PGP Whole Disk Encryption for Windows

Quick Start Guide
Version 10.0

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.

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 Desktop Email 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.

Contents

New to PGP Whole Disk Encryption?

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

- This *Quick Start Guide* helps you install PGP Whole Disk Encryption and get started.
- The *PGP Desktop User's Guide* provides more detailed information on PGP Whole Disk Encryption. 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.

Note: A PGP Whole Disk Encryption license provides you with access to a certain set of PGP Whole Disk Encryption features. Certain other features of PGP Whole Disk Encryption 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 Whole Disk Encryption, see the *PGP Universal Server Administrator's Guide*.

Understanding the Basics

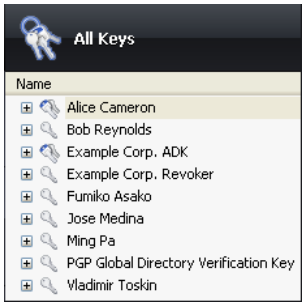
PGP Whole Disk Encryption uses keys to encrypt, sign, decrypt, and verify your messages.

After installation, PGP Whole Disk Encryption 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.



What Am I Installing?

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

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

PGP Whole Disk Encryption (PGP 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 the appropriate passphrase. If you have encrypted a USB device, you can share data on that device with other PGP Whole Disk Encryption for Windows or Mac OS X users.

PGP Virtual Disk volumes uses part of your hard drive space as an encrypted virtual disk volume with its own drive letter. 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 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 Shredder completely destroys files and folders so that even file recovery software cannot recover them. Deleting a file using the Windows Recycle Bin (on Windows systems) or Trash (on Mac OS X systems) 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 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.

System Requirements

- Microsoft Windows 2000 (Service Pack 4),Windows Server 2003 (Service Pack 1 and 2), Windows XP Professional 32-bit (Service Pack 2 or 3), Windows XP Professional 64-bit (Service Pack 2), Windows XP Home Edition (Service Pack 2 or 3), Microsoft Windows XP Tablet PC Edition 2005 (requires attached keyboard), Windows Vista (all 32- and 64-bit editions, including Service Pack 1 and 2), Windows 7 (all 32- and 64-bit editions).

  Note: The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

  PGP Whole Disk Encryption (WDE) is supported on all client versions above as well as the following Windows Server versions:

  - Windows Server 2003 SP 2 (32- and 64-bit editions)
  - Windows Server 2008 SP 1 and 2 (32- and 64-bit editions)
  - Windows Server 2008 R2 (32- and 64-bit editions)

  For additional system requirements and best practices information on using PGP WDE on Windows Server systems, see *PGP KB article 1737* (http://support.pgp.com/?faq=1737).
- 512 MB of RAM
- 64 MB hard disk space

Installing PGP Whole Disk Encryption

PGP Corporation recommends exiting all open applications before you begin the install. The installation process requires a system restart.

Note: If you are using PGP Whole Disk Encryption in a PGP Universal Server-managed environment, your PGP Whole Disk Encryption installer may be configured with specific features and/or settings.

➢ To install PGP Whole Disk Encryption

1. Locate the PGP Whole Disk Encryption installation program you downloaded.

   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 Whole Disk Encryption.

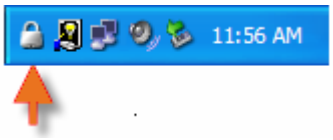
Licensing

To see what features your license supports, open PGP Whole Disk Encryption and select **Help > License**. Those features with a checkmark are supported by the active license.

Starting PGP Whole Disk Encryption

To start PGP Whole Disk Encryption, use any of the following methods:

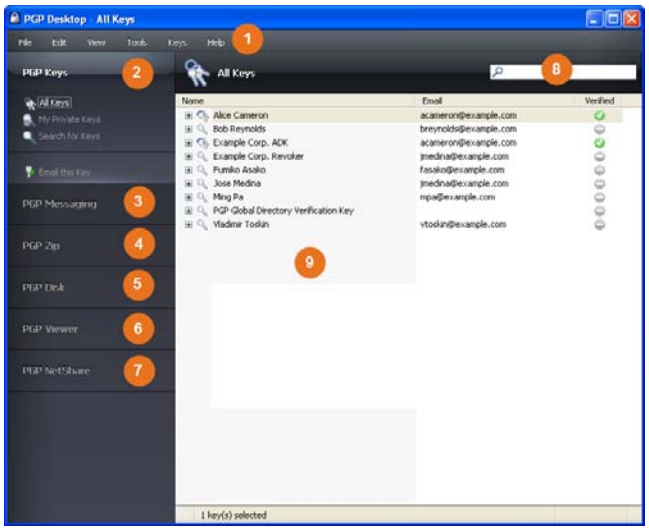
- Double-click the PGP Tray icon.



- Right-click the PGP Tray icon and then select **Open PGP Whole Disk Encryption**.
- From the **Start** menu, select **Programs > PGP > PGP Whole Disk Encryption**.

The PGP Whole Disk Encryption Main Screen

The PGP Whole Disk Encryption application window is your main interface to the product.



The PGP Whole Disk Encryption main screen includes:

1	**The Menu bar**. Gives you access to PGP Whole Disk Encryption commands. The menus on the Menu bar change depending on which Control box is selected.
2	**The PGP Keys Control Box**. Gives you control of PGP keys.
3	**The PGP Messaging Control Box**. Gives you control over PGP Messaging.
4	**The PGP Zip Control Box**. Gives you control of PGP Zip, as well as the PGP Zip Assistant, which helps you create new PGP Zip archives.
5	**The PGP Disk Control Box**. Gives you control of PGP Disk.
6	**The PGP Viewer Control Box**. Gives you the ability to decrypt, verify, and display messages *outside* the mail stream.
7	**The PGP NetShare Control Box**. Gives you control of PGP NetShare.
8	**The PGP Whole Disk Encryption Work area**. Displays information and actions you can take for the selected Control box.
9	**PGP Keys Find box.** Use to search for keys on your keyring. As you type text in this box, PGP Whole Disk Encryption displays search results based on either name or email address.

Each Control box expands to show available options, and collapses to save space (only the Control Box's banner displays). Expand a Control Box by clicking its banner.

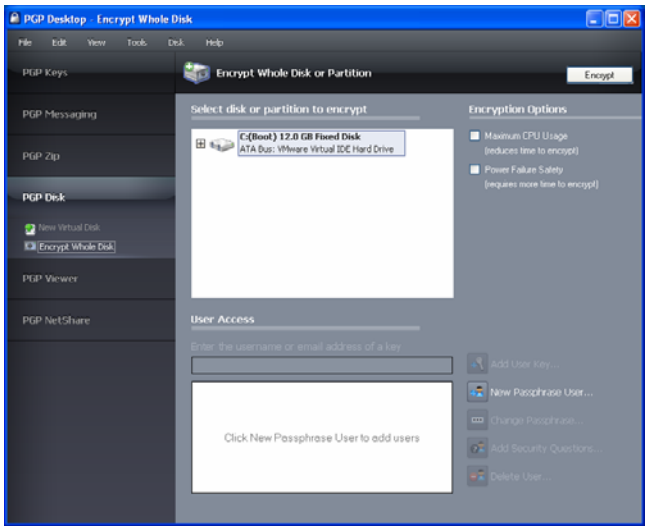
Using PGP WDE to Encrypt a Drive

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

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.

Caution: 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, including if you want to use a USB flash device for two-factor authentication. Follow the instructions displayed in the PGP Disk Assistant dialog boxes.

   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**.

Notes: To encrypt data on floppy disks or CD-RWs, use PGP Virtual Disk volumes; do not use PGP WDE.

You can use the PGP Whole Disk Encryption feature on a dual-boot system, as long as you boot to an operating system supported by PGP WDE (such as Windows XP, Windows 2000, or Windows Vista) and PGP Whole Disk Encryption is installed. Partition mode supports dual-booting with another operating system (such as Linux) as long as you encrypt only your Windows partition. The other operating system must be on another, non-encrypted partition.

Backup software works normally with PGP WDE; any files the software backs up will be decrypted *before* being backed up.

PGP WDE Best Practices

PGP Corporation recommends the following best practices for preparing to encrypt your disk with PGP WDE. 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 are *not* supported. See "Supported Disk Types" in 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. For more information, see *Ensure Disk Health Before Encryption* (page 4).
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 (page 5)* 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* (page 5).
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* (page 5).
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 **Disk > Decrypt** in PGP Whole Disk Encryption, using 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 Whole Disk Encryption software. Once the disk is decrypted, proceed with your recovery activities.
8. **Installing on a Windows Server system**. If you are installing PGP WDE on a Windows Server system, see *PGP KB article 1737* (http://support.pgp.com/?faq=1737) for additional best practices information.

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.

Note: If you are using PGP Whole Disk Encryption in a PGP Universal Server-managed environment, the bad sectors encountered during encryption are logged to the PGP Universal Server and the encryption process continues.

Create a Recovery CD

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

1. Make sure PGP Whole Disk Encryption 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. Select **File > 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 location 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.

Caution: PGP WDE recovery disks are compatible only with the version of PGP Whole Disk Encryption 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 9.7 software, it will render the PGP WDE 9.7 disk inoperable.

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*.

Caution: 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 Whole Disk Encryption Release Notes for the latest updates to this list.

Software that is not compatible:

- Faronics Deep Freeze (any edition)
- Utimaco Safeguard Easy 3.x
- Absolute Software's CompuTrace laptop security and tracking product. PGP Whole Disk Encryption is compatible only with the BIOS configuration of CompuTrace. Using CompuTrace in MBR mode is not compatible.
- Hard disk encryption products from GuardianEdge Technologies: Encryption Anywhere Hard Disk and Encryption Plus Hard Disk products, formerly known as PC Guardian products.

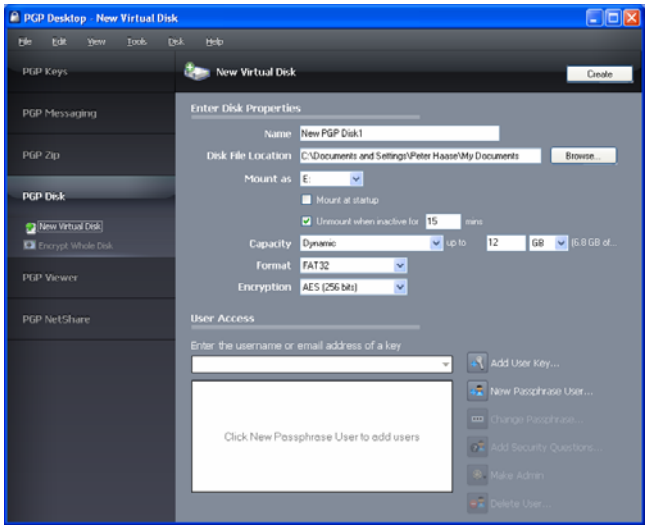
The following programs co-exist with PGP Whole Disk Encryption on the same system, but will block the PGP Whole Disk Encryption feature:

- Safeboot Solo
- SecureStar SCPP

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. To specify your mount preferences, do the following::
   - 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 file system **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.

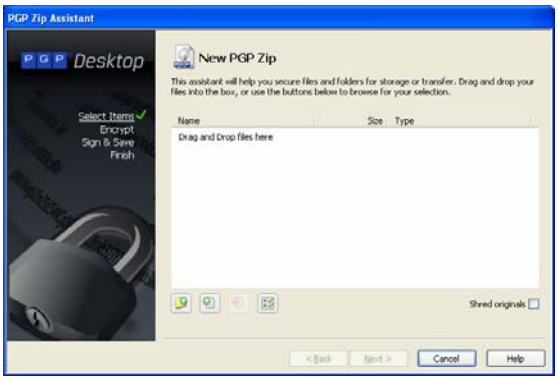
Creating a PGP Zip Archive

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 software (for Windows or Mac OS X).
- **Passphrase**. Encrypts the archive to a passphrase, which must be communicated to the recipients. Recipients must be using PGP software (for Windows or Mac OS X).
- **PGP Self-Decrypting Archive**. Encrypts the archive to a passphrase. Recipients do not need to be using PGP software to open it, but their computer must be running Microsoft Windows. 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 software (for Windows or Mac OS X) 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.

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**.

Note: 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.

Note: 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.

PGP Self-Decrypting Archive

The Create a passphrase screen appears.

1. Type a passphrase for the PGP Zip Self-Decrypting Archive (SDA), then type it again to confirm it.
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**.

Using PGP Shred to Shred 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 shortcut menu.

Shredding Files 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 box appears, asking you to confirm you want to shred the files.
2. Click **Yes**. The specified files and folders are shredded.

Shredding Files Using the PGP Toolbar

➢ To shred files using the PGP Toolbar

1. In the PGP Whole Disk Encryption main application window, select **Tools > Shred Files**. The Open dialog box is displayed.
2. Select the files on your system you want to shred, then click **Open.** A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.
3. Click **Yes.** The files are securely deleted from your system.

Shredding Files Using the PGP Shortcut Menu

➢ To shred files in Windows Explorer

1. In Windows Explorer, right-click files/folders you want to shred. A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.
2. Click **Yes.** The files are securely deleted from your system.

Note: If you do not use the PGP Shredder feature often, you can remove the PGP Shredder icon from your desktop via PGP Options. To do this, select **Tools > Options**, select the Disk tab, deselect the **Place PGP Shredder icon on the desktop** option, and then click **OK**.

Note: 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 box is displayed 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. Open PGP Whole Disk Encryption.
2. Select **Tools > PGP Shred Free Space**.
3. On the Introduction screen, read the information, then click **Next**.
4. On the Gathering Information screen, in the **Shred drive** field, 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.
   - 26 passes for maximum security.
5. 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.
6. On the Perform Shred screen, click **Begin Shred**.

   Note: 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.
7. When the shred session is complete, click **Next**.
8. On the Completing screen, click **Finish**.

Getting Assistance

Contact Information

Contacting Technical Support

- To learn about PGP support options and how to contact PGP Technical Support, please visit the *PGP Corporation Support Home Page* (https://support.pgp.com).
- To access the PGP Support Knowledge Base or request PGP Technical Support, please visit *PGP Support Portal Web Site* (https://support.pgp.com). **Note that you may access portions of the PGP Support Knowledge Base without a support agreement; however, you must have a valid support agreement to request Technical Support.**
- To access the PGP Support forums, please visit *PGP Support* (http://forum.pgp.com). These are user community support forums hosted by PGP Corporation.

Contacting Customer Service

- For help with orders, downloads, and licensing, please visit *PGP Corporation Customer Service* (https://pgp.custhelp.com/app/cshome).

Contacting Other Departments

- For any other contacts at PGP Corporation, please visit the *PGP Contacts Page* (http://www.pgp.com/about_pgp_corporation/contact/index.html).
- For general information about PGP Corporation, please visit the *PGP Web Site* (http://www.pgp.com).

Available Documentation

Prior to installation, complete Product Documentation is available through the *PGP Corporation Support Portal* (https://support.pgp.com).

Unless otherwise noted, online help is installed and is available within the PGP Whole Disk Encryption product. Release notes are also available, which may have last-minute information not found in the product documentation. The users guide and quick start guides, provided as Adobe Acrobat PDF files, are available on the *PGP Corporation Support Portal* (https://support.pgp.com).

Once PGP Whole Disk Encryption is released, additional information regarding the product is entered into the online Knowledge Base available on the *PGP Support Knowledge Base* (https://support.pgp.com/?faq=589).

Copyright and Trademarks