



PGP Whole Disk Encryption

Quick Start Guide
version 9.6

What is PGP Whole Disk Encryption?

The PGP Whole Disk Encryption (WDE) product is a software tool that provides multiple ways to protect your data on desktops, laptops, and removable drives.

You can use PGP WDE to do the following:

- Lock down the entire contents of your system, or an external or USB flash drive you specify.
- Use part of your hard drive space as an encrypted virtual disk volume with its own drive letter.
- Create secure, encrypted Zip archives.
- Put files and folders into a single encrypted, compressed package that can be opened on Windows systems that do not have PGP WDE or PGP Desktop installed.
- Completely destroy files and folders so that even file recovery software cannot recover them.
- Securely erase free space on your drives so that your deleted data is truly unrecoverable.

New to PGP Desktop?

Use this step-by-step guide to get started. You will find that, with PGP Desktop, protecting your data will be as easy as turning a key in a lock.

- This *Quick Start Guide* will help you install PGP WDE. Use it as a guide to getting started with PGP WDE, as well as the other security features included as part of PGP Desktop.
- The *PGP Desktop User's Guide* can provide you with more detailed information on PGP WDE. In it, you will learn what a keypair is, why you might want to create one, how to create one, and how to exchange keys with others so you can encrypt your own data and share data securely with others.



A PGP WDE license provides you with access to a certain set of PGP Desktop features. Certain other features of PGP Desktop may require a different license. For more information, see the Licensing section of the *PGP Desktop User's Guide*.

- For deployment, management, and policy enforcement information for PGP WDE, refer to the *PGP Universal Administrator's Guide*.

Contents

■ "What is PGP Whole Disk Encryption?"	1
■ "New to PGP Desktop?"	1
■ "System Requirements"	1
■ "What Am I Installing?"	2
■ "Understanding the Basics"	2
■ "Installing PGP WDE"	3
■ "Starting PGP WDE"	3
■ "The PGP WDE Main Screen"	4
■ "PGP WDE Best Practices"	5
■ "Using PGP WDE to Whole Disk Encrypt a Drive"	7
■ "Creating PGP Virtual Disk Volumes"	8
■ "Creating a PGP Zip Archive"	9
■ "Shredding Files"	12
■ "Shredding Free Space"	13
■ "For More Information"	14

Icon Conventions



Note



Caution

System Requirements

- Windows Vista (32-bit versions), Windows XP (SP 1 or 2) or Windows 2000 (SP 4). Windows 2000 and Windows 2003 Server not supported.
- 128 MB RAM (256 MB recommended).
- 64 MB hard drive space.

What Am I Installing?

PGP Desktop uses licensing to provide access to the features you purchase. Depending on the license you have, some or all of the PGP Desktop family of applications will be active.

This document contains instructions for viewing the features activated by your license.



PGP Whole Disk Encryption (WDE) is a member of the PGP Desktop family of applications. You can use PGP WDE to lock down the entire contents of your system or an external or USB flash drive you specify. Boot sectors, system files, and swap files are all encrypted. Whole disk encrypting your boot drive means you do not have to worry if your computer is lost or stolen: to access your data, an attacker would need to know your passphrase.

Other components of PGP Desktop that are included with PGP WDE:



PGP Virtual Disk volumes — Uses part of your hard drive space as an encrypted virtual disk volume with its own drive letter. You can create additional users for a volume so that people you authorize can also access the volume. A PGP Virtual Disk is the perfect place for storing your sensitive files; it is as if you have stored them in a safe. When the door of the safe is open (when the volume is mounted), you can change files stored in it, take files out of it, and move files into it. Otherwise (when the volume is unmounted), all the data on the volume is protected.



PGP Zip — Adds any combination of files and folders to an encrypted, compressed, portable archive. PGP WDE or PGP Desktop must be installed on a system to create or open a PGP Zip archive. PGP Zip is a tool for securely archiving your sensitive data, whether you want to distribute it to others or back it up.



PGP Self-Decrypting Archives (SDAs) — Puts files and folders into an encrypted, compressed package that can be opened on a Windows system that does not have PGP WDE or PGP Desktop installed. SDAs are the perfect solution for securely exchanging files with someone who does not have PGP software installed.

PGP Shredder — Completely destroys files and folders so that even file recovery software cannot recover them. Deleting a file using the Windows Recycle Bin does not actually delete it; it sits on your drive and eventually gets overwritten. Until then, it is trivial for an attacker to recover that file. PGP Shredder, in contrast, immediately overwrites files multiple times. This is so effective that even sophisticated disk recovery software cannot recover these files. This feature also completely wipes free space on your drives so your deleted data is truly unrecoverable.



Key Management — PGP WDE also manages PGP keys, both your keypairs and the public keys of others. You use your private key to decrypt messages sent to you encrypted to your public key and to secure your PGP Virtual Disk volumes. You use public keys to encrypt messages to others or to add users to PGP Virtual Disk volumes.

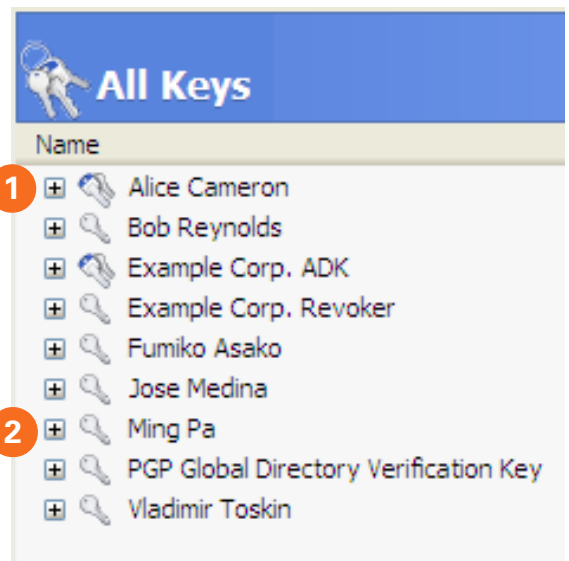
Understanding the Basics

After installation, PGP WDE prompts you to create a PGP keypair. A keypair is the combination of a private key and a public key.

- Keep your **private key** and its passphrase private, as the name suggests. If someone gets your private key and its passphrase, they can read your messages and impersonate you to others. Your private key decrypts incoming encrypted messages and signs outgoing messages.
- Your **public key** you can give to everyone. It does not have a passphrase. Your public key encrypts messages that only your private key can decrypt and verifies your signed messages.

Your keyring holds both your keypairs and the public keys of others, which you use to send encrypted messages to them. Click the PGP Keys Control Box to see the keys on your keyring:

- 1 The icon for a PGP keypair has two keys, denoting the private and the public key. Alice Cameron has a PGP keypair in this illustration, for example.
- 2 The icons for the public keys of others have just one key. Ming Pa's public key, for example, has been added to the keyring shown in this illustration.



Installing PGP WDE

The installation process requires a system restart.

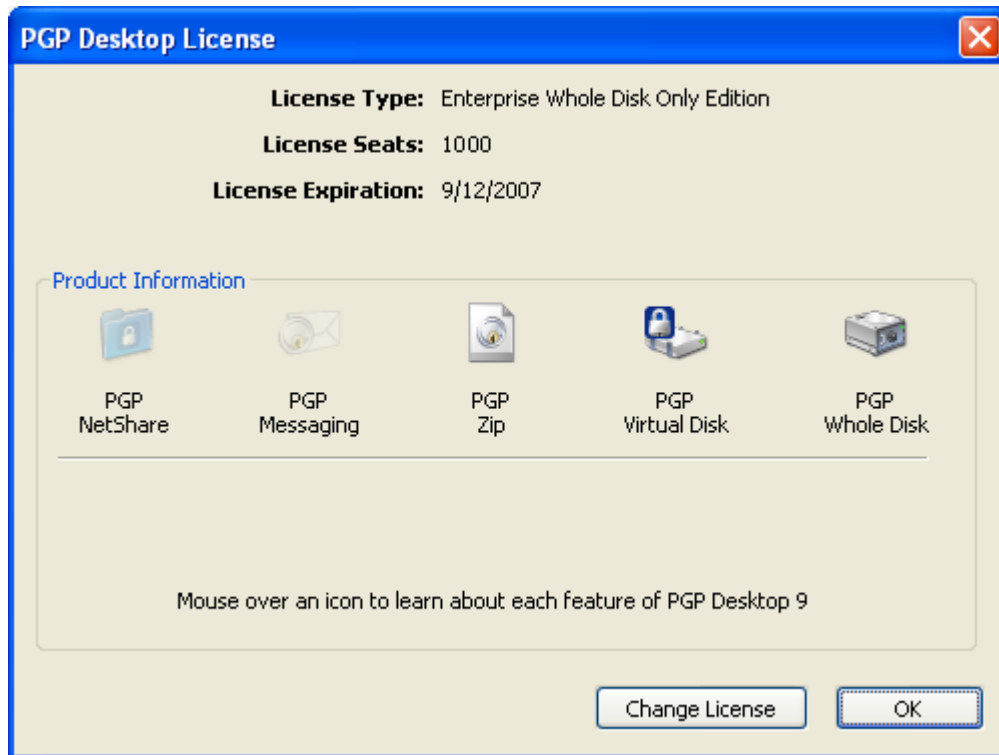
PGP Corporation recommends exiting from open applications before you begin the install.



Depending on your license, you may not have access to certain components of PGP Desktop.

To install PGP WDE:

- 1 Locate the PGP WDE installer program.
The installer program may have been distributed by your PGP administrator using the Microsoft SMS deployment tool.
- 2 Double-click the installer.
- 3 Follow the on-screen instructions.
- 4 Reboot your system when instructed.
- 5 When your system restarts, follow the on-screen instructions to configure PGP WDE.



To see what features your PGP Desktop license supports, open PGP WDE and from the Help menu, select License. Those features with a green checkmark are supported by the active license. In this illustration, PGP Whole Disk Encryption, PGP Zip, and PGP Virtual Disk are supported.

Starting PGP WDE

To start PGP WDE, use any of the following methods:

- Double-click the **PGP Tray** icon.
- Right-click the **PGP Tray** icon, and then select **Open PGP Desktop**.
- From the **Start** menu, select **Programs > PGP > PGP Desktop**.

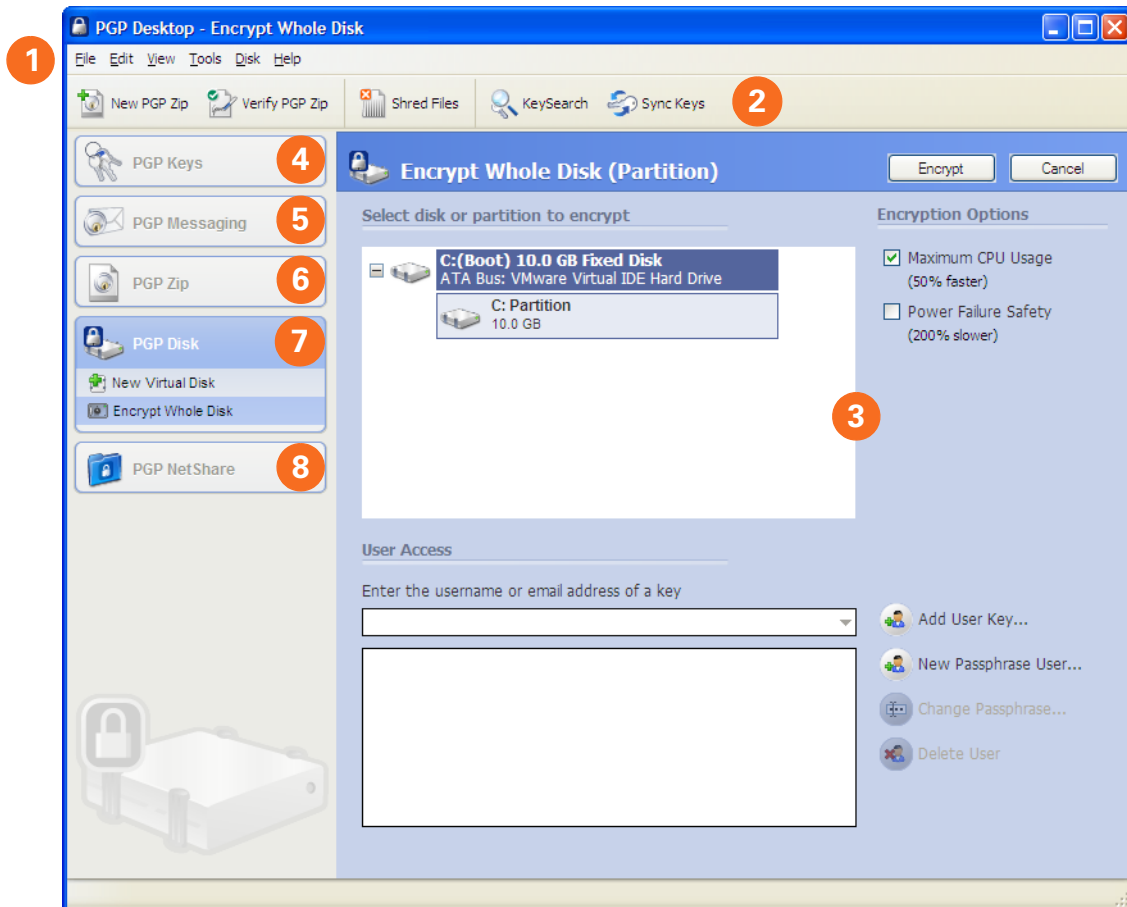


PGP Tray icon.

The PGP WDE Main Screen

The easiest way to access the features of PGP WDE is via its main screen.

- 1 **PGP Menu bar** — Provides access to all PGP WDE features through its menus and commands.
- 2 **PGP Toolbar** — Provides access to several commonly performed PGP WDE tasks.
- 3 **Work Area** — You configure the settings for the active feature in the **work area**.
This illustration shows the PGP WDE work area.



- 4 **PGP Keys Control Box** — Controls your PGP keys.
- 5 **PGP Messaging Control Box** — Controls PGP Messaging.
- 6 **PGP Zip Control Box** — Controls PGP Zip archives.
- 7 **PGP Disk Control Box** — Controls PGP Virtual Disk volumes and PGP Whole Disk Encrypted drives.
- 8 **PGP NetShare Control Box** — Controls PGP NetShare.

PGP WDE Best Practices

PGP Corporation recommends the following best practices for preparing to encrypt your disk. Please follow the recommendations below to protect your data during and after encryption.

Before you encrypt your disk, there are a few tasks you must perform to ensure successful initial encryption of the disk.

- 1 Determine whether your target disk is supported.** PGP WDE feature protects desktop or laptop disks (either partitions, or the entire disk), external disks, and USB flash disks. CD-RW/DVD-RWs and servers are NOT supported. See Chapter 6 of the *PGP Desktop User's Guide* for more details on what types of disks are supported.
- 2 Back up the disk before you encrypt it.** Before you encrypt your disk, be sure to back it up so that you won't lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk.
- 3 Ensure the health of the disk before you encrypt it.** If PGP WDE encounters disk errors during encryption, it will pause encryption so you can repair the disk errors. However, it is more efficient to repair errors before you initiate encryption. See ["Ensure Disk Health Before Encryption"](#) for more information.
- 4 Create a recovery disk.** While the chances are extremely low that a master boot record could become corrupt on a boot disk or partition protected by PGP Whole Disk Encryption, it is possible. Before you encrypt a boot disk or partition using PGP Whole Disk Encryption, create a recovery disk. See ["Create a Recovery CD"](#) for instructions on how to create a recovery disk.
- 5 Be certain that you will have AC power** for the duration of the encryption process. See [Maintain Power Throughout Encryption on page 6](#).
- 6 Run a pilot test to ensure software compatibility.** As a good security practice, PGP Corporation recommends testing PGP WDE on a small group of computers to ensure that PGP WDE is not in conflict with any software on the computer before rolling it out to a large number of computers. This is particularly useful in environments that use a standardized Corporate Operating Environment (COE) image. For a list of software known to have compatibility issues with PGP WDE, see [Run a Pilot Test to Ensure Software Compatibility on page 6](#).
- 7 Perform Disk Recovery on Decrypted Disks.** Where possible, as a best practice, if you need to perform any disk recovery activities on a disk protected with PGP Whole Disk Encryption (WDE), PGP Corporation recommends that you first decrypt the disk. Do this by using the **PGP Desktop Disk > Decrypt** option, your prepared PGP WDE Recovery Disk, or by connecting the hard disk via a USB cable to a second system and decrypting from that system's PGP Desktop software. Once the disk is decrypted, proceed with your recovery activities.

Ensure Disk Health Before Encryption

PGP Corporation deliberately takes a conservative stance when encrypting drives, to prevent loss of data. It is not uncommon to encounter Cyclic Redundancy Check (CRC) errors while encrypting a hard disk. If PGP WDE encounters a hard drive or partition with bad sectors, PGP WDE will, by default, pause the encryption process. This pause allows you to remedy the problem before continuing with the encryption process, thus avoiding potential disk corruption and lost data.

To avoid disruption during encryption, PGP Corporation recommends that you start with a healthy disk by correcting any disk errors prior to encrypting.

- Before you attempt to use PGP WDE, use a third-party scan disk utility that has the ability to perform a low-level integrity check and repair any inconsistencies with the drive that could lead to CRC errors. Microsoft Windows' check disk (chkdsk.exe) utility is not sufficient for detecting these issues on the target hard drive. Instead, use software such as SpinRite or Norton Disk Doctor™. These software applications can correct errors that would otherwise disrupt encryption.
- As a best practice, highly fragmented disks should be defragmented before you attempt to encrypt them.

Create a Recovery CD

The following instructions use Roxio software for illustration purposes. The actual steps you perform may differ.

- 1** Make sure PGP Desktop for Windows and Roxio Easy Media Creator or Roxio Easy CD Creator (or other software that can create a CD from an ISO image) are installed on your system.
- 2** Open Roxio Easy Media Creator or Roxio Easy CD Creator and choose to create a Data CD Project.
- 3** From the **File** menu, select **Record CD from CD Image**.
- 4** From the **Files of Type** menu, select **ISO Image Files (ISO)**.
- 5** Navigate to the PGP directory. The default is: **C:\Program Files\PGP Corporation\PGP Desktop**
- 6** Select **bootg.iso** and click **Open**.

- 7** Insert a blank, recordable CD into a CD drive on your system.
- 8** On the Record CD Setup screen, click **Start Recording**.
- 9** When the file is burned to the CD, click **OK**.
- 10** Remove the recovery CD from the drive and label it appropriately.



PGP WDE recovery disks are compatible only with the version of PGP Desktop that created the recovery CD. For example, if you attempt to use a 9.0.x recovery disk to decrypt a disk protected with PGP WDE 9.6 software, it will render the PGP WDE 9.6 disk inoperable.

PGP WDE Best Practices (continued)

Maintain Power Throughout Encryption

Because encryption is a CPU-intensive process, encryption cannot begin on a laptop computer that is running on battery power. The computer **must** be on AC power. If a laptop computer goes on battery power during the initial encryption process (or a later decryption or re-encryption process) PGP WDE pauses its activity. When you restore AC power, the encryption, decryption, or re-encryption process resumes automatically.

Regardless of the type of computer you are working with, your system must not lose power, or otherwise shut down unexpectedly, during the encryption process, unless you have selected the **Power Failure Safety** option.

Do not remove the power cord from the system before the encryption process is over. If loss of power during encryption is a possibility—or if you do not have an uninterruptible power supply for your computer—consider choosing the **Power Failure Safety** option, as described in the *PGP Desktop User's Guide*.



This holds true for removable disks, such as USB devices. Unless you have selected the **Power Failure Safety** option, you run the risk of corrupting the device if you remove it during encryption.

Run a Pilot Test to Ensure Software Compatibility

Certain other disk protection software is incompatible with PGP WDE and can cause serious disk problems, up to and including loss of data.

Please note the following known interoperability issues, and please review the PGP Desktop Release Notes for the latest updates to this list.

Software that is not compatible:

- **CompuTrace in MBR mode.** PGP Whole Disk Encryption is compatible only with the BIOS configuration of Absolute Software's CompuTrace laptop security and tracking product. Using CompuTrace in MBR mode is not compatible.


- **Utimaco Safeguard Easy 3.x** is incompatible with the PGP Whole Disk Encryption feature; do not install it on a system with PGP Desktop and do not install PGP Desktop on a system with Utimaco Safeguard Easy 3.x.
- **Hard disk encryption products from GuardianEdge Technologies:** Encryption Anywhere Hard Disk and Encryption Plus Hard Disk products, formerly known as PC Guardian products.

The following programs will co-exist with PGP Desktop on the same system, but will block the PGP Whole Disk Encryption feature:

- **Safeboot Solo**
- **SecureStar SCPP**
- **Pointsec.**

Using PGP WDE to Whole Disk Encrypt a Drive

The PGP WDE feature locks down the entire contents of your system or an external or USB flash drive you specify.

 PGP Corporation recommends, as a best practice, that you back up your data before encrypting your disk.

- 1 Click **Encrypt Whole Disk** in the **PGP Disk Control box**.



- 2 Select the drive or partition to be encrypted.

- 3 Select **Maximum CPU Usage** to protect your disk as quickly as possible. The encryption process will take priority over other operations on your system.

- 4 Select **Power Failure Safety** if you think your system could lose power during the encryption process.

When **Power Failure Safety** is selected, the encryption process can safely resume if it is interrupted. This option can cause encryption to take longer to complete.

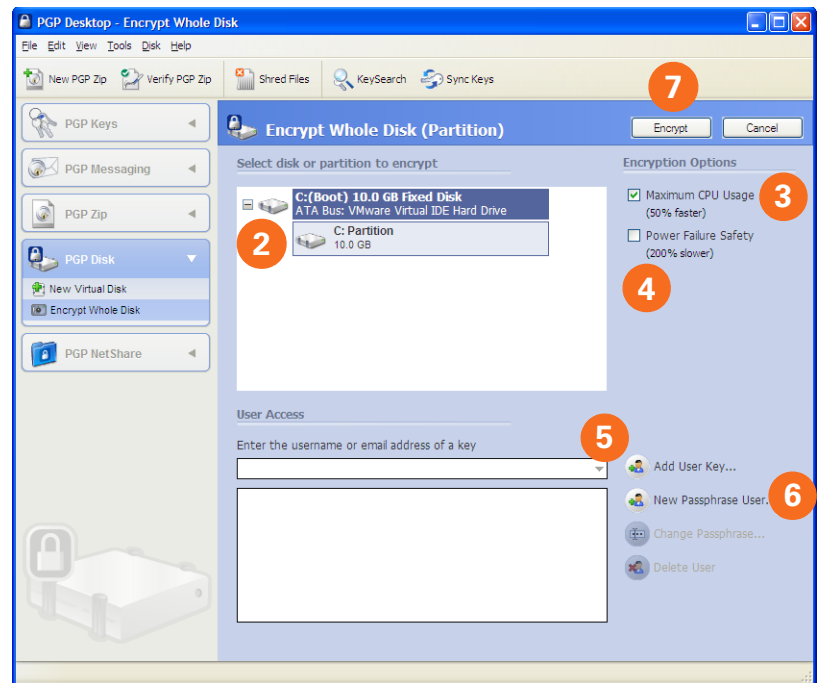
- 5 Click **Add User Key** to add users who will be able to authenticate to the whole disk encrypted drive using public-key cryptography.


If you are encrypting a fixed drive, you can only use a PGP keypair on an Aladdin eToken USB token. If you are encrypting a partition or a removable (non-fixed) drive, you can use any keypair on your system.


- 6 Click **New Passphrase User** to add users who authenticate using a passphrase.

If you are encrypting your boot drive, you have the option of using your Windows logon passphrase so that you only have to enter your credentials once on startup.

- 7 Click **Encrypt**.



 The encryption algorithm used by PGP WDE is AES256. The hashing algorithm is SHA-1. FAT16, FAT32, and NTFS formatted drives are supported. There is no minimum or maximum size. If the drive is supported by the operating system (or your hardware BIOS for the boot drive), it should work with PGP WDE.

 To encrypt data on floppy disks or CD-RWs, use PGP Virtual Disk volumes; do not use PGP WDE. Backup software works normally with PGP WDE; any files the software backs up will be decrypted *before* being backed up.

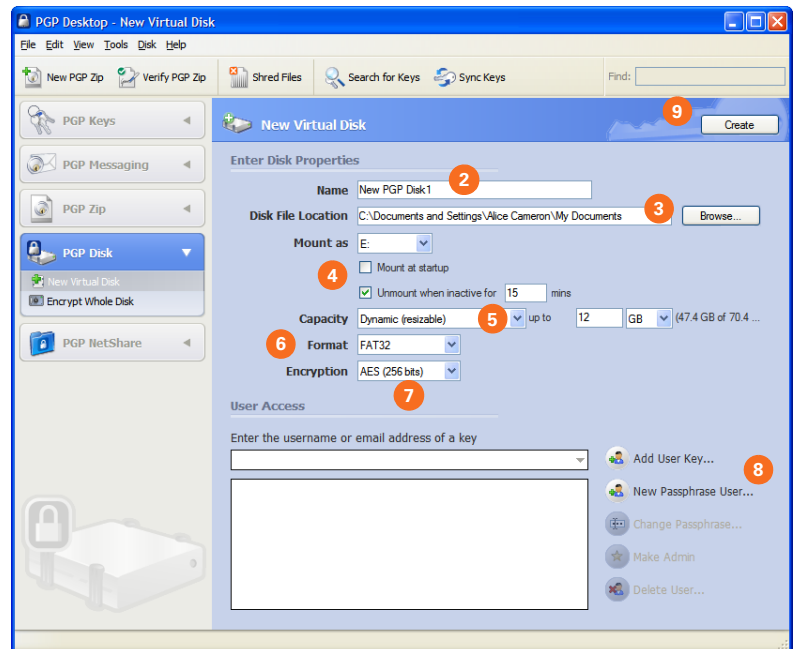
Creating PGP Virtual Disk Volumes

The PGP Virtual Disk Volumes feature uses part of your hard drive space as an encrypted virtual disk volume with its own drive letter. You can create additional users for a volume so that people you authorize can also access the volume.

- 1 Click **New Virtual Disk** in the PGP Disk Control box.

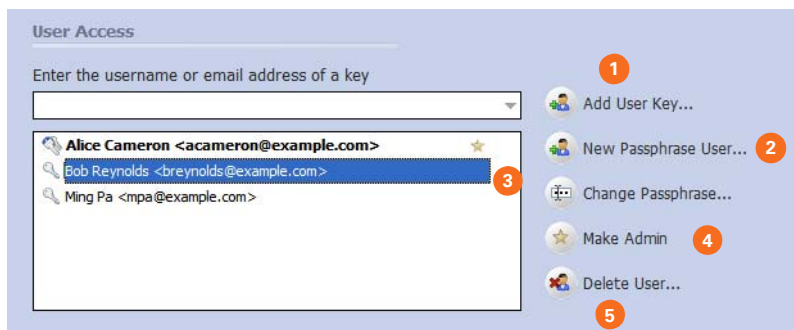


- 2 Type a **Name** for the volume.
- 3 Specify a **Disk File Location** for the volume.
- 4 Select your mount preferences:
 - select a drive letter for the volume to **Mount as**.
 - select **Mount at Startup** to have your new volume mount automatically at startup.
 - select **Unmount when inactive for x mins** to have the volume automatically unmount when it has been inactive for the specified number of minutes.
- 5 From **Capacity**, select **Dynamic (resizeable)** if you want the volume to grow in size as you add files or **Fixed size** if you want the volume to always remain the same size.
- 6 Specify a filesystem **Format** for the volume.
- 7 Specify an **Encryption** algorithm for the volume.
- 8 Click **Add User Key** to add users who authenticate using public-key cryptography or click **New Passphrase User** to add users who authenticate using passphrases.
- 9 Click **Create**.



Use the **User Access** section to control existing users of a PGP Virtual Disk volume:

- 1 Click **Add User Key** to add users who authenticate using public-key cryptography.
- 2 Click **New Passphrase User** to add users who authenticate using passphrases.
- 3 Select a passphrase user, then click **Change Passphrase** to change their passphrase.
- 4 Select a user, then click **Make Admin** to give the user administrative rights.
- 5 Select a user, then click **Delete** to delete the user.



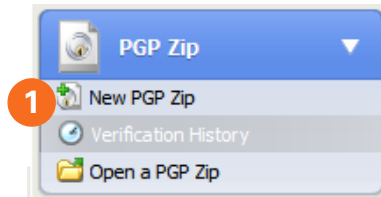
Creating a PGP Zip Archive

PGP Zip archives let you put any combination of files and folders into a compressed, portable archive. There are four kinds of PGP Zip archives:

- **Recipient keys.** Encrypts the archive to public keys. Only the holder of the corresponding private keys can open the archive. This is the most secure kind of PGP Zip archive. Recipients must be using PGP WDE or PGP Desktop for Windows.
- **Passphrase.** Encrypts the archive to a passphrase, which must be communicated to the recipients. Recipients must be using PGP WDE or PGP Desktop for Windows.
- **PGP Self-Decrypting Archive.** Encrypts the archive to a passphrase, but recipients do *not* need to be using PGP WDE or PGP Desktop for Windows to open it. The passphrase must be communicated to the recipients.
- **Sign only.** Signs the archive but does not encrypt it, allowing you to prove you are the sender. Recipients must be using PGP WDE or PGP Desktop for Windows to open and verify the archive.

The Passphrase and Sign only PGP Zip types are described in detail in the *PGP Desktop User's Guide*; they are described briefly here.

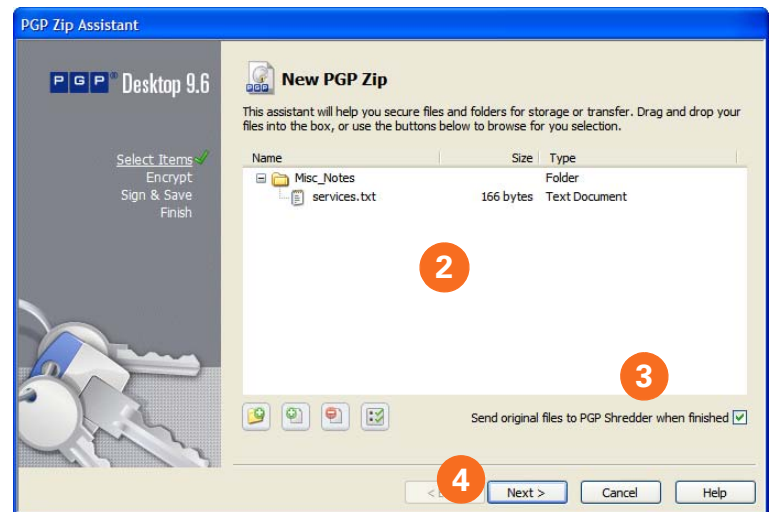
- 1 Click **New PGP Zip** in the PGP Zip Control Box.



- 2 Drag and drop the files/folders you want to be in the archive or use the buttons to select them.

- 3 Select **Send original files to PGP Shredder when finished** if you want the files/folders you put into the archive to be shredded when the archive is created.

- 4 Click **Next**.



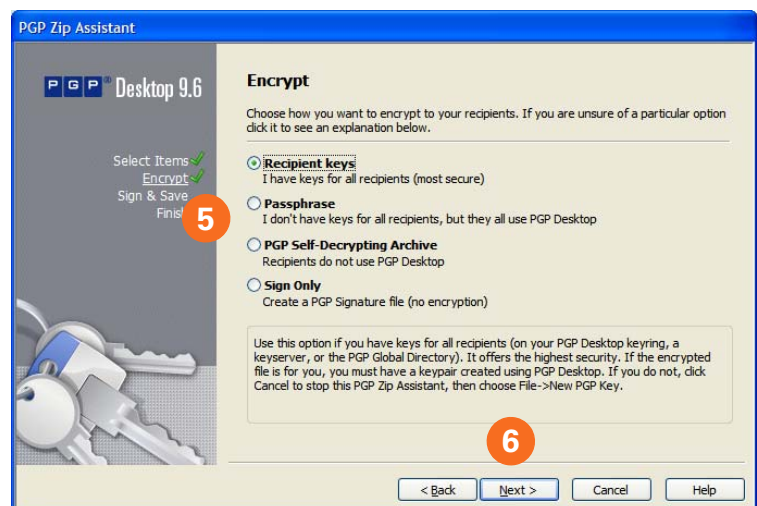
- 5 Select the desired kind of PGP Zip archive:

- **Recipient keys**
- **Passphrase**
- **PGP Self-Decrypting Archive**
- **Sign only**

- 6 Click **Next**.

Passphrase and **Sign only** are described in detail in the *PGP Desktop User's Guide*.

Refer to the appropriate section on the following pages for the kind of PGP Zip archive you specified.



Creating a PGP Zip Archive (continued)

Recipient Keys

The **Add User Keys** screen appears.

- 1 Click **Add** and use the **User Selection** screen to select the public keys of those persons who you want to be able to open the archive
If you want to be able to open the archive yourself, be sure to include your public key.

- 2 Click **Next**.

- 3 Choose a private key on the local system to use to sign the archive.

- 4 Specify a name and a location for the archive.
The default name is the name of the first file or folder in the archive; the default location is the location of the files/folders going into the archive.

- 5 Click **Next**.

The PGP Zip archive is created.

The **Finished** screen displays information about the new archive.

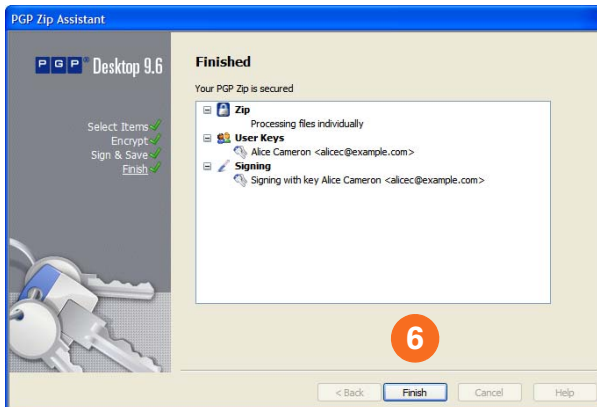
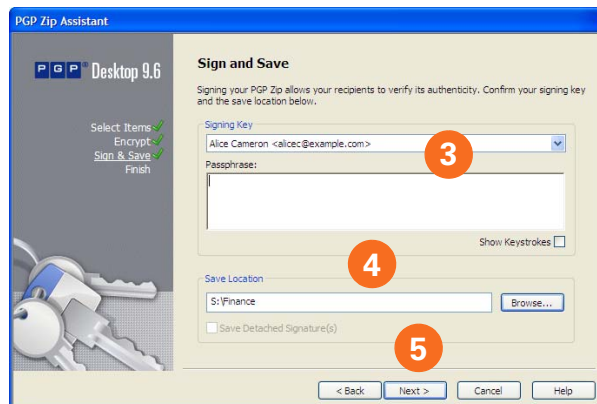
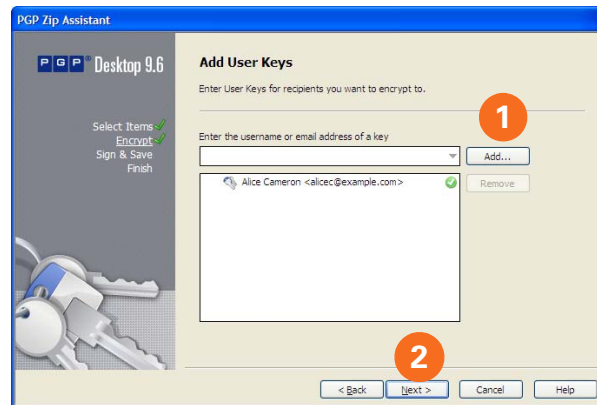
- 6 Click **Finish**.



The **Passphrase** type of PGP Zip archive is very similar to Recipient Keys, the difference being that a passphrase is used to protect the archive instead of a key.



The **Sign only** type of PGP Zip archive is similar to Recipient Keys, the difference being that because the archive is only signed, not encrypted, you do not select public keys.



Creating a PGP Zip Archive (continued)

PGP Self-Decrypting Archive

The **Create a passphrase** screen appears.

- 1 Enter a passphrase for the PGP Zip Self-Decrypting Archive (SDA), then confirm the passphrase by entering it again.

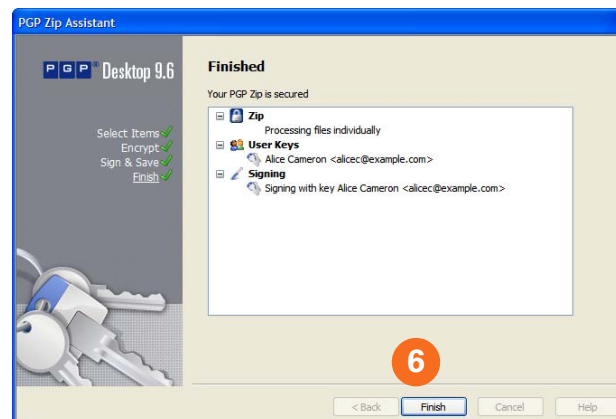
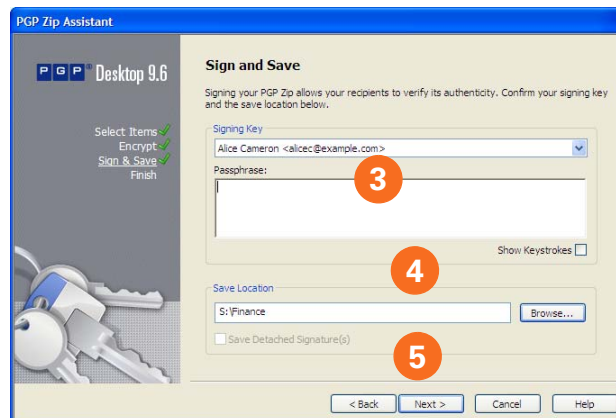
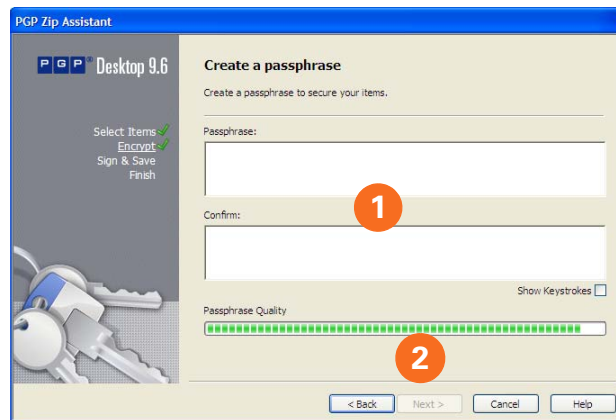
- 2 Click **Next**.

- 3 Choose a private key on the local system to use to sign the archive.

- 4 Specify a name and a location for the archive.
The default name is the name of the first file or folder in the archive; the default location is the location of the files/folders going into the archive.

- 5 Click **Next**.
The PGP SDA is created.

- 6 Click **Finish**.



Shredding Files

The PGP Shredder feature completely destroys files and folders so that even sophisticated file recovery software cannot recover them. While both the PGP Shredder icon and the Windows Recycle Bin appear on your desktop, only PGP Shredder immediately overwrites the files you specify so that they are not recoverable.

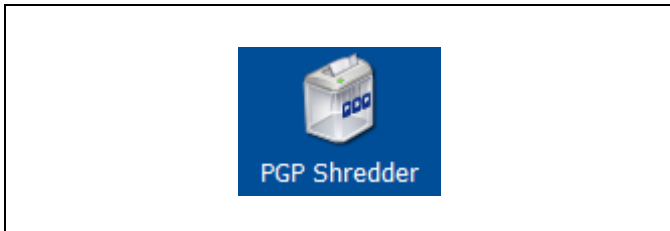
You can shred files using any of the following methods:

- Using the PGP Shredder icon.
- Using the PGP Toolbar.
- Using the PGP Context menu.

Using the PGP Shredder Icon

To shred files using the PGP Shredder icon:

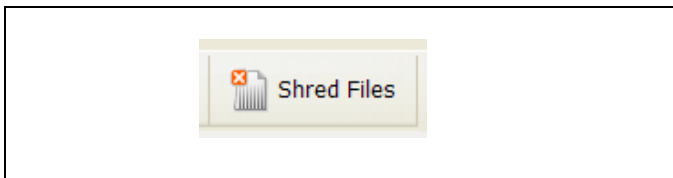
- 1 On your Windows desktop, drag the files and folders you want to shred into the PGP Shredder.
A dialog appears, asking you to confirm you want to shred the files.
- 2 Click **Yes**.
The specified files and folders are shredded.



Using the PGP Toolbar

To shred files using the PGP Toolbar:

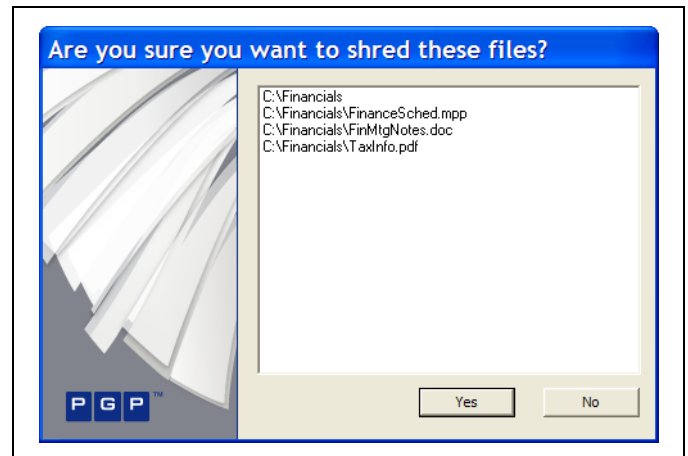
- 1 Click **Shred Files** on the PGP Toolbar.
- 2 Specify which files you want to shred.
You can Control-click to select multiple files or Control-A to select all files showing.
- 3 Click **Open**.
A dialog appears, asking you to confirm you want to shred the files.
- 4 Click **Yes**.
The specified files and folders are shredded.



Using the PGP Context Menu

To shred files in Windows Explorer:

- 1 Open Windows Explorer.
- 2 Right-click on the files or folders you want to shred, then select **PGP Desktop > PGP Shred <filename>**.
You can Control-click to select multiple files or Control-A to select all files showing.
If you selected more than one file, the text says **PGP Shred x items**, where **x** is the number of files selected.
A dialog appears, asking you to confirm you want to shred the files.
- 3 Click **Yes**.
The specified files and folders are shredded.



If you do not use the PGP Shredder feature often, you can remove the PGP Shredder icon from your desktop via PGP Options: access the **Options** panel, click on the **Disk** tab, deselect the **Place PGP Shredder icon on the desktop** option, then click **OK**.



You can also use PGP Options to control the number of passes made when shredding (more passes is more secure but takes longer), whether files in the Windows Recycle Bin should be shredded when you empty it, and whether the warning dialog appears when you shred.

Shredding Free Space

The PGP Shred Free Space feature completely shreds free space on your drives so that your deleted data is truly unrecoverable. Keep in mind that “free space” is actually a misnomer. What PGP Shred Free Space does is overwrite the portions of your hard drive that Windows believes to be empty; in fact, that space could be empty or it could be holding files Windows told you were deleted.

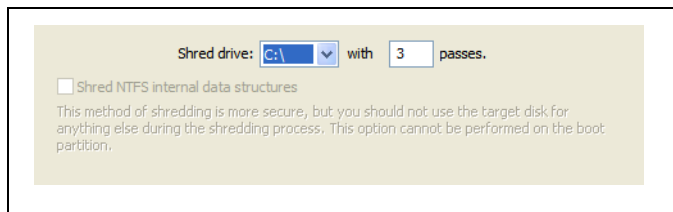
When you put files into the Windows Recycle Bin and empty it, the files are not really deleted; Windows just acts like there is nothing there and eventually overwrites the files. Until those files are overwritten, they are easy for an attacker to recover. PGP Shred Free Space overwrites this “free space” so that even disk recovery software cannot get those files back.

To shred free space on your disks:

- 1 From the **Tools** menu, select **PGP Shred Free Space**.
- 2 On the **Introduction** screen, read the information, then click **Next**.
- 3 On the **Gathering Information** screen, in the **Shred drive** box, select the disk or volume you want shredded and the number of passes you want PGP Shred Free Space to perform.

The recommended guidelines for passes are:

- 3 passes for personal use.
- 10 passes for commercial use.
- 18 passes for military use.
- 49 passes for maximum security.

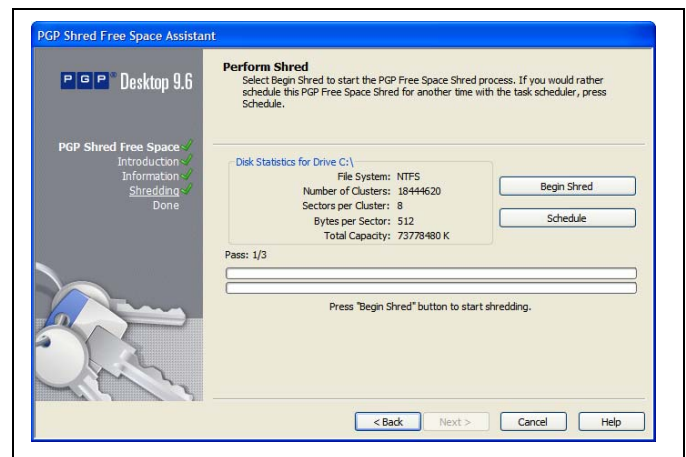


- 4 Choose whether to **Wipe internal NTFS data structures** (not available on all systems), then click **Next**.
This option shreds small (less than 1K) files in internal data structures that might otherwise not get shredded.
- 5 On the **Perform Shred** screen, click **Begin Shred**.



Click **Schedule** to schedule a shred of your free space instead of doing it now. The Windows Task Scheduler must be installed on your system.

The length of the shred session depends on the number of passes you specified, the speed of the processor, how many other applications are running, and so on.



- 6 When the shred session is complete, click **Next**.
- 7 On the **Completing** screen, click **Finish**.

For More Information

Getting Assistance

What product documentation is available?

These documents were installed onto your system when you installed the product:

- *PGP Desktop for Windows User's Guide*
- *PGP Desktop for Windows Release Notes*

A Help menu is available in the product for context-specific information.

How do I contact technical support?

- For PGP Corporation Product Support and Customer Service, please visit the PGP Support Portal: **<https://www.pgp.com/support>**.
- To access the PGP Support forums, please go to: **forums.pgpsupport.com**.

For any other contacts at PGP Corporation, please go to the Contact Us section of the PGP website: **www.pgp.com/company/contact.html**.