Symantec.

PGP Desktop for Mac OS X

Quick Start Guide
Version 10.2

What is PGP Desktop?

PGP Desktop provides comprehensive security for desktops and laptops, making it possible for enterprises, workgroups, and individuals to protect sensitive information without changing the existing IT infrastructure or disrupting work processes. This award winning, easy-to-use solution encrypts email, files, virtual volumes, and entire disks from a single desktop application.

The PGP Desktop family of applications have been combined into several bundles.

- **PGP Desktop Professional** includes PGP Desktop Email and PGP Whole Disk Encryption
- **PGP Whole Disk Encryption** includes PGP Whole Disk Encryption

PGP Desktop Email

Use PGP Desktop Email to automatically and transparently encrypt, sign, decrypt, and verify email message through policies you defined for you by administrators, or policies you control if you are not part of a PGP Universal Server-managed environment.

PGP Whole Disk Encryption

Use PGP Whole Disk Encryption (PGP WDE) to lock down the entire contents of your system or an external or USB flash drive you specify.

In addition, use PGP Desktop to:

- Use part of your hard drive space as an encrypted virtual disk volume with its own drive letter.
- Create protected Zip archives.
- Completely destroy files and folders so that nothing can recover them.

Contents

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* helps you install PGP Desktop and get started.
- The *PGP Desktop User's Guide* provides more detailed information on PGP Desktop. 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 Desktop 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 Desktop, see the *PGP Universal Server Administrator's Guide.*

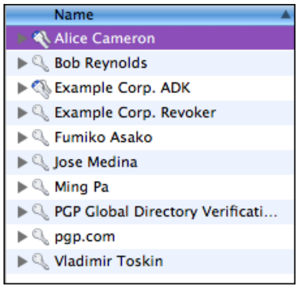
After installation, PGP Desktop prompts you to create a PGP keypair. A keypair is the combination of a private key and a public key.

- 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.



Name
- Alice Cameron
- Bob Reynolds
- Example Corp. ADK
- Example Corp. Revoker
- Fumiko Asako
- Jose Medina
- Ming Pa
- PGP Global Directory Verificati...
- pgp.com
- Vladimir Toskin

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 Desktop Email is a member of the PGP Desktop family of applications. You can use PGP Desktop Email to automatically and transparently encrypt, sign, decrypt, and verify email messages through policies you control. You can also use PGP Desktop Email to encrypt IM sessions for clients such as AIM and iChat. Both users must have PGP Desktop Email enabled.

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.

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

The minimum system requirements to install PGP Desktop on your Mac OS X system are:

- Apple Mac OS X10.5.x, 10.6.x, or 10.7.x (Intel)
- 512 MB of RAM
- 64 MB hard disk space
- PGP Whole Disk Encryption (PGP WDE) is not compatible with any third-party software, other than Apple Boot Camp, that could bypass the PGP WDE protection on the Master Boot Record (MBR) and write to or modify the MBR. Boot Camp needs to modify MBR before installing the Windows OS and cannot be used on a Macintosh system that is already encrypted with PGP WDE. To use Boot Camp with PGP WDE, refer to the installation instructions in the *PGP Desktop for Mac OS X User's Guide*.

PGP Whole Disk Encryption (PGP WDE) is not compatible with any third-party software, other than Apple Boot Camp, that could bypass the PGP WDE protection on the Master Boot Record (MBR) and write to or modify the MBR. Boot Camp needs to modify MBR before installing the Windows OS and cannot be used on a Macintosh system that is already encrypted with PGP WDE. To use Boot Camp with PGP WDE, refer to the installation instructions.

Installing PGP Desktop

Symantec Corporation recommends exiting all open applications before you begin the install. The installation process may require a system restart.

Note: You must have administrative rights on your system in order to install the update.

The PGP Desktop installer walks you through the installation process.

To install PGP Desktop on your Mac OS X system

1 Quit all other applications.

2 Mount the PGP DiskCopy image.

3 Double-click `PGP.pkg`.

4 Follow the on-screen instructions.

5 If prompted to do so, restart your system.

Note: If you are in a domain protected by a PGP Universal Server, your PGP administrator may have preconfigured your PGP Desktop installer with specific features and/or settings. In addition, if your PGP administrator set up silent enrollment, your Windows domain password will be used for all passphrase requirements in PGP Desktop. If specified by policy, PGP Whole Disk Encryption may automatically start to encrypt your disk when your Windows password is entered.

Licensing

To see what features your license supports, open PGP Desktop and select **PGP > License**. Click **Details**. The details of your license are displayed.

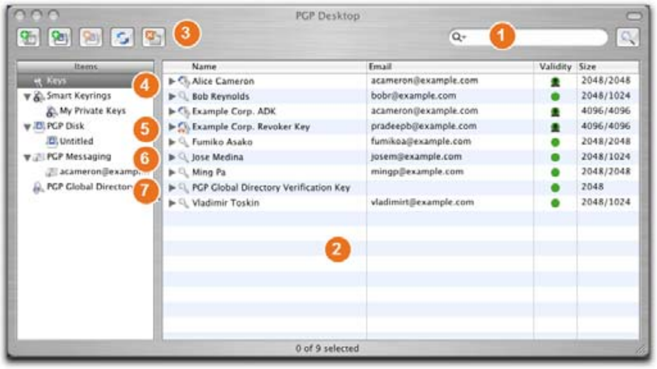
Starting PGP Desktop

There are four main ways to access PGP Desktop:

- PGP Desktop Main Screen
- Using the PGP Desktop Icon in the Menu Bar
- Using the PGP Dock Icon
- Using the Mac OS X Finder

The PGP Desktop Main Screen

The main screen of PGP Desktop is your main interface to the product.



Name	Email	Validity	Size
Alice Cameron	acameron@example.com	●	2048/2048
Bob Reynolds	bobr@example.com	●	2048/1024
Example Corp. ADK	acameron@example.com	●	4096/4096
Example Corp. Revoker Key	pradeepb@example.com	●	4096/4096
Fumiko Asako	fumikoa@example.com	●	2048/2048
Jose Medina	josem@example.com	●	2048/1024
Ming Pa	mingp@example.com	●	2048/2048
PGP Global Directory Verification Key		●	2048
Vladimir Toskin	vladimirt@example.com	●	2048/1024

The PGP Desktop main screen includes:

1 **The search field**. Lets you search for keys on the local keyring. Simply enter characters and the names and email addresses on the local keyring that include those characters will display. Click **Advanced Search** for more search criteria.

2 **The PGP Desktop Work area**. Displays information about and actions you can take for the selected item.

3 **The Toolbar**. Provides access to frequently used features. You can:

- Create a new PGP Zip archive.
- Create a new PGP Virtual Disk.
- Mount an existing PGP Virtual Disk.
- Synchronize keys.
- Shred files.

4 **The Keys item**. Gives you control over the PGP keys that PGP Desktop is managing for you.

5 **The PGP Disk item**. Use this item to view and manage PGP Virtual Disk volumes. Also, you can use this item to create new PGP Virtual Disk volumes, as well as encrypting an entire disk or managing encrypting removable disks using the PGP Whole Disk Encryption feature.

6 **The PGP Messaging item**. Use this item to manage PGP Messaging services. You can also use this item to create new services and policies, and manage existing services and policies.

7 **The Keyservers item**. Use this item to view and manage keyservers.

(not shown) **The PGP Zip item.** Use this item to view and manage PGP Zip archives.

Using PGP Desktop Email

PGP Desktop Email automatically and transparently encrypts and signs outgoing messages and decrypts and verifies incoming messages. All you need to do is to send and receive your email just as you always have; PGP Desktop Email will take care of the rest.

Sending Encrypted Email

After installation, PGP Desktop Email inserts itself between your email client and your mail server and watches your email traffic.

When *incoming* messages arrive, PGP Desktop Email intercepts them before they get to your inbox and automatically attempts to decrypt and verify them; it uses your private keys to decrypt and the public keys of others to verify. When it is done with your messages, PGP Desktop Email delivers them to your inbox.

In most cases, you do not have to do anything special; decrypted incoming messages will appear in your inbox just like any other incoming messages.

When you send *outgoing* messages, PGP Desktop Email intercepts them on the way to your mail server and automatically attempts to encrypt and sign them, based on configured policies.

Again, you do not have to do anything special; just create your messages using your email client and send them—PGP Desktop Email handles everything else.

Details of how PGP Desktop Email transparently handles your incoming and outgoing messaging is found in the following sections.

Incoming Messages

PGP Desktop manages incoming mail messages based on the content of the message. **These scenarios assume standalone PGP Desktop, not in a domain protected by a PGP Universal server** (in which case mail action policies set by your PGP Universal Server administrator can apply):

- **Message not encrypted nor signed.** PGP Desktop does nothing to the content of these messages; it simply passes the message along to your email client.
- **Message encrypted, but not signed.** When PGP Desktop sees a message coming to you that is encrypted, it will attempt to decrypt it for you. To do this, PGP Desktop will check the local keyring for the private key that can decrypt the message. If the private key is not on the local keyring, PGP Desktop will not be able to decrypt it; the message will be passed to your email client still encrypted. If the private key *is* on the local keyring, PGP Desktop will decrypt it immediately if the passphrase for the private key is in memory (cached). If the passphrase is not cached, PGP Desktop will prompt you for the passphrase and decrypt the message when you supply the correct passphrase. Once a message is decrypted, PGP Desktop passes it to your email client.

  If the PGP Desktop messaging proxy is turned off, PGP Desktop will not be able to decrypt incoming encrypted messages; it will pass them along to your email client still encrypted. It is recommended that you leave your messaging proxy on all the time if you expect to be sending and receiving encrypted messages. On is the default setting.
- **Message signed, but not encrypted.** PGP Desktop will search the local keyring for a public key that can be used to verify the signature. If PGP Desktop cannot find the appropriate public key on the local keyring, it will try to search for a keyserver at keys.domain (where **domain** is the domain of the sender of the message), then the *PGP Global Directory* (*https://keyserver.pgp.com*), and finally any other configured keyservers. If PGP Desktop finds the right public key at any of these locations, it verifies the signature (or not, if the signature is bad) and passes the message to your email client annotated with information about the signature—information is also put into the PGP Log. If PGP Desktop cannot find the appropriate public key, it passes the message to your email client unverified.
- **Message encrypted and signed.** PGP Desktop goes through both of the processes described above: first finding the private key to decrypt the message and then finding the public key to verify the signature. However, if a message cannot be decrypted, then it cannot be verified.

If PGP Desktop is unable to either decrypt or verify a message, you might want to consider contacting the sender of the message. If the message could not be decrypted, make sure the sender was using your real public key. If the message could not be verified, ask the sender to publish their key on the PGP Global Directory — older PGP versions or other OpenPGP products can access the web version of this directory at *PGP Global Directory* (*https://keyserver.pgp.com*) , or ask them to send their public key to you directly by email.

Note: PGP Desktop only encrypts by default to keys that are known to be valid. If you did not get a key from the PGP Global Directory, you may need to verify its fingerprint with the owner and sign it for it to be used.

Outgoing Messages

Email messages that you send can be encrypted, signed, both, or neither. Because you probably have different combinations for different recipients or email domains, you need to create policies for all of your outgoing email message possibilities. Once correct policies are in place, your email messages are protected automatically and transparently.

If you are in a PGP Universal Server-managed environment, your PGP Desktop policies are controlled by the policies specified by your PGP Universal Server administrator. Your administrator may also have specified how to handle outgoing email messages if the PGP Universal Server is not available. These policies are called offline (or local) policies.

Default Policies

PGP Desktop Email includes four default policies:

- **Mailing List Admin Requests**. Administrative requests to mailing lists are sent in the clear; that is, not encrypted or signed.
- **Mail List Submissions**. Submissions to mailing lists are sent signed (so they can be authenticated) but not encrypted.
- **Require Encryption: [PGP] Confidential**. Any message flagged as confidential in your email client or containing the text “[PGP]” in the subject line must be encrypted to a valid recipient public key or it will not be sent. This policy gives you a way to easily handle messages that *must* be sent encrypted or not sent at all.
- **Opportunistic Encryption**. Specifies that any message for which a key to encrypt cannot be found should be sent without encryption (in the clear). Having this policy as the last policy in the list ensures that your messages will be sent (unless you flag the message as Confidential), albeit in the clear, even if a key to encrypt it to the recipient cannot be found.

Creating New Policies

PGP Desktop Email includes the ability to create and use new policies in addition to the four default policies. You can create policies based on a wide variety of criteria. If you are using PGP Desktop Email in a PGP Universal Server-managed environment, your messaging policies and other settings may be controlled by your organization’s PGP administrator.

For complete information about how to create and implement messaging policies, see the *PGP Desktop User’s Guide*.

Was My Message Encrypted?

Because PGP Desktop Email does its work automatically and transparently, from time to time you may find yourself wondering, was my message really sent encrypted? The answer is probably yes, but there are ways to make certain.

Notifier Alerts

PGP Desktop Notifier alerts are a feature of PGP Desktop that both tell you what is going on with your messaging and give you control over it.

For example, when you send an encrypted message, the Notifier alert appears in the lower right corner of your screen. It shows:

- Subject.
- Who it is being sent to.
- Keys found for the recipient.
- Status of the message.

To view more information about the message being sent, click **More**. Now you also see:

- What PGP Desktop Email did to the message.
- Who signed the message.

For more information about Notifiers, see the *PGP Desktop User's Guide*.

Note: In a PGP Universal Server-managed environment, your administrator may have specified certain notifications settings (for example, whether notifications are to be displayed or the location of the notifier). In this case, you may not see any notifier messages at all.

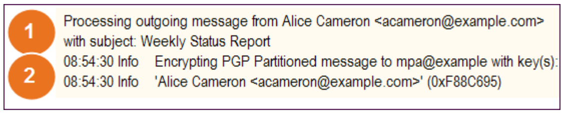
PGP Log

The PGP Log lists a variety of actions that PGP Desktop is taking to secure your messaging.

For example, the message whose Notifiers are shown above generated this entry in the PGP Log. It shows:

1 That an outgoing message was sent, who sent it, and what the subject was.

2 The time it was encrypted, the email address it was encrypted to, and the email address it was sent from.



```
Processing outgoing message from Alice Cameron <acameron@example.com>
with subject: Weekly Status Report
08:54:30 Info    Encrypting PGP Partitioned message to mpa@example with key(s):
08:54:30 Info    'Alice Cameron <acameron@example.com>' (0xF88C695)
```

Using PGP Viewer

In normal usage, PGP Desktop sits between your email client (Mozilla Thunderbird, for example) and your email server so that PGP Desktop can encrypt and sign outgoing messages and decrypt and verify incoming messages. When PGP Desktop is doing this, it is called "in the mail stream."

Use PGP Viewer to decrypt, verify, and display messages *outside* the mail stream.

Opening an Encrypted Email Message or File

Use PGP Viewer to open (decrypt, verify, and display) encrypted message files of the following types:

- **.pgp:** Created by a PGP application.
- **.eml:** Created by Outlook Express or Thunderbird.
- **.emlx:** Created by Apple's Mail.app program on Mac OS X systems.
- **.msg:** Created by Microsoft Outlook.

When PGP Viewer opens an encrypted message, it does *not* overwrite the encrypted text. The original message remains intact.

To decrypt, verify, and display an encrypted message from a file

1 Open PGP Desktop and select the PGP Viewer tab.

2 Click **Open File in PGP Viewer** or select **Viewer > Open File in PGP Viewer**.

3 In the **Open Message File** dialog box, navigate to the file you want to open, select it, then click **Open**. PGP Viewer decrypts, verifies, and displays the message in a separate window.

Note: You can drag and drop the file you want to decrypt onto the portion of the PGP Viewer screen that displays: **Drag Email or Files Here**. PGP Viewer opens the file, decrypts and verifies it, and displays the message.

4 To open another message, click **Open Message** in the toolbar, navigate to the desired file, select it, then click **Open**. PGP Viewer decrypts, verifies, and displays the message.

5 Click **Smaller** to make text smaller or **Bigger** to make text larger.

6 Click **Rich Text** to display the message or file in RTF (rich text format) or **Plain Text** for plaintext.

7 Click **Print** to print the message or file.

Copying Email Messages to Your Inbox

Use PGP Viewer to copy plaintext versions of messages that have been decrypted to the inbox of your email client.

To copy a message to the inbox of your email client

1 With the desired message in the PGP Viewer window, click **Copy to Inbox** .

The **Copy to Inbox** confirmation dialog box is displayed. If you do not want to view this confirmation in the future, select the checkbox to **Don't display this again**.

The **Copy to Inbox** confirmation dialog box displays the name of the email client to which the message will be copied. To change this setting, see PGP Viewer Preferences.

2. Click **OK** to continue.

   If you are copying a message to the Mozilla Thunderbird email client for the first time, a dialog box is displayed advising that you must install an add-on.

3. Click **Yes** to install the add-on and follow the on-screen instructions or click **No**. You must be using Thunderbird 2.0 or greater to install the add-on.

   PGP Viewer opens your email client and copies a plaintext version of the message to the inbox.

Exporting Email Messages

Use PGP Viewer to export a decrypted message to a file.

To export a message from PGP Viewer to a file

1. With the message displayed in the PGP Viewer window, click **Export**.
2. In the **Export Message** dialog box, specify the desired filename, location, and format for the file, then click **Export**.

   PGP Viewer saves the file to the specified location.

Specifying Additional Options

Use the Tools button on the PGP Viewer Toolbar (on the far right) to specify several PGP Viewer features:

- **Text Encoding**: Specify the text encoding format for the message currently being displayed by PGP Viewer.
- **Show Remote Images**: Display external resources (images, CSS style sheets, iframe content, and so on) for the message currently being displayed by PGP Viewer. You can specify that PGP Viewer automatically displays external resources in Preferences.
- **View Message Source**: Display the source of the message currently being displayed by PGP Viewer. Viewing the message source can tell you more information about the message.
- **Preferences**: Display the PGP Viewer Preferences dialog box.

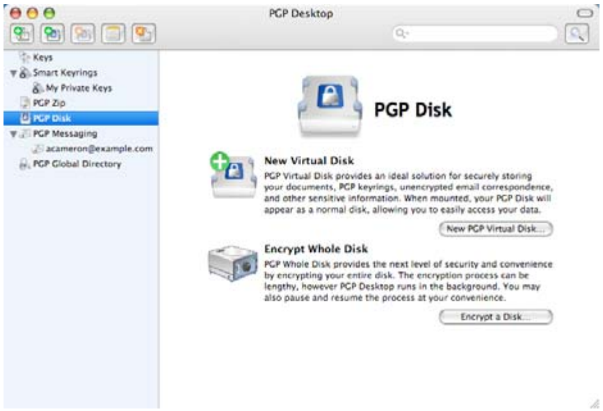
Using PGP WDE to Encrypt a Drive

Use the PGP WDE feature to fully encrypt the boot disk (Intel-based Macintoshes only) and external disks on Mac OS X systems. You can also use it to fully encrypt Windows-formatted external disks.

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.

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

1. Open PGP Desktop and click on the PGP Disk item. The PGP Disk screen is displayed.



PGP Virtual Disk provides an ideal solution for securely storing your documents, PGP keyrings, unencrypted email correspondence, and other sensitive information. When mounted, your PGP Disk will appear as a normal disk, allowing you to easily access your data.

PGP Whole Disk provides the next level of security and convenience by encrypting your entire disk. The encryption process can be lengthy, however PGP Desktop runs in the background. You may also pause and resume the process at your convenience.

2. Click **Encrypt a Disk**. The Encrypt Whole Disk screen is displayed, showing a listing of disks on your system that can be protected.
3. From the **Select a disk** list, select the disk you want to protect.
4. In the **Secure with** section, specify how you want to access your protected disk. Select **Public Key** user or **Passphrase** user.

Note: If you are encrypting a boot disk, you can only use passphrase authentication, so PGP Desktop selects **Passphrase User** for you and skips to the Add PGP Whole Disk User screen.

- To protect your disk with a public key, select **Public Key**, then click **Continue**. The Add PGP Whole Disk User screen is displayed. Select a key from the list, then click **Continue**. The Enter PGP Passphrase dialog box is displayed. Type the passphrase for the key you selected, then click **OK**. The PGP Whole Disk Encryption Summary screen is displayed with a summary of how your disk will be encrypted. This option is only available if you are encrypting a removable disk.
- To protect your disk with a passphrase, select **Passphrase**, then click **Continue.** The Add PGP Whole Disk User screen is displayed. Type a **Name** (or accept the default name), then type the desired passphrase in the **Enter your passphrase** field, and then type it again in the **Confirm your passphrase** field. To see your passphrase as you type, select **Show Keystrokes**. Click **Continue**. The PGP Whole Disk Encryption Summary screen is displayed with a summary of how your disk is will be encrypted.

The Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating by comparing the amount of entropy in the passphrase you type against a true 128-bit random string (the same amount of entropy in an AES128 key). For more information, see The Passphrase Quality Bar (in the *PGP Desktop for Mac OS X User's Guide).*

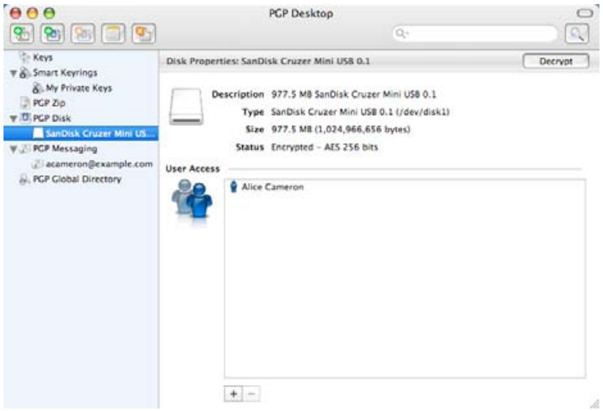
5. Review the information, then click **Encrypt.** The encryption process begins and the Encryption Progress screen is displayed.
6. Click **Close**. The PGP Desktop application window is displayed and the encryption process continues in the background. A bar shows how the encryption process is progressing.

Note: The encryption process continues even if you close the Encryption Progress screen. However, you can not see the progress bar until you close this screen.

7. During the encryption process, you can do the following:
   - To temporarily stop the encryption process, click **Stop**. The Encryption is not complete dialog box is displayed.
   - **Pause** the encryption process, **Decrypt** the portion of the disk that is already encrypted, or **Cancel** to close the dialog box and continue with the encryption process.

Note: If the encryption process stops and PGP Desktop indicates a disk read/write error, it means that PGP Desktop has encountered bad sectors on your disk during the encryption process. Immediately reverse the encryption process by *decrypting* the portion of the disk that has been encrypted. Then use your disk verification tools to find and resolve the problem.

When the encryption process completes, the disk properties for the encrypted disk is displayed.



Disk Properties: SanDisk Cruzer Mini USB 0.1

Description 977.5 MB SanDisk Cruzer Mini USB 0.1
Type SanDisk Cruzer Mini USB 0.1 (/dev/disk1)
Size 977.5 MB (1,024,966,656 bytes)
Status Encrypted – AES 256 bits

PGP WDE Best Practices

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

- **Determine whether your target disk is supported**. See "Supported Disk Types" in the *PGP Desktop User's Guide* for more details on what types of disks are supported.
- **Make sure you use supported characters in your passphrase**. See "Supported Characters" in the *PGP Desktop User's Guide* for more details on what characters are supported for passphrases.
- **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* (on page 7).
- **Back up the disk before you encrypt it**. Before you encrypt your disk, be sure to back it up so that you will not lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk. Also be sure to make regular backups of your disk.
- **Consider the time it will take to encrypt the disk** and prepare accordingly. See *Calculate the Encryption Duration* (on page 8).
- **Run a pilot test to ensure software compatibility**. As a good security practice, Symantec 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. Certain other disk protection software is incompatible with PGP WDE and can cause serious disk problems, up to and including loss of data. See *Run a Pilot Test to Ensure Software Compatibility* (on page 8) for known interoperability issues, and review the *PGP Desktop Release Notes* for the latest updates to this list.
- **Ensure that Sleep mode has been disabled**. PGP Desktop is not compatible with hibernation mode on Mac OS X systems.
- **Using Apple Boot Camp**. If you are using Apple Boot Camp, Symantec Corporation recommends that you perform all encryption and decryption operations from the Mac OS X partition. Be sure that you have installed PGP Desktop on both the Mac OS X and Windows partitions first, before booting into the Mac OS X partition to encrypt or decrypt.

Ensure Disk Health Before Encryption

Symantec 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 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, Symantec Corporation recommends that you start with a healthy disk by correcting any disk errors prior to encrypting.

Note: If you are using PGP Desktop in a managed environment, the bad sectors encountered during encryption are logged to the management server and the encryption process continues.

Best Practices Recommendation

As a best practice, before you attempt to use PGP Desktop to encrypt your disk, 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. These software applications can correct errors that would otherwise disrupt encryption.

If you are using Apple Boot Camp, Symantec Corporation recommends that you perform all encryption and decryption operations from the Mac OS X partition. Be sure that you have installed PGP Desktop on both the Mac OS X and Windows partitions first, before booting into the Mac OS X partition to encrypt or decrypt.

Calculate the Encryption Duration

Encryption is a time-consuming and CPU-intensive process. The larger the disk being encrypted, the longer the encryption process takes. You should consider this as you schedule initial encryption of the disk.

Factors that may affect encryption speed include:

- the size of the disk
- the processor speed and number of processors
- the number of system processes running on the computer
- the number of other applications running on the system
- the amount of processor time those other applications require

With an average system, an 80 GB boot disk takes approximately three hours to encrypt using PGP Desktop (when no other applications are running). A very fast system, on the other hand, can easily encrypt such a disk in less than an hour.

You can still use your system during encryption. Your system is somewhat slower than usual during the encryption process, although it is fully usable.

PGP Desktop automatically slows the encryption process if you are using the system. The encryption process is faster if you avoid using your computer during the initial encryption. The system returns to normal operation when the encryption process is complete.

If you decide to run other applications during the encryption process, those applications will probably run slightly slower than normal until the encryption process is over.

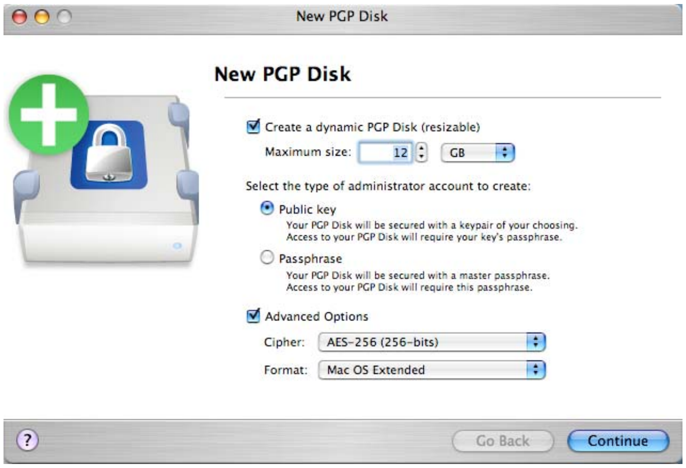
Run a Pilot Test to Ensure Software Compatibility

As a good security practice, Symantec Corporation recommends testing PGP Desktop on a small group of computers to ensure that PGP Desktop is not in conflict with any software on the computer before rolling it out to a large number of computers.

Creating PGP Virtual Disk Volumes

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

8 In PGP Desktop, select the PGP Disk item and then click **New PGP Virtual Disk**.



New PGP Disk

☑ Create a dynamic PGP Disk (resizable)

Maximum size: 12 GB

Select the type of administrator account to create:

● Public key
Your PGP Disk will be secured with a keypair of your choosing.
Access to your PGP Disk will require your key's passphrase.

○ Passphrase
Your PGP Disk will be secured with a master passphrase.
Access to your PGP Disk will require this passphrase.

☑ Advanced Options

Cipher: AES-256 (256-bits)

Format: Mac OS Extended

9 In the **Enter your desired PGP Disk size** field, type the amount of space that you want to reserve for the new PGP Virtual Disk. Use whole numbers, with no decimal places. You can also use the arrows to increase or decrease the number displayed in the field. Choose **KB** (Kilobytes), **MB** (Megabytes), or **GB** (Gigabytes) from the menu.

10 Specify the type of authentication you want to use for the primary user of this PGP Virtual Disk:

- To protect your PGP Virtual Disk with your keypair, select **Public Key**.
- To protect your PGP Virtual Disk with a passphrase, select **Passphrase user**.

11 To view or change the advanced options settings, select the **Advanced Options** checkbox. The **Cipher** and **Format** options are displayed.

Caution: The default **Advanced Options** settings are appropriate for most users. Avoid changing these settings if you are unfamiliar with them.

- From the **Cipher** menu, select the encryption algorithm that you would like to use to protect your

PGP Virtual Disk: **AES-256 (256 bits)** or **CAST5 (128-bits)**. For more information about these encryption algorithms, see The PGP Virtual Disk Encryption Algorithms in the *PGP Desktop for Mac OS X User's Guide*.

- From the **Format** menu, select the disk format that you would like to use with your PGP Virtual Disk:

  MS-DOS. Use if you intend to share this PGP Virtual Disk with someone using PGP Desktop 10.2 for Windows.

  Mac OS Extended. The default format (also the modern Mac OS file-system format); supports large PGP Virtual Disk volumes. The minimum size is 4 MB. The Mac OS Extended format is also called HFS+.

  Mac OS Extended (Journaled). Use if Journaling is enabled on your system. (Journaling causes a copy of everything written to disk to be written a second time in a private area of the file system, making disk recovery easier if necessary.)

  Mac OS Extended (Case-sensitive, Journaled). Use if case-sensitive Journaling is enabled on your system.

  Mac OS Standard. For backwards compatibility with older Mac OS operating systems. The minimum size is 512 KB.

  UNIX File System. Use if you intend to share this PGP Virtual Disk volume with someone using a UNIX file system. The minimum size is 128 KB.

  You can see the format of an existing Mac OS X drive by selecting the drive, then selecting Get Info from the File menu.

12 Click **Continue**.

13 The next step depends on whether you chose public key or passphrase authentication:

- For public key access, the Select a Public Key to Secure Your PGP Disk screen is displayed, displaying the public keys you can use for authenticating to the PGP Virtual Disk that you are creating.

  Select a key from the list, then click **Continue**. You are prompted for the passphrase of the key you selected (unless the passphrase is already cached, in which case this step is skipped).

  Enter the appropriate passphrase, then click **OK**. The Save As dialog box is displayed. Continue with the next step.

- For passphrase access, the Set a Master Passphrase For Your PGP Disk screen is displayed.

  In the **Name** field, type the name that you would like to assign to the primary PGP Virtual Disk user (or administrator).

  In the **Enter your passphrase** field, type the passphrase that you would like to use. The **Passphrase Quality** bar indicates the strength of the passphrase that you have typed. Select the **Show Keystrokes** checkbox to see the characters that you are typing, and if you are certain that no one else can see what you are typing.

  In the **Confirm your passphrase** field, re-type the passphrase that you would like to use. Click **Continue.** The Save As dialog box is displayed. Continue with the next step.

14 Select a file name and location for the PGP Virtual Disk, then click **Save**.

15 Review the information on the PGP Disk Creation Summary screen. When you are finished, click **Create**.

16 The Creating your PGP Virtual Disk screen is displayed, showing you progress as your PGP Virtual Disk is created. Once the disk is created, the Congratulations screen is displayed. Click **Finish**.

17 Your new PGP Virtual Disk is mounted automatically, and information about it is displayed in a Finder window. The name of the disk also is displayed under the **PGP Disk** item.

Creating a PGP Zip Archive

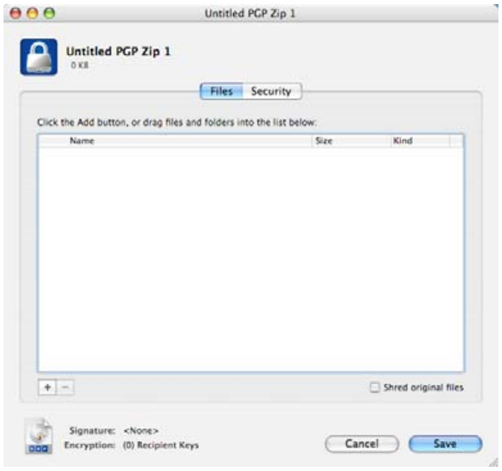
PGP Zip archives let you put any combination of files and folders into a compressed, portable archive. There are three kinds of PGP Zip archives:

- **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).
- **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 Open PGP Desktop and select the PGP Zip item. The PGP Zip dialog box is displayed.

2 Click **Create new PGP Zip**. The Untitled PGP Zip dialog box is displayed.



Click the Add button, or drag files and folders into the list below:

□ Shred original files

Signature: <None>
Encryption: (0) Recipient Keys

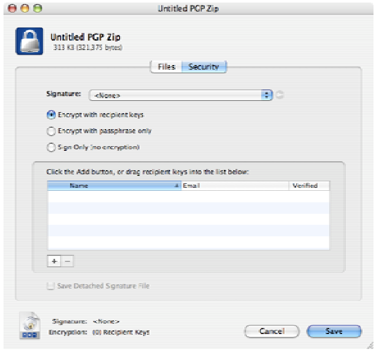
3 In the **Files** tab, specify what files and/or folders you want to be part of the PGP Zip archive you are creating. Do this by:

- Dragging and dropping the files/folders into the list.
- Clicking the plus sign icon below the list, then select the files and/or folders you want to be part of the PGP Zip archive in the dialog box displayed. Click **Add** to add the files to the list.

If you add a file or folder you later decide you do not want, select the file or folder in the list and click the minus sign icon below the list. The file or folder is removed from the list.

4 Select **Shred original files** if you want to securely delete from your system the files/folders you are putting into the PGP Zip archive.

5 When you have specified the files/folder you want included in the PGP Zip archive, click the **Security** tab.



Signature: <None>

● Encrypt with recipient keys
○ Encrypt with passphrase only
○ Sign Only (no encryption)

Click the Add button, or drag recipient keys into the list below:

□ Save Detached Signature File

Signature: <None>
Encryption: (0) Recipient Keys

6 If desired, specify a private key from your keyring to provide a **Signature** for the PGP Zip archive you are creating.

This specified private key is used to digitally sign the PGP Zip archive being created. The recipient(s) can verify who the archive is from by verifying the digital signature using the corresponding public key.

To view the properties of the selected signing key, click the Key icon to the right of the user ID of the key. Close the Key Info dialog box when you are done.

7 Select the type of encryption you want to use:

- **Encrypt with recipient keys**. Use this option to encrypt the PGP Zip archive to the public keys of the recipient(s). This ensures that only those recipient(s) can open the archive.

  If you select public-key encryption, drag and drop the public keys of the recipients onto the list or click the plus sign icon and choose the public keys of the desired recipients.

- **Encrypt with passphrase only**. Use this option to encrypt this PGP Zip archive to a passphrase you specify when saving the archive. Only those persons who know the passphrase can open the archive. Remember that you will need to communicate this passphrase to the person(s) you want to open the PGP Zip archive.

  Enter the passphrase in the **Passphrase** field and then again in the **Confirm** field. If you want to see the passphrase as you type it, select **Show Keystrokes**.

- **Sign Only (no encryption)**. Use this option to create an unencrypted PGP Zip archive. However, because you are not encrypting the PGP Zip archive, you must specify a signing key using the **Signature** field.

8 If you have only one file in your PGP Zip archive and you are signing the file but not encrypting it, create a detached signature file by selecting the **Save Detached Signature File** checkbox.

If you want to create a detached signature file, you can put one file *only* in the archive, you must choose a signing key, and you cannot encrypt the archive.

9 Click **Save**.

10 Specify a file name and a location for the PGP Zip archive, then click **Save**. If you specified a signing key in the **Signature** field, you are prompted for the passphrase to the signing key (if it is not already cached).

11 Enter the appropriate passphrase, then click **OK**. The PGP Zip archive is created in the location you specified.

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 (on Windows systems) or the Trash bin (on Mac OS X systems) 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 Shred menu option in PGP Desktop.
- Using the Finder.

Shredding Files using the PGP Shredder icon

To shred a file or folder using the PGP Shredder icon

1. Locate the file or folder you want to delete securely.
2. Drag the file or folder onto the PGP Shredder icon. 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 **OK**. The file or folder is deleted from your system securely.

Tip: Create an Alias of the PGP Shredder icon on your desktop so you can shred files without having to locate the PGP Shredder icon in the /Applications folder. Then move the Alias to the Desktop (or Dock).

Shredding Files using the Shred Files Icon in the PGP Desktop Toolbar

To shred a file or folder using the PGP Desktop Toolbar

1. Click the **Shred Files** icon in the toolbar.
2. Locate the file or folder you want to Shred, then click **Shred**. 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 **OK**. The file or folder is securely deleted from your system.

Shredding Files using the Shred Command from the File menu

To shred a file or folder using the Shred command

1. Select **File > Shred.**
2. Navigate to the file or folder you want to Shred, then click **Shred**. 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 **OK**. The file or folder is securely deleted from your system.

Shredding Files in the Finder

To shred a file or folder in the Finder

1. In the Finder, locate the file or folder that you want to shred.
2. Ctrl+click the file or folder (or right-click it if you are using a two-button mouse) and select **PGP > Shred.** 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 **OK**. The file or folder is securely deleted from your system.

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level

- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, Africa	semea@symantec.com
North America, Latin America	supportsolutions@symantec.com

Copyright and Trademarks