

# **PWF Hypertext help**

## **MainTable of Contents**

[---PGP WinFront version 3.0 ©1994 Ross Barclay](#)

[---Quick summary of PGP \(Pretty Good Privacy\) ©Phillip Zimmerman](#)

Compiled to hypertext by Jeff Sheets---Xanthur@aol.com  
F1 for context sensitive help on using Windows Help

**Installing**

## Basic Commands

To encrypt a plaintext file with the recipient's public key:

```
pgp -e textfile her_userid
```

To sign a plaintext file with your secret key:

```
pgp -s textfile [-u your_userid]
```

To sign a plaintext file with your secret key, and then encrypt it with the recipient's public key:

```
pgp -es textfile her_userid [-u your_userid]
```

To encrypt a plaintext file with just conventional cryptography, type:

```
pgp -c textfile
```

To decrypt an encrypted file, or to check the signature integrity of a signed file:

```
pgp ciphertextfile [-o plaintextfile]
```

To encrypt a message for any number of multiple recipients:

```
pgp -e textfile userid1 userid2 userid3
```

## **Quick summary of PGP v2.3 commands.**

[Basic Commands](#)

[Key Management Commands](#)

[Esoteric Commands](#)

[Combination Command Options](#)

## Key Management Commands

To generate your own unique public/secret key pair:

```
pgp -kg
```

To add a public or secret key file's contents to your public or secret key ring:

```
pgp -ka keyfile [keyring]
```

To extract (copy) a key from your public or secret key ring:

```
pgp -kx userid keyfile [keyring]
```

or: 

```
pgp -kxa userid keyfile [keyring]
```

To view the contents of your public key ring:

```
pgp -kv[v] [userid] [keyring]
```

To view the "fingerprint" of a public key, to help verify it over the telephone with its owner:

```
pgp -kvc [userid] [keyring]
```

To view the contents and check the certifying signatures of your public key ring:

```
pgp -kc [userid] [keyring]
```

To edit the userid or pass phrase for your secret key:

```
pgp -ke userid [keyring]
```

To edit the trust parameters for a public key:

```
pgp -ke userid [keyring]
```

To remove a key or just a userid from your public key ring:

```
pgp -kr userid [keyring]
```

To sign and certify someone else's public key on your public key ring:

```
pgp -ks her_userid [-u your_userid] [keyring]
```

To remove selected signatures from a userid on a keyring:

```
pgp -krs userid [keyring]
```

To permanently revoke your own key, issuing a key compromise certificate:

```
pgp -kd your_userid
```

To disable or reenable a public key on your own public key ring:

```
pgp -kd userid
```

## **Esoteric Commands**

To decrypt a message and leave the signature on it intact:  
`pgp -d ciphertextfile`

To create a signature certificate that is detached from the document:  
`pgp -sb textfile [-u your_userid]`

To detach a signature certificate from a signed message:  
`pgp -b ciphertextfile`

### **--- Command options that can be used in combination with other command options (sometimes even spelling interesting words!):**

To produce a ciphertext file in ASCII radix-64 format, just add the -a option when encrypting or signing a message or extracting a key:

```
pgp -sea textfile her_userid  
or:  pgp -kxa userid keyfile [keyring]
```

To wipe out the plaintext file after producing the ciphertext file, just add the -w (wipe) option when encrypting or signing a message:

```
pgp -sew message.txt her_userid
```

To specify that a plaintext file contains ASCII text, not binary, and should be converted to recipient's local text line conventions, add the -t (text) option to other options:

```
pgp -seat message.txt her_userid
```

To view the decrypted plaintext output on your screen (like the Unix-style "more" command), without writing it to a file, use the -m (more) option while decrypting:

```
pgp -m ciphertextfile
```

To specify that the recipient's decrypted plaintext will be shown ONLY on her screen and cannot be saved to disk, add the -m option:

```
pgp -steam message.txt her_userid
```

To recover the original plaintext filename while decrypting, add the -p option:

```
pgp -p ciphertextfile
```

To use a Unix-style filter mode, reading from standard input and writing to standard output, add the -f option:

```
pgp -feast her_userid <inputfile >outputfile
```

# **PGP Winfront 3.0**

## **A Windows front end for PGP ©1994 Ross Barclay**

This software is free. All questions, suggestions and comments welcome. If you like this program, send me some e-mail. Send to: RBarclay@TrentU.Ca  
PGP ©Phillip Zimmermann

[Disclaimer](#)

[Overview](#)

[Usage](#)

[\*\*The Main Screen\*\*](#)

[Handling multiple users](#)

[Sample \[PGP WinFront\] Section](#)

## Disclaimer and info

I write and maintain this program in my free time. Please be patient when expecting return mail from me, as I may not be able to answer immediately.

I cannot be responsible for any damage this program causes. You must use it at your own risk

How To Verify The Integrity Of Your Version Of PGP WinFront:

Compare the file PWF.ZIP with the file PWF.SIG. Both of these files will be contained in the zipfile called PWF30.ZIP. If you do not have my key to compare with, please see the section "Using My Mail Access System."

Using My Mail Access System

You can use my mail access system to get my key, get source code for PGP WinFront, register PGP WinFront, and get the PGP FAQ list.

To get my key

- 1) Send me a message with the subject GET KEY. It must read GET KEY and nothing else.
- 2) You may type in a message in the body if necessary, although my automatic mail system will ignore it.

To register for bug fix / update notification:

- 1) Send me a message with the subject REGISTER PWF. It must read REGISTER PWF and nothing else.
- 2) You may type in a message in the body if necessary, although my automatic mail system will ignore it.

To get the source code for PGP WinFront:

- 1) Send me a message with the subject GET SOURCE. It must read GET SOURCE and nothing else.
- 2) You may type in a message in the body if necessary, although my automatic mail system will ignore it.

To get the PGP FAQ List:

- 1) Send me a message with the subject GET FAQ. It must read GET FAQ and nothing else.
- 2) You may type in a message in the body if necessary, although my automatic mail system will ignore it.



## **Installing**

**Upgraders: Version 3.0 has many more features than version 2.0. However, your current WIN.INI entry names will still be valid.**

Run the file Setup.Exe. It will install the program in a directory that you specify. PWF will be able to detect that you are running it for the first time and will take you to the options screen where you can fill out your file paths and options.

## **Overview**

PGP is copyright 1993 by Philip Zimmermann. Philip Zimmermann is not associated with the development of this program in any way. This program makes using PGP from Windows much easier and more convenient. This program requires the file VBRUN300.DLL. It was not included in the distribution because most people already have it and it is quite a large file. You can get this file from many FTP sites, for example, FTP.CICA.INDIANA.EDU. It is called VBRUN300.ZIP. Please do NOT ask me to send you this file as it is too big for my account to hold.

Those of you who use PGP will not have any difficulty figuring out how to use this program. It is hoped that this program will make your PGPing a bit easier.

PWF is a very simple program, yet it has a plethora of features which make it uniquely useful. It was designed from the ground up to make PGP easy to use for beginners, but not to hamper the speed with which expert PGPers use PGP. Play around with the program and read the following notes, and maybe it will be suitable for your needs. It is also very easy to uninstall.

# The Main Screen

There are three sections to the main screen

[The INPUT section \(This is where you specify the input file or location\)](#)

[The OPERATION section \(This is where you perform PGP operations\)](#)

[The BUTTON section \(This is where PWF operations are performed\)](#)

In addition to these three sections, there are two other screens. These are

[The OPTIONS screen \(This is where you can set detailed PWF options\)](#)

[The KEYRING screen \(This is where you can view your PGP keyring\)](#)

## Usage

- 

Simply select the operations you want, for example Encryption and ASCII Armouring on. Then, pick a file from the file section at the top of the dialog. PWF will build the command line parameters for you. This command line parameters are displayed in the edit box directly above the GO button. You may edit these parameters before you press GO. When you press GO, PWF will pass the parameters to your PGP program.

Please read the following notes. They contain information that may make your usage of PWF a bit easier. All of the notes are important and are crucial to getting everything you can out of PWF.

[The Main Screen](#)

## The Input Area

- This is the area above the two selection tabs which read "Files" and "Clipboard". When performing PGP operations, you can either perform them on the contents of a file or the contents of the clipboard. For example, you can encrypt a file or you can take text in the clipboard and encrypt that. When the "Files" tab is selected, you see a list of drives, directories and files. This would be very familiar to Windows users. You can choose a file to operate on by selecting it in the file window. Or, you can type the name of a file in the box immediately above the drive selector. To the right of the drive selector is the Pattern box. You can type a file pattern (ie: "\*.txt") in this box to see only those files which match the pattern. If you double-click on a file, it is run with whatever EXE is associated with it.

If you want to be able to view \*.ASC and \*.PGP files, assign them (using the file manager) to your editor or to a viewer. Then, when you double-click on them, you will be able to see their contents.

If you right-click on the file box or the directory box, the sizes of the boxes will change to allow you a more convenient view of either the files or the directories.

When you click on the "Clipboard" tab, the file list disappears and you will see a note telling you that all subsequent operations will be performed on data in the clipboard. The way that PWF uses clipboard data is very simple. It simply saves the contents of the clipboard to a file and then operates on that file. You can click on "View Clipboard" to open the clipboard to see its contents.

# The OPERATION Area

## Main Tab

•

The operation area has three tabs below it: "Main", "Key Mgmt.", and "Options". The most frequently used and asked-for PGP options are readily available when you click the "Main" tab. You choose what PGP operations you want performed on either the file you have selected or on the data in the clipboard. Depending on your selections, some options will not be available to you. For example, you cannot dump encrypted data to the clipboard unless you have "ASCII Armor" selected. Similarly, you cannot have a Detached Signature unless you first select the "Sign File" option. Most exclusions will be obvious for experienced PGP users, and other exclusions relate to how the "Dump Into Clipboard" option works.

Important Notes about the "Main" Area

--"Comment" is only available with PGP 2.6

--"For:" means "whose key(s) will be used to encrypt this file"

--"Output File" allows you to have PGP redirect the output to a specific file.

## Key Management Tab

•

When you click on the "Key Mgmt." tab, you will be shown a list of key management functions. This allows you to easily perform common key management tasks. However, most of the functionality of this screen has been subsumed into the Key Ring option, which is described later.

Notes about the "Key Mgmt" area

--If you have "Use Pager" selected, PGP will pause by the screen to allow you to read a long list of information.

--When you have "Add New Keys" selected, you need to choose a file from the input area (not the clipboard) which contains the key(s) you want to add.

Prompt For Other Create Names: When you create a new file, you can have PWF ask if you want to use a filename other than the default.

## **Handling Multiple Users**

Often, more than one person will be using PGP on any one computer, and there will be more than one secret key in the keyring. PWF handles this situation well.

Multiple Users: PGP can store a number of secret keys on a keyring. PWF will accommodate this. If you select Multiple Users, PWF will ask you for your name whenever it is loaded, and it will ensure that your key is the one that is used (by passing the `-u` parameter).



## The **BUTTON** Area

Here is a description of what the buttons do:

GO

MOVE

COPY

DELETE

KEYRING

EDITOR

CREATE

DOS

CLEAR

HELP

CHECK SIG

EXIT

## Sample [PGP WinFront] Section

Items followed by SAS are those encryption and decryption options which are stored at the end of a session and then restored at the beginning of the next.

```
[PGP WinFront]
UseCommentSAS=-1
EncryptSAS=-1
DetachedSignatureSAS=0
SignatureSAS=0
ASCIIArmourSAS=-1
ScreenViewingOnlySAS=0
InputFileIsTextSAS=0
WipeInputFileSAS=-1
PagerInKeyModeSAS=-1
OnlyUserSelectsWipe=0
DisplayDecryptedFileOnScreenSAS=0
ClearSignatureSAS=0
TaglineFile=C:\PWF\TAGLINE.TXT
AutomaticallyAddTagline=-1
PromptForPassphrase=0
MultipleUsers=0
LastUser=Ross
PGPProgram=C:\PWF\PGP\PGP.PIF
DOSShellLoader=C:\WINDOWS\DOSPRMPT.PIF
PGPDocPath=c:\pwf\pgp\doc
DefaultStartupDirectory=c:\pwf\
DefaultCreateName=C:\PWF\ROSS.TXT
Editor=C:\WINAPPS\NDW\DESKEDIT.EXE
LoadSelectedIntoEditor=-1
EncryptPattern=*. *
DecryptPattern=*. *
DefaultButtonGO=-1
RefreshDelay=5
PagerInKeyMode=0
CommentText=From Ross Barclay
AutoLoadPwfFiles=-1
ConfirmPassphrase=0
PGPProgramAutoClose=C:\PWF\PGP\AUTOCLS.PIF
AlwaysUseAutoclose=-1
NotefileName=C:\AUTOEXEC.BAT
PromptBeforeOverwrite=0
PromptForOtherCreateNames=0
HighlightPGPCreatedFiles=-1
```

MOVE: This allows you to move the currently selected file to another directory. This will also rename files.

CHECK SIG: When you press this button after having selected a file in the file list box, PWF will pop up another file dialog asking you to select the file which has the detached signature. PWF will then shell to PGP and you will be able to see if the signature matches the file. Irrespective of what your "Always Use Autoclose" setting is, PWF will always select the regular PGP (not autoclose) for performing this operation.

Tagline File: This is the name of a file whose contents you want to be appended at the end of any new file that you create. Usually the tagline displays your name and email address.

Always Use Autoclose PGP: If this option is selected, PWF will always use the AutoClose PGP rather than only using it whenever it isn't being used to decrypt.

Highlight PGP Created Files: When a new file is created by PGP in DOS, you can have PWF select it in the list box so that you can perform further operations (like reading it or moving it) on that file. This will only work if the file that PGP creates is made in the current directory. That is usually the case as long as the PIF file is made properly, and with the "Start-Up Directory" option LEFT BLANK.

KEYRING: This loads the KeyRing Viewer.

PWF will create a special dump (-KVC) of your keyring and place it in a file in your PWF directory. It will read information from this file to allow you to browse your keyring.

When you choose a name from the list, and then click "Add to Recipient / Key List", that name is added to the list. Which list it is added to depends on what option you are using. For example, if you are encrypting a file, it will add the KeyID to the "For:" box. But, if you are in the key management section, it will add it to the "Key:" text box. To refresh the keyring, for example if you have added new keys, press the "Refresh Keyring" button. PWF will make the new dump of the keyring and refresh the lists.

#### Keyring Search

You can search your keyring for a matching substring. Type the substring into the box after you have pressed FIND. The search will begin with the currently selected key. For example, if you have 100 keys in your ring, and the 50th is selected, the FIND function will only search the last 50 keys. To search the entire keyring, select the first key in the ring, and then click FIND. You can search on ANY key characteristic like name, date, bits, email address, etc...

Note: If you go back to the list and remove KeyIDs yourself, the Key Ring Form will not update automatically and it will therefore be inconsistent.



Encrypt Pattern / Decrypt Pattern: (Enc. Pat and Dec. Pat) You can set patterns that PWF will automatically set the File window to when you switch between Encrypt and Decrypt mode. For example, when you encrypt, you can have the pattern set to "\*.txt" but for the decrypt you can set it to "\*.asc". You can always temporarily change the pattern on the main screen by editing the Pattern box.

View Clipboard After Dump: If you have this option selected, after you press GO and you have the "dump into clipboard" option set on the main screen, the clipboard will automatically load so you can see its contents.

EDITOR: Press the EDITOR button to run your editor without any parameters. This is handy for creating quick messages. Remember that the CREATE button makes it easy to type and encrypt text files. The EDITOR button is included so users have increased flexibility in their choice of writing tools.

HELP: This allows you to view the PWF and PGP help files.

Delete Button: If you have a file selected in the file window, pressing the delete button will delete that file. The file is not wiped, just deleted. It would therefore be possible to retrieve that file again using an undelete utility.

DOS: This shells out to DOS.

Pressing the Clear button de-selects all option buttons and clears all fields. This is handy in case you need to type in an esoteric command line, and won't be needing any of your current settings.

# The OPTIONS Screen

Here is a description of what each setting in the option screen does:

**Important: To delete an entry (ie: make it blank) click the RIGHT mouse button over it.**

[PGP Program](#)

[PGP Program \(Autoclose\)](#)

[Startup Directory](#)

[Dos Shell Loader](#)

[Tagline File](#)

[Default Create Name](#)

[Notefile Name](#)

[Go Button is Default](#)

[Only User Can Enable Wipe](#)

[Automatically Add Tagline](#)

[Load Editor With Selected File](#)

[Prompt For Other Create Names](#)

[PWF Uses Pass Phrase](#)

[Always Use Autoclose PGP](#)

[Highlight PGP Created Files](#)

[View Clipboard After Dump](#)

[Encrypt Pattern/Decrypt Pattern](#)

[Multiple Users](#)

[Prompt Before Overwriting file](#)



CREATE: This allows you to create a new file which can then be encrypted. The integrated editor from version 2.0 has been dispensed with as it was too limited. Now, users can use whatever editor they like but still have PWF know what is going on with regards to where the file is located.

COPY: This allows you to copy the currently selected file to another directory.

Prompt Before Overwriting File: When you create a new file, you can choose whether or not be be alerted that you might be overwriting an exisiting file.

GO: this button executes the commands that you see in the Parameter Edit Box. You press GO to make PWF call PGP to perform your PGP operation.

Pressing this button exits and saves all current settings. If you wish to exit without saving your parameters, press ALT-F4 or choose Close from the control menu.

Only User Can Enable Wipe: If this option is selected, PWF will not restore the "WipeFile" option when it reloads nor will it select "Wipe File" when it creates a new file. This is designed so that users don't unwittingly wipe a file when they didn't mean to.

PWF Uses Pass Phrase: If this option is selected, PWF will ask you to type in your pass phrase. Then, it will pass your passphrase to PGP so that you won't have to type it. When you are typing in your password, you can choose to have it request confirmation or not. The confirmation option is saved so that you will need to type the password in twice just to make sure they match. This option was added at the request of a user who routinely used conventional encryption and sometimes typed his password in incorrectly.

Automatically Add Tagline: If this is selected, when a new file is created it will have the contents of the Tagline File in it already. Deselect this if you don't want the tagline file automatically added.



GO Button Is Default: Some users may not want "GO" to be pushed when they press ENTER. Deselect this option if you don't want the GO button to be the default.

DOS Shell Loader: This is the name of `command.com` or your PIF which shells to DOS.

PGP Program: This is where you tell PWF the name of your PGP executable or PGP PIF. It is recommended that you use a PIF file, with the "Start-Up Directory" option LEFT BLANK. You should already have PGP in your PATH. You want to leave "Start-up Directory" blank to ensure that PGP doesn't put files outside of the directory you are currently working in. In addition, if you leave this field blank you can use the "Highligh PGP Created Files Option" described later.

PGP Program (Autoclose): This is where you can define a PIF file with the "Close Window On Exit" option selected. This PIF, which should also have the "Start-Up Directory" option left blank, will be used most of the time. The only time it will not be used is on a Decryption, when you will want to see what is going on after PGP exits. You can make PWF use the AutoClose program all the time by selecting the "Always Use AutoClose PGP" option, described later.

Startup Directory: This is the directory which you want displayed by PWF whenever it loads.

Default Create Name: Whenever you use the "Create" option on the main screen, PWF will create a file with this name. You can set further options relating to this, which are described below.

NoteFile Name: This is the name of a text file which you can load quickly using the "HELP" button. It is designed to be an easy way for you to make quick, easily-referred-to notes relating to your use of PGP (or PWF).

Load Editor With Selected File: If this option is selected, when you click "Editor", the selected file will be loaded into the editor. If this option is not selected, the editor will be loaded without any file.





