



## What is PGP NetShare?

The PGP NetShare product is a software tool that provides multiple ways to protect and share your data.

You can use PGP NetShare to:

- Let authorized users share protected files in a shared space—such as a fileserver, shared folder, or USB removable drive.
- 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 NetShare 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 NetShare. Use it to as a guide to getting started with PGP NetShare, 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 NetShare. 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 NetShare 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 NetShare, refer to the *PGP Universal Administrator's Guide*.

### Contents

■ <a href="#">What is PGP NetShare?</a>	1
■ <a href="#">New to PGP Desktop?</a>	1
■ <a href="#">System Requirements</a>	1
■ <a href="#">What Am I Installing?</a>	2
■ <a href="#">Understanding the Basics</a>	2
■ <a href="#">Installing PGP NetShare</a>	3
■ <a href="#">The PGP NetShare Main Screen</a>	4
■ <a href="#">Using PGP NetShare</a>	5
■ <a href="#">Creating PGP Virtual Disk Volumes</a>	6
■ <a href="#">Creating a PGP Zip Archive</a>	7
■ <a href="#">Shredding Files</a>	10
■ <a href="#">Shredding Free Space</a>	11
■ <a href="#">For More Information</a>	12

### Icon Conventions



**Note**



**Caution**

## System Requirements

- Windows Vista (32-bit versions), Windows XP (SP 1 or 2), Windows 2000 (SP 4), and Windows 2003 Server (SP 1)
- 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 NetShare** is a member of the PGP Desktop family of applications. You can use PGP NetShare to authorize users to share protected files in a shared space, such as on a corporate fileserver, in a shared folder, or on a removable media such as a USB drive. The encrypted files in the Protected Folder continue to appear as normal application files to the authorized users; anyone else with physical access to the files can see them but not use them.

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



**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 NetShare 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 NetShare 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 NetShare 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.

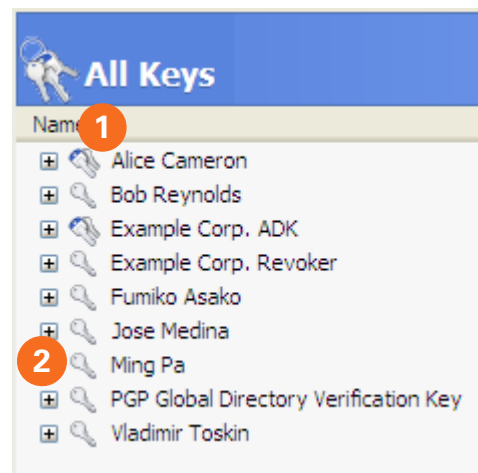
## Understanding the Basics

After installation, PGP NetShare 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 NetShare

The installation process requires a system restart.

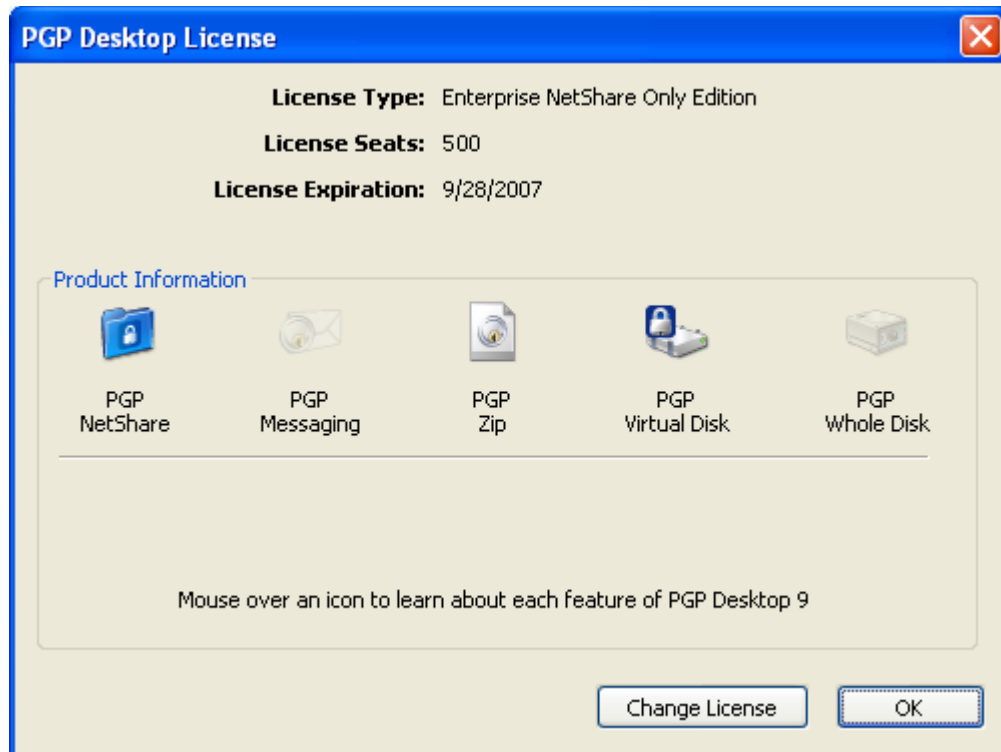
PGP Corporation recommends exiting all open applications before you begin the install.



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

To install PGP NetShare:

- 1 Locate the PGP NetShare 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 NetShare.



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

## Starting PGP NetShare

To start PGP NetShare, 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**.

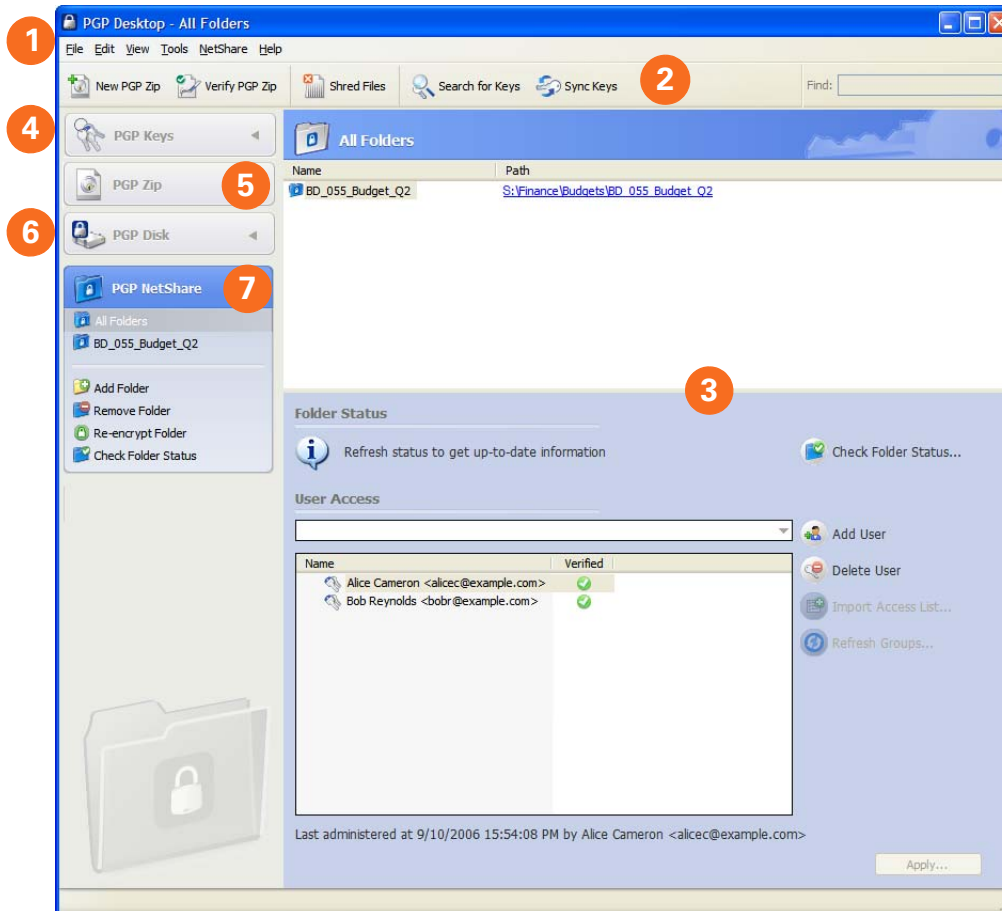


PGP Tray icon

## The PGP NetShare Main Screen

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

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



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

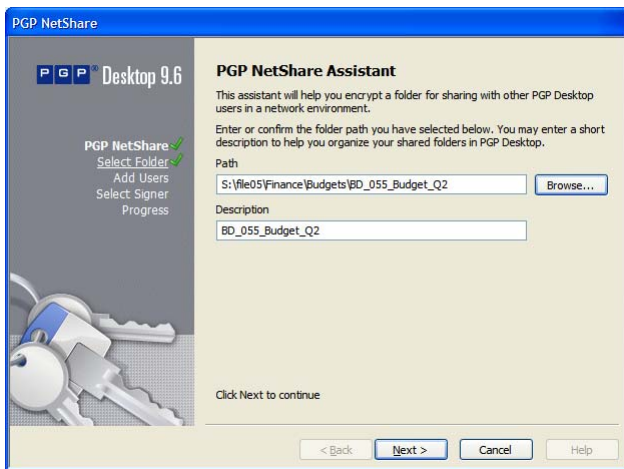
## Using PGP NetShare

The PGP NetShare feature allows authorized users to share protected files. You must first create a Protected Folder and specify those users you want to be authorized to use the files.

- 1 Click **Add Folder** in the PGP NetShare Control Box.

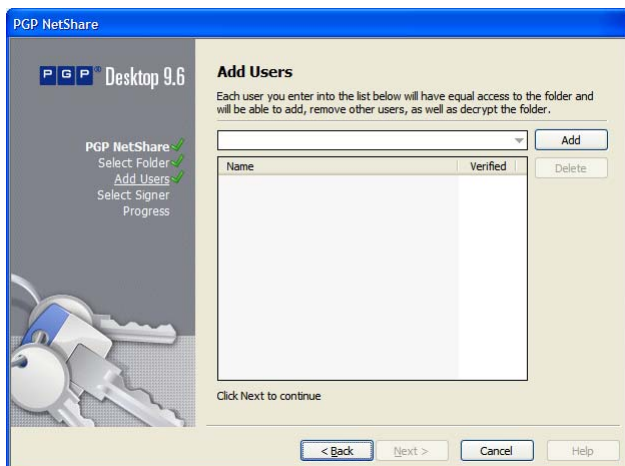


The **Select Folder** screen appears.



- 2 Click **Browse**, then select the folder you want to be the Protected Folder.
- 3 In the **Description** field, enter a description for the Protected Folder you are creating or leave blank to use the default name.
- 4 Click **Next**.

The **Add Users** screen appears.



- 5 To specify authorized users of the files in the Protected Folder, click the down-facing triangle, select a user, then click **Add**.

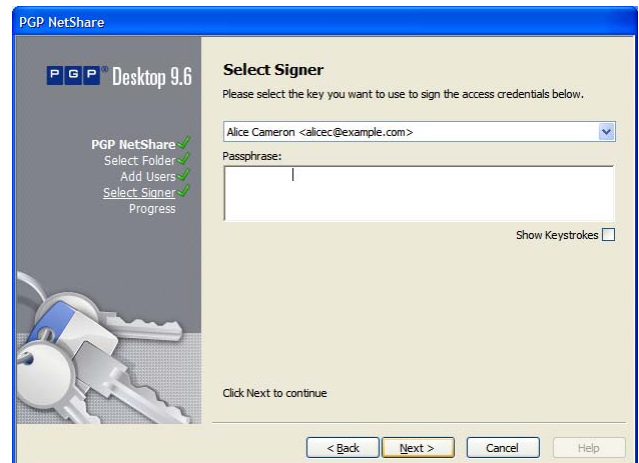
Remember to add yourself if you want to be authorized to access the files in the Protected Folder.



PGP NetShare does not notify authorized users that they can access the protected files; it is the responsibility of the creator of a new Protected Folder to notify authorized users.

- 6 Click **Next**.

The **Select Signer** screen appears.

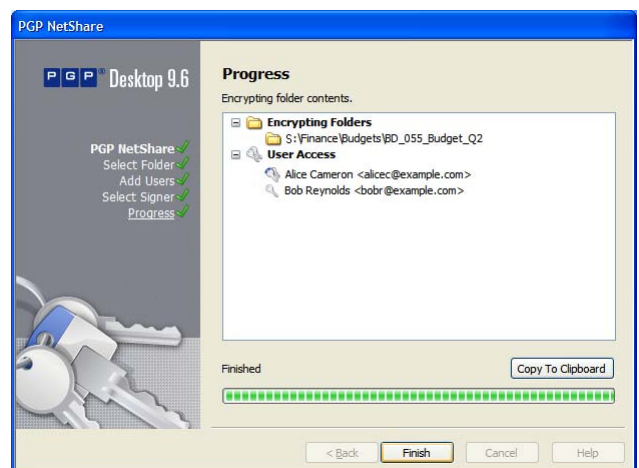


- 7 Select one private key from the private keys on the local keyring and enter the appropriate passphrase (if the passphrase is not cached).

This key will be used to secure the PGP NetShare configuration information for the Protected Folder and the files in it.

- 8 Click **Next**.

The **Progress** screen appears.



The files in the specified Protected Folder are encrypted and the specified users are authorized to use the files.

- 9 Click **Finish**.

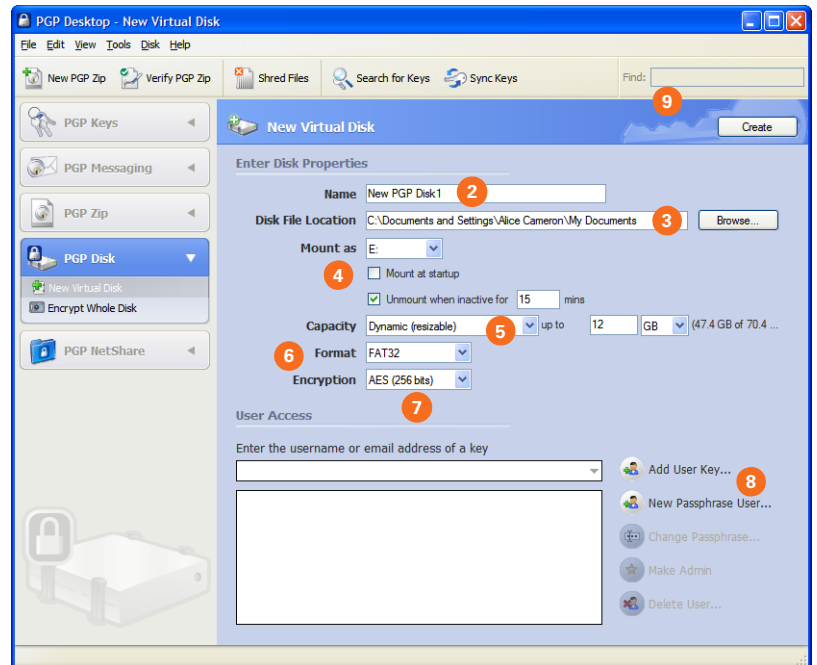
## Creating PGP Virtual Disk Volumes

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.

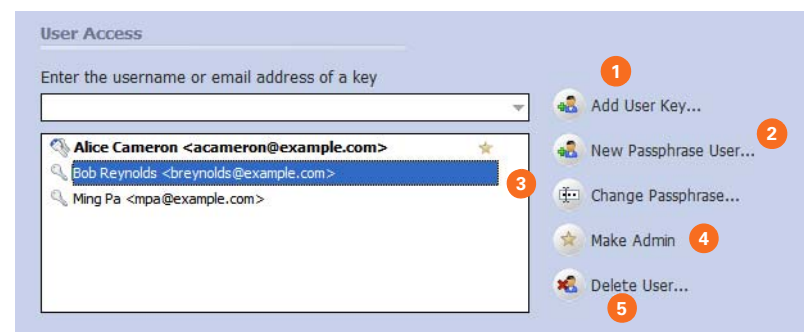


- 2 Type a **Name** for the volume.
- 3 Specify a **Disk File Location** for the volume.
- 4 Select your mount preferences:
  - select a drive letter for the volume to **Mount as**.
  - select **Mount at Startup** to have your new volume mount automatically at startup.
  - select **Unmount when inactive 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.





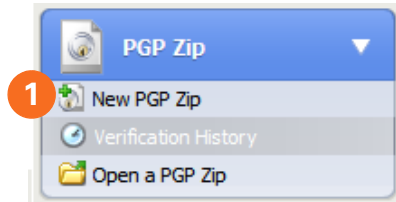
## Creating a PGP Zip Archive

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 NetShare or PGP Desktop for Windows.
- **Passphrase.** Encrypts the archive to a passphrase, which must be communicated to the recipients. Recipients must be using PGP NetShare or PGP Desktop for Windows.
- **PGP Self-Decrypting Archive.** Encrypts the archive to a passphrase, but recipients do *not* need to be using PGP NetShare 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 NetShare 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.

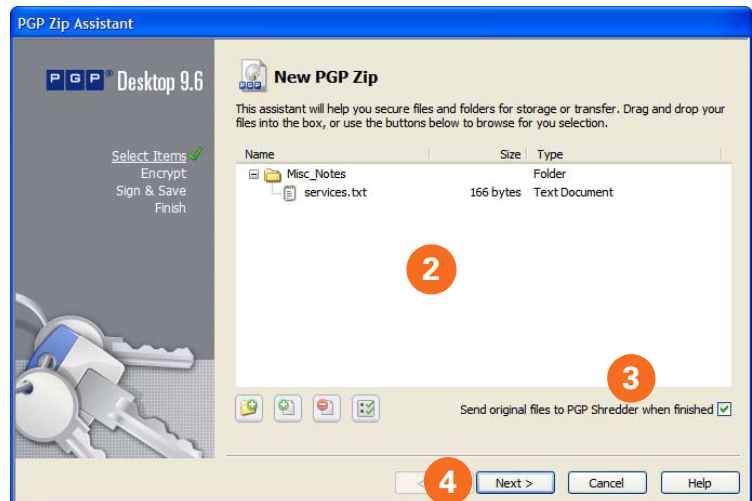
- 1 Click **New PGP Zip** in the PGP Zip Control Box.



- 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**.



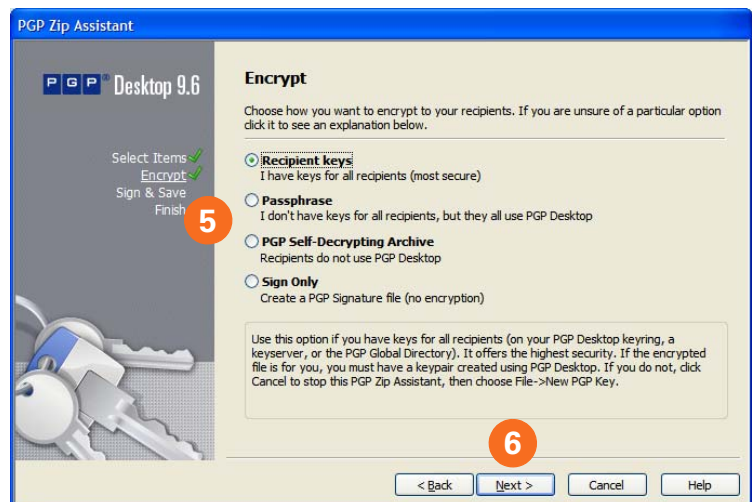
- 5 Select the desired kind of PGP Zip archive:

- **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.

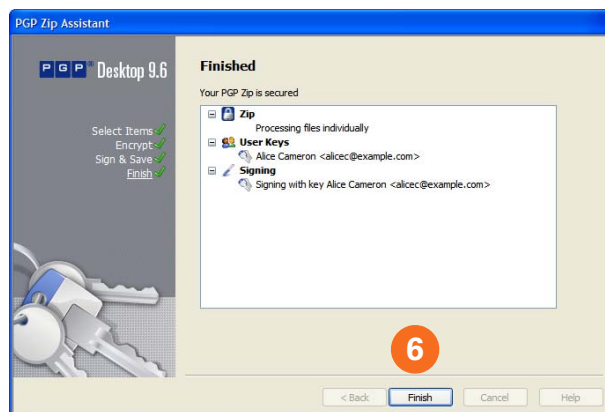
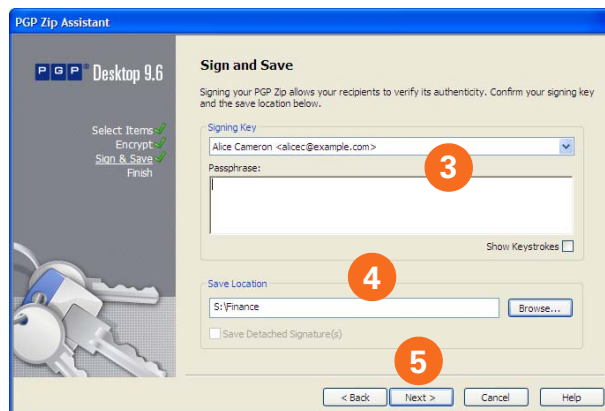
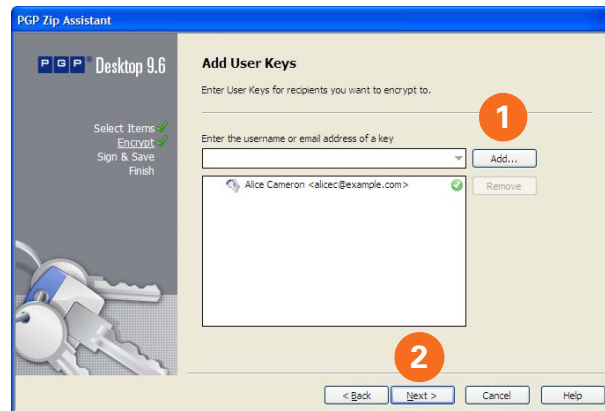
- 6 Click **Finish**.



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.

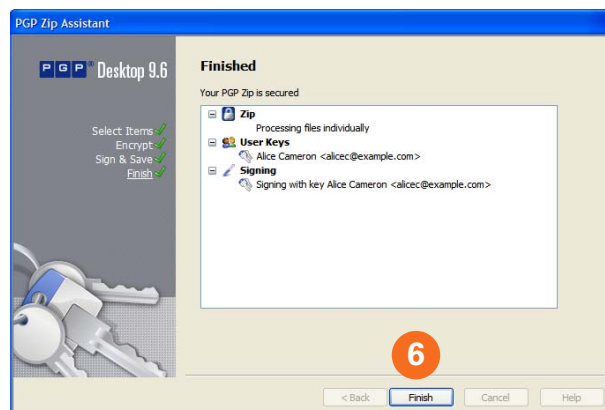
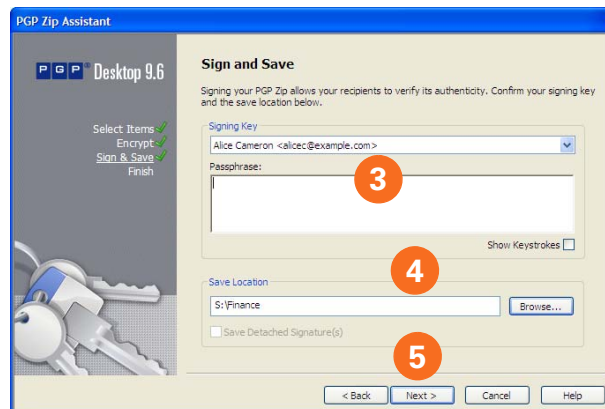
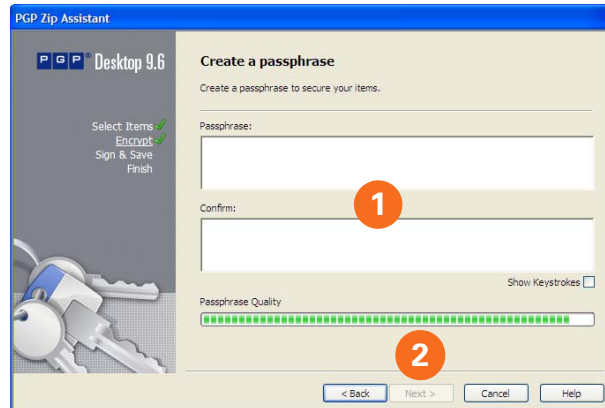
2 Click **Next**.

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:

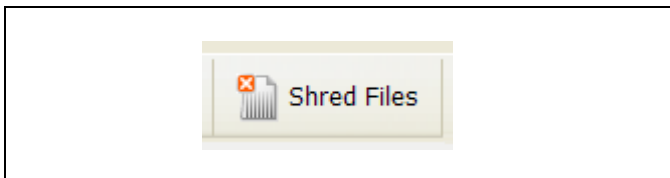
- 1 On your Windows desktop, drag the files and folders you want to shred into the PGP Shredder.  
A dialog appears, asking you to confirm you want to shred the files.
- 2 Click **Yes**.  
The specified files and folders are shredded.



### Using the PGP Toolbar

To shred files using the PGP Toolbar:

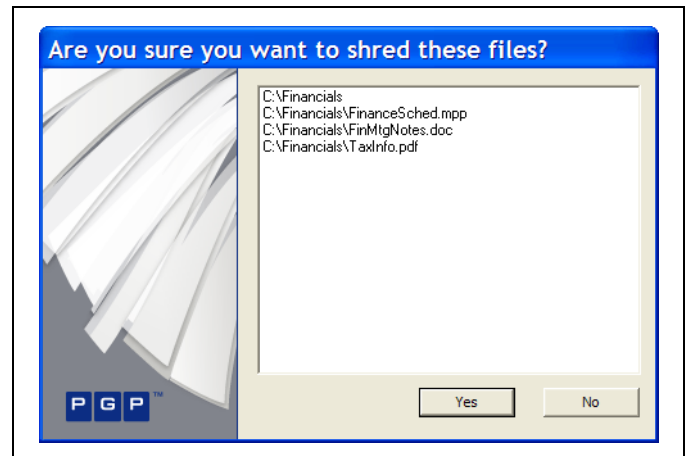
- 1 Click **Shred Files** on the PGP Toolbar.
- 2 Specify which files you want to shred.  
You can Control-click to select multiple files or Control-A to select all files showing.
- 3 Click **Open**.  
A dialog appears, asking you to confirm you want to shred the files.
- 4 Click **Yes**.  
The specified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

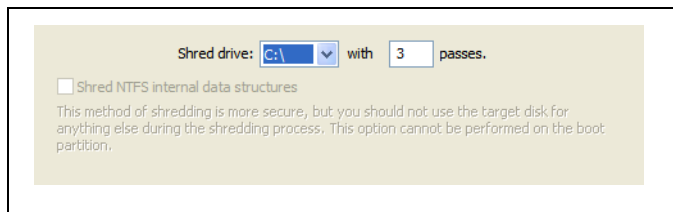
When you put files into the Windows Recycle Bin and empty it, the files are not really deleted; Windows just acts like there is nothing there and eventually overwrites the files. Until those files are overwritten, they are easy for an attacker to recover. PGP Shred Free Space overwrites this “free space”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

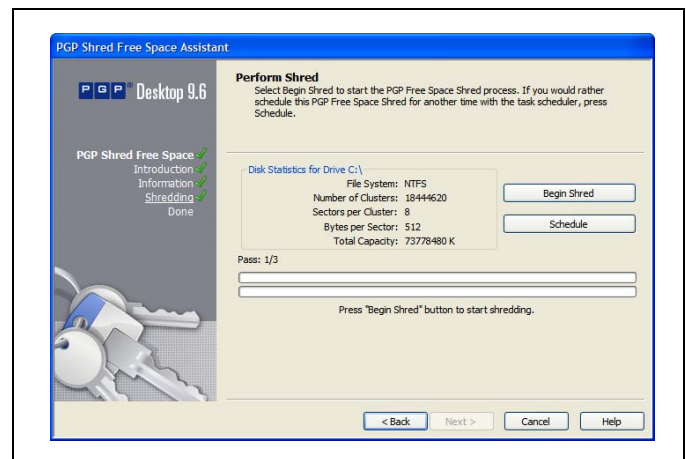
- 3 passes for personal use.
- 10 passes for commercial use.
- 18 passes for military use.
- 49 passes for maximum security.



- 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](https://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](https://www.pgp.com/company/contact.html)**.