encrypted drives.

- **Authentication with both Password and USB memory key** - Both the password and the USB key are required to decrypt the drive, change the encryption settings, etc. Encrypting a drive using both password and USB stick is a highly secure practice that meets the classic two factor authentication criteria of 'something you own' plus 'something you know'.

If you choose to encrypt your Windows boot drive and use both of the authentication factors listed above then you will have implemented 'whole disk encryption with two factor authentication' on your machine. This prevents the machine from being started (and the confidential data upon it from being read) until both authentication factors have been provided. Both factors are required at boot time before Windows starts and before the regular Windows logon screen. Not only that whole disk encryption is an extremely effective way of safeguarding your data from prying eyes on shared machines or networks, but it can also effectively render a lost or stolen laptop useless to whoever comes into possession of it.

1.6. Understanding Passwords

Comodo Disk Encryption uses a two tier password system. **Master passwords** can be used to encrypt/decrypt/modify all drives in (for example) a network environment. **User passwords** allow the user to access but not modify encrypted disks. For example, a user password may be assigned to individual users to decrypt only specific drives (for example, only the drive in their laptop or only the drive that belongs to their department). Please read on for more details.

Master Password

The Master Password is set the first time a user **encrypts a physical disk** or **creates a virtual disk**. With the Master Password, the user is able to encrypt new disk, decrypt existing disks and change encryption settings such as algorithm or mode. In this way, the Master Password serves as a key that can access all encrypted disks and virtual disks. The Master Password is also required for changing the Master Password itself. In corporate environments, the Master Password may, for example, be set by a network administrator that is implementing whole disk encryption on employee laptops. In a home environment, the Master Password could be used by the predominant user of the computer system or systems (for example, the parent of a child).

User Password

The User Password is a secondary, optional password with limited privileges that can be set at anytime for any encrypted disk or virtual disk. This is done via the **Edit Disk** or **Edit Virtual Disk** options.

User Passwords allow the user to access and use encrypted disks but do not allow them to encrypt, decrypt or change the encryption settings of those disks. This means that a user in possession of only the User Password will be able to enter that password at system start up and start their machine/access encrypted disks *but* they will not be able to decrypt, re-encrypt or change encryption settings..

In a corporate setting a User Password may, for example, be provided to an employee by a network administrator so that the employee can gain access to encrypted disks (or to start their laptop). In a home environment, the Master Password could equally be given to subordinate users of a shared computer system (for example, a parent may provide it to their children).

Note 1: If the administrator changes the encryption settings, encrypts an additional disk or changes the Master Password, the User Password will be reset - meaning the User Password will be completely removed. The administrator needs to create a new User Password and notify it to the other users of the system, to enable them access to the encrypted disks.

Note 2: If you mount a virtual disk using the user password, this virtual disk will not be mounted persistently, meaning that you have to manually mount it again after system restart.

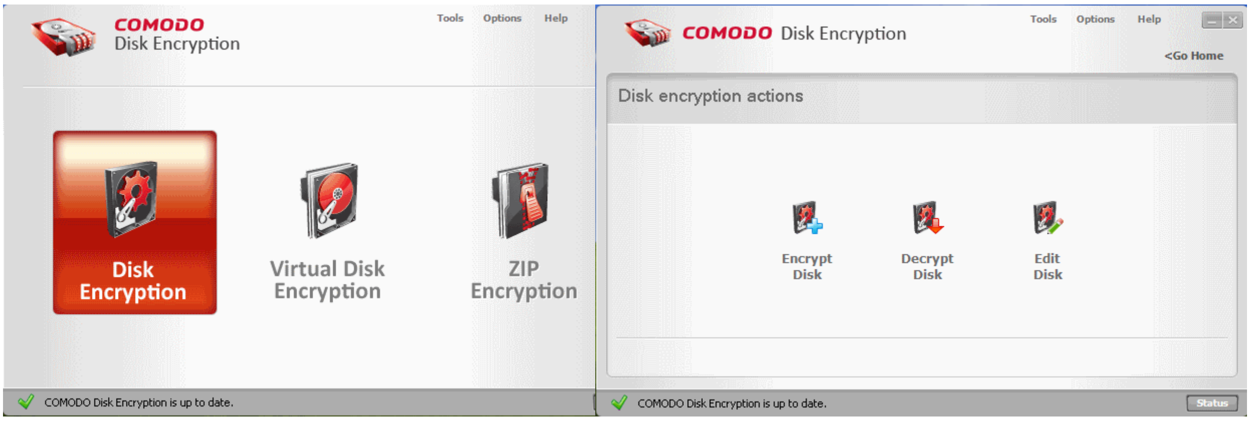
Zip Encryption

Zip Encryption, which allows encryption of individual files/folders, requires a zip encryption specific password in addition to the Master Password. The specific password is created during the first zip encryption operation and is common for all the successive zip operations. This password must be entered to access the encrypted zip files.

2. Disk Encryption

Comodo Disk Encryption (CDE) protects your sensitive information by enabling you to encrypt any disk on your system with the strongest algorithms available.

To access this feature click on the **Disk Encryption** button on the Main Interface.



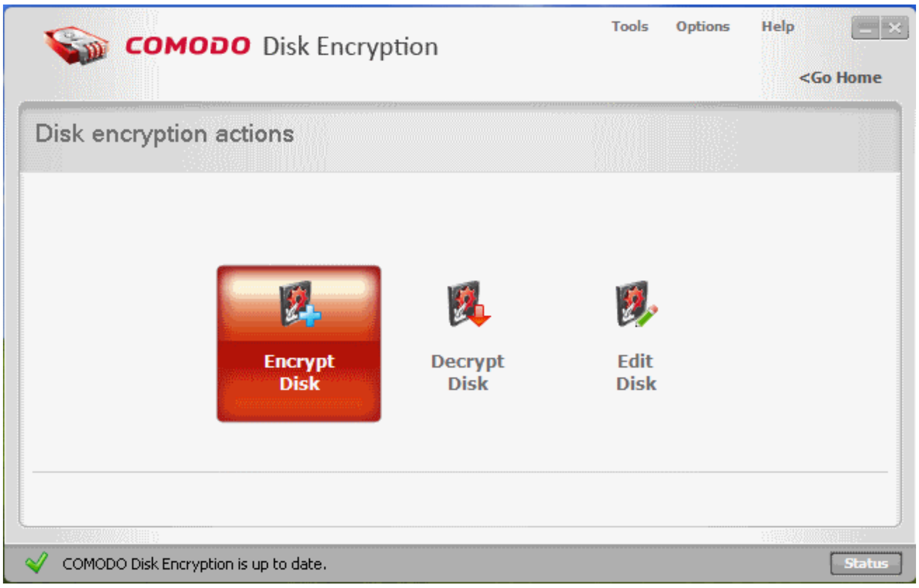
COMODO Disk Encryption is up to date.

From this interface, you can:

- **Encrypt a disk**
- **Decrypt an encrypted disk**
- **Edit encryption parameters like passwords and encryption settings**
- **View the status of your encrypted disks**

2.1. Encrypt Disk

Comodo Disk Encryption allows you encrypt any disk using your choice of the strongest available algorithms.



COMODO Disk Encryption is up to date.

Encrypting a drive protects the confidential information stored in it from being accessed by anybody until the correct **authentication credentials** have been supplied.

Note: If you try to mount a foreign encrypted disk and you provide the correct master password, you are prompted to change that password with the master password of the host computer in order to mount it persistently.

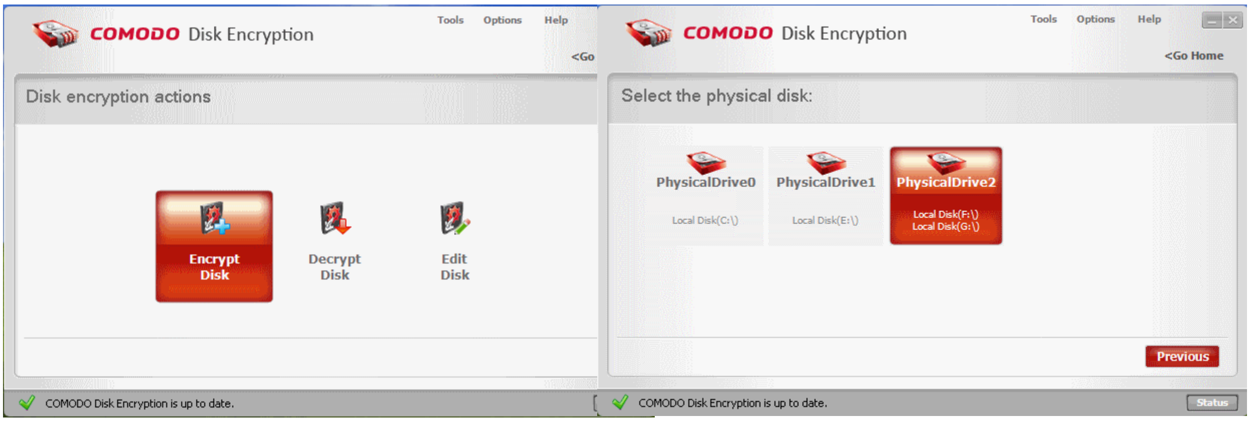
Encrypting a drive involves the following steps:

Step 1: **Choose disk drive**
Step 2: **Select authentication factor(s)**

Step 3: **Choose encryption settings**
Step 4: **Confirm your settings so far**
Step 5: **Execute the encryption**
Step 6: **Check the status of encrypted drive**

Step 1 Choose disk drive

Select from the list, the disk drive which you want to encrypt. Only unencrypted disk drives will be active for selection.



✓ COMODO Disk Encryption is up to date.

Step 2 Input authentication factors

You must type in the following controls:

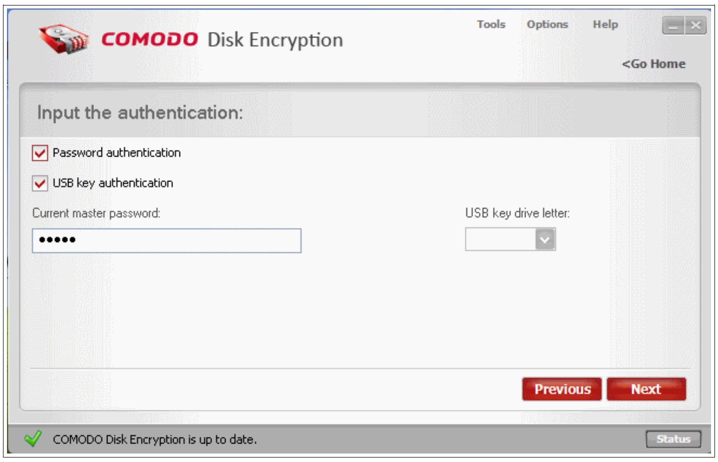
- New master password: the new pass-phrase, if the current disk is the first to be encrypted

OR

- Current master password: the current pass-phrase, the same for other encrypted disks.
- USB drive letter: the drive letter of new encryption USB key

For more information about authentication **click here**.

To understand Passwords **click here**.



☑ Password authentication

☑ USB key authentication

Current master password: •••••

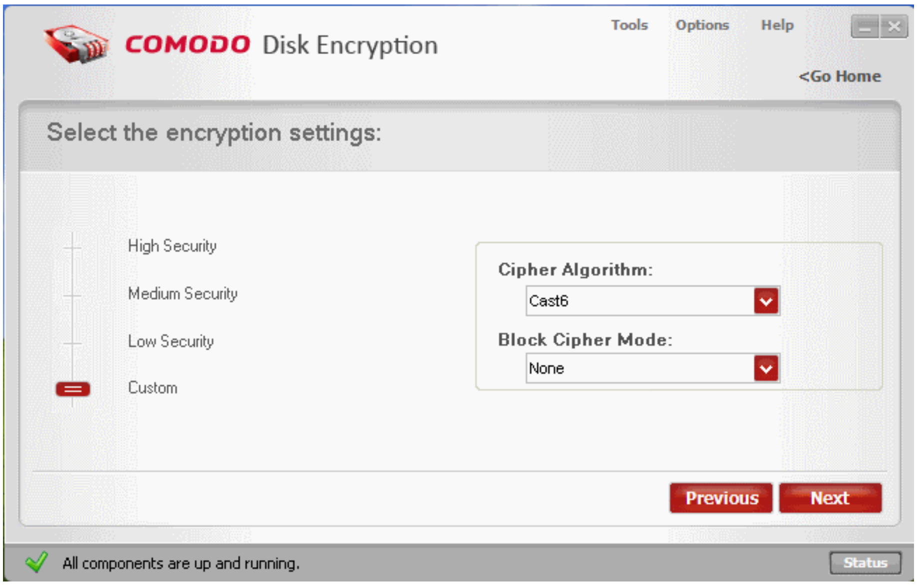
✓ COMODO Disk Encryption is up to date.

Step 3 Encryption settings

The encryption level:

- **High Security:** Cipher algorithm AES, Cipher mode OFB
- **Medium Security:** Cipher algorithm Twofish, Cipher mode CBC
- **Low Security:** Cipher algorithm Cast6, Cipher mode NONE
- **Custom:** Select a combination of a Cipher algorithm and a Block Cipher Mode

Select **The encryption level** you wish to apply to the selected drive. Comodo Disk Encryption provides you with selection of **Cipher Algorithms** and **Block Cipher Modes**. Each has its own advantages in terms of performance and strength. The slider allows you to quickly switch between Comodo suggested combinations of algorithm and cipher mode. You can, however, create your own combination by directly modifying the two drop down menus.
For more information **click here**.



Select the encryption settings:

High Security
Medium Security
Low Security
Custom

Cipher Algorithm: Cast6

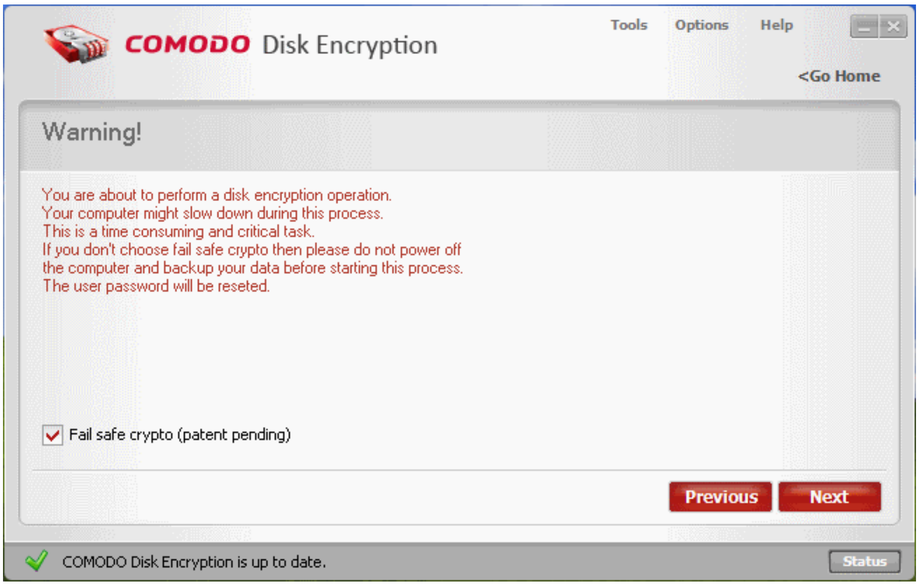
Block Cipher Mode: None

All components are up and running.

Step 4 Warning screen

You can check fail safe crypto in order to perform a slower but safer encryption process.

Note: The user password will be reset (if any defined).



Warning!

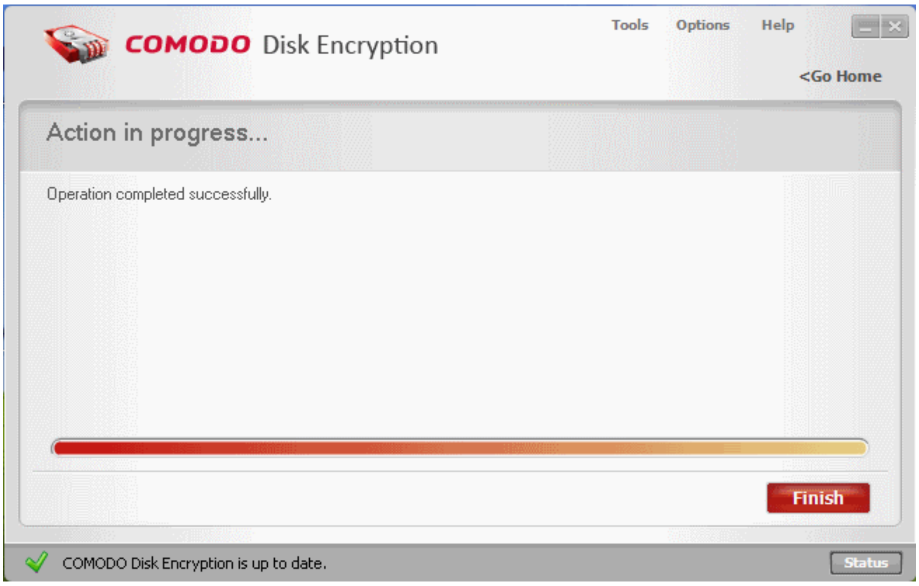
You are about to perform a disk encryption operation.
Your computer might slow down during this process.
This is a time consuming and critical task.
If you don't choose fail safe crypto then please do not power off
the computer and backup your data before starting this process.
The user password will be reseted.

☑ Fail safe crypto (patent pending)

COMODO Disk Encryption is up to date.

Step 5 The operation progress

The application will encrypt the selected drive. This may take some time depending on the size of your disk. Do not power-off the system till the process is completed. The encryption progress is indicated at the progress bar and the remaining time for completion of encryption is displayed above the bar.



Action in progress...

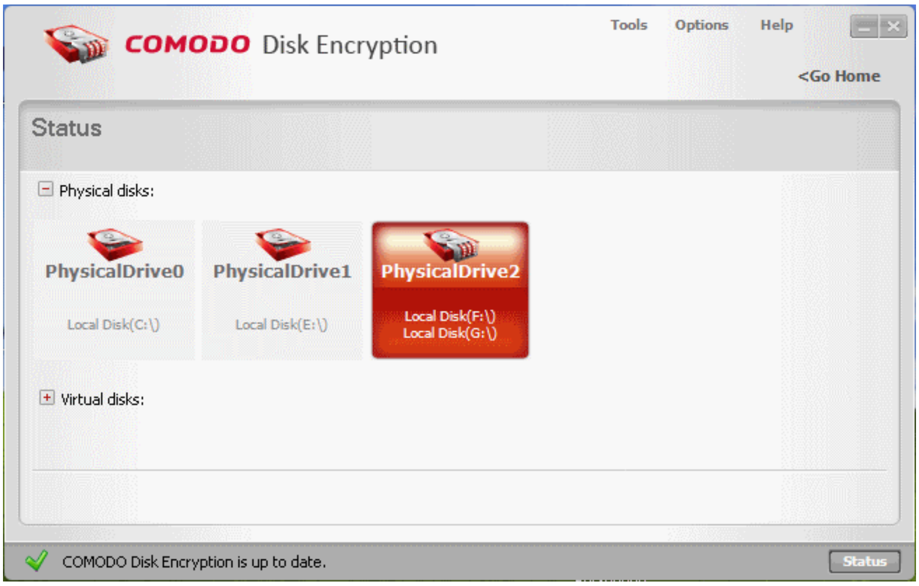
Operation completed successfully.

COMODO Disk Encryption is up to date.

On completion click **Finish**.

Step 6 Check the status of your disks

Click on Status button to view your encrypted disk.



COMODO Disk Encryption is up to date.

2.2. Decrypt Disk

Decrypting an encrypted drive partition brings back the drive to its original (unencrypted) form, the drive becomes accessible by anyone. The protection offered by encrypting the drive is disabled.

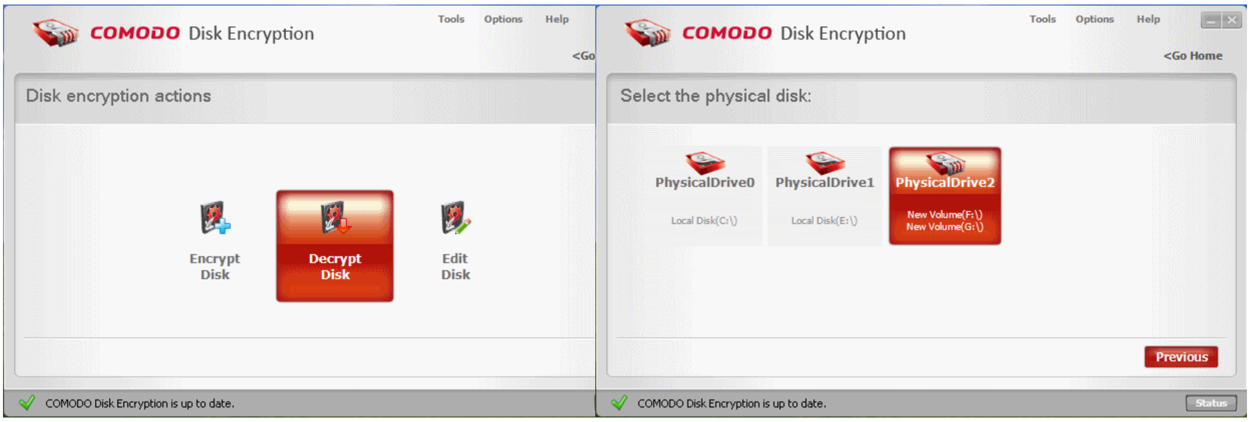
Decrypting a drive involves the following steps:

Step 1: **Choose disk drive**
Step 2: **Input the authentication**
Step 3: **Warning screen**
Step 4: **The operation progress**

Note: Make sure that the USB memory key is inserted into the USB slot of your system before decrypting a drive partition which was encrypted using USB key or both Password and USB key authentication types.

Step 1 Choose disk drive

Select from the list, the disk drive which you want to decrypt. Only encrypted disk drives will be active for selection.



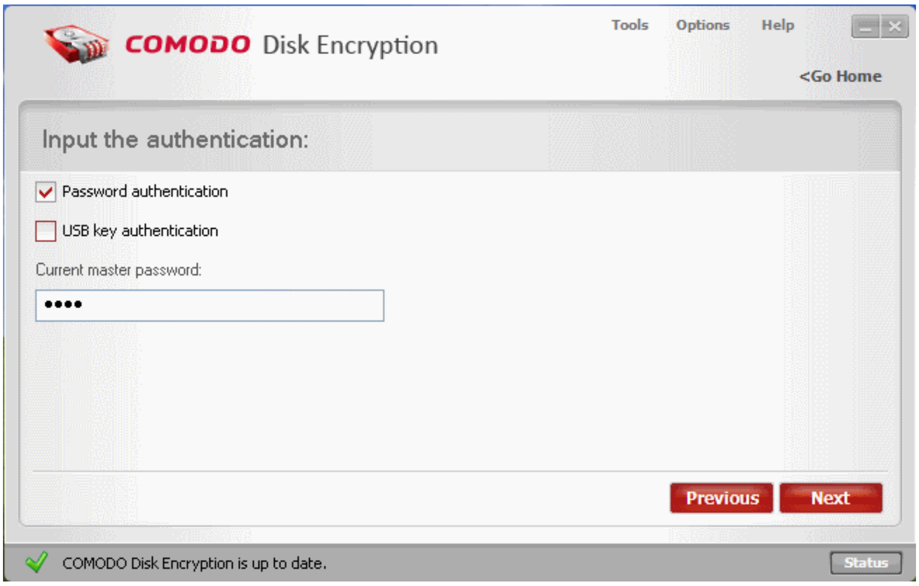
Step 2 Input the authentication

You must type in the following controls:

- Current master password: the current pass-phrase, the same for other encrypted disks.
- USB drive letter: the drive letter of current encryption USB key

For more information about authentication **click here**.

To understand Passwords **click here**.



☑ Password authentication

□ USB key authentication

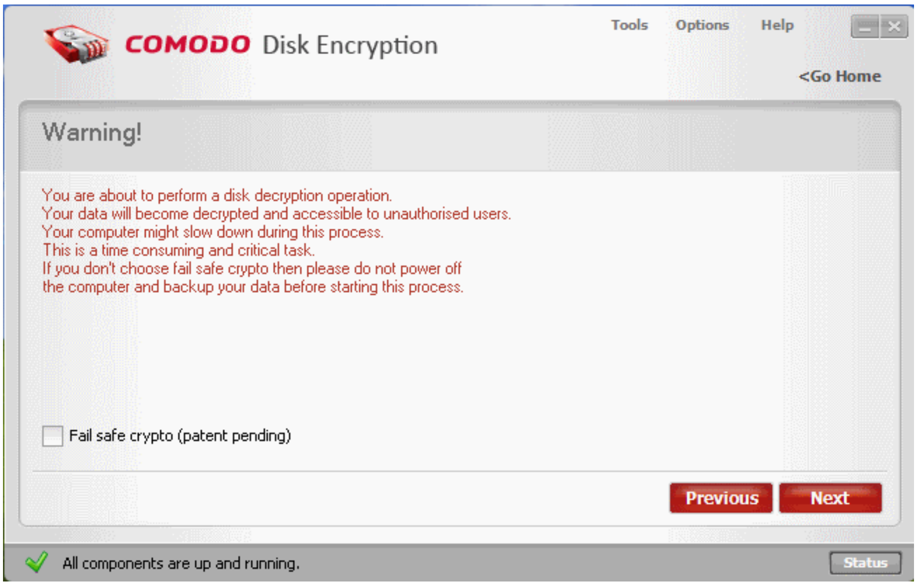
Current master password: ●●●●

Step 3 Warning screen

Warning screen will inform you that you are about to perform a disk decryption operation, your data from this disk will be decrypted and accessible to unauthorized users and this is a time consuming and critical task.

Note: If you don't choose fail safe crypto then please do not power off the computer during the decryption process and backup your data before starting this.

You can check fail safe crypto in order to perform a slower but safer decryption process.
Click 'Next' to continue.



Warning!

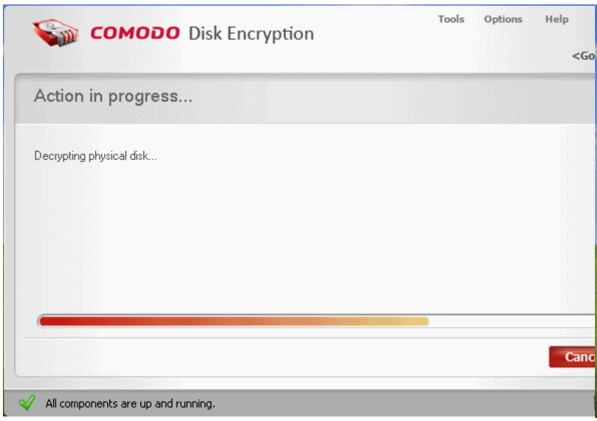
You are about to perform a disk decryption operation.
Your data will become decrypted and accessible to unauthorised users.
Your computer might slow down during this process.
This is a time consuming and critical task.
If you don't choose fail safe crypto then please do not power off
the computer and backup your data before starting this process.

□ Fail safe crypto (patent pending)

All components are up and running.

Step 4 The operation progress

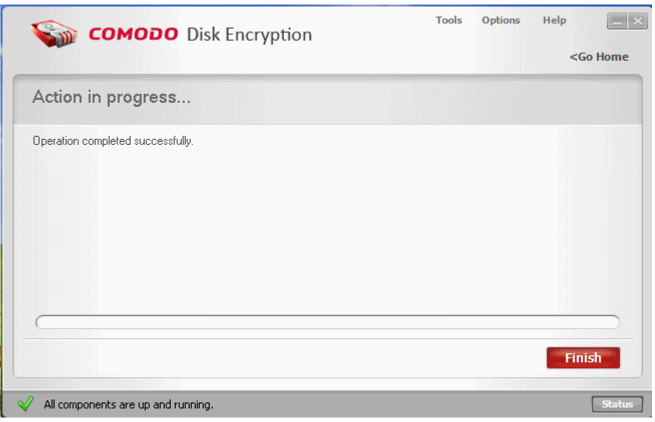
The application starts decrypting the selected drive. This may take some time depending on the size of your disk. Do not power-off the system till the process is completed. The decryption progress is indicated at the progress bar.



Action in progress...

Decrypting physical disk...

All components are up and running.



Action in progress...

Operation completed successfully.

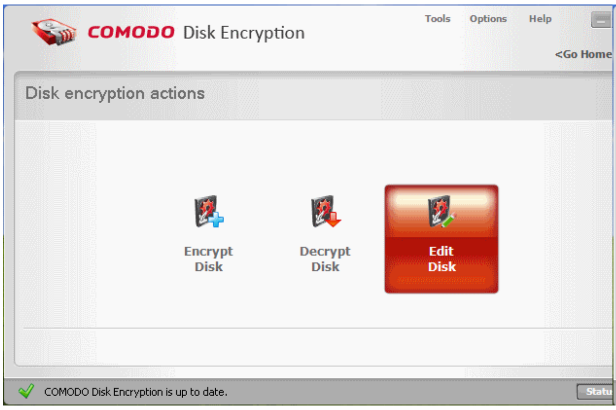
All components are up and running.

On Completion, click **'Finish'**.

2.3. Edit Disk

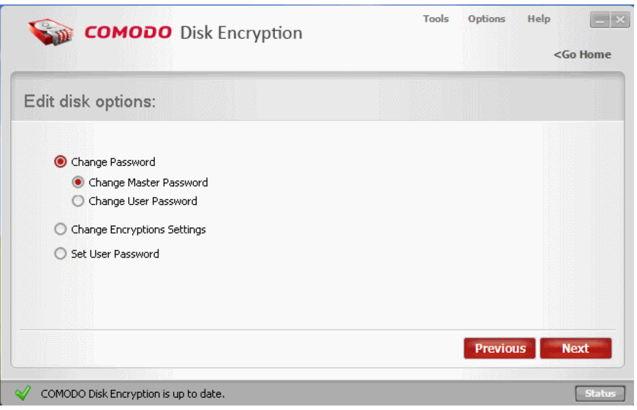
Comodo Disk Encryption allows the user to manage the settings for the encrypted physical disks.

The user can change the master password , create/change a user password and change encryption settings for a specific disk.



Disk encryption actions

COMODO Disk Encryption is up to date.



Edit disk options:

● Change Password
  ● Change Master Password
  ○ Change User Password
○ Change Encryptions Settings
○ Set User Password

COMODO Disk Encryption is up to date.

Click the links below for detailed description:

- **Change Password**
  - **Change Master Password**
  - **Change User Password**
- **Change Encryption Settings**
- **Set User Password**

2.3.1. Change Password

When you create an encrypted disk for the first time you need to choose a master password. This master password enables you to access all encrypted disks from your computer and create new ones.

For your encrypted disk you can create a user password to allow other users to access your confidential data. To learn how to create a user password **click here**.

To understand Passwords **click here**.

Comodo Disk Encryption allow you to:

- **Change Master Password**
- **Change User Password**

2.3.1.1. Change Master Password

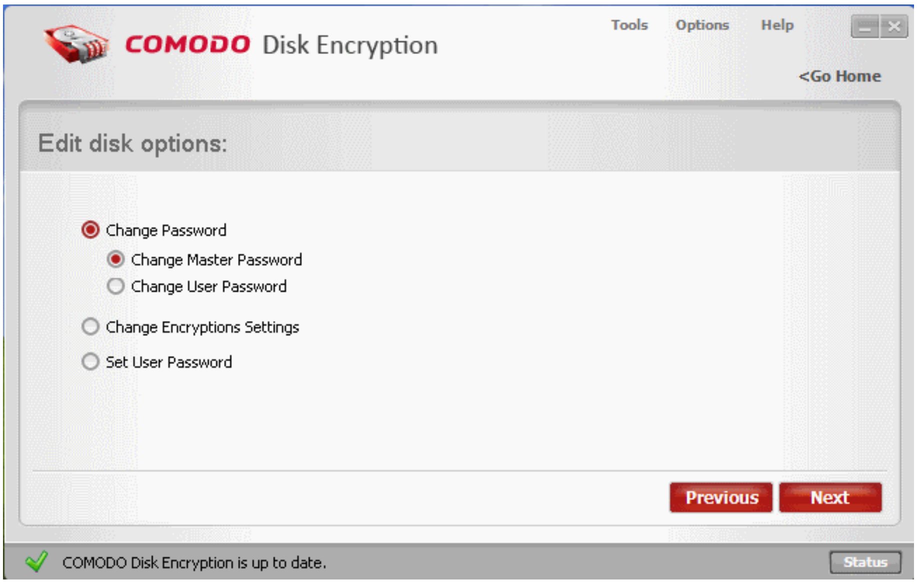
With the Master Password you can encrypt/decrypt a disk, change the encryption settings and manage the user password.

Changing a Master Password involves the following steps:

Step 1: **Select Change Master Password**
Step 2: **Input the authentication and click Next**
Step 3: **Input your new Master Password**
Step 4: **Warning screen**
Step 5: **The operation progress**

Step 1 Select Change Master Password

From Edit Disk interface select **Change Master Password** and click **'Next'.**



Edit disk options:

● Change Password
- ● Change Master Password
- ○ Change User Password

○ Change Encryptions Settings

○ Set User Password

COMODO Disk Encryption is up to date.

Step 2 Input the authentication and click 'Next'

You must type in the following credentials:

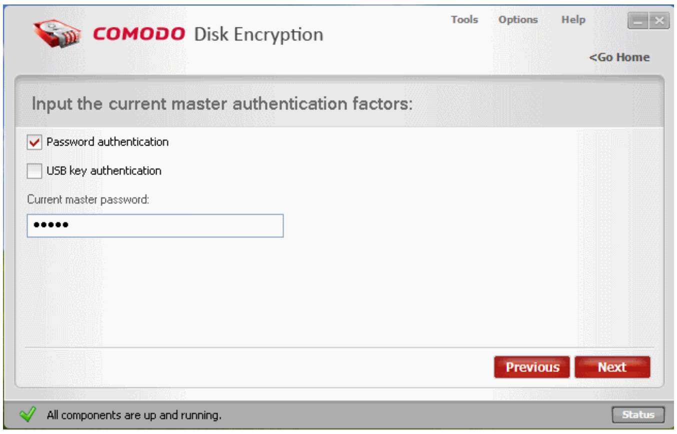
- Current master password: the current pass-phrase, the same for other encrypted disks.

or

- Current master password: the current pass-phrase, the same for other encrypted disks.
- USB drive letter: the drive letter of current encryption USB key

For more information about authentication **click here**.

To understand Passwords **click here**.



Input the current master authentication factors:

☑ Password authentication

□ USB key authentication

Current master password:

•••••

All components are up and running.

Step 3 Input your new Master Password

You must type in the following controls:

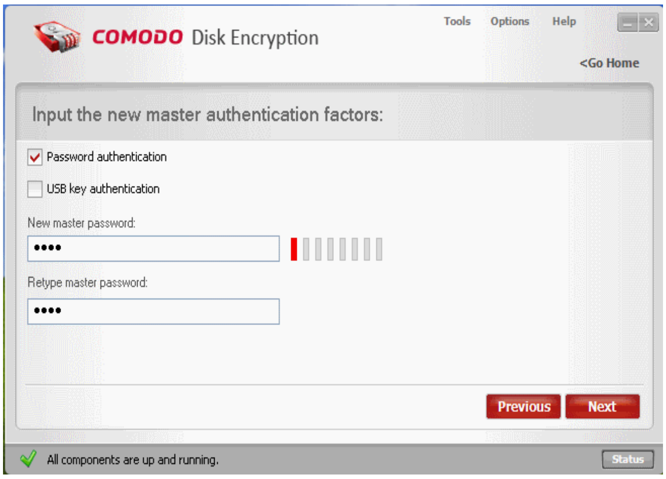
- New master password: the new pass-phrase.

OR

- New master password: the new pass-phrase.
- USB drive letter: the drive letter of new encryption USB key

For more information about authentication **click here**.

To understand Passwords **click here**.



Input the new master authentication factors:

☑ Password authentication

□ USB key authentication

New master password:

••••

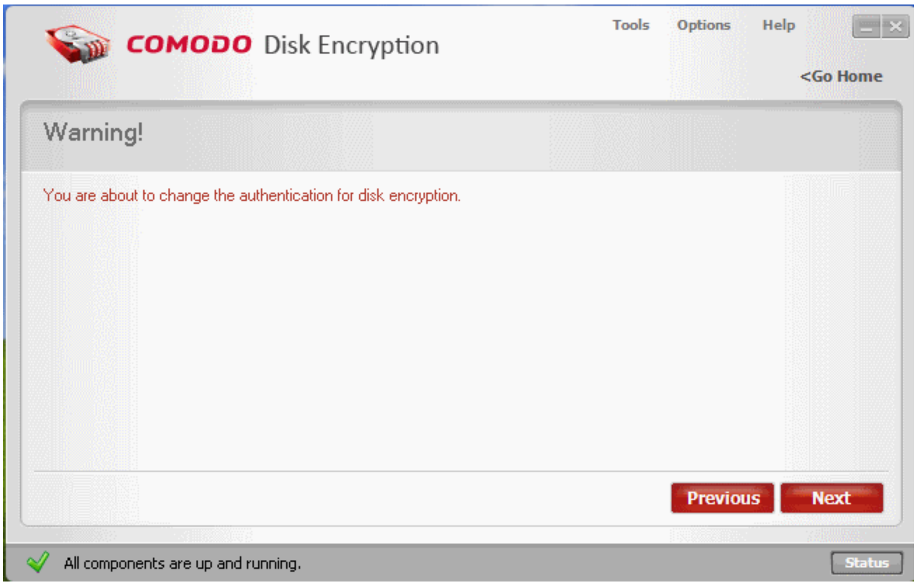
Retype master password:

••••

All components are up and running.

Step 4 Warning screen

Warning screen will inform you that you are about to change the authentication for disk encryption. Click **'Next'** to continue.

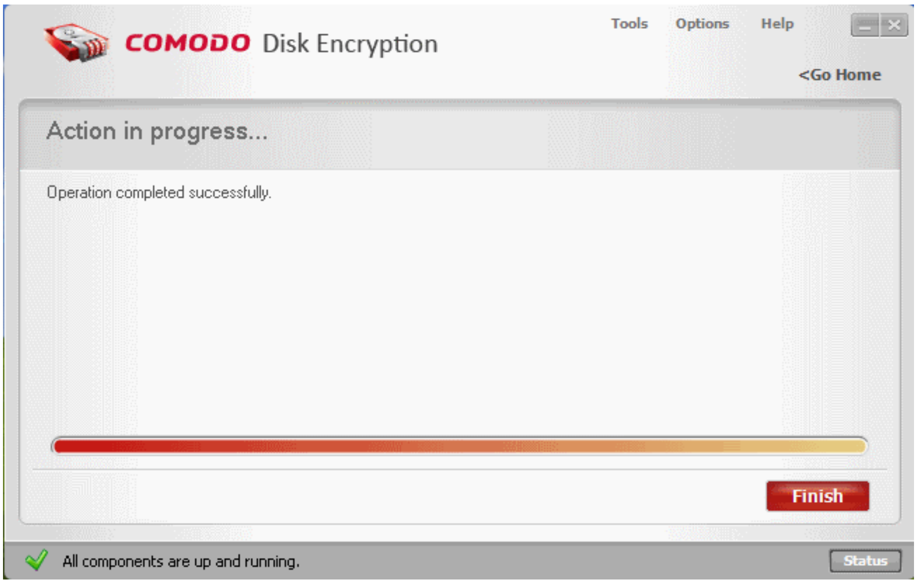


You are about to change the authentication for disk encryption.

All components are up and running.

Step 5 The operation progress

The application starts changing the master password for your encrypted disks. Do not power-off the system till the process is completed. The changing progress is indicated at the progress bar.



Operation completed successfully.

All components are up and running.

On completion, click **'Finish'**.

2.3.1.2. Change User Password

The User Password provides limited access to your secure information.

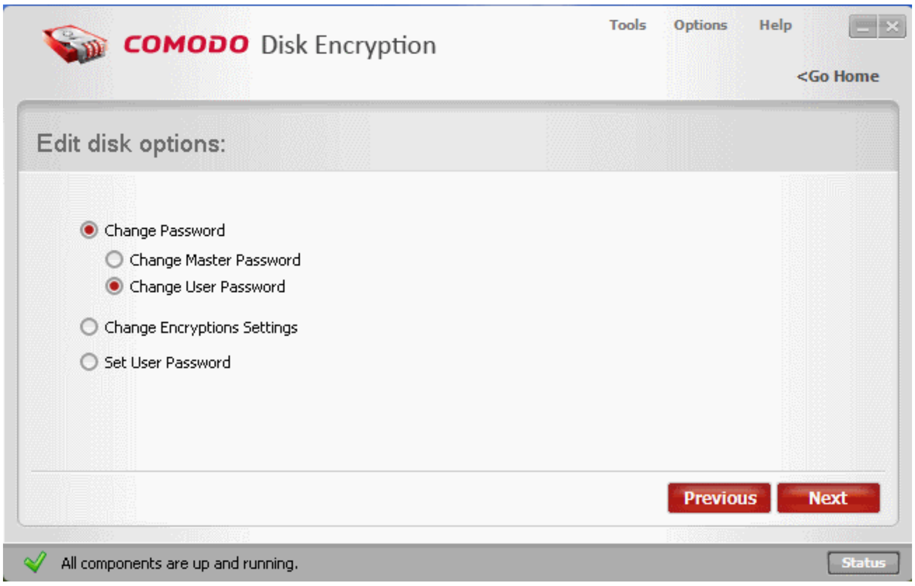
For more information about Passwords **click here**.

Changing a User Password involves the following steps:

Step 1: **Select Change User Password**
Step 2: **Input the authentication**
Step 3: **Input your new User Password**
Step 4: **Warning screen**
Step 5: **The operation progress**

Step 1 Select Change User Password

From Edit Disk interface select **Change User Password** and click **Next.**



Edit disk options:

● Change Password

○ Change Master Password

● Change User Password

○ Change Encryptions Settings

○ Set User Password

All components are up and running.

Step 2 Input the authentication and click Next

You must type in the following controls:

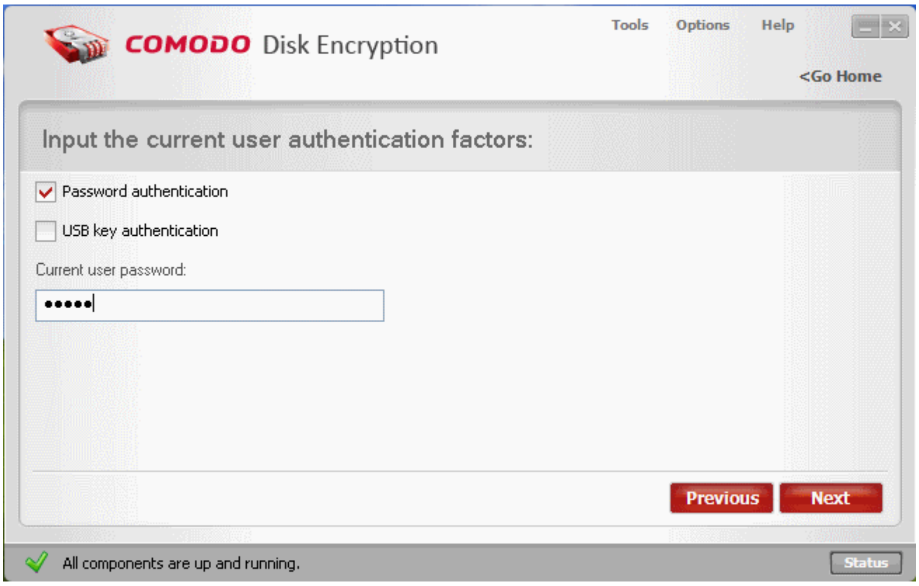
- Current master password: the current pass-phrase, the same for other encrypted disks.

OR

- Current master password: the current pass-phrase, the same for other encrypted disks; and
- USB drive letter: the drive letter of current encryption USB key

For more information about authentication **click here**.

To understand Passwords **click here**.



Input the current user authentication factors:

☑ Password authentication

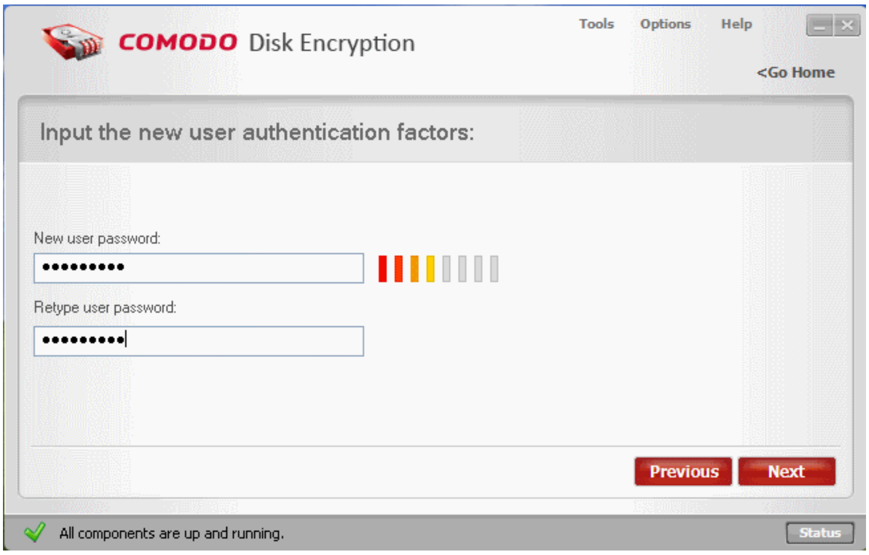
□ USB key authentication

Current user password: •••••

All components are up and running.

Step 3 Input your new User Password

Enter your new User Password and click **'Next'**.



COMODO Disk Encryption

Input the new user authentication factors:

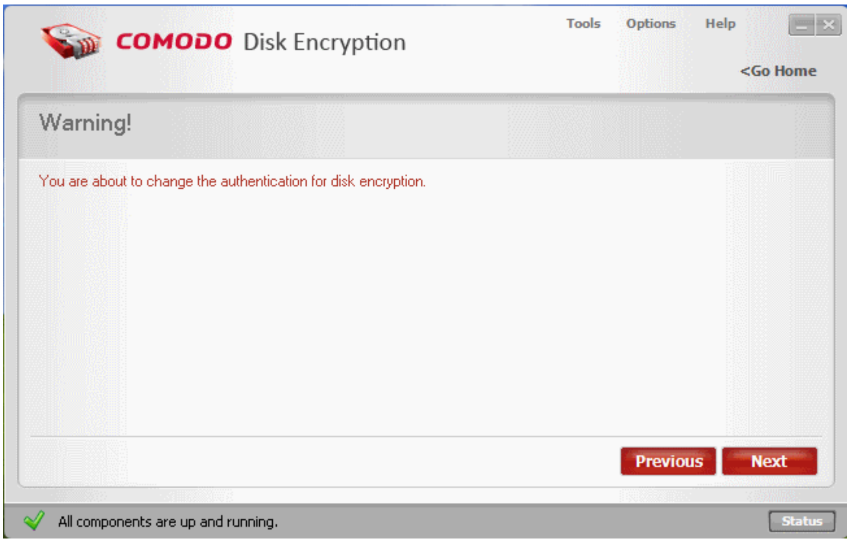
New user password: •••••••••

Retype user password: •••••••••

All components are up and running.

Step 4 Warning screen

Warning screen informs you that you are about to change the authentication for disk encryption. Click **'Next'** to continue.



COMODO Disk Encryption

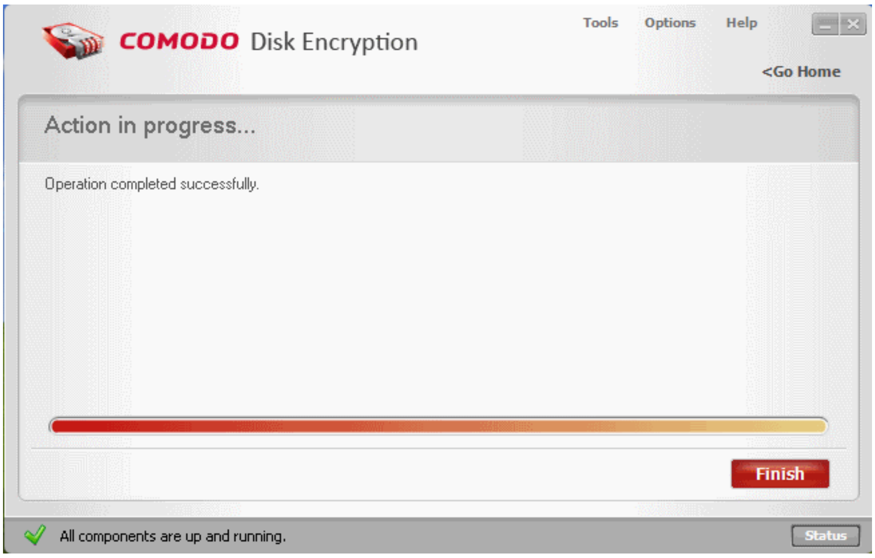
Warning!

You are about to change the authentication for disk encryption.

All components are up and running.

Step 5 The operation progress

The application starts changing the user password for your encrypted disks. Do not power-off the system till the process is completed. The changing progress is indicated at the progress bar.



COMODO Disk Encryption

Action in progress...

Operation completed successfully.

All components are up and running.

On completion click **Finish**.

2.3.2. Change Encryption Settings

Comodo Disk Encryption ships with four encryption levels

- **High Security:** Cipher algorithm AES, Cipher mode OFB
- **Medium Security:** Cipher algorithm Twofish, Cipher mode CBC
- **Low Security:** Cipher algorithm Cast6, Cipher mode NONE
- **Custom:** Select a combination from an Cipher algorithm and Block Cipher Mode

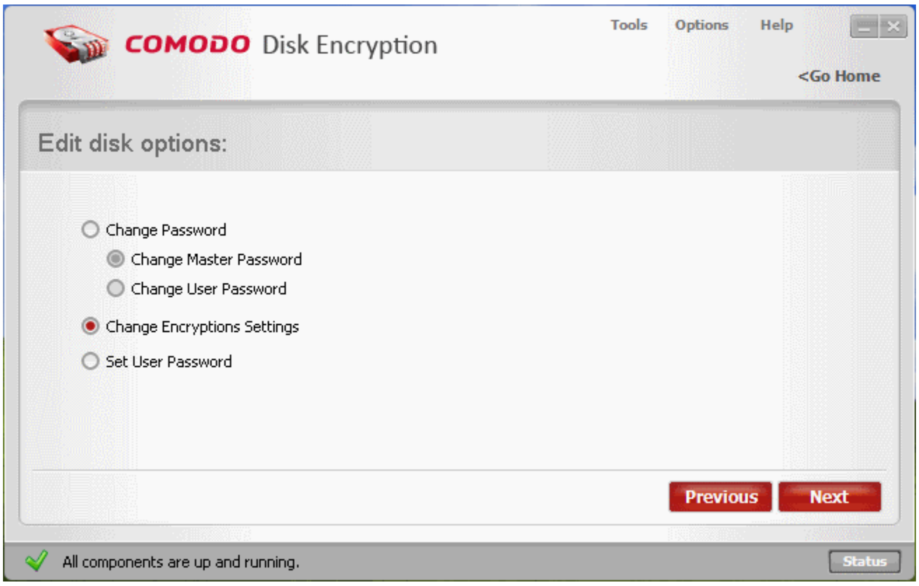
Comodo Disk Encryption provides you with selection of **Cipher Algorithms** and **Block Cipher Modes**. Each has its own advantages in terms of performance and strength. The slider allows you to quickly switch between Comodo suggested combinations of algorithm and cipher mode. You can, however, create your own combination by directly modifying the two drop down menus. For more information about algorithms click here.

Changing Encryption settings involves the following steps:

Step 1: Select Change Encryption Settings
Step 2: Select your encrypted disk
Step 3: Input the authentication
Step 4: Select the new encryption settings
Step 5: Warning screen
Step 6: The operation progress

Step 1 Select Change Encryption Settings

From Edit Disk interface select **Change Encryption Settings** and click **'Next'.**



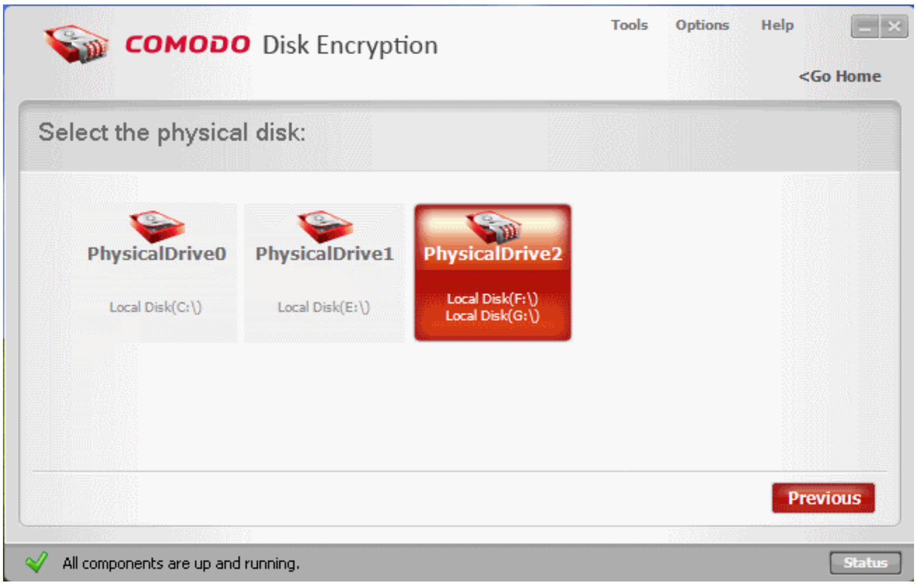
Edit disk options:

○ Change Password
● Change Master Password
○ Change User Password
● Change Encryptions Settings
○ Set User Password

All components are up and running.

Step 2 Select your encrypted disk

In the interface you can select only encrypted disks. Click on the encrypted disk for which you want to change the encryption settings.



Step 3 Input the authentication and click Next

You must type in the following controls:

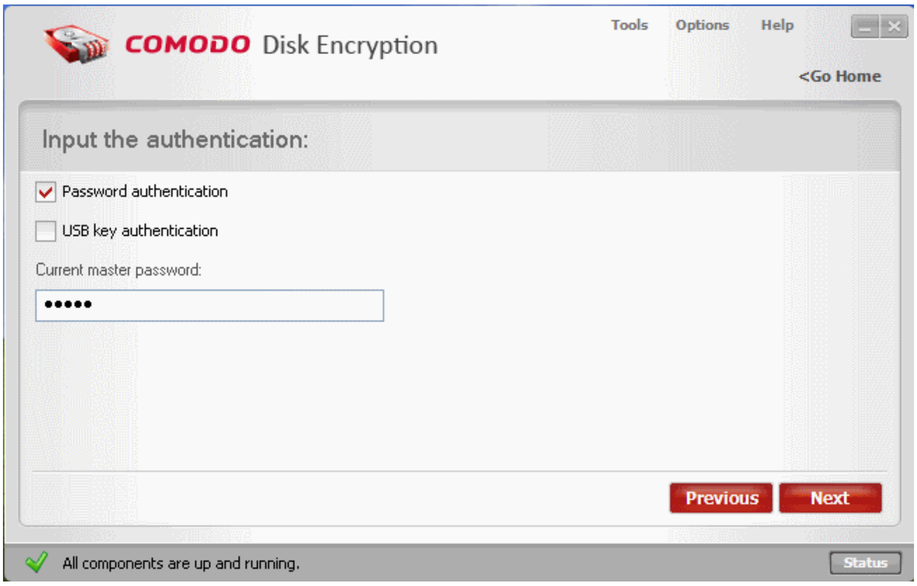
- Current master password: the current pass-phrase, the same for other encrypted disks.

OR

- Current master password: the current pass-phrase, the same for other encrypted disks.
- USB drive letter: the drive letter of current encryption USB key

For more information about authentication **click here**.

To understand Passwords **click here**.



☑ Password authentication

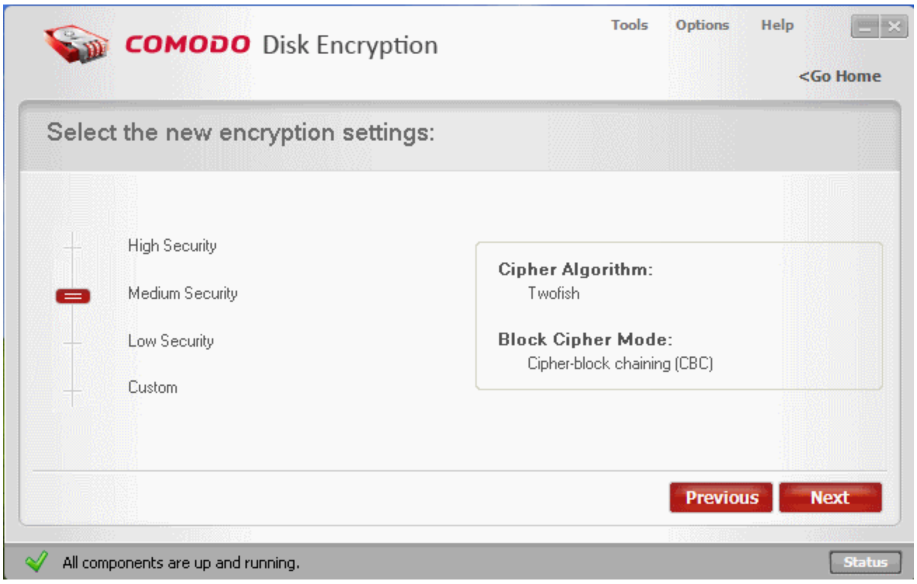
☐ USB key authentication

Current master password:

•••••

Step 4 Select the new encryption settings

Select your new encryption level and click **'Next'**. For more information about algorithms **click here**.



Select the new encryption settings:

Cipher Algorithm: Twofish

Block Cipher Mode: Cipher-block chaining (CBC)

All components are up and running.

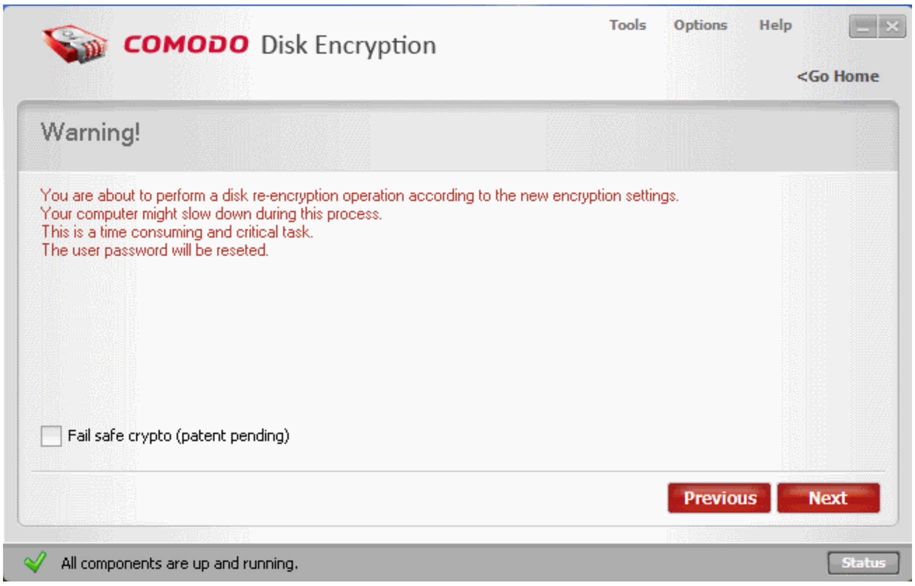
Step 5 Warning screen

Warning screen inform you that you are about to perform a disk re-encryption according with your new settings and your computer might slow down during this process because it is a time consuming and critical task.

Note: This process will reset your user password. To create a new user password **click here**.

You can check fail safe crypto in order to perform a slower but safer encryption process.

Click **'Next'** to continue.



Warning!

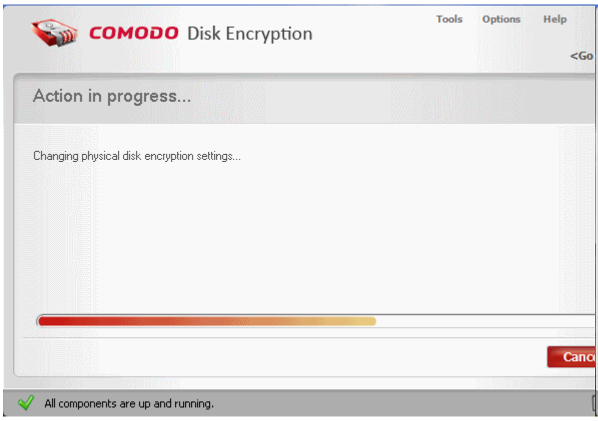
You are about to perform a disk re-encryption operation according to the new encryption settings.
Your computer might slow down during this process.
This is a time consuming and critical task.
The user password will be reseted.

□ Fail safe crypto (patent pending)

All components are up and running.

Step 6 The operation progress

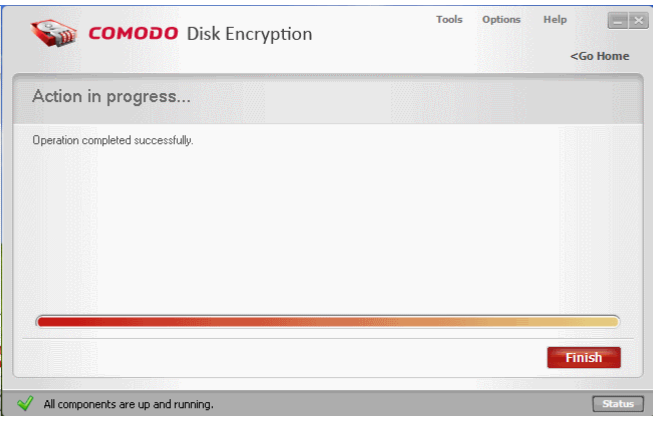
The application starts decrypting the selected drive. This may take some time depending on the size of your disk. Do not power-off the system till the process is completed. The progress is indicated at the progress bar.



Action in progress...

Changing physical disk encryption settings...

All components are up and running.



Action in progress...

Operation completed successfully.

All components are up and running.

On Completion, click **Finish**.

2.3.3. Set User Password

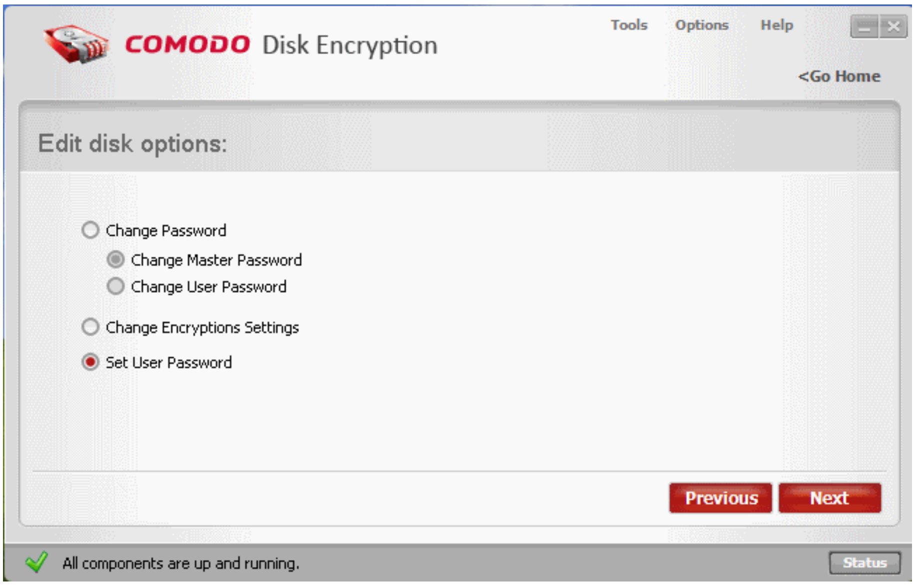
For your encrypted disks you can create a user password to allow other users to have limited access.

Creating a User Password involves the following steps:

Step 1: **Select Set User Password**
Step 2: **Input the authentication**
Step 3: **Input your User Password**
Step 4: **Warning screen**
Step 5: **The operation progress**

Step 1 Select Set User Password

From Edit Disk interface select **Set User Password** and click **'Next'.**



Edit disk options:

○ Change Password
● Change Master Password
○ Change User Password
○ Change Encryptions Settings
● Set User Password

All components are up and running.

Step 2 Input the authentication

You must type in the following controls:

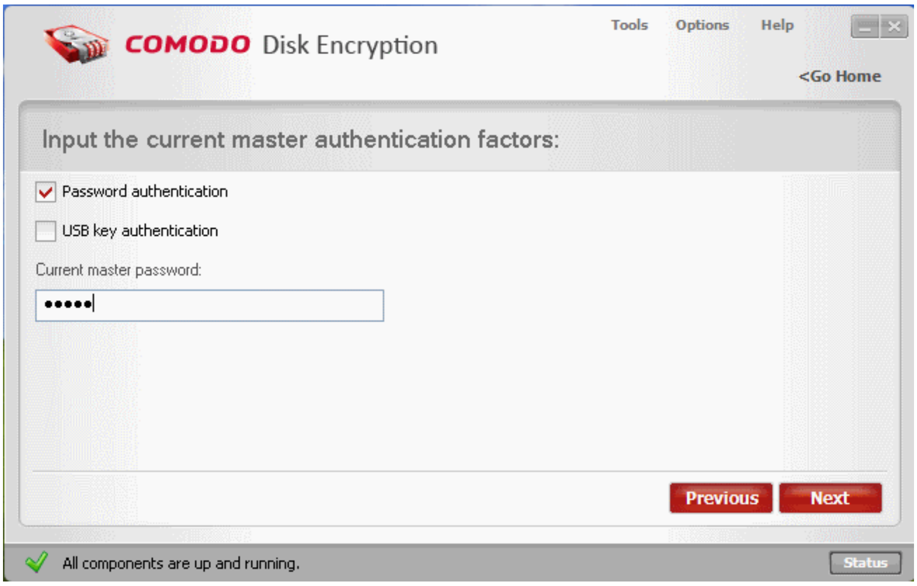
- Current master password: the current pass-phrase, the same for other encrypted disks.

OR

- Current master password: the current pass-phrase, the same for other encrypted disks; and
- USB drive letter: the drive letter of current encryption USB key

For more information about authentication **click here**.

To understand Passwords **click here**.



Input the current master authentication factors:

☑ Password authentication

□ USB key authentication

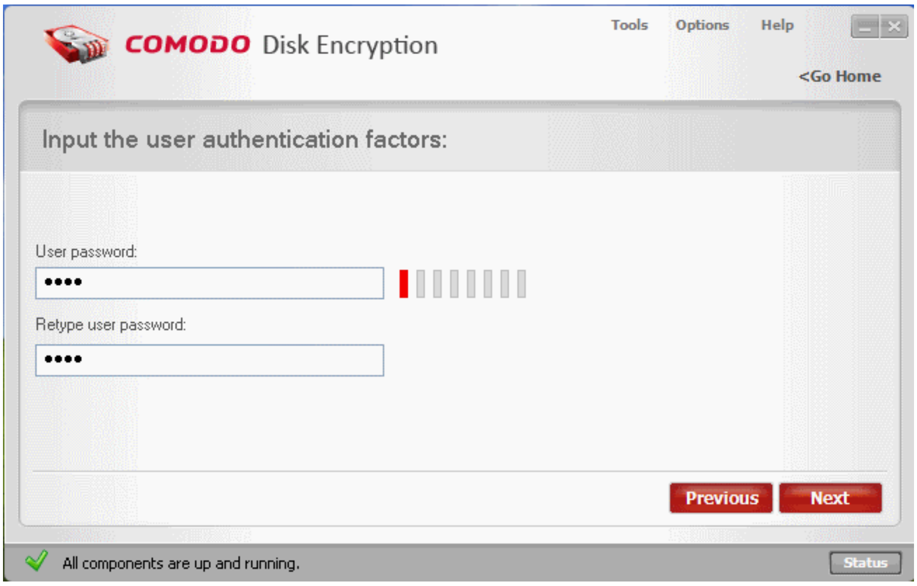
Current master password:

•••••

All components are up and running.

Step 3 Input your User Password

Enter your new User Password and click **'Next'**.



Input the user authentication factors:

User password:

••••

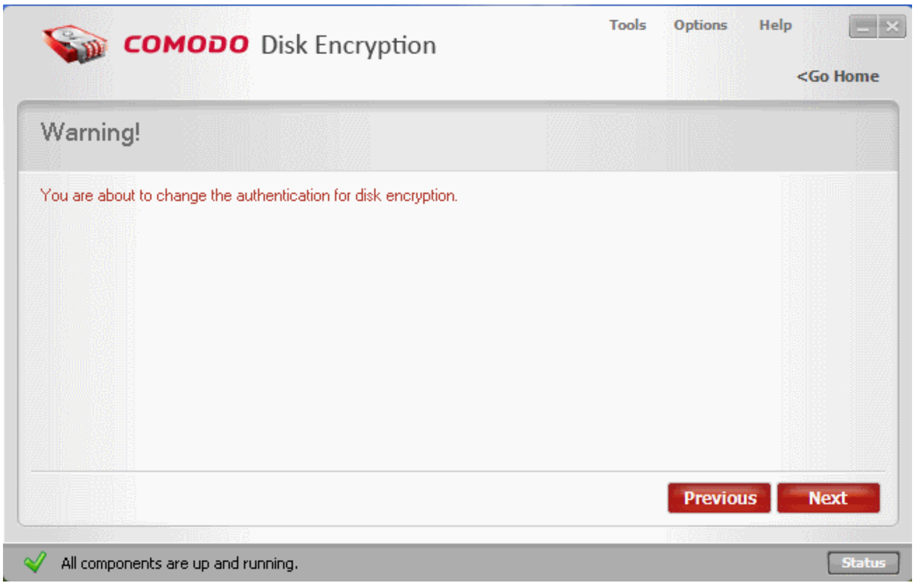
Retype user password:

••••

All components are up and running.

Step 4 Warning screen

Warning screen will inform you that you are about to change the authentication for disk encryption. Click **'Next'** to continue.



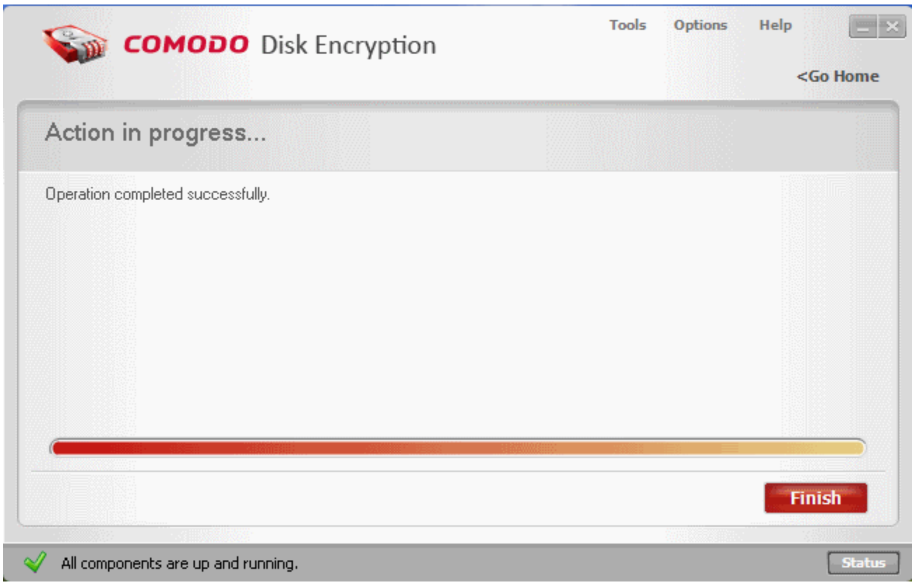
Warning!

You are about to change the authentication for disk encryption.

All components are up and running.

Step 5 The operation progress

The application starts creating the user password for your encrypted disks. Do not power-off the system till the process is completed. The progress is indicated at the progress bar.



Action in progress...

Operation completed successfully.

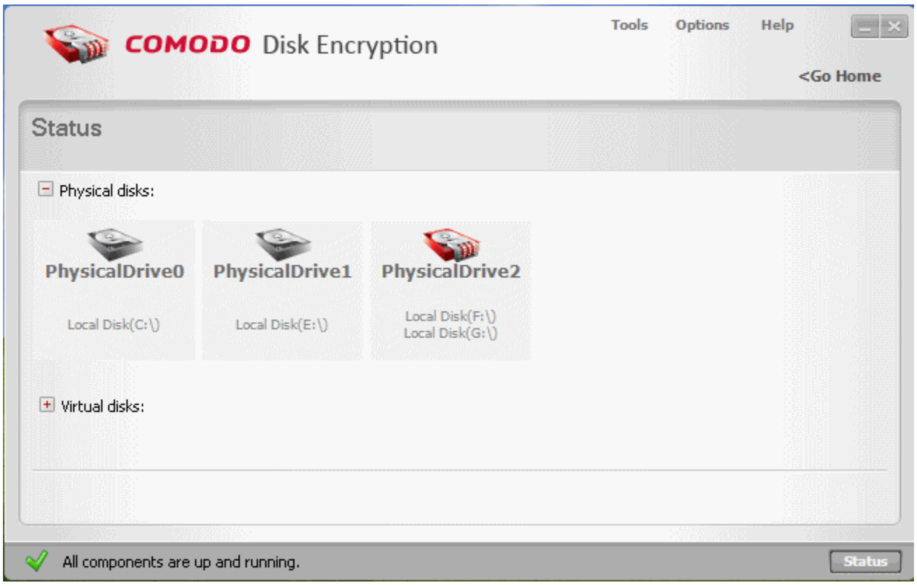
All components are up and running.

On completion, click **Finish**.

2.4. Status

The Status interface provides a visual representation of your disks.

You can find out which disks are encrypted or and which are not at a glance. To access the interface click on the **Status** button from the **Status Bar**.



3. Virtual Disk Encryption

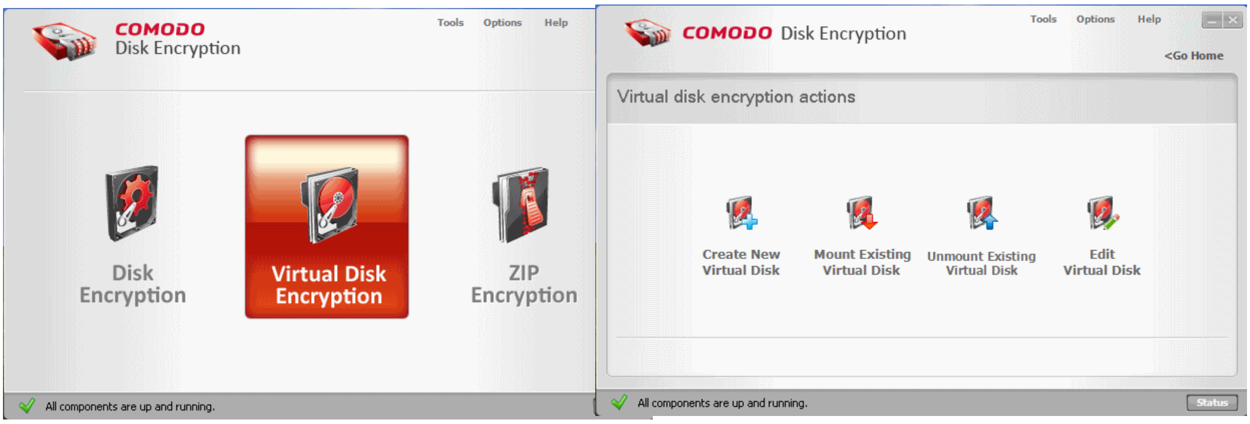
A Virtual drive is a drive partition that is created to emulate an optical disk (such as a dvd or cd) or a hard drive partition.

Comodo Disk Encryption contains a wizard that allows you to create two types of virtual drives depending on your requirements:

- **Virtual Memory drives**, which reside in the system memory, enable very fast read write access but last only till the system is turned-off. The memory drive is created in the system memory, i.e. a portion of RAM is set up to act as a hard drive partition. The memory drive has fast read/write access. Because of the volatile nature of the system memory, the memory drive will last only till the system is powered-off. Memory drives can be used while working with a decrypted copy of an encrypted document and to hold larger files like image files for shorter period of times, e.g. when working on several images using image editing software. To create a virtual memory drive, select ' Memory Drive' as the ' disk type' during the virtual drive creation wizard. See ' **Creating New Virtual Disk**' for more details.
- **Virtual File drives**, which reside in your hard disk. The file drive is created as single disk image file at any location of your choice in your hard drive. This file acts as a disk image, resembling a separate hard drive partition. You can set any drive letter of your choice to this virtual drive partition and encrypt with any hash and encryption algorithms. The virtual drive will be displayed as a hard drive partition in My Computer Explorer window. You can format this drive and store your data to be protected in it for permanent storage. To create a virtual file drive, select ' File Drive' as the ' disk typestore location' during the virtual drive creation wizard. See ' **Creating New Virtual Disk**' for more details.

A new drive letter can also be assigned for a virtual drive and this will resemble a hard drive partition in My Computer Explorer window.

To access this feature click on the **Virtual Disk Encryption** button on the Main Interface.



From this interface, you can:

- **Create New Virtual Disk**
- **Mount Existing Virtual Disk**
- **Unmount Existing Virtual Disk**
- **Edit Virtual Disk Parameters**
- **View status of the virtual disks**

3.1. Create New Virtual Disk

Comodo Disk Encryption allows you to create Virtual Disks on your system using the strongest encrypt algorithms available.

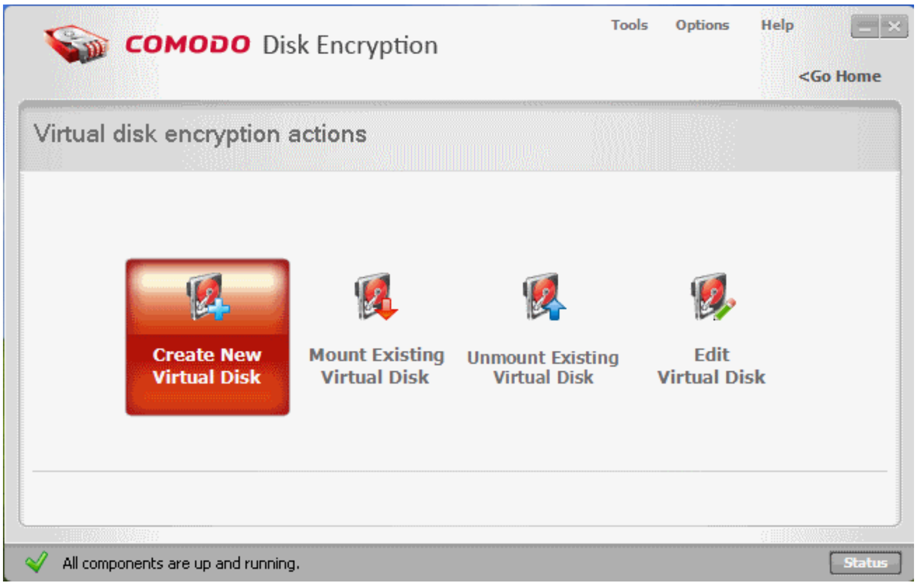
Encrypting a Virtual Disk protects the confidential information stored in it from being accessed by anybody until the correct **authentication credentials** have been supplied.

Creating a Virtual Disk involves the following steps:

Step 1: **Create New Virtual Disk**
Step 2: **Choose the disk type**
Step 3: **Input authentication factors**
Step 4: **Encryption settings**
Step 5: **Warning screen**
Step 6: **The operation progress**

Step 1 Select Create New Virtual Disk

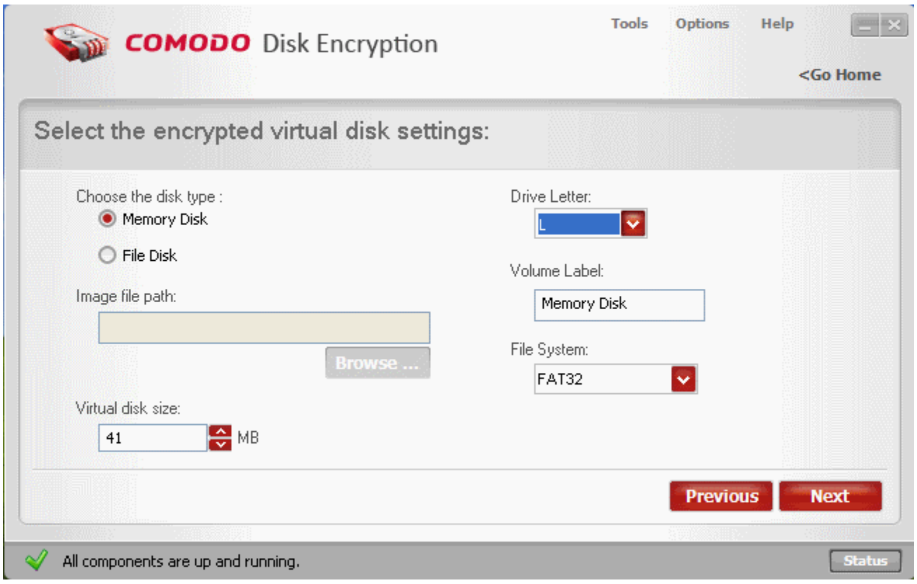
Click on **Create New Virtual Disk** from Virtual disk encryption interface.


COMODO Disk Encryption
Tools
Options
Help
<Go Home
Virtual disk encryption actions
Create New Virtual Disk
Mount Existing Virtual Disk
Unmount Existing Virtual Disk
Edit Virtual Disk
All components are up and running.
Status

Step 2 Choose the disk type

In the virtual disk settings interface, you can create a **Memory Drive** or a **File Drive**.

- **Memory Drive** - The memory drive is created in the system memory, i.e. a portion of RAM is set up to act as a hard drive partition. The memory drive has fast read/write access. Because of the volatile nature of the system memory, the memory drive will last only till the system is powered-off. Memory drives can be used while working with a decrypted copy of an encrypted document and to hold larger files like image files for shorter period of times, e.g. when working on several images using image editing software. **Click here** for more details on Memory Drive.


COMODO Disk Encryption
Tools
Options
Help
<Go Home
Select the encrypted virtual disk settings:
Browse ...
Previous
Next
All components are up and running.
Status

Choose the disk type :
● Memory Disk
○ File Disk

Image file path:

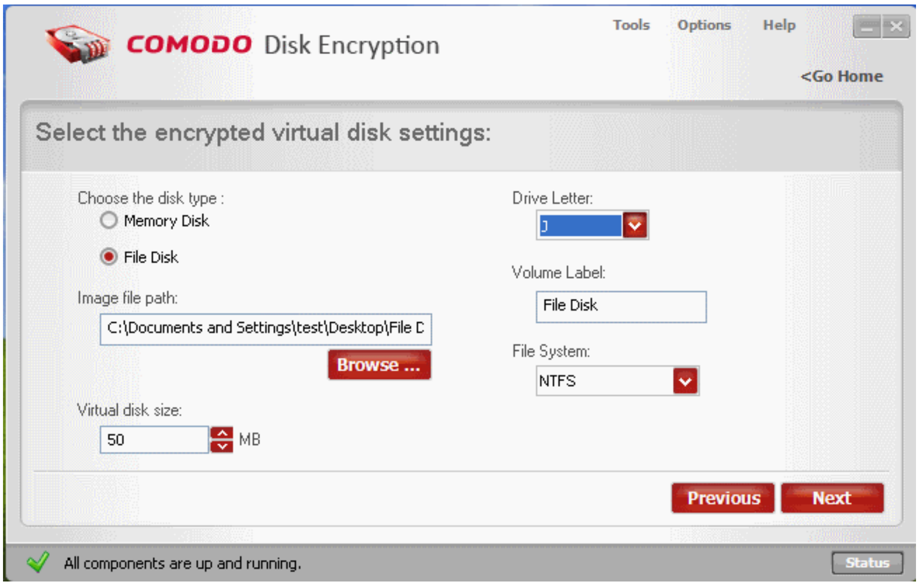
Virtual disk size: 41 MB

Drive Letter: L

Volume Label: Memory Disk

File System: FAT32

- **File Drive** - The file drive is created as single file at any location of your choice in your hard drive. This file acts as a disk image, resembling a separate hard drive partition. You can set any drive letter of your choice to this virtual drive partition and encrypt with any hash and encryption algorithms. The virtual drive will be displayed as a hard drive partition in My Computer Explorer window. You can format this drive and store your data to be protected in it for permanent storage. **Click here** for more details about File Drive.



Select the encrypted virtual disk settings:

Choose the disk type :
○ Memory Disk
● File Disk

Image file path: C:\Documents and Settings\test\Desktop\File D

Virtual disk size: 50 MB

Drive Letter: J

Volume Label: File Disk

File System: NTFS

All components are up and running.

- **Image file path -** Refers to the file location where the encrypted virtual disk should be saved. This field is enabled only if you choose to create an encrypted file disk. This will become active if you select File disk type.
- **Virtual disk size -** This control will be activated after you select the image file path. The size depends on free space available on the drive where the image file is saved. This is the size of the encrypted virtual disk to be created.
- **Drive Letter** - The drive letter which will appear in Windows Explorer for the encrypted virtual disk.
- **Volume Label** - A short description or name for the encrypted virtual drive.
- **File System** - The file system to be used for the encrypted virtual drive. This can be FAT, FAT32 or NTFS.

After making your settings click **'Next'.**

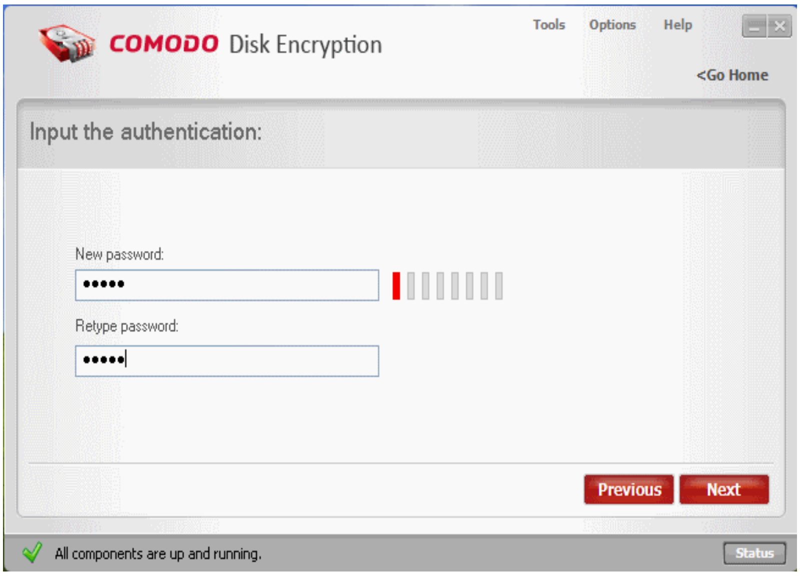
Step 3 Input authentication factors

You must type in the following credentials:

- New master password: the new pass-phrase, if the current disk is the first virtual disk to be encrypted

OR

- Current master password: the current pass-phrase, the same for other virtual disks.



Input the authentication:

New password: •••••

Retype password: •••••

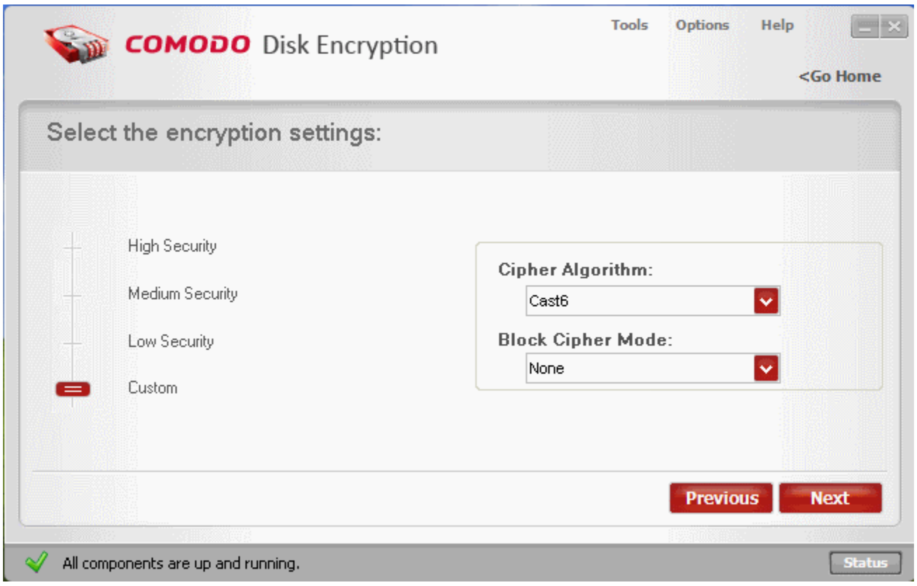
All components are up and running.

Step 4 Encryption settings

The encryption level:

- **High Security:** Cipher algorithm AES, Cipher mode OFB
- **Medium Security:** Cipher algorithm Twofish, Cipher mode CBC
- **Low Security:** Cipher algorithm Cast6, Cipher mode NONE
- **Custom:** Select a combination from an Cipher algorithm and Block Cipher Mode

Select **The encryption level** you wish to apply to the selected drive. Comodo Disk Encryption provides you with selection of **Cipher Algorithms** and **Block Cipher Modes**. Each has its own advantages in terms of performance and strength. The slider allows you to quickly switch between Comodo suggested combinations of algorithm and cipher mode. You can, however, create your own combination by directly modifying the two drop down menus.
For more information about algorithms **click here**.



Select the encryption settings:

High Security
Medium Security
Low Security
Custom

Cipher Algorithm: Cast6

Block Cipher Mode: None

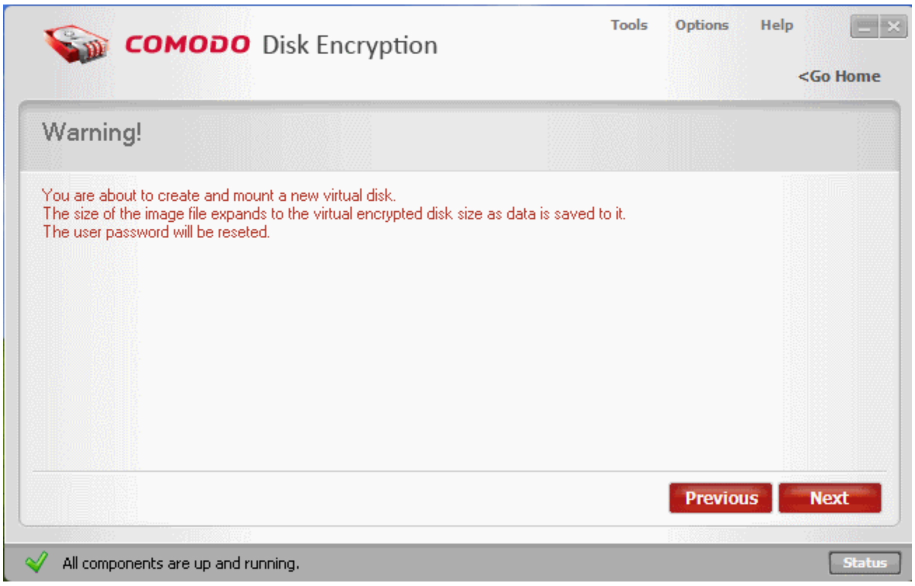
All components are up and running.

Step 5 Warning screen

Warning screen will inform you that you are about to create and mount a new virtual disk.

Note: This process will reset your user password. To create a new user password **click here**.

Click **'Next'** to continue.



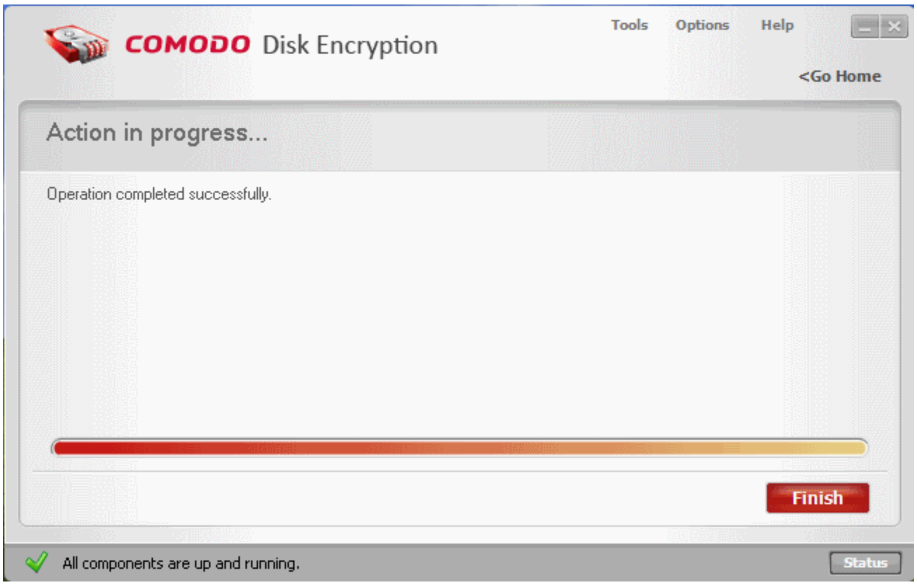
Warning!

You are about to create and mount a new virtual disk.
The size of the image file expands to the virtual encrypted disk size as data is saved to it.
The user password will be reseted.

All components are up and running.

Step 6 The operation progress

The application starts to create and mount the new virtual disk . This may take some time depending on the size of your disk. Do not power-off the system till the process is completed. The progress is indicated at the progress bar.
Click **'Finish'** to continue.



Action in progress...

Operation completed successfully.

All components are up and running.

3.2. Mount Existing Virtual Disk

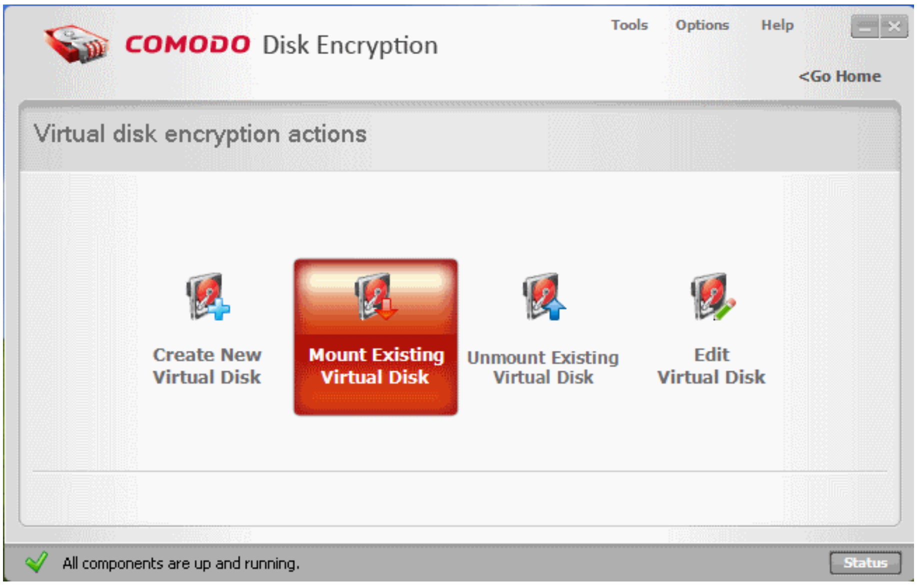
Comodo Disk Encryption allows you to mount Virtual Disks created on your computer or imported from other computers.

Mounting a Virtual Disk involves the following steps:

Step 1: **Select Mount Existing Virtual Disk**
Step 2: **Select the encrypted virtual disk image**
Step 3: **Input authentication factors**
Step 4: **Warning screen**
Step 5: **The operation progress**

Step 1 Select Mount Existing Virtual Disk

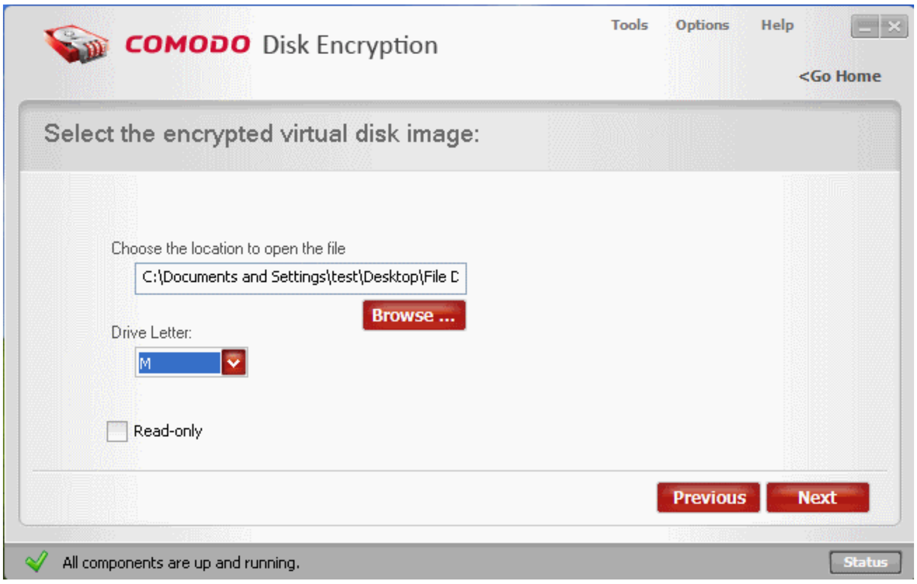
Click on **Mount Existing Virtual Disk** from Virtual disk encryption interface.



All components are up and running.

Step 2 Select the encrypted virtual disk image

- **Choose the location to open the file:** Select the path to the image file of your encrypted virtual disk.
- **Drive Letter:** The drive letter of the mounted virtual disk.
- **Read-Only:** The access rights for that virtual drive.



Select the encrypted virtual disk image:

Choose the location to open the file: C:\Documents and Settings\test\Desktop\File D

Drive Letter: M

□ Read-only

✓ All components are up and running.

- Click **'Next'** to continue.

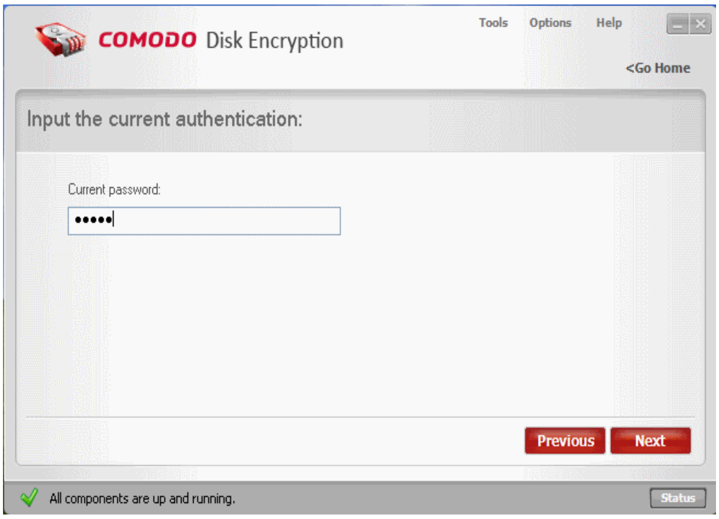
Step 3 Input authentication factors

You must type in the following credentials:

- Current master password: the current pass-phrase, the same for other virtual disks.

OR

- Current user password: the current pass-phrase, the same for other virtual disks.



Input the current authentication:

Current password: •••••

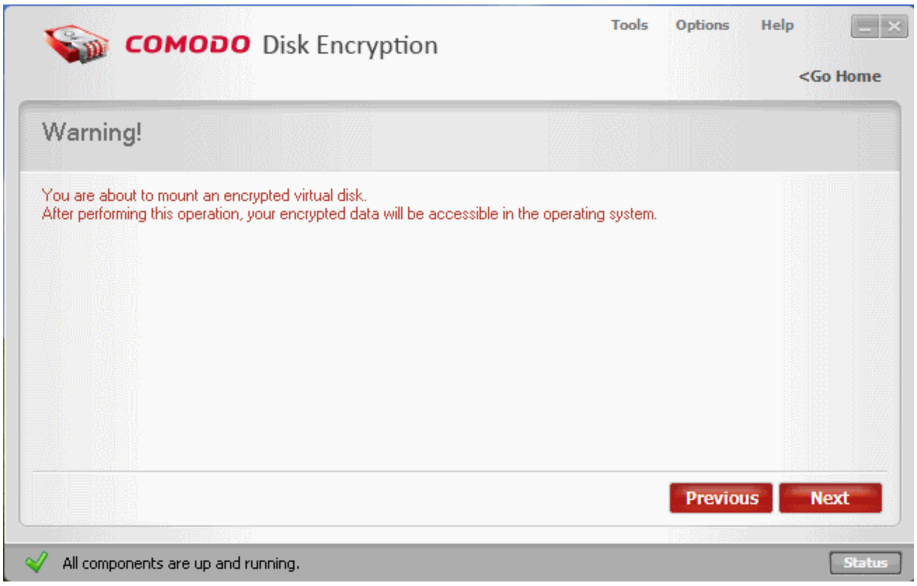
✓ All components are up and running.

Note: If you mount a virtual disk using the user password, this virtual disk will not be mounted persistently, meaning that you have to manually mount it again after system restart.

Note: If you try to mount a foreign virtual disk image and you provide the correct master password of the image, you will be prompted to change that password with the master password of the host computer in order to mount it persistently.

Step 4 Warning screen

Warning screen will inform you that you are about to mount an encrypted virtual disk and after this operation your information will be accessible on this operating system.

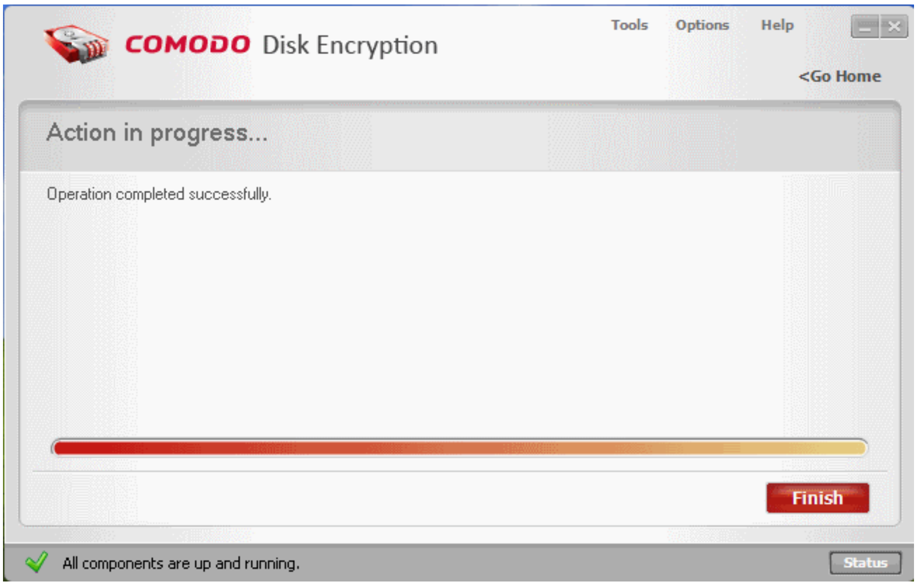


Warning!

You are about to mount an encrypted virtual disk.
After performing this operation, your encrypted data will be accessible in the operating system.

Step 5 The operation progress

The application starts to mount the existing virtual disk. The progress is indicated at the progress bar.



Action in progress...

Operation completed successfully.

On completion, click **'Finish'**.

3.3. Unmount Existing Virtual Disk

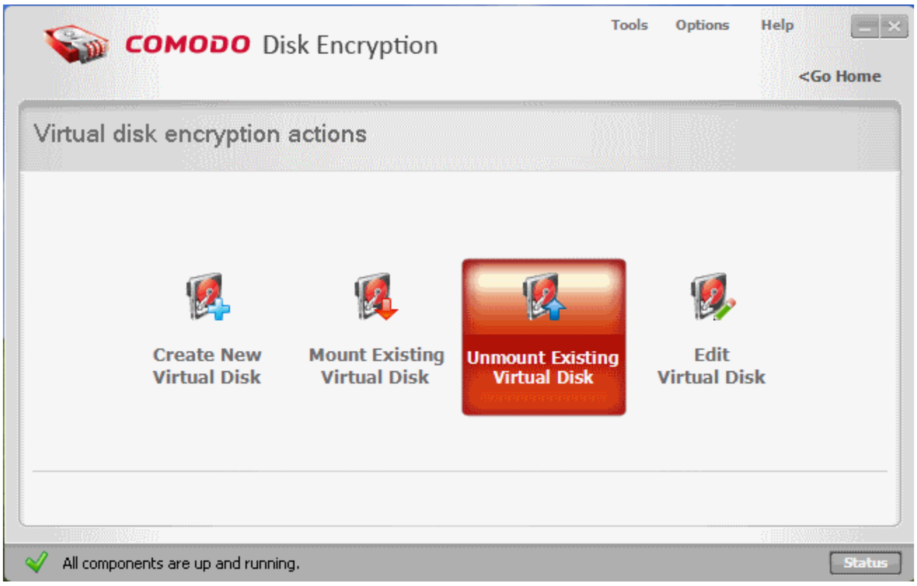
Comodo Disk Encryption allows you to unmount Virtual Disks from your computer.

Unmounting a Virtual Disk involves the following steps:

Step 1: **Select Unmount Existing Virtual Disk**
Step 2: **Choose the virtual disk to be unmouted**
Step 3: **Warning screen**
Step 4: **The operation progress**

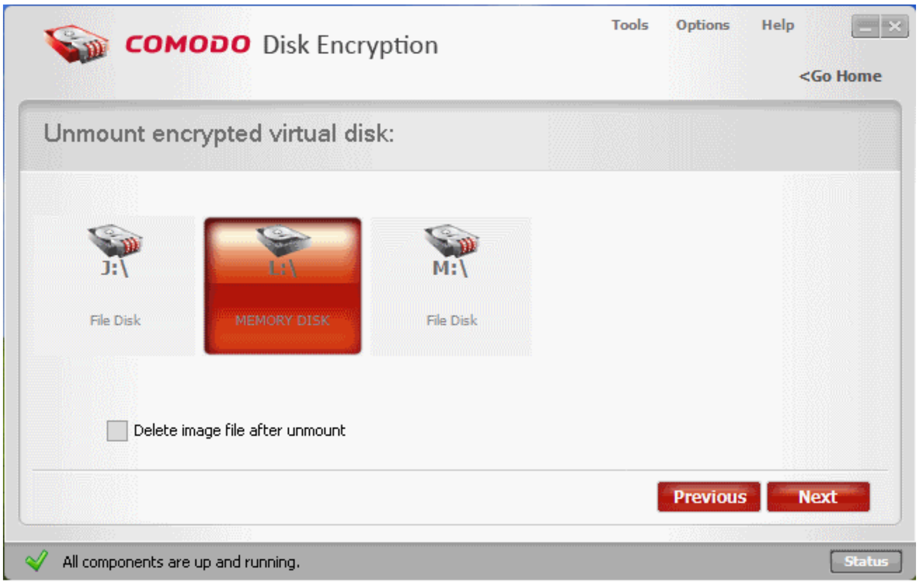
Step 1 Select Unmount Existing Virtual Disk

Click on **Unmount Existing Virtual Disk** from Virtual disk encryption interface.


COMODO Disk Encryption
Tools
Options
Help
<Go Home
Virtual disk encryption actions
Create New Virtual Disk
Mount Existing Virtual Disk
Unmount Existing Virtual Disk
Edit Virtual Disk
All components are up and running.
Status

Step 2 Choose the virtual disk to be unmouted

Select your virtual disk that you want to unmount and click **'Next'**.



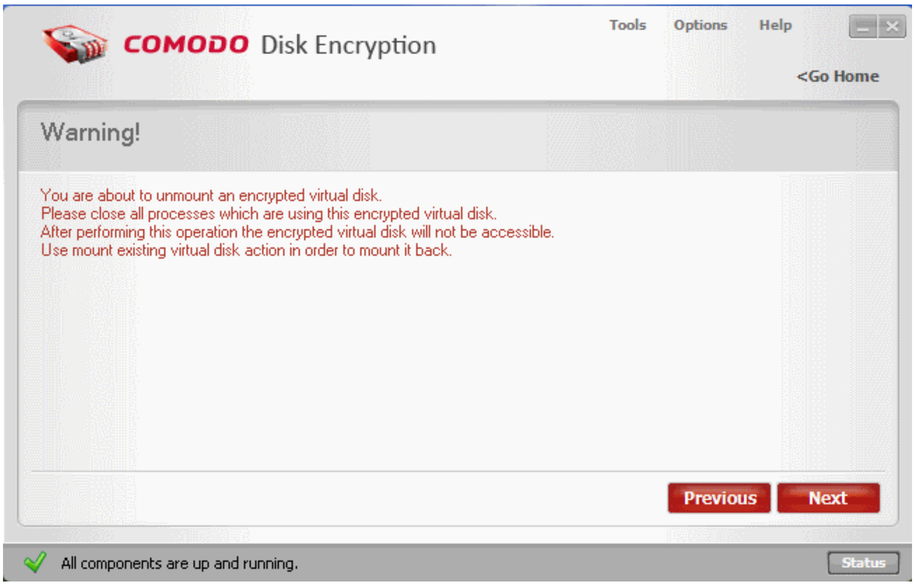
Delete image file after unmount - Deletes the virtual disk image file from your computer after unmount.

- Click **'Next'**.

Step 3 Warning screen

Warning screen inform you that you are about to unmount an encrypted virtual disk, you need to close all processes which are using this virtual disk, because all the information will not be accessible.

To continue click **'Next'**.



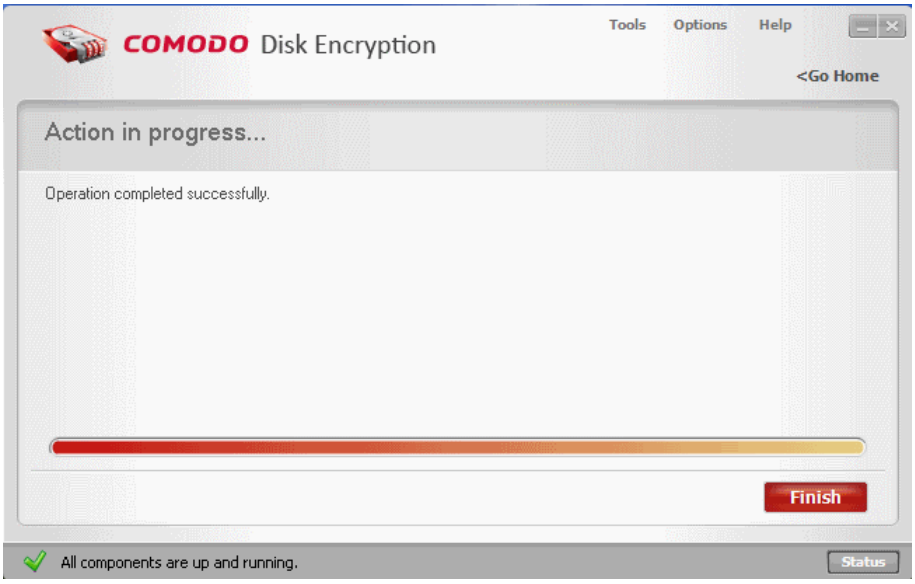
Warning!

You are about to unmount an encrypted virtual disk.
Please close all processes which are using this encrypted virtual disk.
After performing this operation the encrypted virtual disk will not be accessible.
Use mount existing virtual disk action in order to mount it back.

All components are up and running.

Step 4 The operation progress

The application starts to unmount the existing virtual disk . The progress is indicated at the progress bar.



Action in progress...

Operation completed successfully.

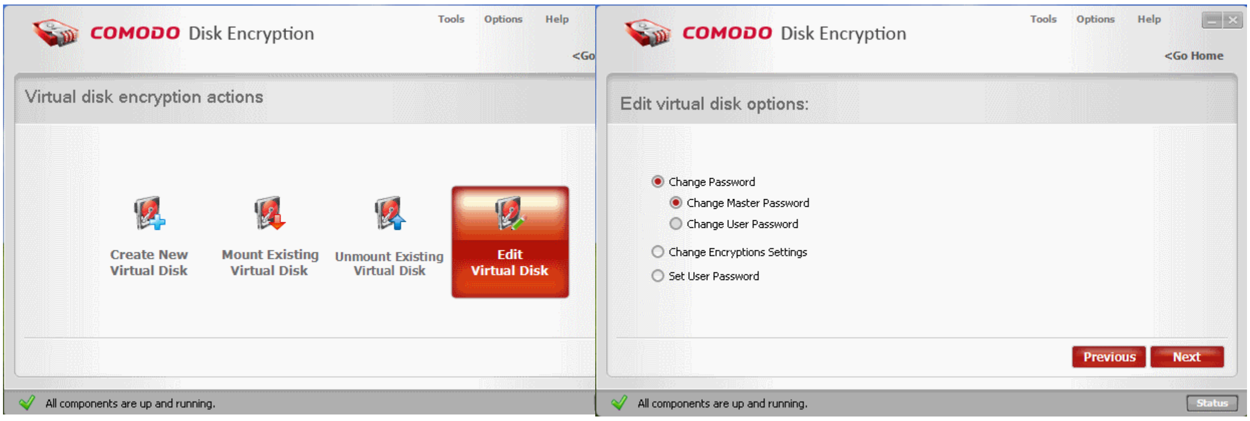
All components are up and running.

On completion, click **Finish**.

3.4. Edit Virtual Disk

Comodo Disk Encryption allows the user to manage the settings for his encrypted virtual disks.

The user can change the master password , create/change a user password and change encryption settings for a specific virtual disk.


COMODO Disk Encryption
Tools Options Help
<Go
Virtual disk encryption actions
Create New Virtual Disk
Mount Existing Virtual Disk
Unmount Existing Virtual Disk
Edit Virtual Disk
All components are up and running.
COMODO Disk Encryption
Tools Options Help
<Go Home
Edit virtual disk options:
Previous
Next
All components are up and running.
Status

● Change Password
● Change Master Password
○ Change User Password
○ Change Encryptions Settings
○ Set User Password

Click the links below for detailed descriptions:

- Change Password
  - Change Master Password
  - Change User Password
- Change Encryption Settings
- Set User Password

3.4.1. Change Password

When you create an encrypted virtual disk for the first time, you need to choose a master password. This master password enables you to access all the encrypted virtual disks from your computer and create new ones.

For your encrypted virtual disk you can create a user password to allow other users to access your confidential data. To learn how to create a user password **click here**. To understand Passwords **click here**.

Comodo Disk Encryption allow you to:

- **Change Master Password**
- **Change User Password**

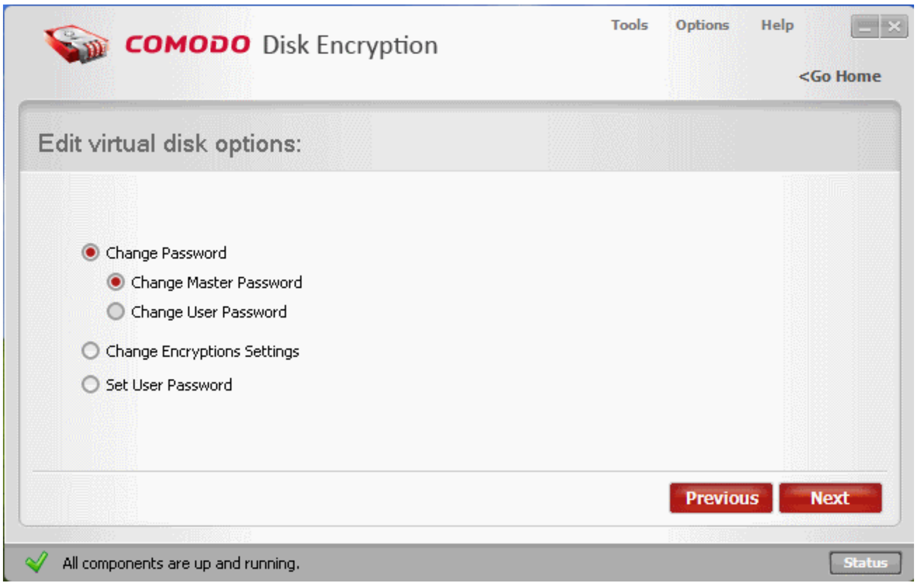
3.4.1.1. Change Master Password

With the Master Password you can encrypt/decrypt, mount/unmount a virtual disk, change his encryption settings and manage the user password.

Changing a Master Password involves the following steps:

Step 1: **Select Change Master Password**
Step 2: **Input the authentication and your new Master password**
Step 3: **Warning screen**
Step 4: **The operation progress**

Step 1 Select Change Master Password
From Edit Virtual Disk interface select **Change Master Password** and click **'Next'.**



Edit virtual disk options:

- ● Change Password
  - ● Change Master Password
  - ○ Change User Password
- ○ Change Encryptions Settings
- ○ Set User Password

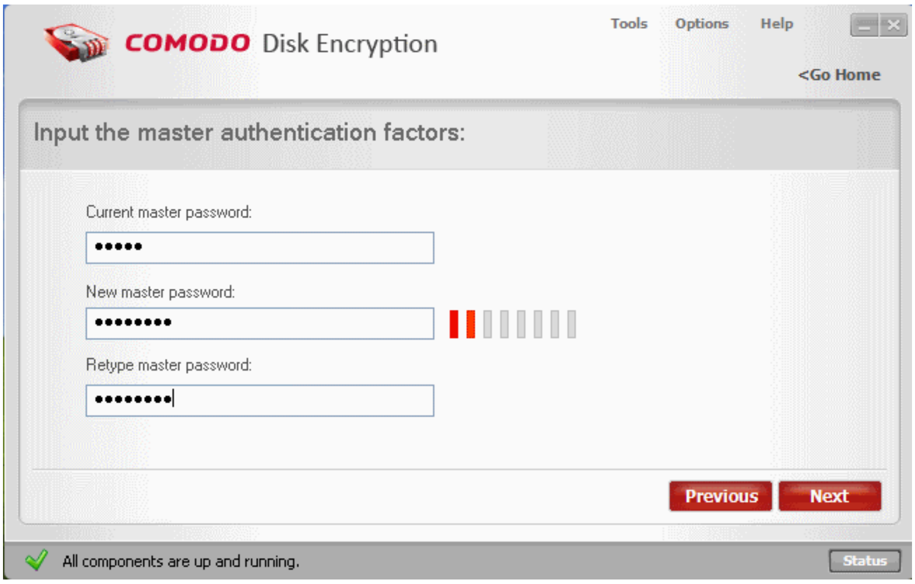
Step 2 Input the authentication and your new Master password

You must type in the following credentials:

- Current master password: the current pass-phrase, the same for other encrypted virtual disks.
- New master password: the new pass-phrase.

For more information about authentication **click here**.

To understand Passwords **click here**.



Input the master authentication factors:

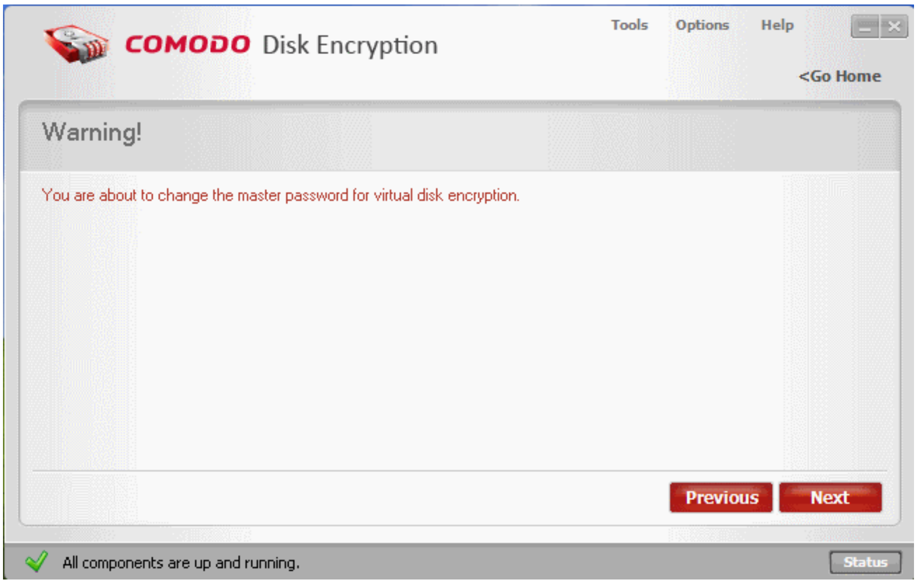
Current master password: •••••

New master password: ••••••••

Retype master password: ••••••••

Step 3 Warning screen

Warning screen inform you that you are about to change the authentication for virtual disk encryption. Click **'Next'** to continue.



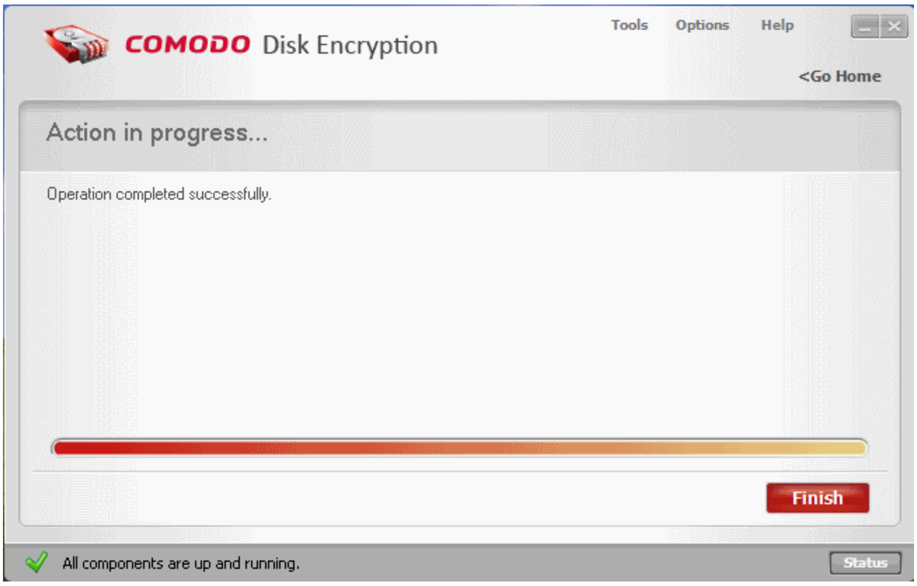
Warning!

You are about to change the master password for virtual disk encryption.

All components are up and running.

Step 4 The operation progress

The application starts changing the master password for your encrypted virtual disks. Do not power-off the system till the process is completed. The changing progress is indicated at the progress bar.



Action in progress...

Operation completed successfully.

All components are up and running.

On completion, click **'Finish'**.

3.4.1.2. Change User Password

The User Password provide limited access to your secure information.

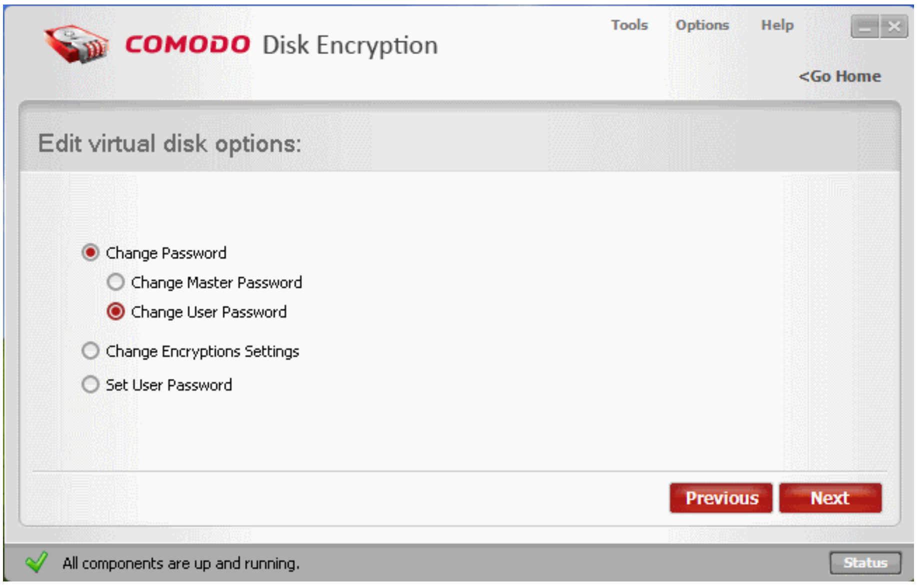
For more information about Passwords **click here**.

Changing a User Password for your virtual disks involves the following steps:

Step 1: **Select Change User Password**
Step 2: **Input the authentication and your new User password**
Step 3: **Warning screen**
Step 4: **The operation progress**

Step 1 Select Change User Password

From Edit Virtual Disk interface select **Change User Password** and click **'Next'.**



● Change Password
○ Change Master Password
● Change User Password
○ Change Encryptions Settings
○ Set User Password

All components are up and running.

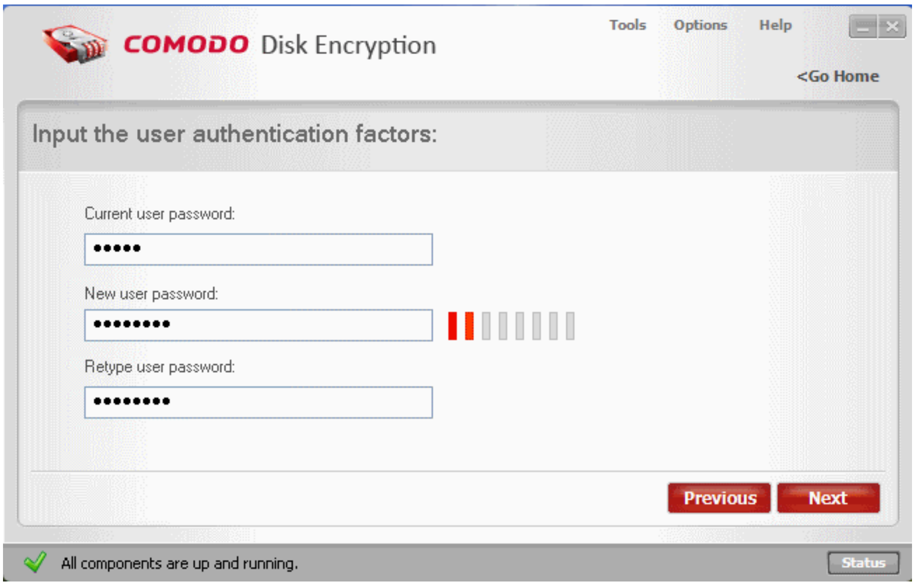
Step 2 Input the authentication and your new User password

You must type in the following credentials:

- Current user password: the current pass-phrase, the same for other encrypted virtual disks.
- New user password: the new pass-phrase.

For more information about authentication **click here**.

To understand Passwords **click here**.



Current user password: •••••

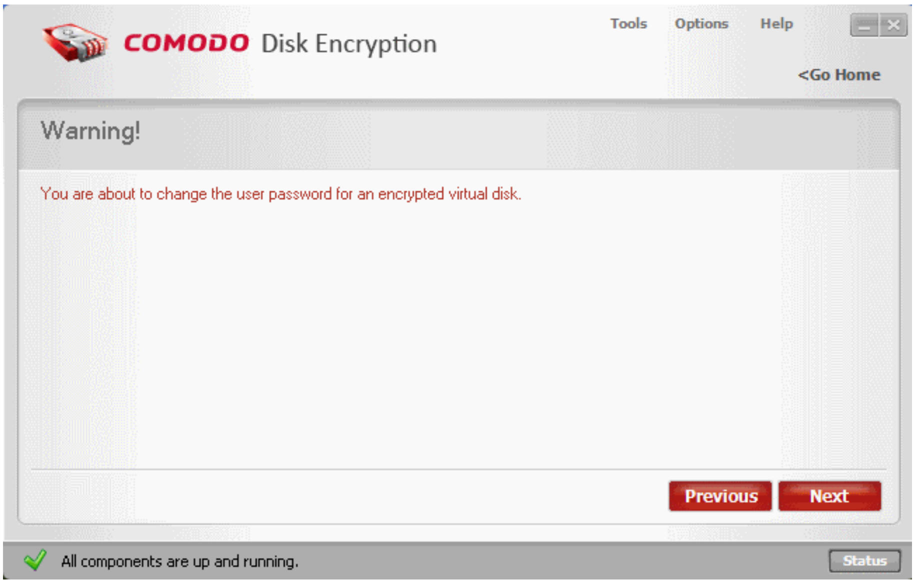
New user password: ••••••••

Retype user password: ••••••••

All components are up and running.

Step 3 Warning screen

Warning screen will inform you that you are about to change the authentication for virtual disk encryption. Click **'Next'** to continue.



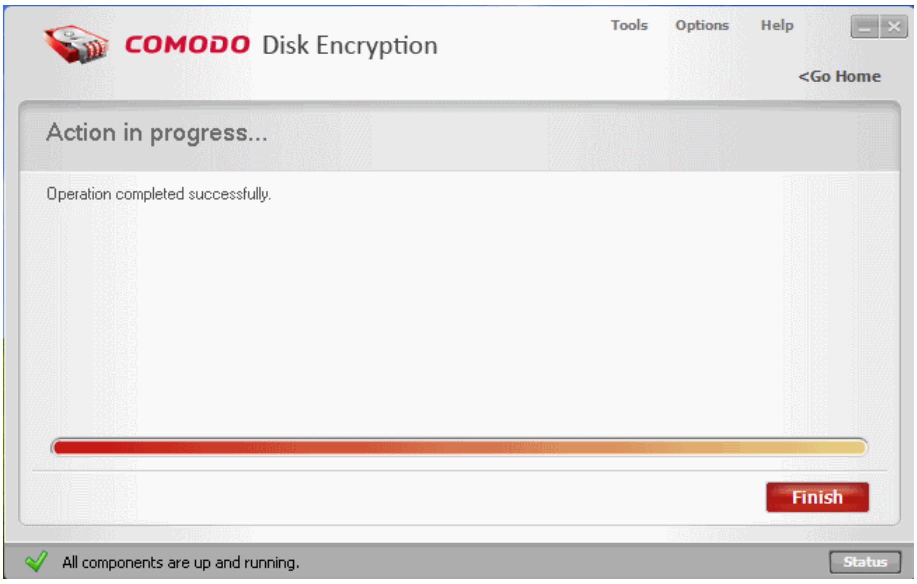
Warning!

You are about to change the user password for an encrypted virtual disk.

All components are up and running.

Step 4 The operation progress

The application starts changing the user password for your virtual encrypted disks. Do not power-off the system till the process is completed. The progress is indicated at the progress bar.



Action in progress...

Operation completed successfully.

All components are up and running.

On completion, click **'Finish'**.

3.4.2. Change Encryption Settings

Comodo Disk Encryption ships with four encryption levels

- **High Security:** Cipher algorithm AES, Cipher mode OFB
- **Medium Security:** Cipher algorithm Twofish, Cipher mode CBC
- **Low Security:** Cipher algorithm Cast6, Cipher mode NONE
- **Custom:** Select a combination from an Cipher algorithm and Block Cipher Mode

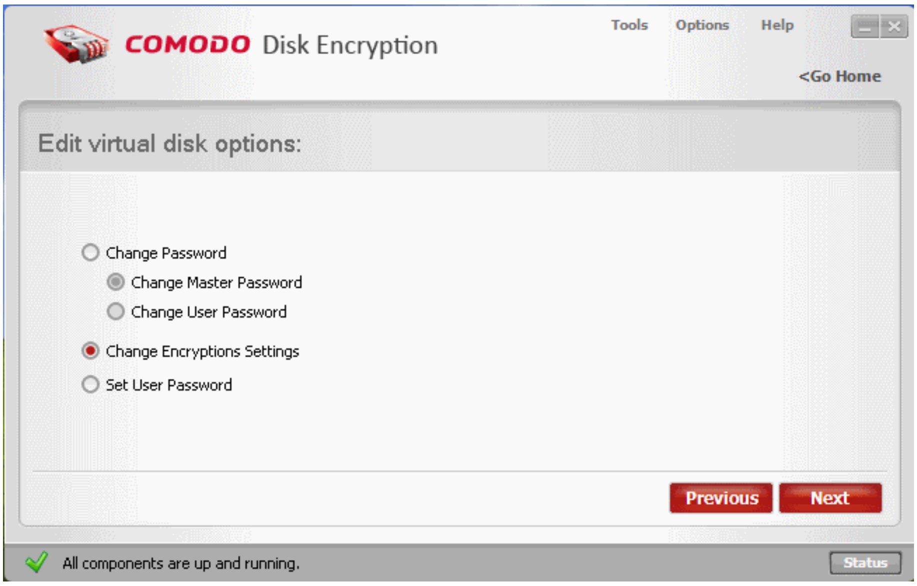
Comodo Disk Encryption provides you with selection of **Cipher Algorithms** and **Block Cipher Modes.** Each has its own advantages in terms of performance and strength. The slider allows you to quickly switch between Comodo suggested combinations of algorithm and cipher mode. You can, however, create your own combination by directly modifying the two drop down menus. For more information about algorithms click here.

Changing Encryption settings of one of your virtual disks involves the following steps:

Step 1: Select Change Encryption Settings
Step 2: Select the encrypted disk
Step 3: Input the authentication
Step 4: Select the new encryption settings
Step 5: Warning screen
Step 6: The operation progress

Step 1 Select Change Encryption Settings

From Edit Virtual Disk interface select **Change Encryption Settings** and click **'Next'.**



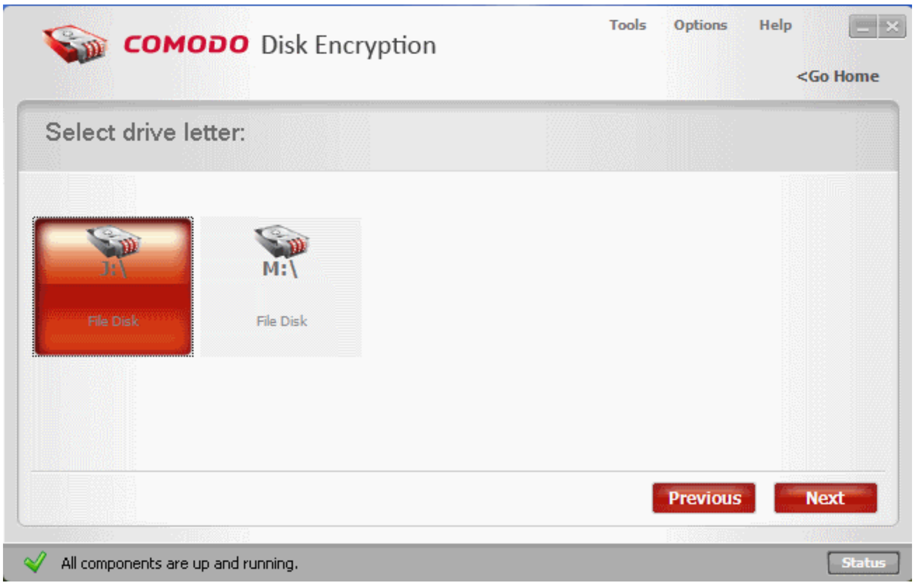
Edit virtual disk options:

○ Change Password
  ● Change Master Password
  ○ Change User Password
● Change Encryptions Settings
○ Set User Password

✓ All components are up and running.

Step 2 Select the encrypted disk

Next, select the encrypted virtual disk for which you want to change the encryption settings and click **'Next'** to continue.



Select drive letter:

✓ All components are up and running.

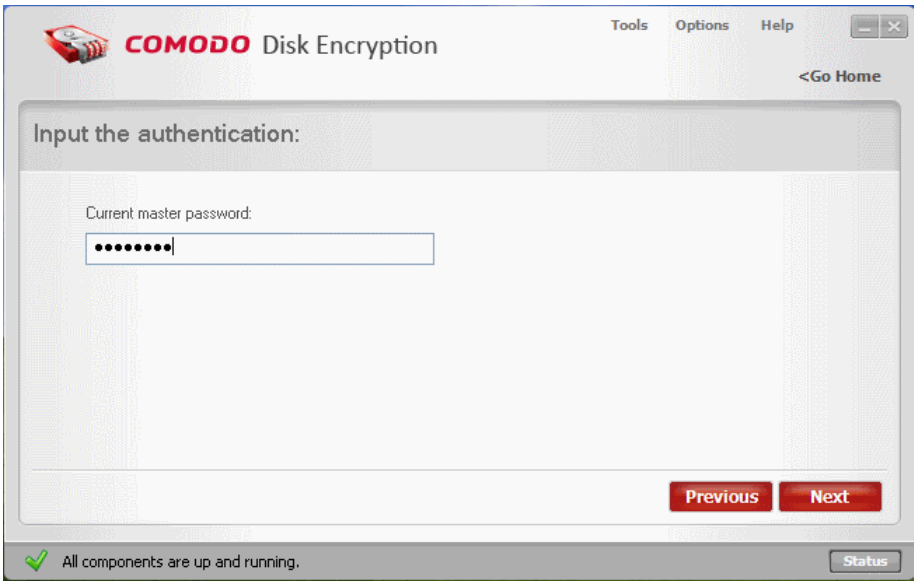
Step 3 Input the authentication

Enter the following credentials:

- Current master password: the current pass-phrase, the same for other encrypted virtual disks.

For more information about authentication click here.

To understand Passwords click here.

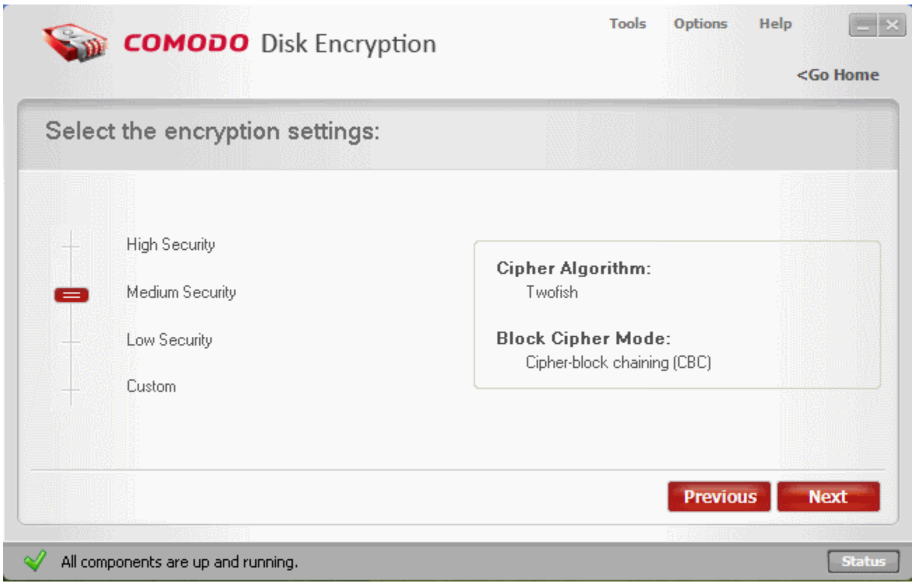


Input the authentication:

Current master password: ••••••••

Step 4 Select the new encryption settings

Select your new encryption level and click **'Next'**. For more information about algorithms **click here**.



Select the encryption settings:

- High Security
- Medium Security
- Low Security
- Custom

Cipher Algorithm:
Twofish

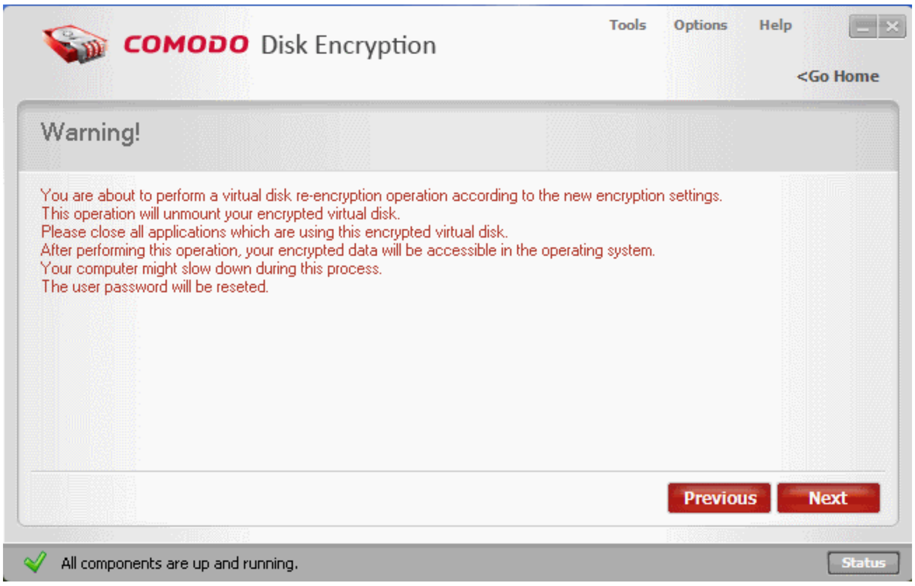
Block Cipher Mode:
Cipher-block chaining (CBC)

Step 5 Warning screen

Warning screen will inform you that you are about to perform a virtual disk re-encryption according with your new settings and your computer might slow down during this process.

Note: This process will reset your user password. To create a new user password **click here**.

Click **'Next'** to continue.



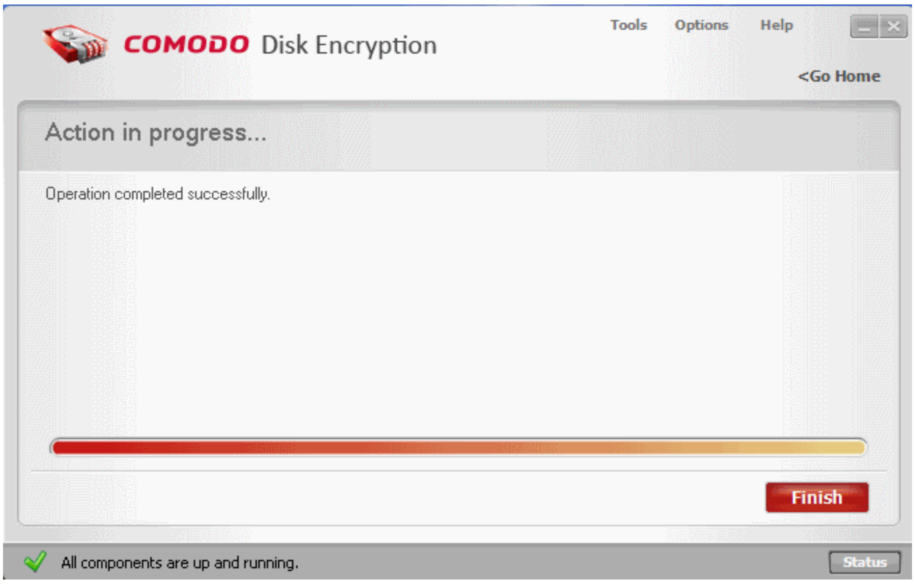
Warning!

You are about to perform a virtual disk re-encryption operation according to the new encryption settings.
This operation will unmount your encrypted virtual disk.
Please close all applications which are using this encrypted virtual disk.
After performing this operation, your encrypted data will be accessible in the operating system.
Your computer might slow down during this process.
The user password will be reseted.

All components are up and running.

Step 6 The operation progress

The application starts re-encrypting the selected virtual drive. This may take some time depending on the size of your virtual disk. Do not power-off the system till the process is completed. The re-encrypting progress is indicated at the progress bar.



Action in progress...

Operation completed successfully.

All components are up and running.

On completion, click **'Finish'**.

3.4.3. Set User Password

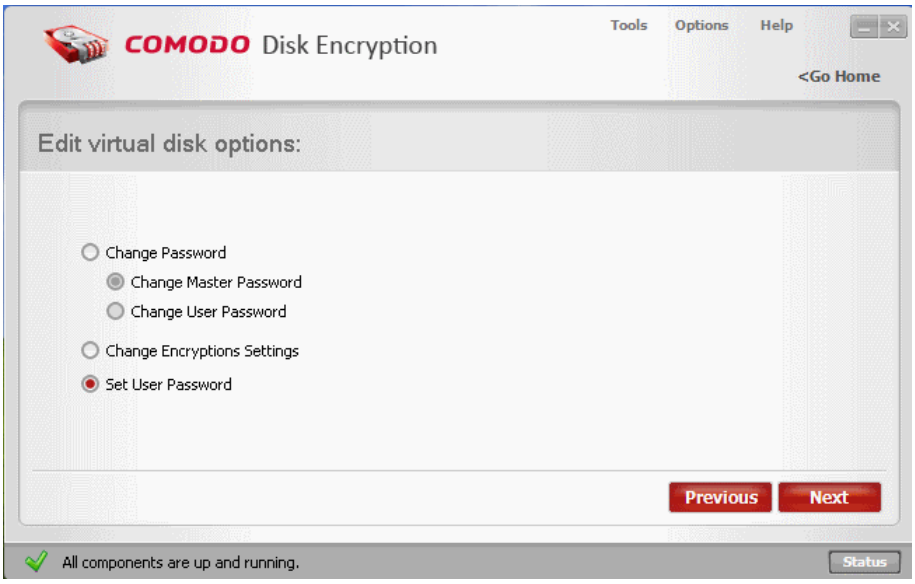
For your encrypted virtual disks you can create a user password to allow other users to have limited access.

Creating a User Password for tour virtual disks involves the following steps:

Step 1: **Select Set User Password**
Step 2: **Input the authentication and your new User password**
Step 3: **Warning screen**
Step 4: **The operation progress**

Step 1 Select Set User Password

From Edit Virtual Disk interface select **Set User Password** and click **'Next'.**



○ Change Password

● Change Master Password

○ Change User Password

○ Change Encryptions Settings

● Set User Password

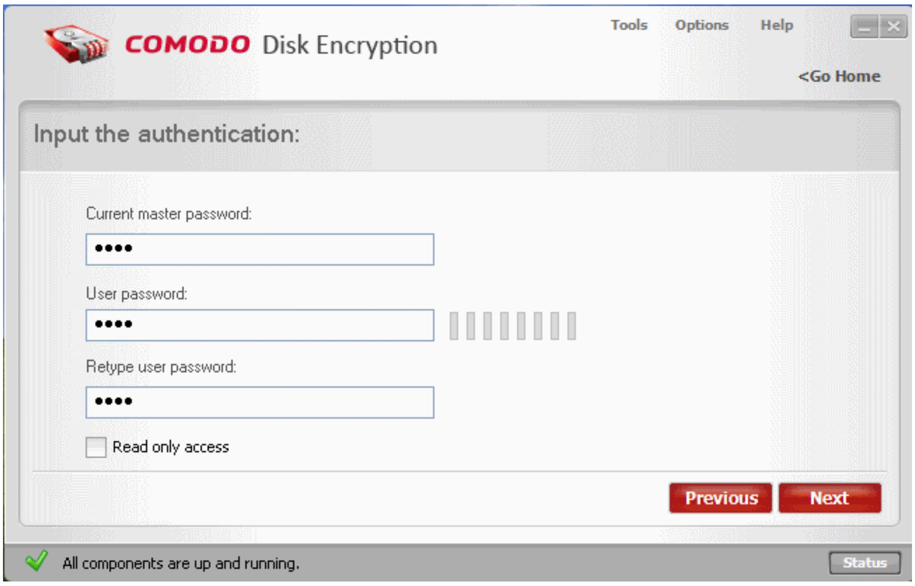
Step 2 Input the authentication and your new User password

Enter the following credentials:

- Current Master password: the current pass-phrase, the same for other encrypted virtual disks.
- New user password: the new pass-phrase.

For more information about authentication **click here**.

To understand Passwords **click here**.



Current master password: ••••

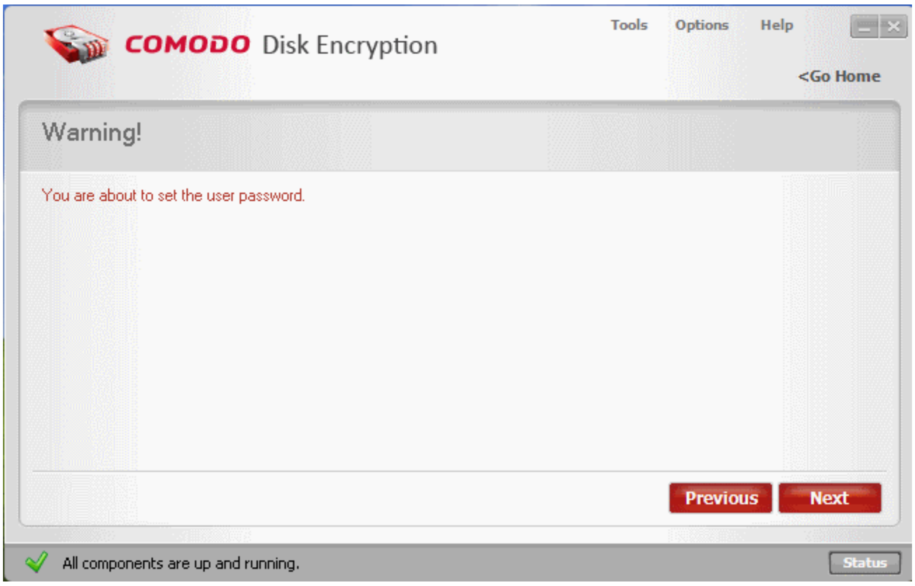
User password: ••••

Retype user password: ••••

□ Read only access

Step 3 Warning screen

The warning screen will inform you that you are about to change the authentication for disk encryption. Click **'Next'** to continue.



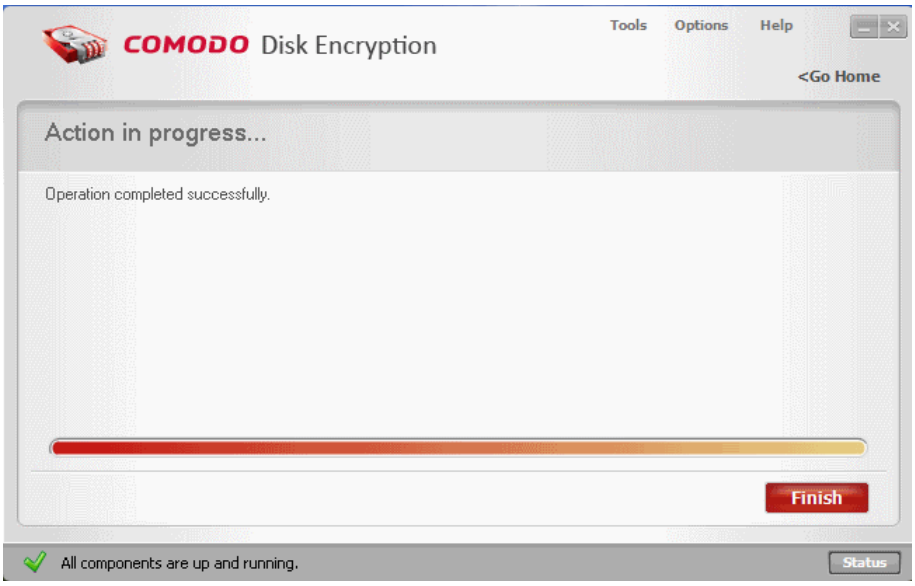
Warning!

You are about to set the user password.

All components are up and running.

Step 4 The operation progress

The application starts creating the user password for your encrypted virtual disks. Do not power-off the system till the process is completed. The changing progress is indicated at the progress bar.



Action in progress...

Operation completed successfully.

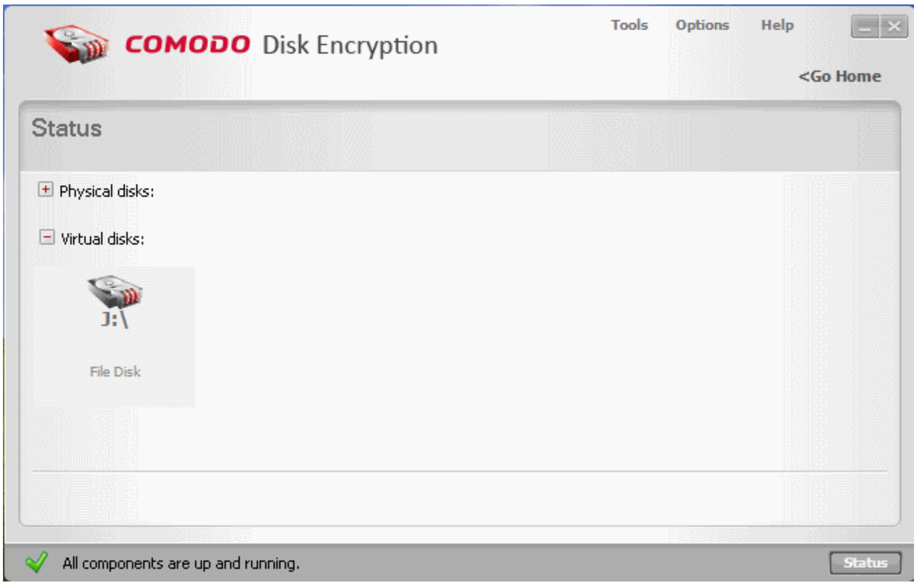
All components are up and running.

On completion, click **'Finish'**.

3.5. Status

Status interface provide a visual representation of your virtual disks.

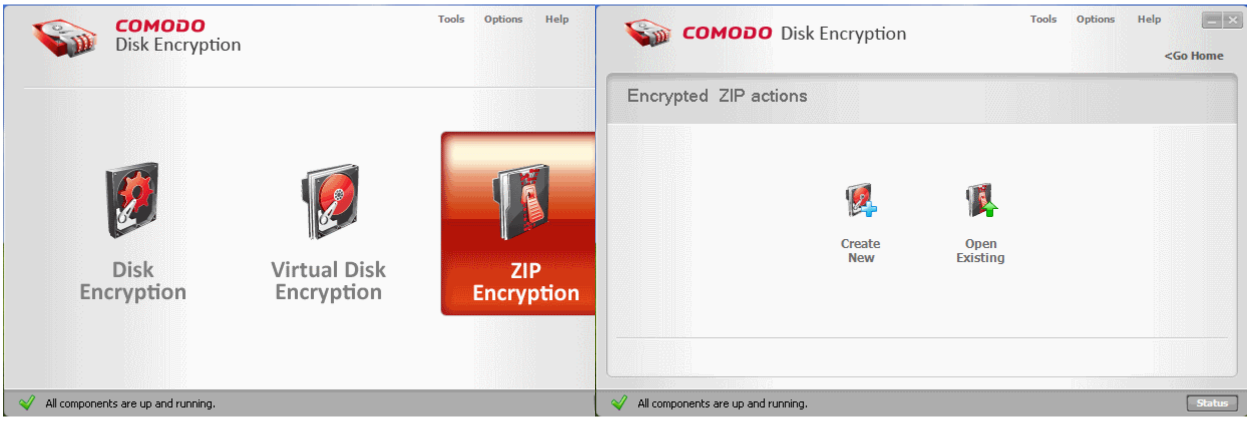
In a moment you can find out what virtual disks are mounted or not. To access the interface click on the **Status** button from the **Status Bar**.



4.ZIP Encryption

You can create encrypted ZIP containers where you can save several files and folders with the encryption level of your choice.

To access this feature click on the **ZIP Encryption** button on the Main Interface.



From this interface, you can:

- **Create New Zip Container**
- **Open existing Zip Container**

4.1.Create New

You can protect specific files and folders including them in a secure ZIP encrypted container.

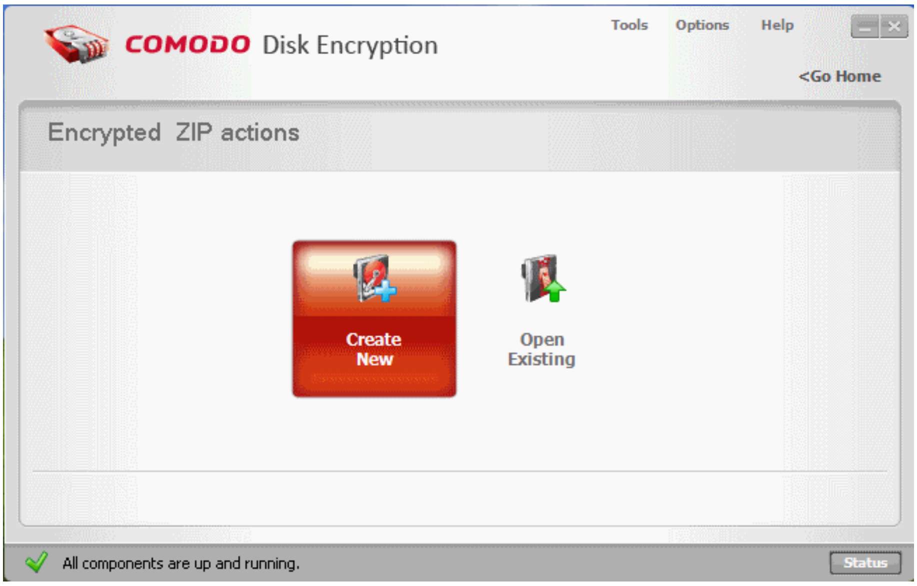
Creating a ZIP encryption involves the following steps:

Step 1: **Select Create New**
Step 2: **Add files and folders**
Step 3: **Input the authentication**
Step 4: **Encryption settings**

Step 5: **ZIP destination**
Step 6: **Warning screen**
Step 7: **The operation progress**

Step 1 Select Create New

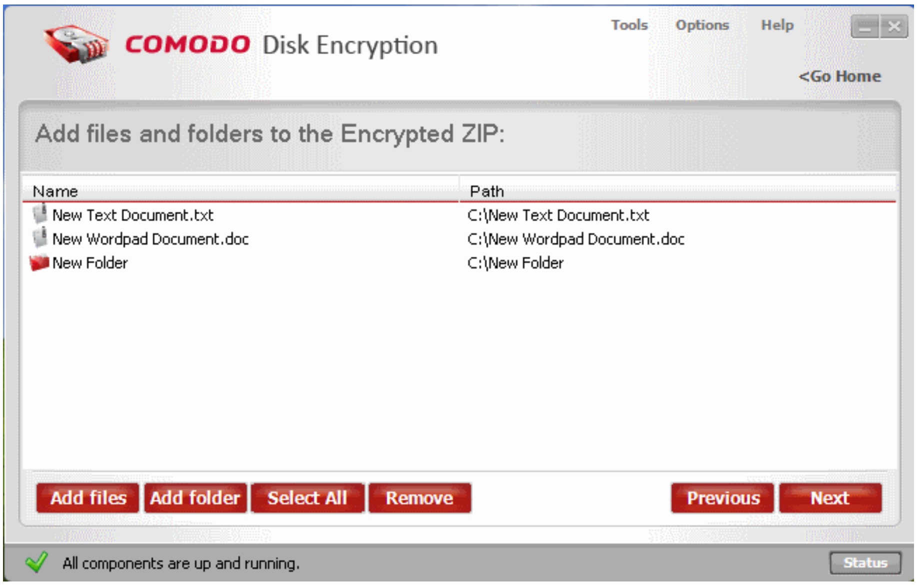
From Encrypted ZIP interface click on **'Create New'.**



Step 2 Add files and folders

Manage your file/folders that you want to include in the ZIP container using **Add files, Add folders** and **Remove.** Click **'Next'** to continue.

Add files - add files for the new encrypted ZIP
Add folder - add folders for the new encrypted ZIP
Remove - remove file/folder from the list of the new encrypted ZIP



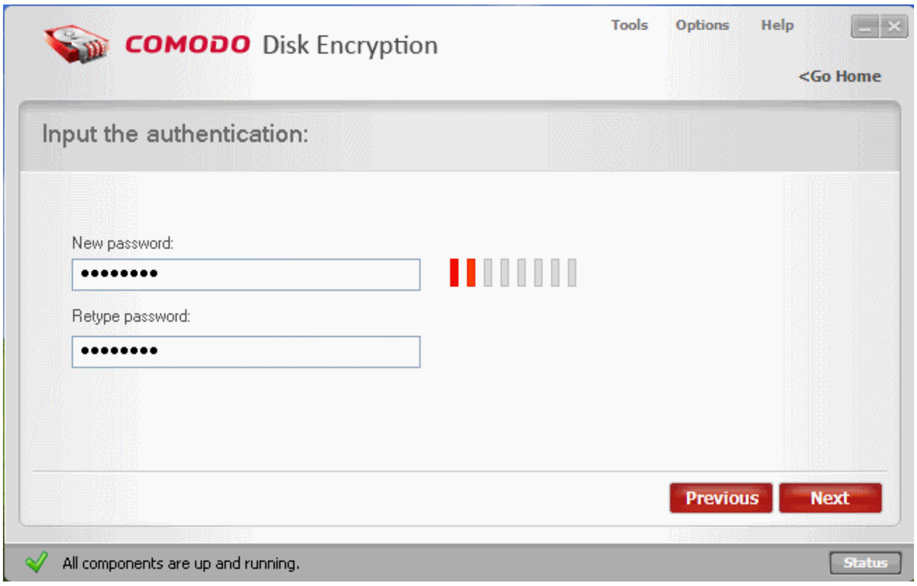
Name	Path
New Text Document.txt	C:\New Text Document.txt
New Wordpad Document.doc	C:\New Wordpad Document.doc
New Folder	C:\New Folder

Step 3 Input the authentication

You must type in the following credentials:

- New specific password: the new pass-phrase.

To understand Passwords **click here**.



Input the authentication:

New password: ●●●●●●●●●

Retype password: ●●●●●●●●●

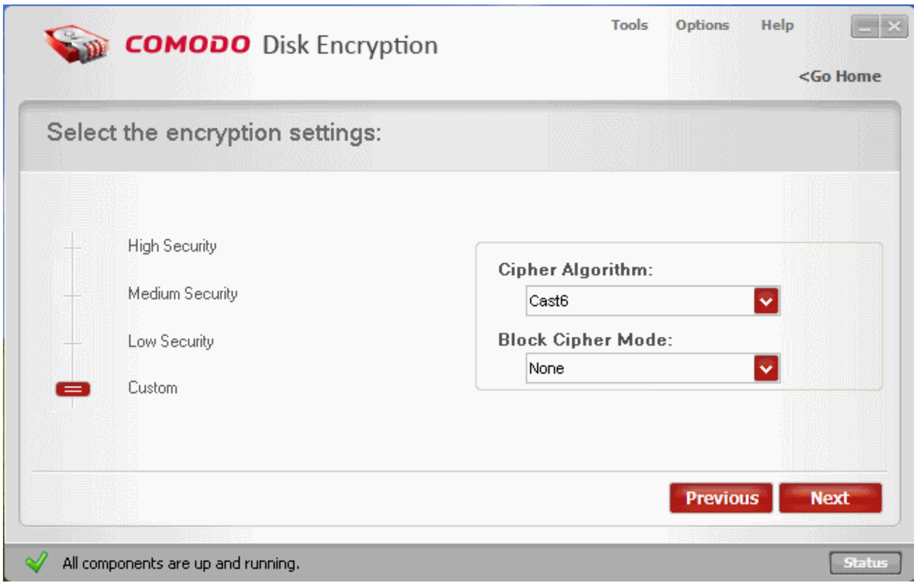
All components are up and running.

Step 4 Encryption settings

The encryption level:

- **High Security:** Cipher algorithm AES, Cipher mode OFB
- **Medium Security:** Cipher algorithm Twofish, Cipher mode CBC
- **Low Security:** Cipher algorithm Cast6, Cipher mode NONE
- **Custom:** Select a combination from an Cipher algorithm and Block Cipher Mode

Select **The encryption level** you wish to apply to the selected drive. Comodo Disk Encryption provides you with selection of **Cipher Algorithms** and **Block Cipher Modes**. Each has its own advantages in terms of performance and strength. The slider allows you to quickly switch between Comodo suggested combinations of algorithm and cipher mode. You can, however, create your own combination by directly modifying the two drop down menus.For more information about algorithms **click here**.



Select the encryption settings:

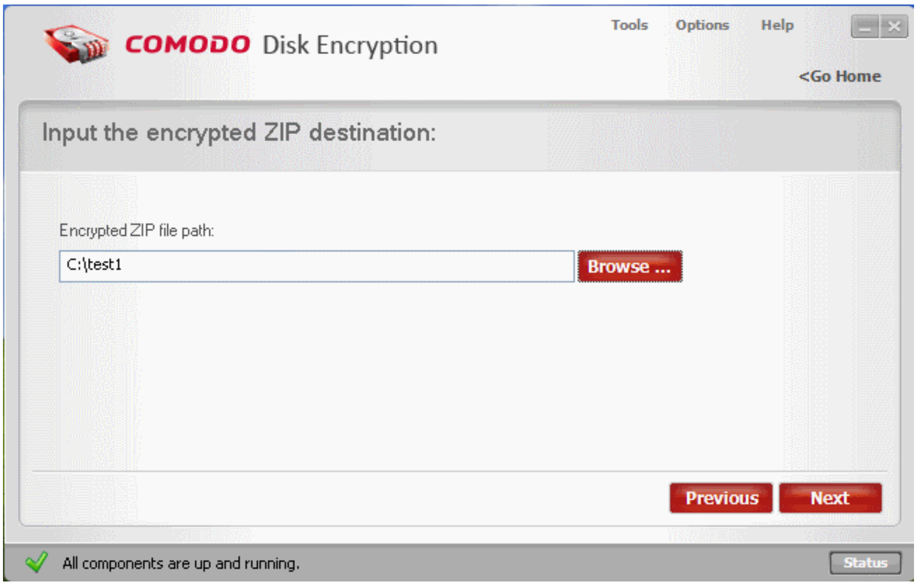
Cipher Algorithm: Cast6

Block Cipher Mode: None

All components are up and running.

Step 5 ZIP destination

Select where you want to save your Encrypted ZIP on your computer.



Input the encrypted ZIP destination:

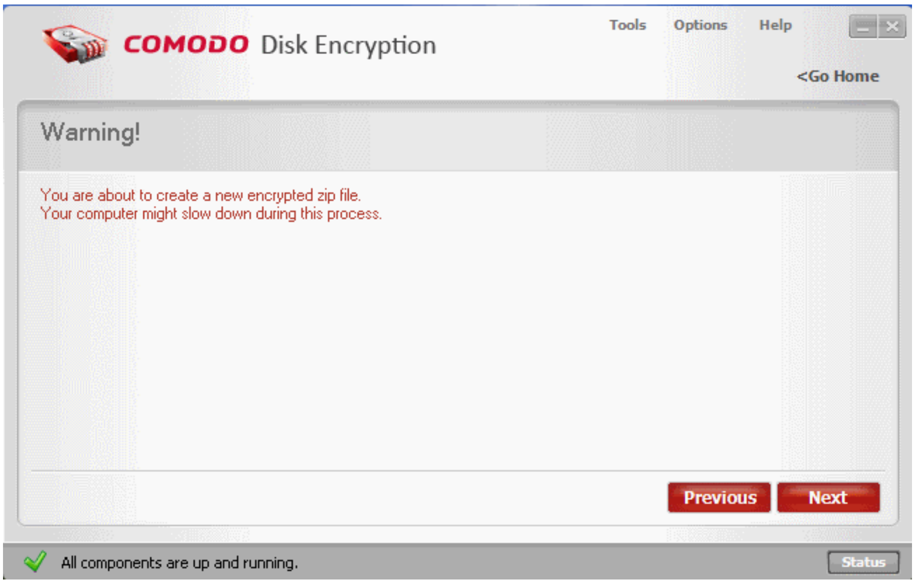
Encrypted ZIP file path: C:\test1

All components are up and running.

Click **'Next'** to continue.

Step 6 Warning screen

The warning screen will inform you that you are about to create a new encrypted ZIP file.



Warning!

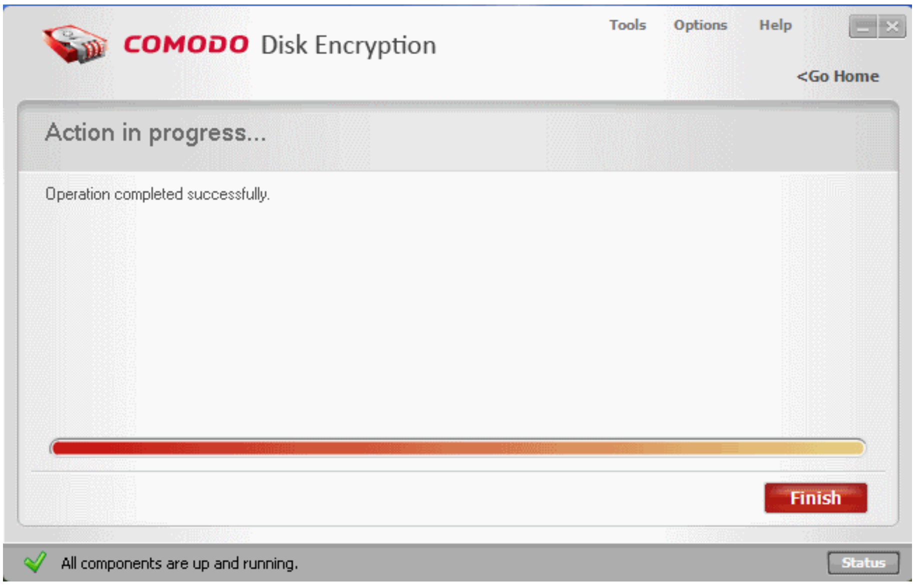
You are about to create a new encrypted zip file.
Your computer might slow down during this process.

All components are up and running.

Click **'Next'** to continue.

Step 7 The operation progress

The application starts creating the encrypted ZIP file. Do not power-off the system till the process is completed. The progress is indicated at the progress bar.



Operation completed successfully.

On completion, click **'Finish'**.

4.2. Open Existing

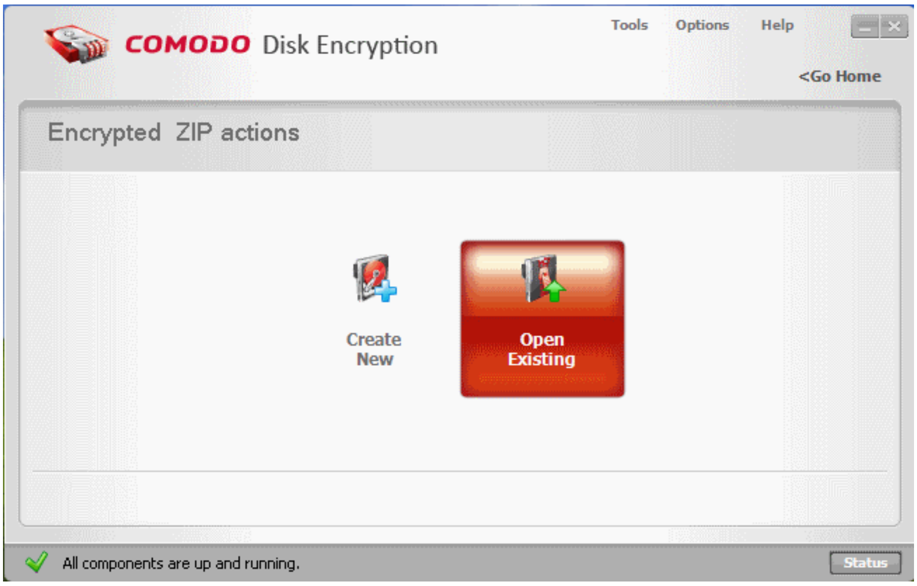
The files that are protected in the secure ZIP encrypted container can be accessed at any time by providing the correct authentication credentials.

Opening a ZIP encryption involves the following steps:

Step 1: **Select Open Existing**
Step 2: **Input the authentication and make your settings**
Step 3: **The content of encrypted ZIP (files and folders)**
Step 4: **Warning screen**
Step 5: **The operation progress**

Step 1 Select Open Existing

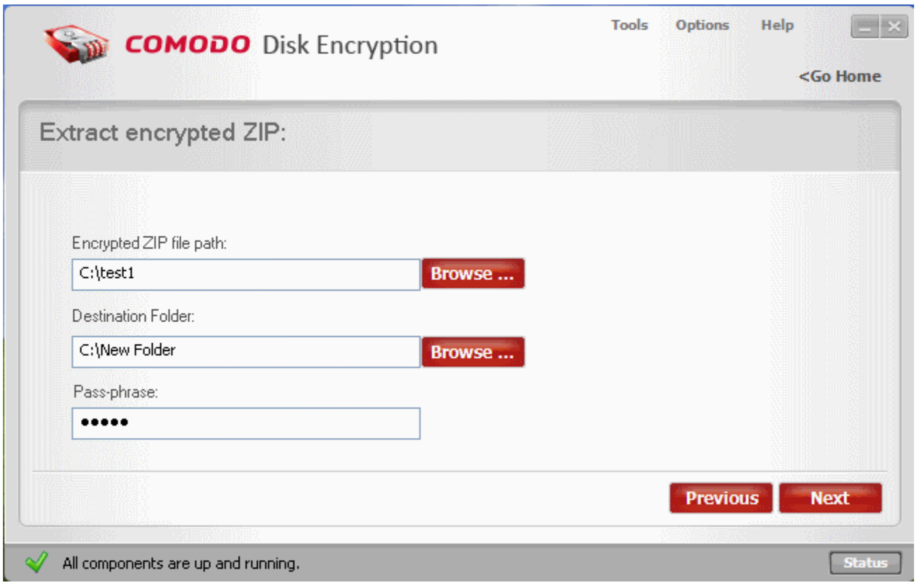
From Encrypted ZIP interface click on **Open Existing.**



Step 2 Input the authentication and make your settings

Select your ZIP file, select where you want to extract the files, input your the specific password for the encrypted Zip and click **'Next'** to continue.

File path: the location of encrypted ZIP
Destination folder: location where to extract encrypted ZIP
Pass-phrase: the pass-phrase specific to encrypted ZIP



Extract encrypted ZIP:

Encrypted ZIP file path: C:\test1

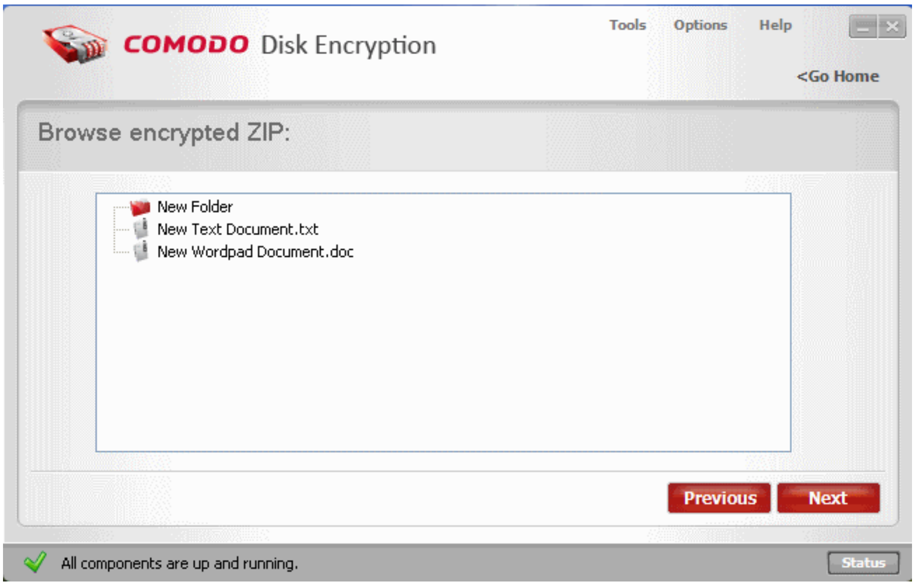
Destination Folder: C:\New Folder

Pass-phrase: •••••

All components are up and running.

Step 3 The content of encrypted ZIP (files and folders)

From this interface you can browse the encrypted ZIP file. Click **Next** to continue.



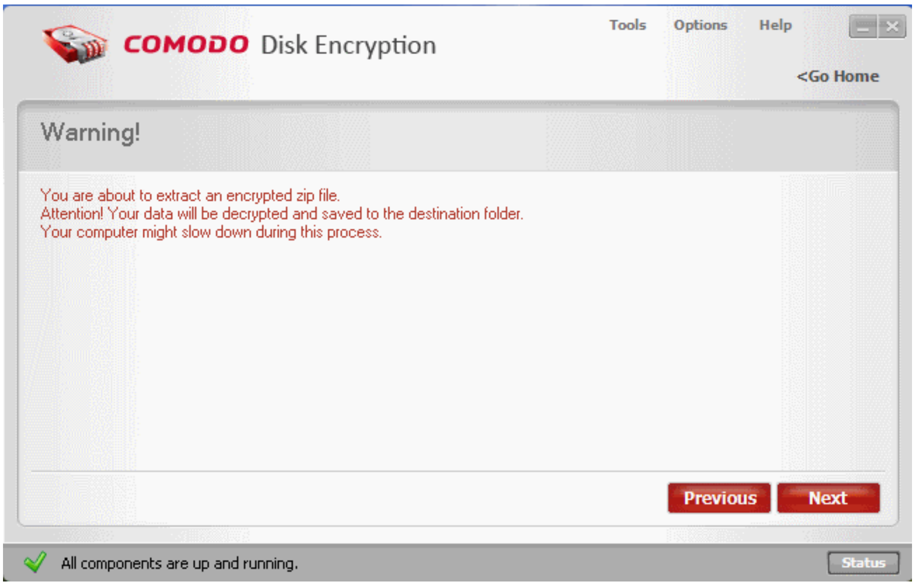
Browse encrypted ZIP:

- New Folder
- New Text Document.txt
- New Wordpad Document.doc

All components are up and running.

Step 4 Warning screen

The warning screen will inform that you are about to extract the encrypted file in the destination folder and your data will be decrypted. Click **'Next'** to continue.

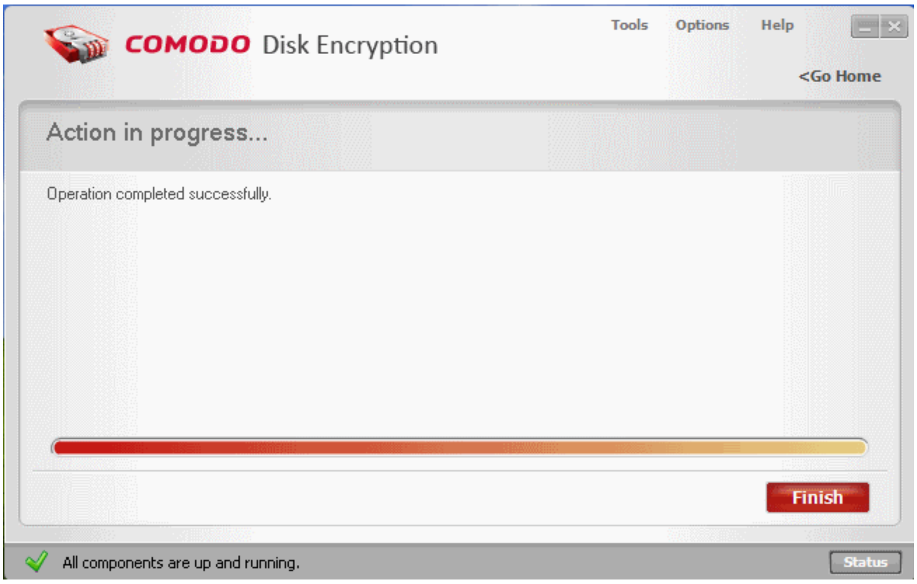


Warning!

You are about to extract an encrypted zip file.
Attention! Your data will be decrypted and saved to the destination folder.
Your computer might slow down during this process.

Step 5 The operation progress

The application starts decrypting your ZIP file. Do not power-off the system till the process is completed. The progress is indicated at the progress bar.



Action in progress...

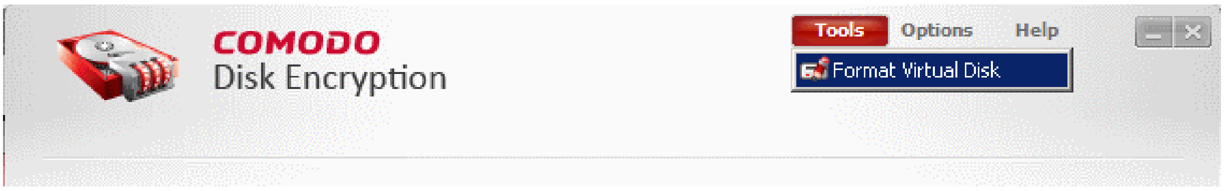
Operation completed successfully.

On completion, click **'Finish'**.

5. Tools

The **Tools** menu in Comodo Disk Encryption allows you to perform additional tasks which are related to Comodo Disk Encryption.

These **Tools** menu options can be accessed by clicking on the **Tools** in the menu bar.



Click on the following link for detailed description on the option available under Tools.

- **Format Virtual Disk**

5.1. Format Virtual Disk

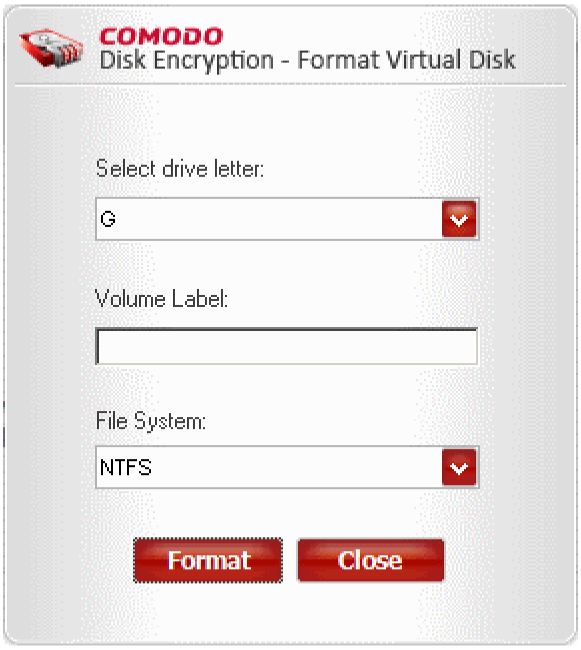
Once a blank virtual disk is mounted, it needs to be formatted first to the required file system in order to store Folders/Files and to perform other disk operations. Also formatting a disk stored with unnecessary files enables complete wiping of the files so that the files are rendered unrecoverable by using any third party file recovery software.

The 'Format Virtual Disk' option under Tools menu enables you to format a pre-mounted virtual disk, with the options of assigning a new Volume Label (name given to a specific drive), and selecting the file system for the mounted virtual disk.

Note: You should have at least one virtual disk mounted with full read/write access, to format. Refer to **Virtual Disk Encryption** > **Create New Virtual Disk** for more details on creating a Virtual Disk.

To format a virtual disk

1. Click Tools > Format Virtual Disk. The Format Wizard will start.

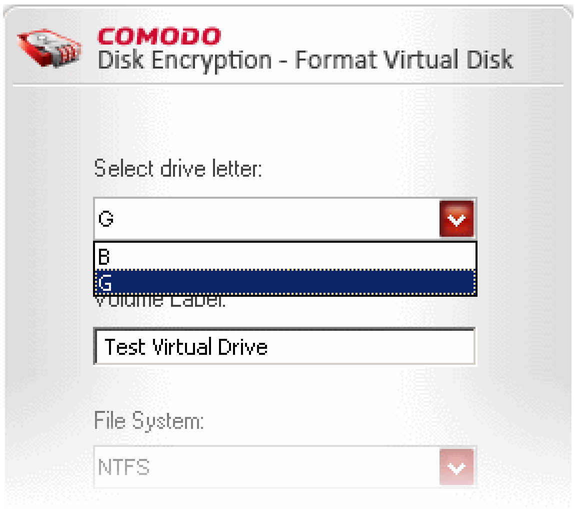


Select drive letter: G

Volume Label:

File System: NTFS

2. Select the virtual drive to be formatted from the Select drive letter: drop-down menu.

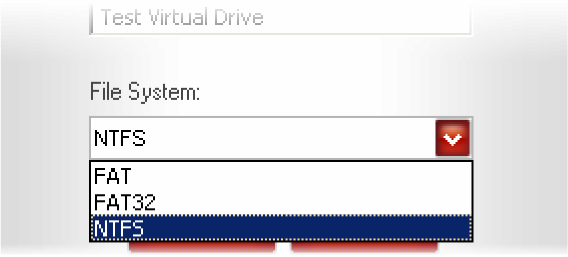


Select drive letter: G

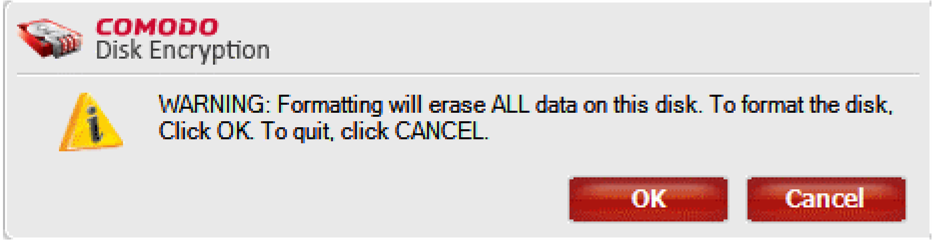
Volume Label: Test Virtual Drive

File System: NTFS

3. Type a new name for the drive in the 'Volume Label:' text box. Leaving this box blank will keep a default name 'New Volume' to the formatted drive.
4. Select the file system for the formatted drive from the 'File System:' drop-down menu.

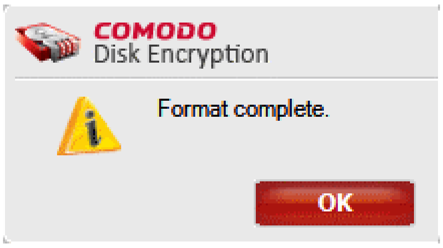


5. Click 'Format'. A warning dialog will be displayed. Formatting will erase all the data contained in the disk.



WARNING: Formatting will erase ALL data on this disk. To format the disk, Click OK. To quit, click CANCEL.

6. Make sure that you are formatting a blank virtual drive or drive containing unwanted files and click 'OK'. The selected disk will be formatted and a 'Format Complete' dialog will be displayed.



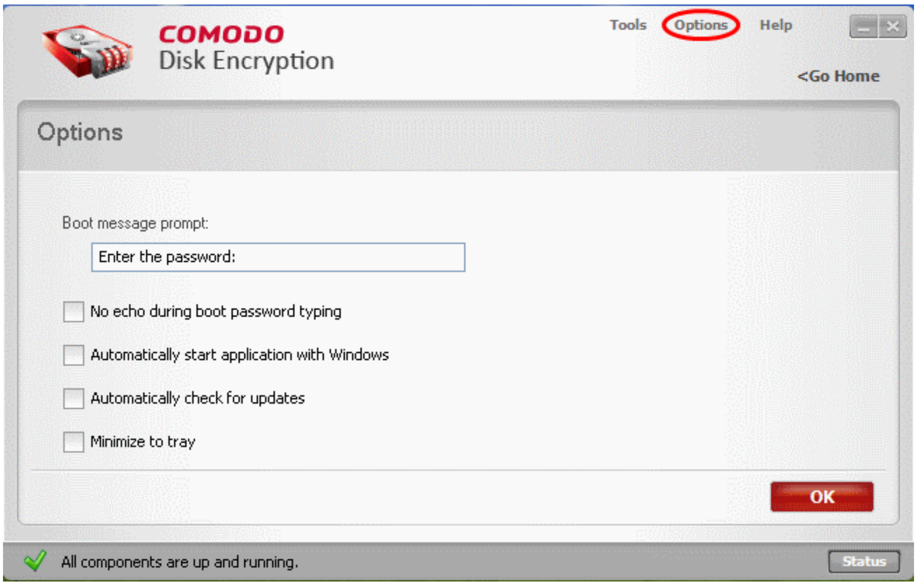
Format complete.

7. Click **'OK'**.

6.Options

The **Options** menu in Comodo Disk Encryption allows you to configure miscellaneous settings concerning the overall behavior of the application.

These Options menu can be accessed by clicking on the **Options** in the menu bar.



Boot message prompt: Enter the password:

□ No echo during boot password typing

□ Automatically start application with Windows

□ Automatically check for updates

□ Minimize to tray

All components are up and running.

You can configure the following settings from the **Options** panel:

- **Set Boot message prompt for boot time password**;
- **Automatically start application with Windows**;
- **Automatically check for updates**;
- **Minimize to tray**.

Boot message prompt - The disks encrypted using Password authentication type or both Password and USB key authentication type cannot be accessed unless the password you have set during encrypting a drive, is entered during system start-up. By default, a message 'Enter the password:' will be displayed during the system start up, to prompt you to enter the password that you have set for the encrypted disks. If you want the system to display a prompt message of your choice, you can enter your customized message (E.g. 'Type the password for Comodo Disk Encryption' or 'Enter the password for accessing encrypted drives') in the text box below 'Boot message prompt'.

Note: This option is activated if at least one of your drives is encrypted.

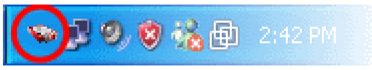
If you have cleared this text box, no prompt will be displayed during system start-up, but the system waits for you to enter the password. If you type the password and press Enter, the system starts normally and you can access the encrypted drive. If you do not type the password or type a wrong password and press enter, the system will start-up but you cannot access the encrypted drive. If the OS drive is encrypted, the system will start only on input of the correct password.

No echo during boot password typing - By default, the password you are typing during system start up in order to access the encrypted drive, will be displayed as asterisk characters. If you don't want the asterisk characters to be displayed, select this option.

Automatically start application with Windows - Enabling this option starts Comodo Disk Encryption every time during system start-up automatically. You can also start the application by clicking Start > All Programs > Comodo > Disk Encryption.

Automatically check for updates - Enabling this option makes the application to connect to Comodo server and check for product updates every time the application is started. If any updates are available, you will be prompted to download and install the updates. You can also manually check for updates.

Minimize to Tray - By default, on clicking the minimize button from the windows controls of the application GUI, the application minimizes to the Windows Task Bar. Enabling this option will make the application to minimize into the system tray and to be displayed as a system tray icon as shown below.

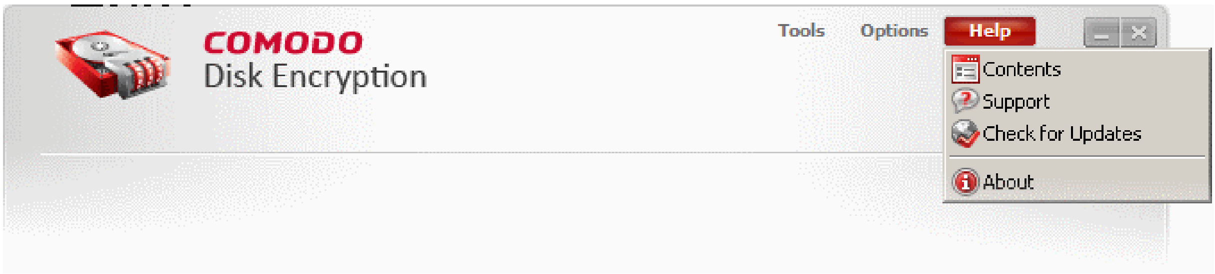


You can always restore the application by double-clicking on the system tray icon.

- Click **'OK'** for your settings to take effect.

7. Help

The **Help** menu allows you to access different options which aid you in using Comodo Disk Encryption.



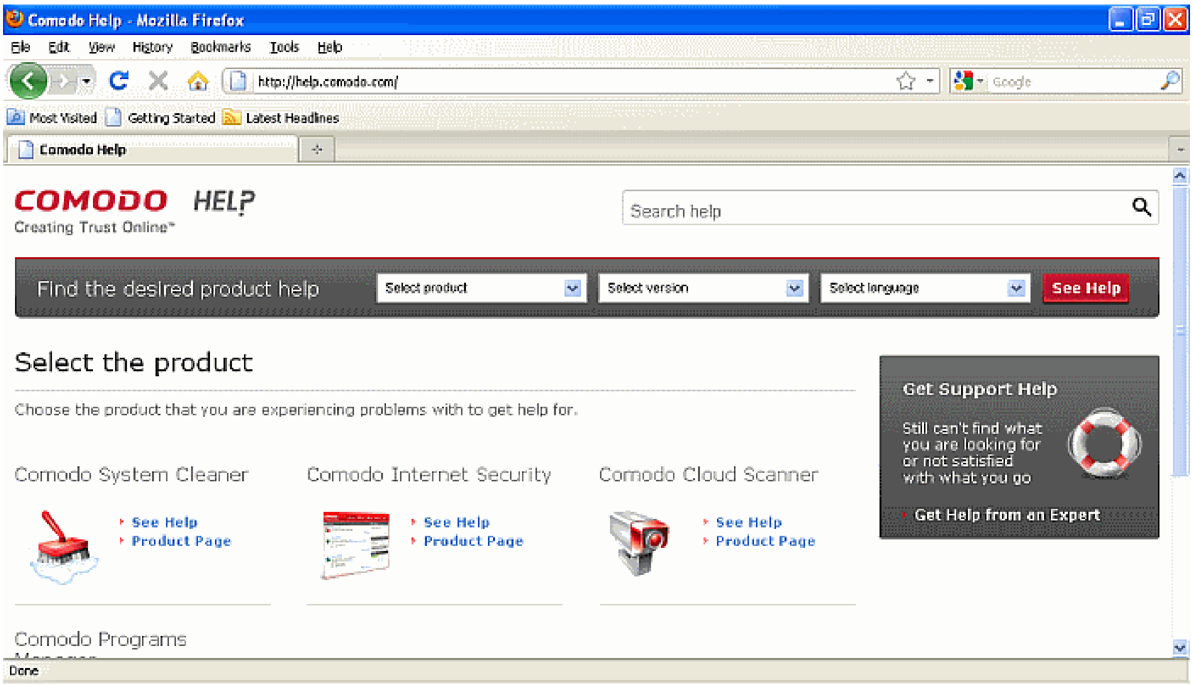
Click on the links below to get details on options in the Help menu.

- **Contents;**

- **Support;**
- **Product Updates;**
- **About.**

7.1. Contents

Clicking the **Content** option in the **Help** menu opens the online Help guide for Comodo Disk Encryption. Each functionality of Comodo Disk Encryption, has its own dedicated page containing detailed descriptions of it in the help guide.



Choose the product that you are experiencing problems with to get help for.

Still can't find what you are looking for or not satisfied with what you go

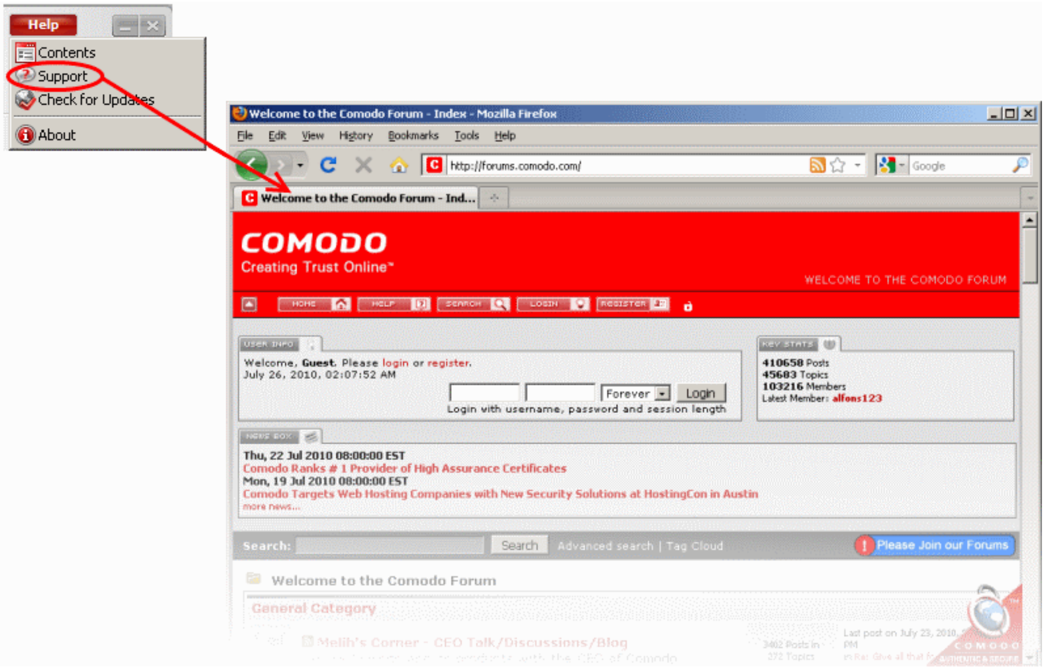
7.2. Support

The fastest way to get further assistance on Comodo Disk Encryption is by posting your question on Comodo Forums, a message board is exclusively created for our users to discuss anything related to our products.

To access Comodo Forum

- On the Help menu, click **Support** option.

This will open the website at **http://forums.comodo.com**. Registration is free and you'll benefit from the expert contributions of developers and fellow users alike.

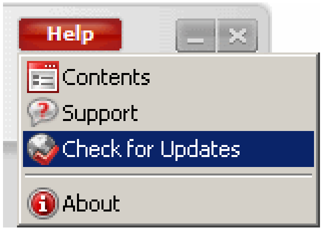

Help
Contents
Support
Check for Updates
About
Welcome to the Comodo Forum - Index - Mozilla Firefox
http://forums.comodo.com/
COMODO
Creating Trust Online
WELCOME TO THE COMODO FORUM

Online Knowledge Base

We also have an online knowledge base and support ticketing system at **http://support.comodo.com**. Registration is free.

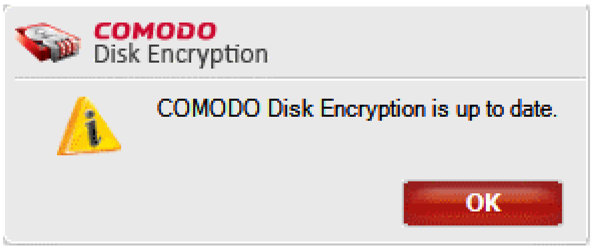
7.3. Check for Updates

The Check for Updates option in the Help menu allows you to manually check for the availability of the updated version of Comodo Disk Encryption from the Comodo server. You can also configure the application to **check for updates automatically** by accessing the **Options** panel.



To manually check for updates

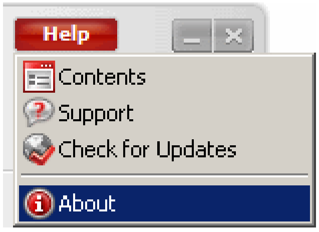
- On the Help menu, click **Check for Updates** option. The application will start checking any available updates from the Comodo Servers.
  - If any updates are available, the application will start downloading and installing the updates.
  - If you have the latest version installed in your system and no updates are available, a dialog will be displayed indicating that you have the up-to-date version.



COMODO Disk Encryption is up to date.

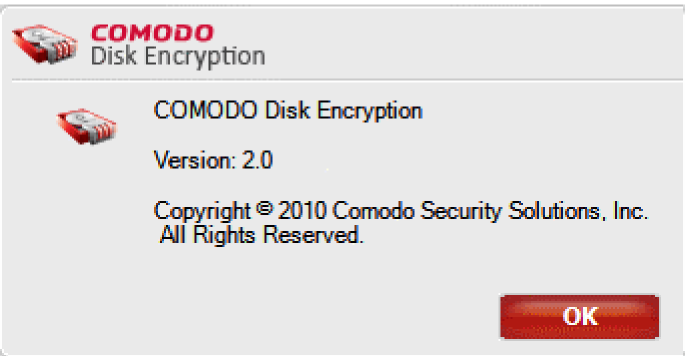
7.4. About

The **About** option in the **Help** menu displays the Comodo Disk Encryption About dialog.



To open About dialog

- On the Help menu, click **About** option.



COMODO Disk Encryption

Version: 2.0

Copyright © 2010 Comodo Security Solutions, Inc.
All Rights Reserved.

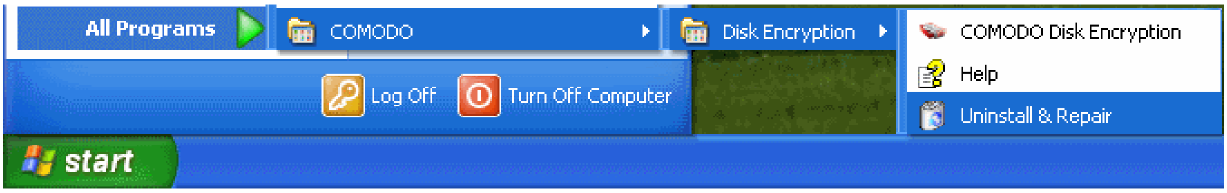
The About dialog will display the version information and copyright information of Comodo Disk Encryption installed in your system.

8. Uninstalling Comodo Disk Encryption

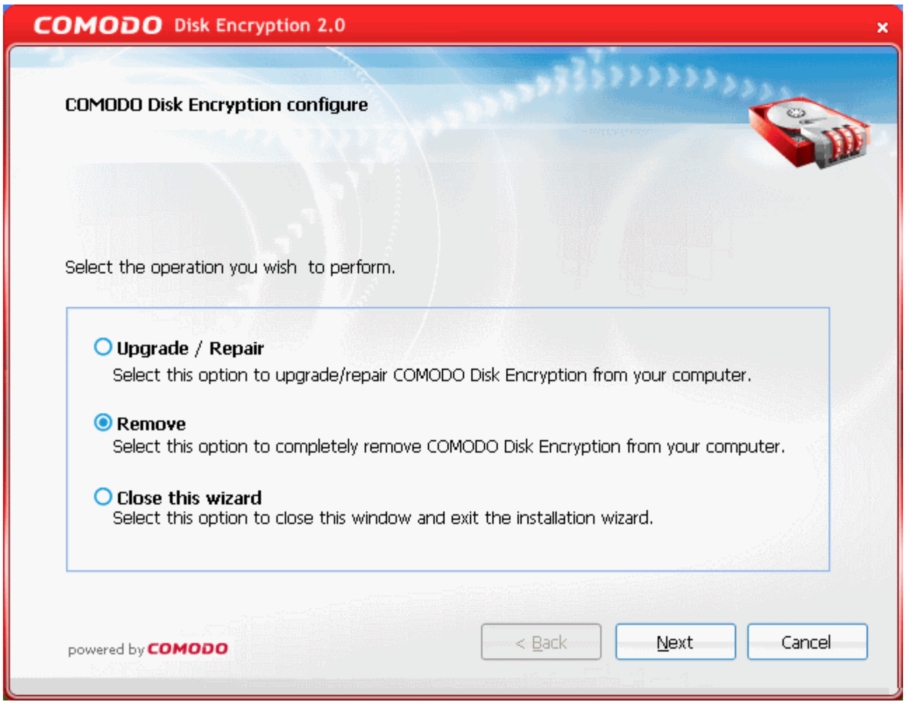
To uninstall Disk Encryption:

- Click Start > Settings > Control Panel
- In the Control Panel, double-click Add/Remove Programs
- In the list of currently installed programs, click Comodo Disk Encryption
- Click the 'Remove' button.

  Or
- Click Start > Programs > Comodo > Disk Encryption > Uninstall & Repair



- Select **Remove** from the 'configure' dialog and click **Next** to continue.



COMODO Disk Encryption configure

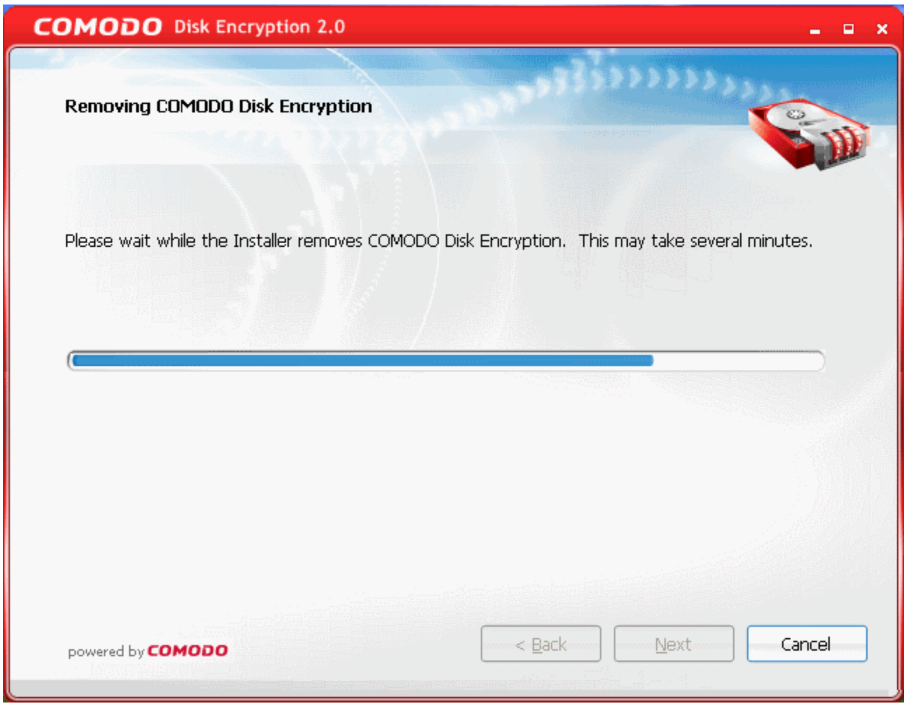
Select the operation you wish to perform.

○ **Upgrade / Repair**
Select this option to upgrade/repair COMODO Disk Encryption from your computer.

● **Remove**
Select this option to completely remove COMODO Disk Encryption from your computer.

○ **Close this wizard**
Select this option to close this window and exit the installation wizard.

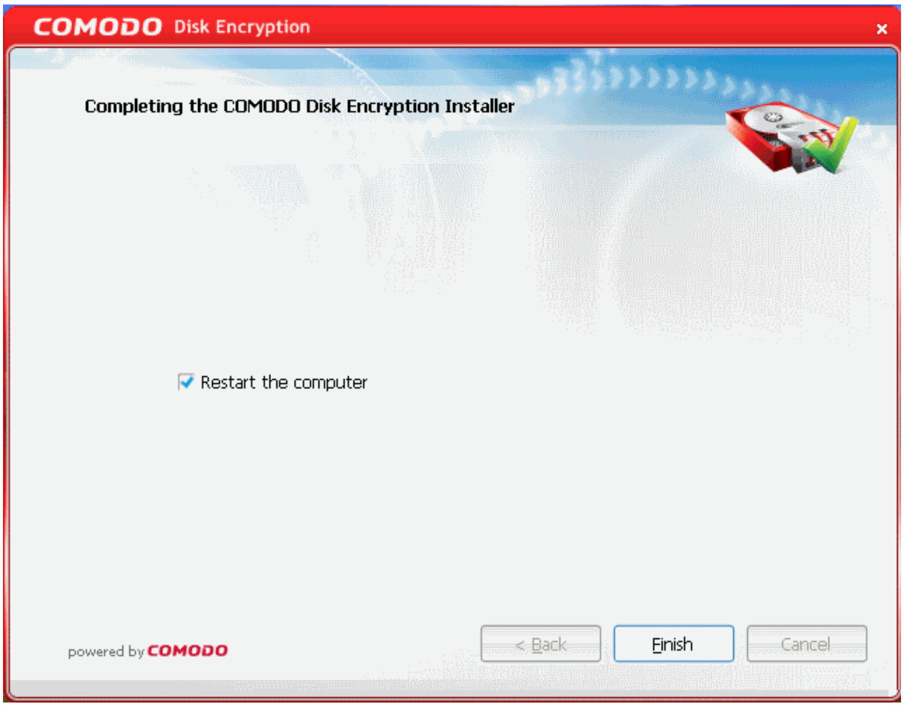
- Please wait while the installer removes Comodo Disk Encryption from your computer.



Removing COMODO Disk Encryption

Please wait while the Installer removes COMODO Disk Encryption. This may take several minutes.

- On completion, you will be prompted to restart your computer. Click on **'Finish'** to continue.



Completing the COMODO Disk Encryption Installer

☑ Restart the computer

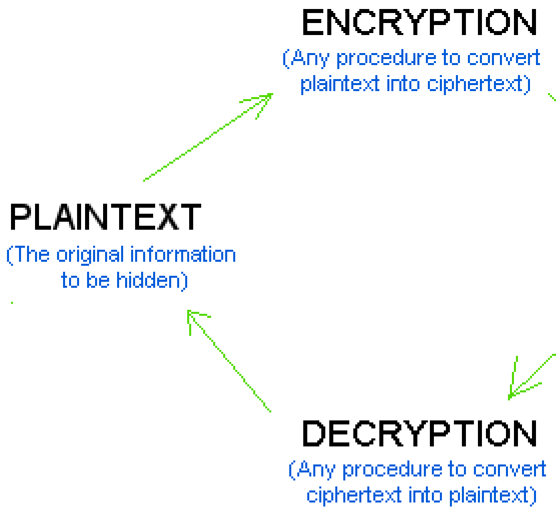
- Click on **Finish.** Your system will be restarted for the uninstallation to take effect. If you want to restart the system at a later time, uncheck 'Restart the computer' and click **'Finish'**.

Note: The uninstallation will take effect only on restarting your system.

Appendix - 1 Cipher Algorithms - A Brief Overview

Different algorithms are used for encryption, but all of them have certain common elements.

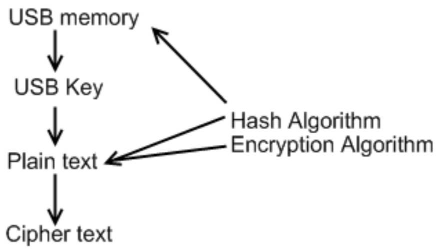
There are several classes of algorithms, in Comodo Disk Encryption are used the strongest types. At it's most simple level, encrypting your data prevents it from being stolen, modified or accessed by unauthorized persons.


ENCRYPTION
(Any procedure to convert plaintext into ciphertext)
PLAINTEXT
(The original information to be hidden)
CIPHERTEXT
(The hidden information)
DECRYPTION
(Any procedure to convert ciphertext into plaintext)

The only person with the ability to view the data is the person in possession of the encryption key that was used to encrypt it. In the case of Comodo Disk Encryption, this key, and other crucial encryption settings, can be stored on the USB drive that must be inserted in your machine at boot up and/or within your system with a password which is to be entered during boot-up. With the USB inserted/password entered, CDE is able to load the key and decrypt your drive, making it available for use. If you do not insert the USB / do not enter the password at start up, the drive will not be useable by anyone - including thieves and hackers. If (as Comodo strongly advise) you select encryption algorithms of 128 bits and above, then you will be creating a drive so secure that it is computationally infeasible that it could be decrypted and accessed by unauthorized persons.

To generate this secret USB key, CDE uses a keyed-Hash Message Authentication Code (HMAC or KHMAC). This is a type of message authentication code which is figured out using a specific algorithm: combination of cryptographic hash function with a secret key. The cryptographic strength of the HMAC depends upon the cryptographic strength of the underlying hash function, on the size and quality of the key and the size of the hash output length in bits.

To encrypt data CDE uses symmetric algorithms, they represented by stream ciphers and block ciphers. Stream ciphers encrypt the bits of the data one at a time, and block ciphers take a number of bits and encrypt them as a single unit.

Generate secret USB key	
Visual representation	**Description**
 USB memory USB Key Plain text Cipher text Hash Algorithm Encryption Algorithm	During Encryption, You are: 1. Inserting the USB memory; 2. Selecting the Hash and Encryption algorithms to be used. Since KHMAC is used, the selected hash algorithm generates a secret key and stores it in the USB memory. The hash algorithm, in combination with the selected encryption algorithm, encrypts the contents of the disk.

Encryption Algorithms			
Algorithm	**Block Size / Encryption level**	**Brief Description**	**Recommendation**
AES	128 bits/ Strongest	Also known as Rijndael. This cipher is used for encryption by default.	Ideal for both domestic and exportable use.
Twofish	128-bit block/ 28-, 192-, or 256-bit key/ strong/	Symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits.	A widely used and recommended choice for most cases.
Cast6	128 medium	CAST-256 is composed of 48 rounds, sometimes described as 12 "quad-rounds"	A widely used and recommended choice for most cases.

Block Cipher mode	
Algorithm	**Brief Description**
None mode	Identical plaintext blocks are encrypted into identical ciphertext blocks. Thus, data patterns are not hidden well. This encryption mode is very fast but it is not recommended for use when you are encrypting text messages or intuitive data patterns
Any other mode	Each ciphertext block is dependent on all plaintext blocks processed up to that point. An initialization vector must be used in the first block to make each encrypted message unique. This encryption modes are a little bit slower, but are recommended for use in cryptography.

About Comodo

The Comodo companies are leading global providers of Security, Identity and Trust Assurance services on the Internet. Comodo CA offers a comprehensive array of PKI Digital Certificates and Management Services, Identity and Content Authentication (Two-Factor - Multi-Factor) software, and Network Vulnerability Scanning and PCI compliance solutions. In addition, with over 10,000,000 installations of its threat prevention products, Comodo Security Solutions maintains an extensive suite of endpoint security software and services for businesses and consumers.

Continual innovation, a core competence in PKI and a commitment to reversing the growth of Internet-crime distinguish the Comodo companies as vital players in the Internet's ongoing development. Comodo, with offices in the US, UK, China, India, Romania and the Ukraine, secures and authenticates the online transactions and communications for over 200,000 business customers and millions of consumers, providing the intelligent security, authentication and assurance services necessary for trust in on-line transactions.

Comodo Security Solutions, Inc.

525 Washington Blvd. Jersey City,

NJ 07310

United States

Tel: +1.888.256.2608

Tel: +1.703.637.9361

Email: **EnterpriseSolutions@Comodo.com**

Comodo CA Limited

3rd Floor, 26 Office Village, Exchange Quay, Trafford Road,
Salford, Greater Manchester M5 3EQ,

United Kingdom.

Tel : +44 (0) 161 874 7070

Fax : +44 (0) 161 877 1767

For additional information on Comodo - visit **http://www.comodo.com**.