



December 2006

PGP[®] Desktop 9.5 for Windows User's Guide

Rest Secured[™]

Version Information

PGP Desktop 9.5 for Windows User's Guide. PGP Desktop version 9.5.2. Released December 2006.

Copyright Information

Copyright © 1991–2006 by PGP Corporation. All Rights Reserved. No part of this document can be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of PGP Corporation.

Trademark Information

"PGP", "Pretty Good Privacy", and the PGP logo are registered trademarks and "Rest Secured" is a trademark of PGP Corporation in the U.S. and other countries. "IDEA" is a trademark of Ascom Tech AG. "Windows" is a registered trademark of Microsoft Corporation. "AOL" is a registered trademark, and "AOL Instant Messenger" is a trademark, of America Online, Inc. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Licensing and Patent Information

The IDEA cryptographic cipher described in U.S. patent number 5,214,703 is licensed from Ascom Tech AG. The CAST encryption algorithm is licensed from Northern Telecom, Ltd. PGP Corporation has secured a license to the patent rights contained in the patent application Serial Number 10/655,563 by The Regents of the University of California, entitled Block Cipher Mode of Operation for Constructing a Wide-blocksize block Cipher from a Conventional Block Cipher. PGP Corporation may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents.

Acknowledgments

The Zip and ZLib compression code in PGP Desktop was created by Mark Adler and Jean-Loup Gailly; the Zip code is used with permission from the free Info-ZIP implementation. The BZip2 compression code in PGP Desktop was created by Julian Seward.

Export Information

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restricts the export and re-export of certain products and technical data.

Limitations

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement provided with the software. The information in this document is subject to change without notice. PGP Corporation does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by PGP Corporation.

About PGP Corporation

PGP Corporation, a global security software company, is the leader in email and data encryption. Based on a unified key management and policy infrastructure, the PGP® Encryption Platform offers the broadest set of integrated applications for enterprise data security. The platform enables organizations to meet current needs and expand as security requirements evolve for email, laptops, desktops, instant messaging, PDAs, network storage, FTP and bulk data transfers, and backups. PGP solutions are used by more than 30,000 enterprises, businesses, and governments worldwide, including 84 percent of the Fortune® 100 and 66 percent of the Fortune® Global 100. As a result, PGP Corporation has earned a global reputation for innovative, standards-based, and trusted solutions. PGP solutions help protect confidential information, secure customer data, achieve regulatory and audit compliance, and safeguard companies' brands and reputations. Contact PGP Corporation at <http://www.pgp.com/> or +1 650 319 9000.

Contents

	Introduction	viii
	Who Should Read This User's Guide	viii
	What's New in This Version of PGP Desktop?	viii
	Using this Guide	xvi
	About PGP Desktop Licensing	xvii
	Getting Assistance	xix
1	PGP Desktop Basics	1
	PGP Desktop Terminology	1
	Using PGP Desktop for the First Time	4
2	Installation	7
	Before You Install	7
	Installing PGP Desktop for Windows	8
	Upgrading the Software	8
	Running the Setup Assistant	9
	Uninstalling PGP Desktop	9
	Moving Your PGP Desktop Installation From One Computer to Another ..	10
3	The PGP Desktop User Interface	13
	Accessing PGP Desktop Features	13
	PGP Desktop Notifier alerts	19
4	Securing Email Messages	25
	How PGP Desktop Secures Email Messages	25
	Services and Policies	27
	Creating a Service and Editing Account Properties	29
	Disabling, Enabling, and Deleting a Service	34
	PGP Desktop and SSL	35
	Multiple Services	37
	Troubleshooting Services	37
	Creating a New Security Policy	39
	Wildcards and Regular Expressions in Policies	44
	Security Policy Information and Examples	44
	Working with the Security Policy List	47
	Key Modes	53
	Viewing the PGP Messaging Log	56

5	Securing Instant Messaging	59
	About PGP Desktop's Instant Messaging Support	59
	Encrypting your IM Sessions	60
6	Protecting Disks with PGP Whole Disk Encryption	63
	About PGP Whole Disk Encryption	63
	Prepare Your Disk for Encryption	64
	Determine the Authentication Method for the Disk	70
	Setting Encryption Options	71
	Encrypting a Disk or Partition	74
	Using a PGP WDE-Encrypted Disk	80
	Using PGP WDE Single Sign-On	83
	Maintaining the Security of Your Disk	86
	Using PGP-WDE in a PGP Universal-Managed Environment	92
	Decrypting a PGP WDE-Encrypted Disk	94
	Special Security Precautions Taken by PGP Desktop	96
7	Using PGP Virtual Disks	99
	About PGP Virtual Disks	99
	Creating a New PGP Virtual Disk	100
	Finding PGP Virtual Disks	103
	Mounting a PGP Virtual Disk	104
	Using a Mounted PGP Virtual Disk	104
	Unmounting a PGP Virtual Disk	104
	Adding Alternate User Accounts to a PGP Virtual Disk	105
	Deleting Alternate User Accounts From a PGP Virtual Disk	106
	Disabling Alternate User Accounts	106
	Toggling Read/Write Statuses	107
	Granting Administrator Status to an Alternate User	107
	Changing User Passphrases	108
	Re-Encrypting PGP Virtual Disks	108
	Deleting PGP Virtual Disks	109
	Maintaining PGP Virtual Disks	110
	About PGP Virtual Disk Volumes	111
	The PGP Virtual Disk Encryption Algorithms	112
	Special Security Precautions Taken by PGP Virtual Disk	112
8	PGP NetShare	115
	About PGP NetShare	115
	Licensing PGP NetShare	117

	Authorized User Keys	118
	Establishing a PGP NetShare Coordinator	119
	Working with Protected Folders	119
	Working with Authorized Users	131
	Importing PGP NetShare Access Lists.	135
	Working with Active Directory Groups.	136
	Removing a Folder	137
	Re-Encrypting a Folder	138
	Clearing a Passphrase	139
	Protecting Files Outside of a Protected Folder	140
	Accessing PGP NetShare Features using the Context Menu	141
	PGP NetShare in a PGP Universal-Managed Environment	142
	The Properties Tab.	143
	PGP Desktop Menus	144
9	PGP Zip	147
	About PGP Zip	147
	Creating PGP Zip Archives	148
	Opening a PGP Zip SDA.	167
	Verifying Signed PGP Zip Archives	168
	Opening and Editing a PGP Zip Archive	169
10	PGP Keys	173
	Viewing Keys	173
	Creating a Keypair	174
	Protecting Your Private Key	177
	Distributing Your Public Key.	178
	Getting the Public Keys of Others	180
	Working with Keyservers.	182
11	Managing PGP Keys	183
	Examining and Setting Key Properties	183
	Adding and Removing Photographic IDs	188
	Adding a New User Name and Email Address to a Key.	189
	Importing Keys and X.509 Certificates.	190
	Changing Your Passphrase	191
	Deleting Keys, User IDs, and Signatures	192
	Disabling and Enabling Public Keys	192
	Verifying a Public Key.	193
	Signing a Public Key.	194
	Granting Trust for Key Validations	195

	Working with Subkeys	196
	Working with ADKs	200
	Working with Revokers	201
	Splitting and Rejoining Keys	203
	PGP Key Reconstruction	205
	Protecting Your Keys	207
12	PGP Shred	209
	About Shredding Data with PGP Shred	209
	Using PGP Shredder to Permanently Delete Files and Folders	209
	Using the PGP Shred Free Space Assistant	210
	Scheduling Free Space Shredding	212
13	Storing Keys on Smartcards and Tokens	215
	About Smartcards and Tokens	215
	Supported Smartcards	216
	Recognizing Smartcards	217
	Examining Smartcard Properties	218
	Generating a PGP Keypair on a Smartcard	218
	Copying your Public Key from a Smartcard to a Keyring	220
	Wiping Keys from Your Smartcard	220
	Copying a Keypair from Your Keyring to a Smartcard	221
	Using Multiple Smartcards	223
	Special-Use Tokens	223
A	Setting PGP Desktop Options	227
	Accessing the PGP Options dialog box	227
	General Options	228
	Keys Options	229
	Master Keys Options	233
	Messaging Options	234
	PGP NetShare Options	241
	Disk Options	242
	Notifier Options	243
	Advanced Options	245
B	Passwords and Passphrases	249
	Passwords and Passphrases	249
	The Passphrase Quality Bar	250
	Creating Strong Passphrases	251

C	PGP Desktop and PGP Universal.	253
	Overview	253
	For PGP Administrators	254
D	Messaging with Lotus Notes and MAPI.	255
	About Lotus Notes and MAPI Support	255
	Using PGP Desktop with Lotus Notes	255
	Binding to a Universal Server.	256
	Notes IDs.	258
	Notes Client Settings	258
	Glossary.	259
	Index.	267

Introduction

The *PGP Desktop for Windows User's Guide* explains how to use PGP Desktop for Windows, a software product from PGP Corporation that uses encryption to protect data while it is on your system and while it is in transit.

This section contains the following information:

- [“Who Should Read This User's Guide”](#)
- [“What's New in This Version of PGP Desktop?”](#)
- [“Using this Guide”](#) on page xvi
- [“About PGP Desktop Licensing”](#) on page xvii
- [“Getting Assistance”](#) on page xix

Who Should Read This User's Guide

This Guide is for anyone who is going to be using the PGP Desktop for Windows software to protect their data.



If you are new to cryptography and would like an overview of the terminology and concepts in PGP Desktop, please refer to *An Introduction to Cryptography* (it was installed onto your computer when you installed PGP Desktop).

What's New in This Version of PGP Desktop?

This release of PGP Desktop for Windows introduces the following new features:

- [“PGP NetShare”](#) on page ix
- [“PGP Whole Disk Encryption - Single Sign-On”](#) on page ix
- [“PGP Whole Disk Encryption - Partition Encryption”](#) on page x
- [“PGP Whole Disk Encryption - Enhancements”](#) on page x
- [“PGP Virtual Disk - Resizable Virtual Disks”](#) on page xi
- [“PGP Messaging Policy Enhancements”](#) on page xi
- [“PGP Universal Server HTTPS Proxy Support”](#) on page xii
- [“Notifiers”](#) on page xii
- [“Network Key and Group Selection”](#) on page xiii

- [“Mailing List Expansion” on page xiii](#)
- [“Full S/MIME Support for Outlook MAPI and Lotus Notes” on page xiii](#)
- [“PGP Universal Migration” on page xiv](#)
- [“PGP Universal Server Messaging Policy” on page xiv](#)
- [“International Character Support Enhancements” on page xiv](#)
- [“Signing Subkeys” on page xiv](#)
- [“Bundle Keys” on page xv](#)
- [“Support for Windows Remote Desktop \(Terminal Services\)” on page xv](#)
- [“FIPS 140-2 Integrity Checking” on page xv](#)
- [“FIPS 186-3 \(Read Only\)” on page xvi](#)

PGP NetShare

Changes in this release

PGP NetShare is a new feature that introduces on-the-fly encryption and decryption of files and folders, whether stored locally or on network volumes. Featuring integration with Active Directory via PGP Universal, PGP NetShare allows groups of users to work together on secure documents.

Benefits

PGP NetShare enables users in disparate locations or groups, for example, to share encrypted files in a single location. Teams can read and write files in a common project folder at the same time. This enables groups to work securely, and provides secure collaboration.

Where to find

Check to make sure your license supports PGP NetShare:

- 1 Open PGP Desktop.
- 2 From the **Help** menu, select **License**. If you see a green checkmark by PGP NetShare, your license supports its use.

To access PGP NetShare, click the PGP NetShare Control box.

Click **Add Folder** to add a protected folder, and click **Add User** to authorize users to enable them to use the protected data.

For more information

See [“About PGP NetShare” on page 115](#).

PGP Whole Disk Encryption - Single Sign-On

Changes in this release

Single Sign-On (SSO) allows you to synchronize your Windows password with your PGP Whole Disk Encryption passphrase. Then, at boot time, the PGP Whole Disk Encryption Single Sign-On feature automatically logs in to the Windows session for you.

Benefits

Single Sign-On allows you to use your existing Windows passphrase to both authenticate to your PGP WDE-encrypted drive and automatically log you into Windows.

Where to find

Check to make sure your license supports PGP WDE:

- 1 Open PGP Desktop.
- 2 From the **Help** menu, select **License**. If you see a green checkmark by PGP Whole Disk Encryption, your license supports its use.

To use Single Sign-On: When encrypting your disk, select **Use Windows Passphrase**, and PGP WDE will use your Windows password when encrypting the disk.

For more information

See [“Passphrase and Single Sign-On Authentication”](#) on page 70.

PGP Whole Disk Encryption - Partition Encryption

Changes in this release

Partition Encryption enables PGP Whole Disk Encryption to encrypt select partitions of your disks, instead of the entire disk.

Benefits

This feature provides compatibility with multi-partition disks that have data or other operating systems on them. It also allows the laptop recovery partitions commonly used on recent laptops to be unaffected.

Where to find

Check to make sure your license supports PGP Whole Disk Encryption:

- 1 Open PGP Desktop.
- 2 From the **Help** menu, select **License**. If you see a green checkmark by PGP Whole Disk Encryption, your license supports its use.

To access PGP Whole Disk Encryption, click the PGP Disk Control box.

Click **Add Folder** to add a protected folder, and click **Add User** to authorize users to enable them to use the protected data.

For more information

See [“Encrypting a Disk or Partition”](#) on page 74.

PGP Whole Disk Encryption - Enhancements

Changes in this release

Significant performance enhancements have been made to all aspects of the underlying PGP Whole Disk Encryption infrastructure. The PGP Whole Disk Encryption feature also has been enhanced in this release to provide additional options for enhanced power failure safety choices and initial encryption speed.

Benefits

WDE now offers journaled initial encryption of disks to ensure recovery even if a power failure or serious system event occurs during the initial encryption. You can also choose to reduce the time of initial encryption by increasing use of system resources. All WDE operations, including general disk usage, are significantly faster in this release.

Where to find

Check to make sure your license supports PGP Whole Disk Encryption:

- 1 Open PGP Desktop.
- 2 From the **Help** menu, select **License**. If you see a green checkmark by PGP Whole Disk Encryption, your license supports its use.

To access PGP Whole Disk Encryption, click the PGP Disk Control box.

For more information

See ["About PGP Whole Disk Encryption"](#) on page 63.

PGP Virtual Disk - Resizable Virtual Disks

Changes in this release

Resizable Virtual Disks now automatically expand to fit their contents. A PGP Virtual Disk can automatically expand as files are copied to it to the maximum size of the physical media on which the disk file resides. A PGP Virtual Disk can also be compacted down to the minimum size of the enclosed files.

Benefits

You can now use PGP Virtual Disk without worrying about running out of space on the Virtual Disk before your physical disk is full.

Where to find

Open PGP Desktop and click the PGP Disk Control box.

For more information

See ["Creating a New PGP Virtual Disk"](#) on page 100.

PGP Messaging Policy Enhancements

Changes in this release

This release provides the following new policies in the Messaging Policy Editor:

- **Send Signed** policy action has been added to support signing messages without encryption, even when a key is found.
- **Message Size** policies are now available to execute actions based on whether a message is greater than or less than specific sizes.
- **Search keys.domain and** policy has been added to allow implicit keys.domain lookup prior to searching any of the configured keyservers. This is now configured in all default policies.

For PGP Universal-managed environments, this release now allows the local keyring to be used for key lookups. The local keyring is queried when this option is on before all other key sources.

Benefits

Unmanaged users continue to have full control over their messaging policy, with additional granular control over how and when to apply encryption policy. In managed environments, messaging policies can be centrally configured and distributed across an organization.

Where to find

Check to make sure your license supports PGP Messaging:

- 1 Open PGP Desktop.
- 2 From the **Help** menu, select **License**. If you see a green checkmark by PGP Messaging, your license supports its use.

To access PGP Messaging, click the PGP Messaging Control box.

Click **New Policy** to create a new policy.

For more information

See "[Services and Policies](#)" on page 27.

PGP Universal Server HTTPS Proxy Support

Changes in this release

This feature enables policy connections from the client to PGP Universal through HTTPS proxies.

Benefits

In a PGP Universal-managed environment, this feature allows an administrator to configure the proxy settings used by PGP Desktop for the purpose of connecting to the PGP Universal server.

Notifiers

Changes in this release

The Notifier feature displays the results of all automated key lookup operations and conveys exactly how an outgoing message will be sent to each recipient, enabling you to decide whether or not to send the message. The Notifier fades into view in a user-selected screen corner whenever a message is sent. Inbound messages also show notifications, including details about the signature on the message.

Other functions such as PGP Whole Disk and PGP NetShare are also fully integrated with the Notifier to provide a view into the actions taken by PGP Desktop.

Benefits

Notifiers for PGP Messaging describe exactly how a message is being processed: which messages are encrypted, which go out in the clear, and so on, according to the defined mail policy. In environments where mail policy allows messages to be sent in the clear, this feature also provides the option to prevent a message from being sent unencrypted if a recipient's key is not found.

Where to find

- 1 Open PGP Desktop, and then from the **Tools** menu, select **PGP Options**.
- 2 Click the Notifier tab.

For more information

See [“Notifier Options”](#) on page 243.

Network Key and Group Selection

Changes in this release

Network Key and Group Selection for PGP Zip, PGP Whole Disk, PGP Virtual Disk, and PGP NetShare has been completely redesigned to support selection of keys from all local keyrings, smart keyrings, and key servers. Additionally, this new interface fully integrates with LDAP directories on both Windows and Mac OS X, enabling selection of groups or mailing lists—when configured for policy synchronization with PGP Universal 2.5.

Benefits

This provides easy encryption of files, messages, and disks to defined groups in your enterprise directory.

Where to find

To encrypt to a group of users:

- 1 When selecting users' keys for encryption, Click **Add...**
- 2 Click the button representing your key server.
- 3 Search for and choose a group.

For more information

See [“Encrypting to Recipient Keys”](#) on page 151.

Mailing List Expansion

Changes in this release

In Active Directory environments, PGP Desktop automatically expands each mailing list to list all individual recipients for encryption, enabling creation of secured mailing lists when PGP Desktop is configured for policy synchronization with both PGP Universal Server 2.5 and a configured directory server.

Benefits

Allows end-to-end encryption of content to individual recipients who are part of a distribution list.

Full S/MIME Support for Outlook MAPI and Lotus Notes

Changes in this release

Full S/MIME support has been added to the Outlook MAPI and Lotus Notes messaging components. All supported environments now include full support for S/MIME encryption, decryption, and signing.

Benefits

Ensures end-to-end encryption and S/MIME interoperability in environments using MAPI or Lotus Notes.

PGP Universal Migration

Changes in this release

PGP Universal Migration allows PGP Desktop software stamped from PGP Universal Server to be installed on top of an unstamped installation of PGP Desktop; this stamped version of PGP Desktop will reset the policies and bind the existing installation to the policies set on the Server.

Benefits

This enables easy migration from a standalone deployment of PGP Desktop to a managed deployment of PGP Desktop. This is especially useful in environments using PGP WDE-encrypted drives, as moving to a managed environment previously required decryption and then re-encryption of users' PGP WDE-encrypted disks.

PGP Universal Server Messaging Policy

Changes in this release

PGP Universal Server Messaging Policy extends PGP Desktop messaging policy to support the new PGP Universal 2.5 content filtering system.

Benefits

In PGP Universal-managed environments, a PGP administrator can control when and how email encryption is applied by PGP Desktop, enabling centralized control and enforcement of your organization's security policy.

International Character Support Enhancements

Changes in this release

International character support in messages has been enhanced significantly in this release.

Benefits

Ensures interoperability with international message encoding standards and international character sets.

Signing Subkeys

Changes in this release

Signing Subkeys treats your master key as a subkey authorizer, to authorize sets of signing and encryption subkeys over time.

Benefits

This mode helps to ensure compliance with local laws and corporate policies in some areas requiring that signing keys must not leave the control of the end user while ensuring that encryption keys can be escrowed.

Where to find

- 1 Open PGP Desktop, click the PGP Keys control box, then click **All Keys**.
- 2 Right-clicking on a key, then select **Key Properties** from the context menu.
- 3 Click the **Subkeys** heading in the Key Properties dialog.

For more information

See [“Viewing Subkeys”](#) on page 198.

Bundle Keys

Changes in this release

Bundle Keys allows you to import multiple X.509 certificates, including those on smartcards, as subkeys onto a new PGP key so as to retain the integrated identity inherent in such certificate collections. Additionally, X.509 certificates can be imported from PKCS 12 or PFX files as subkeys of existing PGP keys. Export as certificates is also supported.

Benefits

This feature provides greater support for X.509 certificates with PGP Desktop.

Support for Windows Remote Desktop (Terminal Services)

Changes in this release

PGP Desktop supports typical CITRIX / TS usage. Some functionality—such as starting encryption of a disk with PGP Whole Disk—is explicitly prevented when you are logged in over a Terminal Services connection.

Benefits

In environments where organizations use virtual desktops to enable remote access, PGP Desktop is now compatible with those environments for mail encryption, and for other select functionality.

For more information

See the PGP Desktop Release Notes, which are installed with the software, for information on what features are supported in a CITRIX / TS environment.

FIPS 140-2 Integrity Checking

Changes in this release

FIPS 140-2 Integrity Checking provides a comprehensive test suite used to verify the PGP SDK for NIST FIPS validation that can now be executed whenever PGP Desktop starts up.

Benefits

This test suite verifies PGP Corporation's signatures on each PGP SDK binary and verifies the algorithmic integrity of each FIPS-validated cipher and public key algorithm. This activates the FIPS power-up and operational self-tests to ensure the integrity of cryptographic operations in accordance with FIPS standards.

Where to find

From the **Tools** menu, select **PGP Options**, and then click **Advanced**.

For more information

See [“Advanced Options”](#) on page 245.

FIPS 186-3 (Read Only)

Changes in this release	This feature provides support for verification of signatures from the newly defined DSA key sizes of 2048 and 3072.
Benefits	This feature provides support for emerging standards.

Using this Guide

This Guide provides information on configuring and using the components within PGP Desktop. Each chapter of the guide is devoted to one of the components of PGP Desktop.

“Managed” versus “Unmanaged” Users


A PGP Universal Server can be used to control the policies and settings used by components of PGP Desktop. This is often the case in enterprises using PGP software. PGP Desktop users in this configuration are known as *managed* users, because the settings and policies available in their PGP Desktop software are pre-configured by a PGP administrator and managed using a PGP Universal Server. If you are part of a managed environment, your company may have specific usage requirements. For example, managed users may or may not be allowed to send plaintext email, or may be required to encrypt their disk with PGP Whole Disk Encryption.


Users not under the control of a PGP Universal Server are called *unmanaged* or *standalone* users.


This Guide describe how PGP Desktop works in both situations; however, managed users may discover while working with the product that some of the settings described in this document are not available in their environments. See [“Appendix C, PGP Desktop and PGP Universal”](#) for more information.

Symbols Used in This Guide

Notes, Cautions, and Warnings are used in the following ways.

 Notes are extra, but important, information. A Note calls your attention to important aspects of the product. You will be able to use the product better if you read the Notes.

 Cautions indicate the possibility of loss of data or a minor security breach. A Caution tells you about a situation where problems could occur unless precautions are taken. Pay attention to Cautions.

 Warnings indicate the possibility of significant data loss or a major security breach. A Warning means serious problems are going to happen unless you take the appropriate action. Please take Warnings very seriously.

About PGP Desktop Licensing

A *license* is used within the PGP software to enable the functionality you purchased, and sets the expiration of the software. Depending on the license you have, some or all of the PGP Desktop family of applications will be active. Once you have entered the license, you must then authorize the software with PGP Corporation, either manually or online.

To license PGP Desktop:

Do one of the following:

- If you are a managed user, you are most likely already using a licensed copy of PGP Desktop. Check your license details as described in [“Checking License Details” on page xvii](#). If you have questions, please contact your PGP administrator.
- If you are an unmanaged user, or a PGP administrator, check your license details as described in [“Checking License Details”](#). If you need to authorize your copy of PGP Desktop, do so as described in [“Authorizing PGP Desktop for Windows”](#).


Checking License Details

To see the details of your PGP Desktop license:

- 1 Double-click the PGP Desktop icon in the system tray.
- 2 From the **Help** menu, click **License**.


The **License** window appears, displaying the following details:

Item	Description
License Type	The name of the licensed product.
License Seats	The number of seats available for this license.
License Expiration	The date when the license will expire.
Product Information	Which components are active in your license. Active components are indicated with a green checkmark.

 If you do not authorize your copy of PGP Desktop, only limited features will be available to you (PGP Zip and Keys).

Authorizing PGP Desktop for Windows

If you need to change to a new license number, or if you skipped the license authorization process during configuration, follow these instructions to authorize your software.


 Make sure your Internet connection is active before proceeding. If you have no Internet connection, you must submit a request for a manual authorization.

Before you begin:


If you purchased PGP Desktop, you received an email order confirmation with an attached .PDF file.

- 1 Make a note of the name, organization, and license number you received in the email order confirmation. These are shown in the section titled **Important Note** in the .PDF. You will need these details during the licensing process.


During configuration of your PGP Desktop software, you must type the name, organization, email address, and license number to authorize your copy of PGP Desktop with PGP Corporation's authorization server.

 Your license number also appears on the download page of your PGP product.

- 2 Double-click the PGP Desktop icon in the System Tray.
- 3 From the **Help** menu, click **License**.
- 4 Click **Change License**.
- 5 Type the **Name** and **Organization** exactly as specified in your PGP email order confirmation .PDF. These will be shown in the section titled **Important Note** in the .PDF. If the **Important Note** section does not exist in your .PDF, your first authorization attempt will set the name and organization permanently.
- 6 Type the email address you wish to assign to the licensing of the product.
- 7 Type the email address again to confirm it.

 If you have previously authorized the same license number, you must enter the same Name, Organization, and Email Address as you did the previous time. If you enter different information, authorization will fail.

- 8 Do one of the following:
 - Type your 28-character license number in the provided fields (for example, DEMO1-DEMO2-DEMO3-DEMO4-DEMO5-ABC).

 To avoid typing errors and make the authorization easier, copy the entire license number, put the cursor in the first "License Number" field, and paste. Your license number will be correctly entered into all six "License Number" fields.

- To request a one-time, 30-day evaluation of PGP Desktop, select **Request a one-time 30 day Evaluation of PGP Desktop**. When you purchase a license, you can enter it any time before the end of the 30-day evaluation period. If you don't enter a valid license, PGP Desktop will revert to unlicensed functionality when the 30-day evaluation period is over.
- To purchase a PGP Desktop license, select **Purchase a license number now**. A Web browser will open and take you to the online PGP Store.

- 9 Click **Next** to authorize.
- 10 When PGP is authorized, the features enabled by your license will be displayed. Click **Next**, and then click **Finish** to complete the process.

Resolving License Authorization Errors

If you receive any error messages while authorizing your software, the ways to resolve this issue vary based on the error message. See the **HOWTO: License PGP Desktop 9.x** section in the PGP Support Portal at <https://pgp.custhelp.com> for suggestions.

Getting Assistance

Refer to these sections for additional resources.

Getting product information

Unless otherwise noted, the product documentation is provided as Adobe Acrobat PDF files that are installed with PGP Desktop. Online help is available within the PGP Desktop product. Release notes are also available, which may have last-minute information not found in the product documentation.

Once PGP Desktop is released, additional information regarding the product is entered into the online Knowledge Base available on PGP Corporation's Support Portal.

Contact information

Contacting Technical Support

- To learn about PGP support options and how to contact PGP Technical Support, please visit <http://www.pgp.com/support>
- To access the PGP Support forums, please visit <http://forums.pgpsupport.com>
- To access the PGP Support Knowledge Base or request PGP Technical Support, please visit <http://support.pgp.com>

You must have a valid support agreement to request Technical Support.

- For any other contacts at PGP, please go to the Contact Us page on the PGP website at <http://www.pgp.com/company/contact>.
- For general information about PGP Corporation, please visit the PGP website at <http://www.pgp.com>.

1

PGP Desktop Basics

Getting started with PGP Desktop

PGP Desktop is a security tool that uses cryptography to protect your data against unauthorized access.

PGP Desktop protects your data while being sent by email or by instant messaging (IM). It lets you encrypt your entire hard drive (or hard drive partition) so everything is protected all the time, or just a portion of your hard drive, on which you can securely store your most sensitive data. It also lets you put any combination of files and folders into an encrypted, compressed package for easy distribution or backup. And, you can use PGP Desktop to shred (secure delete) sensitive files, so that no one can retrieve them.

PGP Desktop lets you create PGP keypairs and manage both your personal keypairs and the public keys of others. It is available for both the Mac OS X and Windows platforms.

Some high-level conceptual information is presented in these topics:

- [“PGP Desktop Terminology” on page 1](#)
- [“Using PGP Desktop for the First Time” on page 4](#)

PGP Desktop Terminology

To make the most of PGP Desktop, you should be familiar with the following terms:

PGP Product Component Terms

- **PGP Desktop:** A software tool that uses cryptography to protect your data against unauthorized access. PGP Desktop is available for Mac OS X and Windows.
- **PGP Global Directory:** A free, public keyserver hosted by PGP Corporation. The PGP Global Directory provides quick and easy access to the universe of PGP keys. It uses next-generation keyserver technology that verifies the email address on a key (so that the keyserver doesn't get clogged with unused keys) and lets users manage their own keys. Using the PGP Global Directory significantly enhances your chances of finding a valid public key of someone to whom you want to send secured messages. PGP Desktop is designed to work closely with the PGP Global Directory.
- **PGP Keys:** A feature of PGP Desktop that gives you complete control over both your own PGP keys, and the keys of those persons with whom you are securely exchanging email messages.
- **PGP Messaging:** A feature of PGP Desktop that automatically and transparently supports all of your email clients through policies you control. PGP Desktop accomplishes this using a new proxy technology; the older plugin technology is also available. PGP Messaging also protects many IM clients, such as AIM and iChat (both users must have PGP Messaging enabled).

- **PGP NetShare:** A feature of PGP Desktop for Windows with which you can securely and transparently share files and folders among selected individuals. PGP NetShare users can protect their files and folders simply by placing them within a folder that is designated as protected.
- **PGP Shred:** A feature of PGP Desktop that lets you securely delete data from your system. PGP Shred overwrites files so that even file recovery software cannot recover them.
- **PGP Universal:** A tool for enterprises to automatically and transparently secure email messaging for their employees. If you are using PGP Desktop in a PGP Universal-protected environment, your messaging policies and other settings may be controlled by your organization's PGP administrator.
- **PGP Virtual Disk volumes:** PGP Virtual Disk volumes are a feature of PGP Desktop that let you use part of your hard drive space as an encrypted virtual disk. You can protect a PGP Virtual Disk volume with a key or a passphrase. You can even create additional users for a volume, so that people you authorize can also access the volume. The PGP Virtual Disk feature is especially useful on laptops, because if your computer is lost or stolen, the sensitive data stored on the PGP Virtual Disk is protected against unauthorized access.
- **PGP Whole Disk Encryption:** Whole Disk Encryption is a feature of PGP Desktop that encrypts your entire hard drive or drives, including your boot record, thus protecting all your files when you aren't using them. You can use PGP Whole Disk Encryption and PGP Virtual Disk volumes on the same system. You can protect whole disk encrypted drives with a passphrase or with a keypair on a USB token for added security.
- **PGP Zip:** A feature of PGP Desktop that lets you put any combination of files and folders into a single encrypted, compressed package for convenient transport or backup. You can encrypt a PGP Zip archive to a PGP key or to a passphrase, allowing you to send the archive to someone who doesn't even have PGP Desktop on their system.
- **Self-Decrypting Archives (SDAs):** Another way to put files and folders into a single encrypted and compressed package. An SDA is slightly larger in size than a PGP Zip archive because the executable file is included in the archive, but this means that the SDA can be opened on Windows systems that don't have PGP Desktop installed. SDAs can only be protected by passphrases, so you have to find a secure way to communicate the passphrase of the SDA to the intended recipient.
- **Separate Signing Subkey:** A PGP keypair consists of a master key for signing, and a subkey for encryption. You can also generate a separate subkey for signing. Among other uses, this feature is needed in regions where separate subkeys for signing are required for legally-binding digital signatures.
- **Single Sign-On:** A feature of PGP Desktop for Windows Whole Disk Encryption that you can use to make booting your computer easier. With this feature, your Windows login password and your PGP Whole Disk Encryption password are synchronized, so you only need to login at the PGP Whole Disk Encryption Bootguard screen. Your password is then passed to Windows—you do not need to type it again for Windows.

PGP Product Concepts

- **Conventional cryptography:** Uses the same passphrase to encrypt and decrypt data. Conventional cryptography is great for data that isn't going anywhere (because it encrypts and decrypts quickly). However, conventional cryptography is not as well suited for situations where you need to send encrypted data to someone else, especially if you want to send encrypted data to someone you have never met.
- **Decrypting:** The process of taking encrypted (scrambled) data and making it meaningful again. When you receive data that has been encrypted by someone using your public key, you use your private key to decrypt the data.
- **Encrypting:** The process of scrambling data so that if an unauthorized person gets access to it, they cannot do anything with it. The data is so scrambled, it's meaningless.
- **Public-key cryptography:** Public-key cryptography uses two keys (called a keypair) for encrypting and decrypting. One of these two keys is your private key; and, like the name suggests, you need to keep it private. Very, very private. The other key is your public key, and, like its name suggests, you can share it with the general public. In fact, you're supposed to share.

Public-key cryptography works this way: let's say you and your cousin in another city want to exchange private messages. Both of you have PGP Desktop. First, you both need to create your keypair: one private key and one public key. Your private key you keep secret, your public key you send to a public keyserver like the PGP Global Directory (keyserver.pgp.com), which is a public facility for distributing public keys. (Some companies have their own private key servers.)

Once the public keys are on the PGP Global Directory, you can go back to the PGP Global Directory and get your cousin's public key, and she can go to the keyserver and get yours (there are other ways to exchange public keys; refer to [Chapter 10, PGP Keys](#) for more information). This is important because to send an encrypted email message that only your cousin can decrypt, **you encrypt it using your cousin's public key**. What makes this work is that only your cousin's private key can decrypt a message that was encrypted using her public key. Even you, who have her public key, cannot decrypt the message once it has been encrypted using her public key. **Only the private key can decrypt data that was encrypted with the corresponding public key.**

- **Signing:** The process of applying a digital signature to data using your private key. Because data signed by your private key can be verified only by your public key, the ability to verify signed data with your public key proves that your private key signed the data and thus proves the data is from you.
- **Verifying:** The process of proving that the private key was used to digitally sign data by using that person's public key. Because data signed by a private key can only be verified by the corresponding public key, the fact that a particular public key can verify signed data proves the signer was the holder of the private key.

PGP Product Terms

- **Keypair:** A private key/public key combination. When you create a PGP “key,” you are actually creating a keypair. As your keypair includes your name and your email address, in addition to your private and public keys, it might be more helpful to think of your keypair as your digital ID—it identifies you in the digital world as your driver’s license or passport identifies you in the physical world.
- **Keyserver:** A repository for keys. Some companies host keyservers for the public keys of their employees, so other employees can find their public keys and send them protected messages. The PGP Global Directory (<https://keyserver.pgp.com/>) is a free, public keyserver hosted by PGP Corporation.
- **Private key:** The key you keep very, very private. Only your private key can decrypt data that was encrypted using your public key. Also, only your private key can create a digital signature that your public key can verify.



Do not give your private key, or its passphrase, to anyone! And keep your private key safe.

- **Public key:** The key you distribute to others so that they can send protected messages to you (messages that can only be decrypted by your private key) and so they can verify your digital signature. Public keys are meant to be widely distributed.

Your public and private keys are mathematically related, but there’s no way to figure out your private key if someone has your public key.

- **Smart cards and tokens:** Smart cards and tokens are portable devices on which you can create your PGP keypair or copy your PGP keypair. Creating your PGP keypair on a smart card or token adds security by requiring possession of the smart card or token in order to encrypt, sign, decrypt, or verify. So even if an unauthorized person gains access to your computer, your encrypted data is secure because your PGP keypair is with you on your smart card or token. Copying your PGP keypair to a smart card or token is a good way to use it away from your main system, back it up, and distribute your public key.

For more terms, see the Glossary [on page 259](#).

Using PGP Desktop for the First Time

PGP Corporation recommends the following procedure for getting started with PGP Desktop:

1 Install PGP Desktop on your computer.

If you are a corporate user, your PGP administrator may have specific installation instructions for you to follow. Your PGP administrator may also have configured your PGP installer with certain settings.

2 Let the Setup Assistant be your guide.

To help you get started, after you install PGP Desktop and reboot your computer, the Setup Assistant appears. It assists with:

- Licensing PGP Desktop
- Creating a keypair—with or without subkeys (if you do not already have a keypair).
- Publishing your public key on the PGP Global Directory.
- Enabling PGP Messaging
- Giving you a quick overview of other features.

If your PGP Desktop installer application was configured by a PGP administrator, the Setup Assistant may perform other tasks.

3 Exchange public keys with others.

After you have created a keypair, you can begin sending and receiving secure messages with other PGP Desktop users. You can also use the PGP Desktop disk-protection features.

Exchanging public keys with others is an important first step. To send them secure messages, you need a copy of their public key, and to reply with a secure message, they need a copy of your public key. If you did not upload your public key to the PGP Global Directory using the Setup Assistant, do so now. If you do not have the public key for someone to whom you want to send messages, the PGP Global Directory is the first place to look. PGP Desktop does this for you—when you send email, it finds and verifies the keys of other PGP Desktop users automatically. It then encrypts your message to the recipient public key, and sends the message.

4 Validate the public keys you get from untrusted keyservers.

When you get a public key from an untrusted keyserver, try to make sure that it has not been tampered with, and that the key really belongs to the person it names. To do this, use PGP Desktop compare the unique fingerprint on your copy of someone's public key to the fingerprint on that person's original key. Keys from trusted keyservers like the PGP Global Directory have already been verified.

5 Start securing your email, files, and instant message (IM) sessions.

After you have generated your keypair and exchanged public keys, you can begin encrypting, decrypting, signing, and verifying email messages and files.

6 After you have sent or received some messages, check the messaging logs to make sure everything is working correctly.

As you send or receive messages, the PGP Desktop Notifier feature displays information boxes that pop up from your Windows System tray. These Notifier boxes tell you the action that PGP Desktop took. After you grow familiar with the process of sending and receiving messages, you can change options for the Notifier feature—or turn it off. If you want more information than the Notifier feature displays, the Messaging Log provides detailed information about all messaging operations.

7 Modify your messaging policies, if necessary.

Email messages are sent and received—automatically and seamlessly—if PGP Desktop messaging policies are configured correctly. If your message recipient has a key on the PGP Global Directory, the default PGP Desktop policies provide *opportunistic* encryption. Opportunistic encryption means that, if PGP Desktop has what it needs (such as the recipient public key) to encrypt the message automatically, then it does so. Otherwise, it sends the message in *clear text* (unencrypted). The default PGP Desktop policies also provide optional *forced* encryption. This means that, if you include the text “[PGP]” in the Subject line of a message, then the message **must** be sent securely. If verified keys cannot be found, then the message is not sent, and a Notifier box alerts you.

8 Start using PGP Desktop's other features.

Along with its messaging features, you can also use PGP Desktop to secure the disks that you work with:

- Use the PGP **Whole Disk Encryption** feature to encrypt a disk or disk partition. All files on the disk or partition are secured, except the files you are working with.
- Use the **PGP Virtual Disk** feature to create a secure “virtual hard disk.” You can use this virtual disk like a bank vault for your files. Use PGP Desktop or Windows Explorer to lock the virtual disk, and your files are secure, even if the rest of your computer is unlocked.
- Use the **PGP Netshare** feature to share files and folders securely and easily among any number of people—with maximum access control.
- Use the **PGP Zip** feature to create compressed and encrypted PGP Zip archives. These archives offer an efficient way to transport or store files securely.
- Use the **PGP Shredder** feature to delete sensitive files that you no longer need. PGP Shredder removes them completely, eliminating any possibility of recovery.

2

Installation

Installing PGP Desktop on your system

This section describes how to install PGP Desktop onto your computer and how to get started after installation. The following topics are covered here.

- [“Installing PGP Desktop for Windows” on page 8](#)
- [“Upgrading the Software” on page 8](#)
- [“Running the Setup Assistant” on page 9](#)
- [“Uninstalling PGP Desktop” on page 9](#)
- [“Moving Your PGP Desktop Installation From One Computer to Another” on page 10](#)

Before You Install

This section describes the minimum system requirements for installing PGP Desktop on your Windows computer.

System Requirements

Before you begin the installation, verify that your system meets these minimum requirements:

- Operating system—Windows 2000 (Service Pack 4), Windows XP (Service Pack 1 or 2), or Windows Server 2003 (Service Pack 1).



PGP Whole Disk Encryption is not supported on Windows Server 2003.

- Memory—128 Megabytes (MB) RAM (256 MB recommended).
- Free disk space—64 MB free disk space.



Version 9.5 of PGP Desktop for Windows does not support Microsoft Windows NT, Windows 98, nor Windows ME.

Installing PGP Desktop for Windows

This section describes both the minimum system requirements for installing PGP Desktop on your Windows system and the actual installation procedure.


Installing the Software

To install PGP Desktop on your Windows system:

- 1 Locate the PGP Desktop installer program.

The installer program is an .MSI file, which your PGP administrator may have distributed to you using the Microsoft SMS deployment tool.

- 2 Double-click the PGP Desktop installer.
- 3 Follow the on-screen instructions.
- 4 If prompted to do so, restart your system.


 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.

Upgrading the Software

You can upgrade to PGP Desktop for Windows from a previous version of one of the following products:

- PGP Desktop for Windows.
- PGP Universal Satellite for Windows.

If you are using Windows XP with your computer, you can upgrade only to PGP Desktop 9.5 or greater from PGP Desktop 8.x. If you are using a Windows 2000 system, you can upgrade from PGP Desktop Versions 6.x, 7.x, or 8.x.

 PGP Desktop 9.5 for Windows or greater and PGP Universal Satellite 2.5 for Windows or greater **cannot** both be installed on the same system. The installers for both products will detect the presence of the other program and end the install.

To upgrade to PGP Desktop 9.5 for Windows:

- **From PGP Desktop 8.x for Windows:** Follow the standard installation process for PGP Desktop 9.5 for Windows.

PGP Desktop for Windows 8.x is automatically uninstalled, and PGP Desktop 9.5 for Windows is installed. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version.

- **From a version of PGP Desktop for Windows prior to 8.0:** Manually uninstall versions of PGP Desktop prior to 8.0 before beginning the installation of PGP Desktop 9.5 for Windows. Existing keyrings and PGP Virtual Disk files will be usable in the upgraded version.
- **From PGP Universal Satellite 1.2 for Windows or previous:** Follow the installation process for PGP Desktop 9.5 for Windows.

Existing versions of PGP Universal Satellite for Windows are automatically uninstalled, and PGP Desktop 9.5 for Windows will be installed. Existing settings will be retained.



Installing any version of PGP Universal Satellite 1.x on top of PGP Desktop 9.5 for Windows is an unsupported configuration. Neither program will work correctly. Uninstall both programs and then reinstall only PGP Desktop.

- **From PGP Desktop for Windows (Version 8.x) and PGP Universal Satellite:** Follow the installation process for PGP Desktop 9.5 for Windows.

PGP Desktop and PGP Universal Satellite for Windows are automatically uninstalled, and then PGP Desktop 9.5 for Windows is installed. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version.

Running the Setup Assistant

When the installation of PGP Desktop is complete, you are prompted to restart your computer. Once the computer restarts, as soon as you see the Windows Desktop, the PGP Desktop Setup Assistant starts automatically. The Assistant displays a series of screens that ask you questions—then uses your answers to configure PGP Desktop for you.

Based on a number of factors, the Setup Assistant for your system will contain only the appropriate set of screens.

The Setup Assistant does not configure all PGP Desktop settings. When you finish going through the Setup Assistant screens, you can then configure those settings not covered in the Setup Assistant.

Uninstalling PGP Desktop

You can uninstall PGP Desktop using the PGP Desktop uninstaller, or by using the **Windows Add or Remove Programs** feature. The following procedure describes using the PGP Desktop uninstaller directly.

If you are upgrading PGP Desktop 8.x or later, you do **not** have to uninstall first. For more information, see [“Upgrading the Software” on page 8](#).

To uninstall PGP Desktop:

- 1 Click the **Start** menu, select **Programs > PGP > Uninstall PGP Desktop**.

A confirmation dialog appears.

- 2 Click **Yes** to continue with the uninstallation process.

The PGP Desktop software is removed from your system.

Keyring, PGP Virtual Disk, and PGP Zip (.pgp) files are *not* removed from your system, in case you decide to reinstall PGP Desktop in the future.

- 3 If prompted, restart your computer to complete the uninstallation.



An alternative to uninstalling PGP Desktop is stopping PGP Desktop background services. Doing this prevents PGP Desktop from protecting your email and instant messages, but both PGP Virtual Disk volumes and disks or partitions protected by PGP Whole Disk Encryption are still accessible. If you just need to turn off the PGP Desktop email or IM proxies, you can do that from the PGP Tray icon.

Moving Your PGP Desktop Installation From One Computer to Another

Moving a PGP Desktop installation from one computer to another is not a difficult process, although there are a few crucial steps which must be completed successfully. The process consists of the following steps:

- Uninstall PGP Desktop from the old computer,
- Transfer the public and private keyring files from the old computer to the new computer,
- Install PGP Desktop on the new computer,
- Configure PGP Desktop to use the keyring files transferred from the old computer, and finally,
- License PGP Desktop on the new computer.

To transfer your PGP Desktop installation to another computer:

- 1 Uninstall PGP Desktop. To do this, choose **Start > Programs > PGP > Uninstall PGP Desktop**. You can also use the Add/Remove Programs functionality in the Windows Control Panel, and is the only way to do remove PGP Desktop if you are running an older version of the program.

Note that this step does not remove the keyring files.

- 2 Transfer the keyrings. To do this, copy the keyring files (both `pubring.pkr` and `secring.skr`) from the old computer to diskette or other removable media, and then copy them to the new computer. The default location for the keyring files is `C:\Documents and Settings\<user>\My Documents\PGP\`.

If PGP Desktop has never been installed on the new computer, create this folder first before copying the keyring files to the computer.

- 3** Install PGP Desktop on the new computer. To do this, download PGP Desktop by clicking the download link in your original PGP order confirmation email.
- 4** During the installation process, do the following:
 - During the PGP Desktop setup wizard on the new computer select **No, I have existing keyrings** and specify the location where you copied the keyring files to on the new computer.
 - Use the same name, organization, and license number used when PGP Desktop was originally authorized.

3

The PGP Desktop User Interface

Getting familiar with PGP Desktop

This section describes the PGP Desktop user interface. It contains the following topics:

- [“Accessing PGP Desktop Features” on page 13](#)
- [“PGP Desktop Main Screen” on page 14](#)
- [“The PGP Tray Icon” on page 15](#)
- [“Context Menus in Windows Explorer” on page 17](#)
- [“The Start Menu” on page 18](#)
- [“PGP Desktop Notifier alerts” on page 19](#)

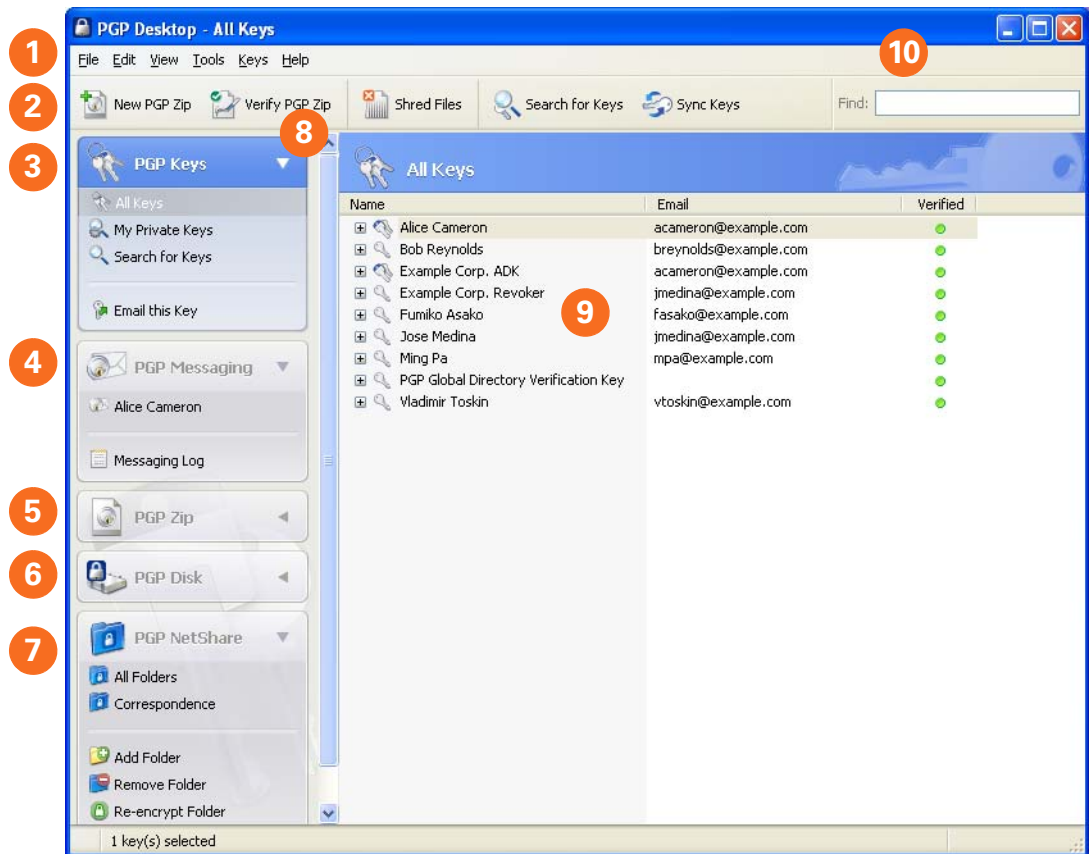
Accessing PGP Desktop Features

There are four main ways to access PGP Desktop:

- [“PGP Desktop Main Screen” on page 14](#)
- [“The PGP Tray Icon” on page 15](#)
- [“Context Menus in Windows Explorer” on page 17](#)
- [“The Start Menu” on page 18](#)

PGP Desktop Main Screen

PGP Desktop's main screen is your main interface to the product.



The PGP Desktop main screen includes:

- 1 The Menu bar.** Gives you access to PGP Desktop commands. The menus on the Menu bar change depending on which Control box is selected.

- 2 The Toolbar.** Gives you access to frequently used features. You can create a new PGP Zip archive, verify an existing PGP Zip archive, shred selected files, search for a key, synchronize your keys, or find text in the user IDs of the keys currently visible in the PGP Keys work area.

- 3 The PGP Keys Control Box.** Gives you control of PGP keys.

- 4 The PGP Messaging Control Box.** Gives you control over PGP Messaging.

- 5 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.

- 6 The PGP Disk Control Box.** Gives you control of PGP Disk.

- 7 The PGP NetShare Control Box.** Gives you control of PGP NetShare.

- 8 Expand/Collapse Control Box Control.** Use to display or hide Control Boxes.

- 9 The PGP Desktop Work area.** Displays information and actions you can take for the selected Control box.
-
- 10 PGP Keys Find box.** Use to search for keys on your keyring. As you type text in this box, PGP Desktop displays search results based on either name or email address.

Each Control box can expand to show available options, and collapse to save space (only the Control Box's banner displays). Expand a Control Box by clicking its banner. Collapse a Control Box by clicking its Expand/Collapse arrow in the upper right corner.

When expanded, the contents of Control Boxes change depending on what is appropriate for what you are working on, or what is selected. For example, when the PGP Keys Control Box is selected, if a public key is selected, the options **Email this Recipient** and **Email this Key** appear at the bottom of the PGP Keys Control Box. If a private key is selected, only **Email this Key** appears. If no key is selected, neither option appears.

- i** Click **Email this Recipient** to open your system's default email client and create a new email using the address of the selected key. This makes it easy to send a message to someone on your keyring. Click **Email this Key** to open your system's default email client and create a new email with the selected public key attached (the message is not addressed). This is useful for sending your public key, or a public key on your keyring, to someone who does not already have it.




The PGP Tray Icon

One way to access many PGP Desktop features is from the PGP Tray icon.

Hint: You can open PGP Desktop by double-clicking the PGP Tray icon.

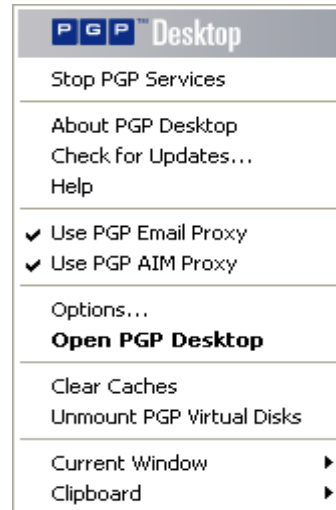


The PGP Tray displays one of four icons:

- **Normal operation** (): PGP Desktop is operating normally; no passphrases are cached, message proxying is enabled, no other PGP operations are in progress.
- **Cached passphrase** (): PGP Desktop is operating normally; additionally, one or more private key passphrases has been cached. Caching passphrases is an optional time-saving feature, in that you don't have to type your passphrase if it's cached to sign a key, for example, but it's also a security risk in that if you leave your system with the passphrase cached, whoever walks up to your system could use PGP Desktop without having to type the appropriate passphrase.
- **Message proxying disabled** (): Proxying of email messages has been disabled; incoming encrypted messages will not be decrypted or verified and outgoing messages will not be encrypted or signed. You can turn message proxying back on using the PGP Tray menu or the PGP Options.

- **Busy** (🔒): PGP Desktop is in the middle of an operation, such as encrypting a disk. When the operation is complete, the PGP Tray icon will change back to the appropriate icon.

When you right or left click on the PGP Tray icon, a menu appears giving you access to (from the top down):



- **Stop PGP Services.** Stops PGP Desktop services on this computer. Be very careful with this command; it will stop automatic encryption and decryption of email and instant messaging sessions.

If you Stop PGP Services, you can start them again by restarting your computer or by selecting PGP Desktop from the Start menu (**Start > Programs > PGP > PGP Desktop**).

- **About PGP Desktop.** Displays information about the version of PGP Desktop you are using, including licensing information.
- **Check for Updates.** Contacts the PGP Corporation update server to see if a newer version of PGP Desktop is available for download.
- **Help.** Opens PGP Desktop's integrated online help.
- **Use PGP Email Proxy.** When selected, PGP Desktop's email proxies automatically and transparently encrypt, sign, decrypt, and/or verify your email messages.
- **Use PGP AIM Proxy.** When selected, PGP Desktop's IM proxies encrypt your IM sessions if the other user has also enabled their PGP AIM proxy.
- **Options.** Opens the PGP Desktop Options dialog.
- **Open PGP Desktop.** Opens the PGP Desktop main screen.

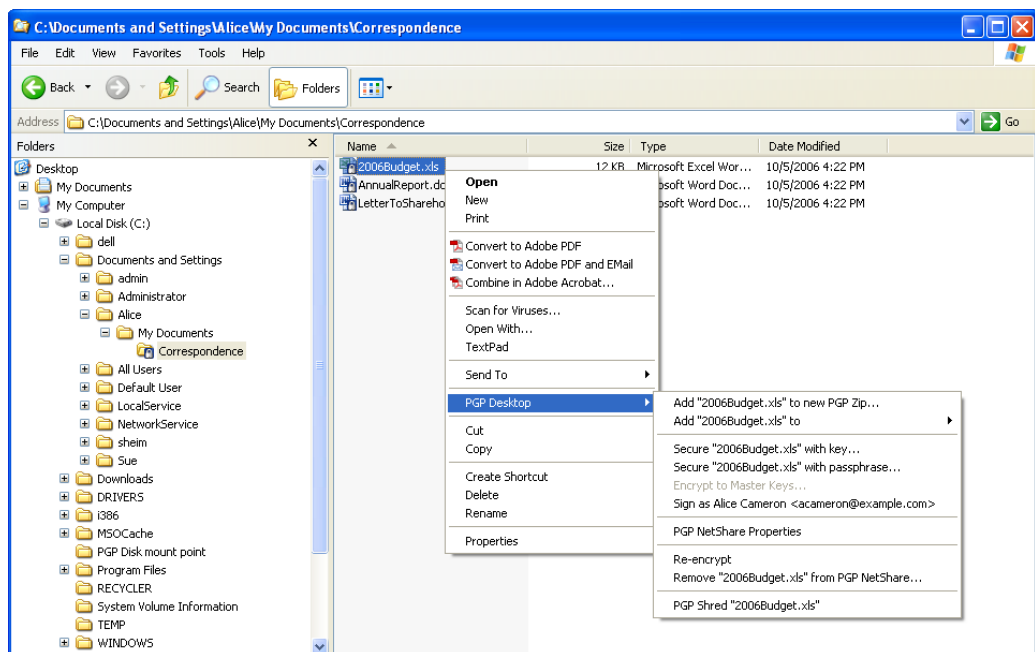
You can also open PGP Desktop by *double-clicking* the PGP Desktop Tray icon.

- **Clear Caches.** Clears from memory any cached information, such as passphrases and cached public keys.

- **Unmount PGP Virtual Disks.** Unmounts all mounted PGP Virtual Disk volumes.
- **Current Window.** Lets you use PGP Desktop functionality (Decrypt & Verify, Encrypt & Sign, Sign, Encrypt) on the contents of the current window.
- **Clipboard.** Lets you use PGP Desktop functionality (Decrypt & Verify, Encrypt & Sign, Sign, Encrypt) on the contents of the Clipboard. Also lets you clear or edit the contents of the Clipboard.

Context Menus in Windows Explorer

You can also access PGP Desktop functions via context menus in Windows Explorer. Simply open Windows Explorer and then right-click the items you want to work on.



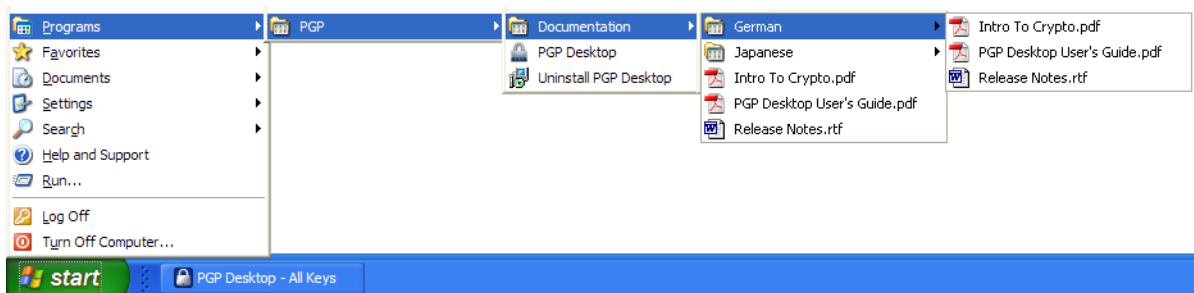
Windows Explorer gives you access to PGP Desktop functions appropriate to what you right-clicked:

- **Drive.** If you right-click a drive on your system in Windows Explorer and select PGP from the menu that appears, you can do the following to the drive:
 - Encrypt, Sign, or Encrypt & Sign it
 - Decrypt & Verify it
 - Wipe Free Space on it
 - Create a self-decrypting archive (SDA) of the drive
- **Folder.** If you right-click a folder in Windows Explorer and select PGP from the menu that appears, you can do the following to the folder:
 - Encrypt, Sign, or Encrypt & Sign it

- Decrypt & Verify it
- Shred it
- Create an SDA with the contents of the folder in the archive
- **File.** If you right-click a file in Windows Explorer, the PGP submenu lets you perform various PGP functions on the file, depending on what kind of file it is:
 - If you select an unencrypted file, you can Encrypt & Sign, Encrypt, Sign, Shred, or Create an SDA
 - If you select an encrypted file, you can decrypt/verify or Shred it
 - If you select an unmounted PGP Virtual Disk volume (.PGD), you can mount or edit it; if you select a mounted volume, you can unmount it
 - If you select a PGP Zip (.PGP) file, you can Decrypt & Verify it, View it, or Shred it
 - If you select a PGP key file (.ASC), you can decrypt/verify or Shred it. If you select decrypt/verify, you are given the option of importing the file
 - If you select a PGP public or private keyring file (PKR or SKR files, respectively), you can add the keys in it to your keyring or Shred it

The Start Menu

You can access PGP Desktop is through the Windows Start menu.



Click **Start > Programs > PGP**

The **Start** menu gives you access to:

- PGP Desktop documentation, in English, German, and Japanese
- The PGP Desktop application
- Uninstalling PGP Desktop

PGP Desktop Notifier alerts

The PGP Desktop Notifier feature displays a small information box that tells you the status of incoming and outgoing email messages.



The PGP Desktop Notifier feature also displays the status of the PGP Whole Disk Encryption and PGP NetShare features on your computer. For more information, see [“PGP Desktop Notifier for Disk features” on page 22.](#)

PGP Desktop Notifier for Messaging

With the PGP Desktop Notifier for Messaging feature:

- See whether or not incoming email is properly decrypted and/or signed.
- See whether or not outgoing email is properly encrypted and/or signed.
- Stop an email message from being sent if the encryption options are not what you want.
- View a quick summary of the sender, subject, and encryption key of an email.
- Review, at any time, the status of previous incoming or outgoing messages for that Windows session.

You can use the PGP Desktop Notifier feature to monitor all of your incoming email, or some of it—as well as maintain precise control over every outgoing message, or only some of them. The choice is yours. You can set various Notifier options, or turn the PGP Desktop Notifier feature completely off if you prefer.

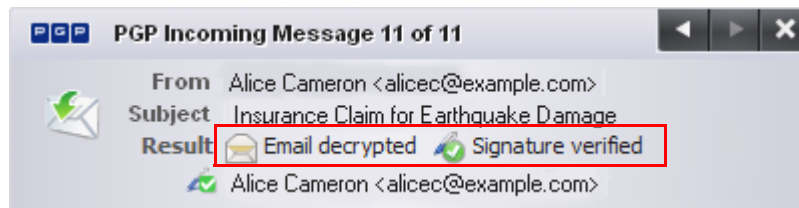
Some additional points about the PGP Desktop Notifier feature:

- For message notifications, you can use left and right arrow buttons in the upper-right corner of the Notifier box to scroll Notifier messages forward or backward. This way, you can review messages that came before or after the message you are viewing currently.
- When they first display, Notifier message boxes have a partially transparent appearance to prevent obscuring anything on your screen. Notifier message boxes become opaque if you move your cursor over them, and become translucent again when you move your mouse away from them.
- Unless the pointer is over them, Notifier messages display for approximately five seconds. If you need more time to read a Notifier, move your pointer over the Notifier and it remains on your display.
- If you completely miss reading a Notifier, or you would like to review previous ones, choose **View Notifier** from the PGP Tray icon.
- You can close a Notifier box by clicking the **X** in the upper right.

For more information about setting PGP Desktop Notifier options, see [Appendix A, Notifier Options](#).

Incoming PGP Desktop Notifier Messages

Notifications for incoming email provide information on whether the email was decrypted and verified, or decrypted and signed by an unverified or unknown key. The following example shows an email message that was received, decrypted successfully, and verified that it came from the person who it says it was from.

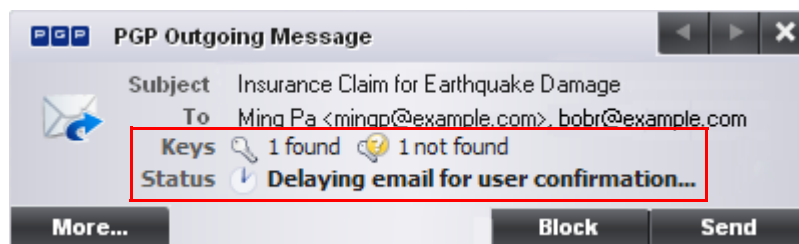


To enable or disable this Notifier:

- 1 Open PGP Desktop and choose **PGP Options...** from the **Tools** menu
- 2 Click the **Notifier** tab
- 3 From **Display notifications for incoming email**, do one of the following:
 - To display notifications when secured email is received, select **When receiving secured email**.
 - To display notifications only when PGP Desktop is unable to verify the sender, select **Only when message verification fails**.
 - To disable this Notifier, select **Never**.

Outgoing PGP Desktop Notifier Messages

For simple notification, choose to have a PGP Desktop Notifier appear momentarily when mail is sent (all mail, or mail meeting certain criteria). The following example shows an outgoing email message that is ready to be sent secured. The email is sent with no intervention from you.



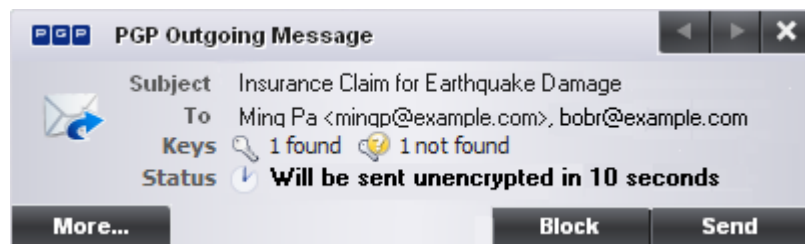
You can also set PGP Desktop to include **Block** and **Send** buttons in the Notifier box (see the following section).

To manage the outgoing email with this Notifier:

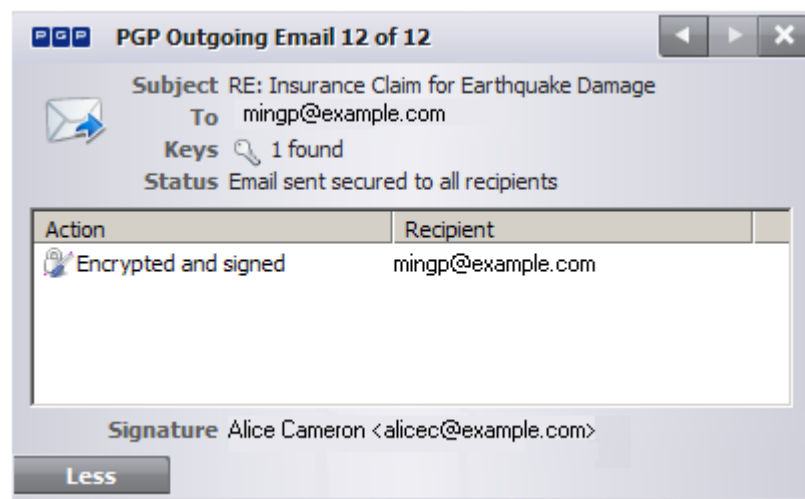
- In the PGP Outgoing Message Notifier box, do the following:

- To stop this email message from being sent, click **Block**. Note that this blocks only this outgoing email message; future email messages to this sender can be sent.
- To send this message, even though the recipient's key cannot be found, click **Send**.
- To continue to delay a message from being processed, hover your mouse over the Notifier box. When you move your mouse away from the Notifier box, the message is then processed using the default rule.

In Notifier options, the **Delay outbound mail for** setting specifies how long (in seconds) the Notifier gives you before it sends the mail without your intervention. The Notifier displays a countdown before it sends your mail.



- To view additional information, including the Action, Recipient, Policy, and Signing Key, click **More**.



It is not necessary for you to view this additional information unless you want to see it. To hide it again, click **Less**.

To specify Notifier options for outgoing mail:

- 1 Open PGP Desktop and choose **PGP Options...** from the **Tools** menu
- 2 Click the **Notifier** tab
- 3 In the **Messaging section**, specify the following:

- **Notify when processing outbound email:** Select this checkbox if you want PGP Desktop Notifiers to appear, informing you of encryption and/or signing status when you send mail. Deselect this checkbox to stop PGP Desktop Notifiers from appearing when you send mail.
- **Ask me before sending email when the recipient's key is not found:** PGP Desktop looks for a public key for every recipient of the email messages that you send. By default, if it cannot find a public key for a recipient, it sends that email in the clear (without encryption). If you select this Notifier option, you are notified that this is the case, and given a chance to block the email so that it is not sent.


(For more information on the PGP Desktop default policy settings, see [“Services and Policies” on page 27.](#))

- **Always ask me before sending email:** You can select this checkbox if you would prefer approving every email that you send. You can review the encryption status in the Notifier, and either send or block the email.
- **Delay outbound email for n second(s) to confirm** (where n is a number from 1-30). If you would like a Notifier for every message that you send—but you would prefer that they did not wait for your explicit approval—you can select this option. Outbound email is delayed, and a Notifier displays, for the time period that you choose. If you want the email to be sent, do nothing: the email is sent once the time interval elapses. If you would like a closer look at the Notifier, move your cursor over it. The Notifier changes from translucent to opaque in appearance, and the outbound email is delayed while you review the Notifier information. You can then allow the email to be sent, or block it.

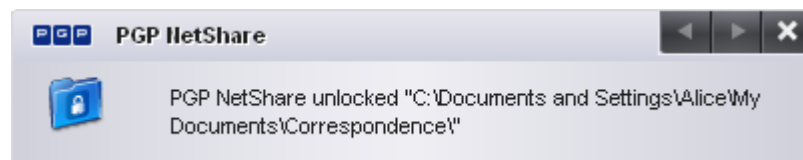
PGP Desktop Notifier settings can be changed in the Options box. For more information, see [Appendix A, Notifier Options.](#)

PGP Desktop Notifier for Disk features

The PGP Desktop Notifier for Disk features keep you informed when you are working with the PGP NetShare and the PGP Whole Disk Encryption features.

-  The PGP Desktop Notifier feature also displays the status of incoming and outgoing email messages on your computer. For more information, see [“PGP Desktop Notifier for Messaging” on page 19.](#)

PGP NetShare



When used with PGP NetShare, the PGP Desktop Notifiers feature alerts you to these things:

- Actions taken to a shared folder.
- Location of the affected folder.
- Name of the affected folder.
- Who performed the action.

PGP Whole Disk Encryption



When used with the PGP Whole Disk Encryption feature, the PGP Desktop Notifiers feature alerts you to these things:

- The disk being encrypted.
- The size and type of disk.
- Status of the encryption process.

4

Securing Email Messages

Using PGP Desktop to protect your email

This chapter describes how to use PGP Desktop Email to automatically and transparently secure your email messages.

- [“How PGP Desktop Secures Email Messages” on page 25](#)
- [“Services and Policies” on page 27](#)
- [“Creating a Service and Editing Account Properties” on page 29](#)
- [“Disabling, Enabling, and Deleting a Service” on page 34](#)
- [“PGP Desktop and SSL” on page 35](#)
- [“Multiple Services” on page 37](#)
- [“Troubleshooting Services” on page 37](#)
- [“Creating a New Security Policy” on page 39](#)
- [“Wildcards and Regular Expressions in Policies” on page 44](#)
- [“Security Policy Information and Examples” on page 44](#)
- [“Working with the Security Policy List” on page 47](#)
- [“Key Modes” on page 53](#)
- [“Viewing the PGP Messaging Log” on page 56](#)



If you are using PGP Desktop with Lotus Notes or MAPI email clients in a PGP Universal-protected environment, refer to [“Appendix D, Messaging with Lotus Notes and MAPI”](#) for important additional information about how to configure PGP Desktop messaging policies.

How PGP Desktop Secures Email Messages

When secure email messaging is enabled, PGP Desktop monitors the email traffic between your email client and your mail server. Depending on the circumstances, PGP Desktop will intercede on your behalf to encrypt, sign, decrypt, or verify messages.


Once configured correctly—and it’s very likely PGP Desktop can do that for you automatically—you don’t have to do anything to encrypt and/or sign outgoing messages or to decrypt and/or verify incoming messages; the PGP Desktop messaging proxy does it for you.

How this happens is different for incoming and outgoing messages.

For incoming messages, PGP Desktop automatically evaluates all incoming email messages and takes the appropriate actions (described in the following section).


For outgoing messages, there are a range of actions that PGP Desktop can take on your behalf based on configured *policies*. A *policy* is a set of instructions that tells PGP Desktop what to do in specific situations. PGP Desktop comes pre-configured with a set of policies that suit the needs of the vast majority of users. However, you are also provided with fine-grained control over these policies should you wish to change them. A policy is a set of one or more instructions, generally of a form like: "In this circumstance, do this." By combining these instructions, policies can be tailored to meet all of your email security requirements.

By default, when you are using PGP Desktop standalone and are sending an outgoing message, PGP Desktop looks for a key it can trust to encrypt the message. It looks first on the default keyring for the public key of the recipient (the standard name for the default keyring is All Keys). If it does not find such a key, it will, again by default, check the PGP Global Directory for a trusted key for the recipient. If it does not find a trusted key there, the message is sent in the clear; that is, unencrypted. This default behavior, called *Opportunistic Encryption*, strikes a balance between protecting outgoing messages and making sure they get sent.

 PGP Desktop checks only the default keyring. To send encrypted email to a recipient whose key is on your local keyring, be sure to import the key to your default keyring.

If you have multiple keyrings, the default keyring is the first keyring listed in the PGP Keys control box. To specify a different default keyring, right-click the keyring in the PGP Keys control box, choose Properties, and select the **Default Keyring** checkbox.

Creating new policies is covered in detail in ["Creating a New Security Policy" on page 39](#).

 If you are in a PGP Universal-protected domain, your local PGP Desktop policies determine how your messages are encrypted and when. For more information, consult with your organization's PGP Universal administrator.

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 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 (at `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 Messaging 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 couldn't be decrypted, make sure the sender was using your real public key. If the message couldn't 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 <https://keyserver.pgp.com>, or ask them to send their public key to you directly by email.



PGP Desktop only encrypts by default to keys that are known to be valid. If you didn't 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-protected domain, your local PGP Desktop policies are controlled by the policies specified by your PGP Universal Server.

Services and Policies

To understand how to use PGP Desktop to automatically and transparently protect your outgoing messages, you need to understand two terms: service and policy.

- **Service.** Information about one email account on your system and the policies that apply to that account. In most cases, PGP Desktop will automatically create and configure a service for each email account on your system. In some circumstances, you may want to create and configure a service manually.
- **Policy.** A set of one or more instructions that tell PGP Desktop what to do in specific situations. Policies are associated with services—often more than one (a policy can be reused by different services). Conversely, a service can (and usually does) have more than one policy.

When deciding how to handle a specific outgoing email message, PGP Desktop checks the policies configured for the service one at a time (from the top of the list going down). When it finds a policy that applies, it stops checking policies and implements the one that applies.

All new services are created with the following default policies:

- **Mailing List Admin Requests.** Specifies that administrative requests to mailing lists are sent in the clear; that is, not encrypted or signed.
- **Mail List Submissions.** Specifies that submissions to mailing lists are sent signed (so they can be authenticated) but not encrypted.
- **Require Encryption: [PGP] Confidential.** Specifies that 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 cannot be sent.
- **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 always be sent, albeit in the clear, even if a key to encrypt it to the recipient cannot be found.

Do not put Opportunistic Encryption first in the list of policies (or anywhere but last, for that matter) because when PGP Desktop finds a policy that matches, and Opportunistic Encryption matches everything, it stops searching and implements the matching policy. So if a policy is lower on the list than Opportunistic Encryption, it will never be implemented.

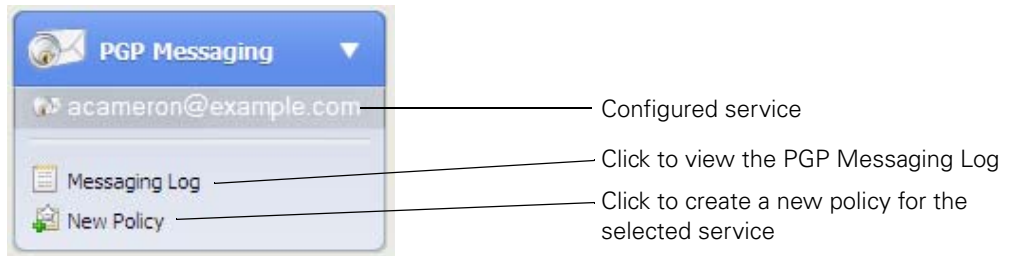


The default policies can be modified, but not deleted. Alternatively, they can be disabled, then moved up or down in the list of policies.

To view services and policies:

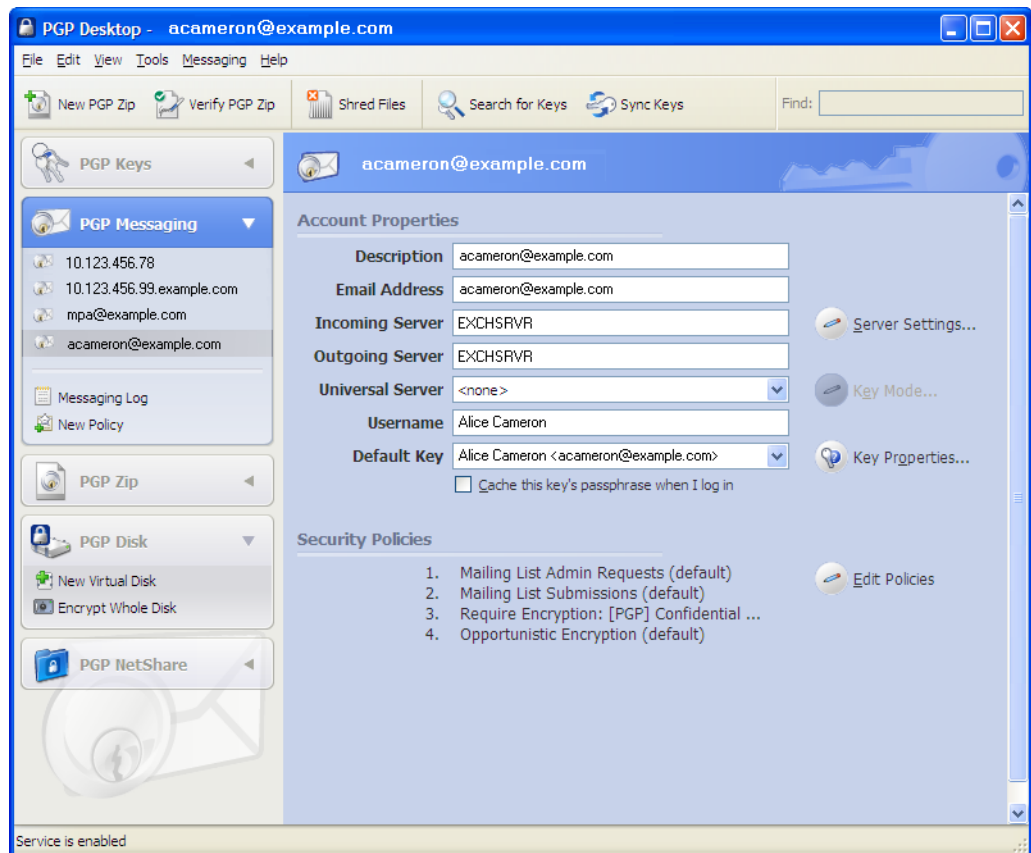
- 1 Open PGP Desktop.
- 2 Click the PGP Messaging Control box.

The PGP Messaging Control box highlights.




All currently configured services are listed at the top of the PGP Messaging Control box.

- 3 Click on a service to see the account properties and the security policies that are part of the service.



Creating a Service and Editing Account Properties

A service is information about an email account, as well as the security policies that are to be applied to outgoing messages for that email account.

 In most cases, PGP Desktop creates services for you as you use your email accounts to send or receive messages. If you need to create a service yourself, make sure to read and understand these instructions. Incorrect configuration of a service could result in problems sending or receiving email messages.

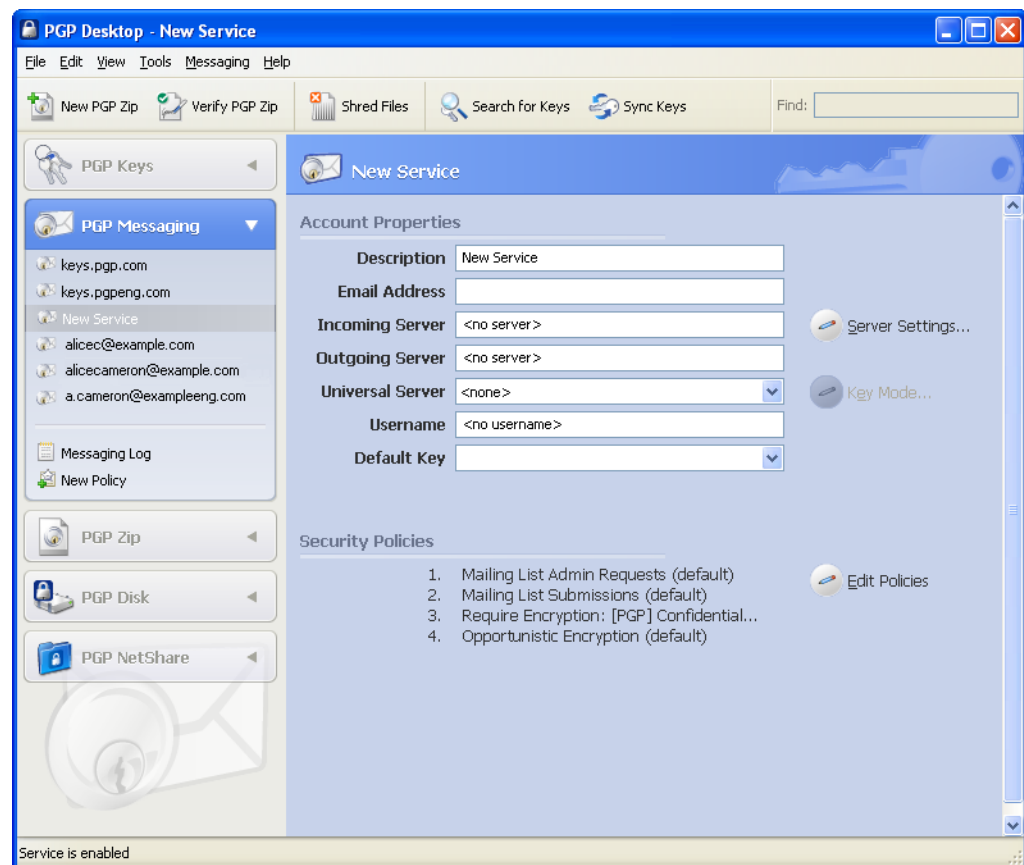
To create a new service:

- 1 Open PGP Desktop and click the PGP Messaging Control box.

The PGP Messaging Control box highlights.

- 2 Click **New Messaging Service** in the PGP Messaging Control box. You can also select **Messaging > Create New Service**.

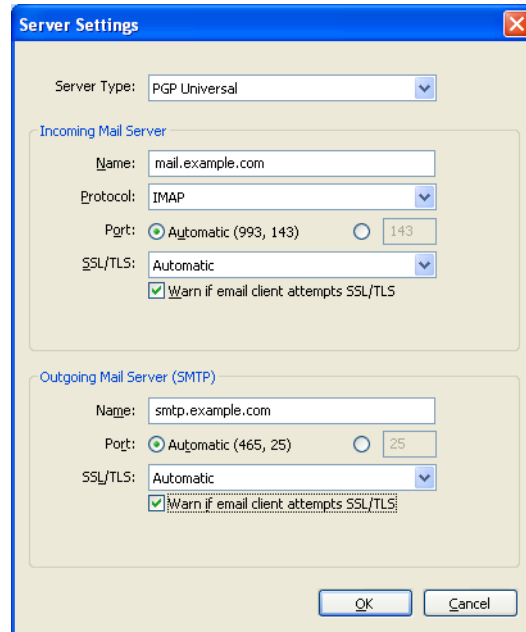
In the PGP Messaging Work area, "New Service" appears at the top of the screen, the account properties appear with no values, and the default security policies appear in the Security Policies section.



- 3 In the **Description** field of the Account Properties section, specify a name for this service.
- 4 Type your email address in the **Email Address** field.
- 5 Type the name of your incoming and outgoing email servers, or click **Server Settings** if you want to set advanced options.

If you chose to set advanced options, the Server Settings dialog appears

- 6 Type the appropriate settings:



Server Type

Select the type of server that the new service will be using:

- **Internet Mail**—for standalone PGP Desktop users who have a POP or IMAP mail connections.
- **PGP Universal**—for PGP Desktop users who are in a PGP Universal-managed environment. Contact your PGP Universal administrator for more details on correct settings.
- **MAPI/Exchange**—for PGP Desktop users who are using Microsoft Outlook as a client on a Microsoft Exchange/MAPI server. Contact your mail administrator for more information on correct settings.
- **Lotus Notes**—for PGP Desktop users who are using Lotus Notes as their email client with a Lotus Domino server. Contact your email administrator for more information on correct settings.

Some of the fields in the **Server Settings** dialog box change depending on what type of server you select.

Incoming Mail Server

- **Name:** Type the name of the mail server that handles incoming messages.
- **Protocol:** Select the protocol used to pick up messages on the incoming mail server.

The **Automatic** setting (available with the **Internet Mail** or **PGP Universal** settings) can automatically detect either POP or IMAP connections.

- **Port:** Keep Automatic (the default) or specify a port to connect to on the incoming mail server to pick up messages (if you have selected either the **Internet Mail** or **PGP Universal** settings and either **POP** or **IMAP**—not **Automatic**).
- **SSL/TLS:** Specify how PGP Desktop interacts with your mail server. Choose one:
 - a Automatic:** PGP will do its best to provide SSL/TLS protection. It first tries the alternate port, then it attempts STARTTLS (if supported by the server), finally, if the above fails, it connects to the server unprotected.
 - b Require STARTTLS:** PGP Desktop requires that the server honor the STARTTLS command.
 - c Require SSL:** PGP Desktop requires that the server honor SSL-protected connections on the specified alternate port.
 - d Do Not Attempt:** PGP Desktop does not attempt any SSL/TLS protection of the connection with the mail server.
- **Warn if email client attempts SSL/TLS:** When selected, PGP Desktop displays a warning dialog if the email client attempts SSL/TLS, as this is a condition that is incompatible with PGP Desktop proxying your email. (This option is selected by default.)



This option should only be enabled if you are certain your mail server supports SSL. It ensures that PGP Desktop will not fall back to sending or receiving messages with the mail server over an unprotected connection if, for example, a problem occurs while negotiating SSL protection for the connection. **If you enable this option and your mail server does not support SSL, PGP Desktop will not send or receive any of your messages.**

Outgoing Mail Server (SMTP)

- **Name:** Type the name of the mail server that handles outgoing messages.
- **Port:** Keep **Automatic (465, 25)** or specify another port to connect to on the outgoing mail server to send messages.

This option is only available for the outgoing mail server if your settings permitted choosing it for the incoming mail server.

- **SSL/TLS:** Specify how PGP Desktop interacts with your mail server. Choose one:
 - a Automatic:** PGP will do its best to provide SSL/TLS protection. It first tries the alternate port, then it attempts STARTTLS (if supported by the server), finally, if the above fails, it connects to the server unprotected.
 - b Require STARTTLS:** PGP Desktop requires that the server honor the STARTTLS command.
 - c Require SSL:** PGP Desktop requires that the server honor SSL-protected connections on the specified alternate port.
 - d Do Not Attempt:** PGP Desktop does not attempt any SSL/TLS protection of the connection with the mail server.
- **Warn if email client attempts SSL/TLS:** When selected, PGP Desktop displays a warning dialog if the email client attempts SSL/TLS, as this is a condition that is incompatible with PGP Desktop proxying your email. (This option is selected by default.)



This option should only be enabled if you are certain your mail server supports SSL. It ensures that PGP Desktop will not fall back to sending or receiving messages with the mail server over an unprotected connection if, for example, a problem occurs while negotiating SSL protection for the connection. **If you enable this option and your mail server does not support SSL, PGP Desktop will not send or receive any of your messages.**

- 7 Click **OK** when you are finished.
- 8 In the **Universal Server field**, select the name of the PGP Universal Server protecting the email domain you are in. **<None>** appears if you are not in an email domain protected by a PGP Universal Server. If your domain is protected by a PGP Universal Server, but it is not listed, select **<create new>** to enter the name of your PGP Universal Server. Check with your PGP Universal administrator for more information.
- 9 Click **Key Mode**

The **Key Management Mode** dialog box appears, displaying your current key mode. If necessary, click **Reset Key**, which launches the Key Setup Assistant.
- 10 Click **OK**.
- 11 In the **Username** field, type the username on the email account.
- 12 In the **Default Key** field, the current key displays.
 - If you are using PGP Desktop as a standalone product, you can either keep the default key, or select another one from the menu (if another key is available).
 - If you are using PGP Desktop in a PGP Universal-managed environment, the default key is displayed and you cannot change it. If you need to change your key, you must click Key Mode and go through the procedure to reset your key on the PGP Universal server.

- 13** Enable **Cache this key's passphrase when I log in** (by selecting the checkbox) if you want to cache the passphrase for the keypair you just selected when you log in.

If you don't cache the key's passphrase, you will be prompted for it when you are sending signed messages or receiving encrypted messages.

- 14** In the **Security Policies provided by [server name]** section, the current policies that apply to you are displayed. You can keep the default security policies, disable the default security policies, or add new policies if you are using PGP Desktop as a standalone product. If you are using PGP Desktop in a PGP Universal-managed environment, your options are likely to be different, depending on what your PGP Universal administrator has specified.

See "[Creating a New Security Policy](#)" on page 39 for more information about creating a new policy or editing existing ones.

- 15** If you have edited any policies, you must click **Done** when you are finished.

Otherwise, when you are done with the security policies, the account is ready. It is not necessary to click a button to save your information. It was saved as soon as you typed it.

To make changes to the account properties of an existing service:

- 1** Open PGP Desktop and click the PGP Messaging Control box.

The PGP Messaging Control box highlights.

- 2** Click on the name of the service whose account properties you want to edit.

The settings for the selected service appear in the PGP Messaging Work area.

- 3** Make the desired changes to the account properties of the service.

Disabling, Enabling, and Deleting a Service

If you want to stop a service from working, but you don't want to delete the service because you might need it again, you can disable the service. This is useful if you only want PGP Desktop to process mail on particular accounts, but not others. If you are certain that you won't need the service again, delete it.

To disable an existing service:

- 1** In the PGP Messaging Control box, click the name of the service you want to disable.

The settings for the service appear in the PGP Messaging Work area.

- 2** Select **Messaging > Disable Service**.

The service is disabled.

PGP Desktop alerts you that the change may not take place until you restart your email client.

To enable a disabled service:

- 1 In the PGP Messaging Control box, click on the name of the service you want to enable.

The settings for the service appear in the PGP Messaging Work area.

- 2 Select **Messaging > Enable Service**.

The service is enabled.

PGP Desktop alerts you that the change may not take place until you restart your email client.

To delete a service:

- 1 Click the name of the service you want to delete.

The settings for the service appear in the PGP Messaging Work area.

- 2 From the **Messaging** menu, select **Delete Service**.

The service is deleted.

You can disable, enable, and delete services by right-clicking the name in the PGP Messaging Control Box and selecting the desired command.

PGP Desktop and SSL

When you use PGP Desktop, PGP Corporation's goal is for your data to be automatically protected whenever possible. This includes protecting your data in transit between your email client and your mail server.



SSL stands for Secure Sockets Layer, which is a cryptographic protocol that secures communications between two devices; in this case, between your email client or PGP Desktop and your mail server.

PGP Desktop protects your data to and from your mail server in different ways depending on the circumstances. The following information applies only if you selected **Automatic** (the default) for the SSL/TLS setting in the server settings dialog:

- **When the connection is not SSL protected.** If the connection between your email client and your mail server is not SSL protected, PGP Desktop will automatically attempt to upgrade that connection to SSL (it will negotiate with your mail server and upgrade the connection if the mail server supports it).

If the mail server does not support SSL, the message(s) PGP Desktop sends and receives during the session will be over an unprotected connection. Whether or not those messages will be encrypted/decrypted by PGP Desktop does not affect the attempt by PGP Desktop to upgrade the connection. Messages encrypted by PGP Desktop can be sent or received over a connection protected by SSL or not protected by SSL.

PGP Desktop always attempts to upgrade an unprotected connection to the mail server to SSL protection because an SSL-protected connection not only protects any non-PGP-encrypted messages on their way to the mail server or coming from it, but it also protects your mail server authentication passphrase when it is sent to the mail server.

- **When the connection is protected by SSL.** If you have SSL protection turned on in your email client for the connection to your mail server, you must turn it off if you want PGP Desktop to encrypt or decrypt your messages; PGP Desktop cannot process your messages if they are already SSL-encrypted.

Turning off SSL protection in your email client does not mean that your non-PGP-encrypted messages are now unprotected going to or coming from your mail server. As with any connection that is not SSL protected, PGP Desktop will automatically attempt to upgrade the connection to SSL protection if the mail server supports it (if you selected **Automatic** for the SSL/TLS setting in the server settings dialog). If the mail server does not support SSL connections, the messages PGP Desktop sends during the session will be over an unprotected connection.

The only time your messages will be sent in the clear to your mail server is if the messages are not PGP encrypted and the connection to the mail server cannot be upgraded to SSL protected, or you have selected the **Do Not Attempt** option in the SSL/TLS setting.

- **When you can't have messages sent in the clear.** Some security policies require that only protected messages can be sent; in other words, unprotected messages must never be sent. If necessary, you can configure PGP Desktop to support this kind of security policy.

Select the applicable PGP Messaging service, access the Server Settings dialog (click the name of the server currently in the Server field of the Account Properties for the service), and choose an option from the SSL/TLS menu **other than Automatic**.

When this option is enabled, PGP Desktop will only send messages to or receive messages from your mail server if the connection between them is SSL protected. If an SSL-protected connection cannot be established, PGP Desktop will not interact with the server.



This option should only be enabled if you are certain your mail server supports SSL. It ensures that PGP Desktop will not fall back to sending or receiving messages with the mail server over an unprotected connection if, for example, a problem occurs while negotiating SSL protection for the connection. If you enable this option and your mail server does not support SSL, PGP Desktop will not send or receive any of your messages.

- **When you want SSL enabled in your email client.** If you want to use PGP Desktop with SSL enabled in your email client, you can do that; you just have to tell PGP Desktop that you are doing it by deselecting the option **Warn if email client attempts SSL/TLS** for your incoming or outgoing mail server, or both. When you disable this option for a connection to a mail server, PGP Desktop will ignore traffic coming in from or going out over that connection when the connection is protected by SSL.

PGP Desktop will monitor the connections to and from this server, ignoring traffic sent or received on SSL-protected connections. If, however, PGP Desktop detects a non-SSL-protected connection, it will handle the traffic like any other unprotected connection; it will attempt to upgrade the connection to SSL (if in Automatic mode) and it will apply applicable policies to messages.

Multiple Services

Some email services and Internet Service Providers use multiple mail servers for a single DNS name in a round-robin fashion such that PGP Desktop may create multiple messaging services for a single email account, seeing each mail server as separate and thus requiring its own messaging service.

PGP Desktop ships with wildcard support for common email services, such as ***.yahoo.com** and ***.mac.com**. However, if you are using a less-common email service or if the services change their mail server configurations, you could run into this problem.

If you see PGP Desktop create multiple services for a single email account, and you check the settings and see they are the same except the mail server for the first service is **mail1.example.com**, the mail server for the second service is **mail2.example.com**, and the mail server for the third is **mail3.example.com**, and so on, you may need to manually edit one of the services.

The best solution is to manually edit one of the services such that the mail server entry for that service can support *multiple* mail servers being used round robin. For the example cited above, you could manually change the server name on the Server Settings screen for one of the services to **mail*.example.com**, then delete the other services.

Some round-robin setups may be more complicated, requiring a slightly different solution. For example, if PGP Desktop were to create services with mail servers of **pop.frodo.example.com**, **smtp.bilbo.example.com**, and **mail.example.com**, then the best wildcard solution would be ***.example.com**.


Troubleshooting Services

By default, PGP Desktop automatically determines your email account settings and creates a PGP Messaging service that proxies messaging for that email account.

Because of the large number of possible email account settings and mail server configurations, on some occasions a messaging service that PGP Desktop automatically creates may not work quite right.

If PGP Desktop has created a messaging service that isn't working right for you, one or more of the following items may help correct the problem:

- Verify that you can both connect to the Internet and send and receive email with PGP Services stopped (right-click the PGP Desktop tray icon and select **Stop PGP Services** from the list of commands).

 You should always restart your email client after starting or stopping PGP Services.

- Read the PGP Desktop Release Notes for the version of PGP Desktop you are using to see if your problem is a known issue.
- Make sure SMTP authentication is enabled for the email account (in your email client). This is recommended for PGP Desktop to proxy your messaging. If you only have one email account and you are not using PGP Desktop in a PGP Universal-managed environment, then SMTP authentication is not needed. It **is** required when using a PGP Universal server as your SMTP server, or when you have multiple email accounts on the same SMTP server.
- Open the Messaging Log to see if the entries offer any clues as to what the problem might be.
- If SSL/TLS is enabled in your email client, you must disable it there if you want PGP Desktop to proxy your messaging. (This does **not** leave the connection to and from your mail server unprotected; PGP Desktop by default automatically attempts to upgrade any unprotected connection to SSL/TLS protection. The mail server must support SSL/TLS for the connection to be protected.)
- If either **Require STARTTLS** or **Require SSL** are selected (in the SSL/TLS settings of the Server Settings screen) your mail server *must* support SSL/TLS or PGP Desktop won't send or receive any messages.
- If your email account uses non-standard port numbers, make sure these are included in the settings of your messaging service.
- If PGP Desktop is creating multiple messaging services for one email account, refer to the PGP Desktop Release Notes for instructions how to create a wildcarded mail server name.
- Delete the PGP Messaging service that is not working correctly and send/receive email, which regenerates the messaging service.

If none of these items help correct the problem, try the following:

- 1 Delete the PGP Messaging service that isn't working right.
- 2 Stop all PGP Desktop services (right-click the PGP Desktop tray icon and select **Stop PGP Services** from the list of commands), then exit from PGP Desktop if it was open.
- 3 Verify that you have Internet connectivity and can send and receive email with PGP Messaging services stopped.
- 4 Open your email client and write down your email account settings (including username, email address, incoming and outgoing mail server, incoming mail server protocol, and any non-standard mail server ports).
- 5 Close your email client and restart PGP Desktop, which restarts PGP services (either restart Windows or open PGP Desktop from the Windows start menu).

- 6 Manually create a PGP Messaging service using the account settings you wrote down.
- 7 Open your email client and begin sending and receiving messages.

If you continue to have problems with a PGP Messaging service, access any of the following for assistance:

- The PGP Corporation website: www.pgp.com
- The PGP Support website: www.pgp.com/support
- The PGP Support forums: forums.pgpsupport.com

Creating a New Security Policy

Security policies are what control how PGP Desktop handles outgoing email messages.



When you create a new security policy, you are creating a messaging security policy, not a mailing list policy. You cannot create a new mailing list policy, but you can edit the default mailing list policies.

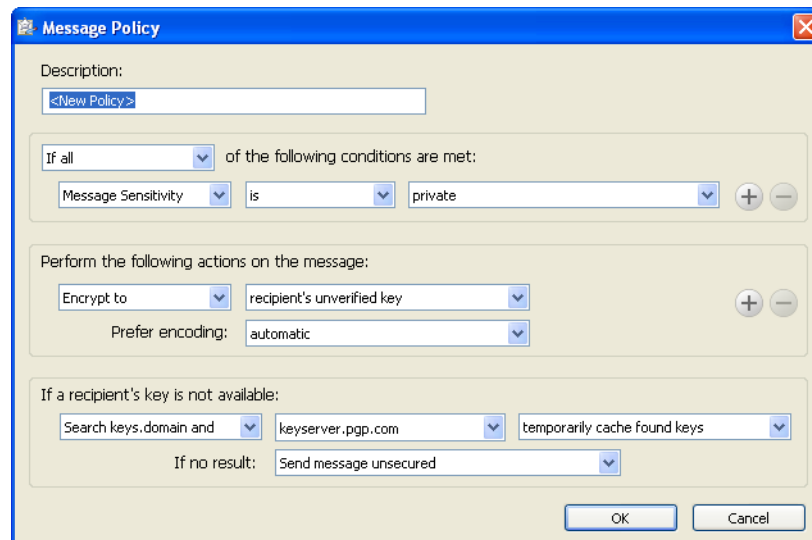
To create a new security policy:

- 1 In the PGP Messaging Control box, click on the name of the service for which you want to create a new security policy.

The settings for the service appear in the PGP Messaging Work area, including the list of existing security policies.

- 2 Do one of the following"
 - Click **New Policy** in the PGP Messaging Control box.
 - From the **Messaging** menu, select **New Messaging Policy**.

The Message Policy dialog appears.



If your email domain is protected by a PGP Universal Server, and you look at the Message Policy settings for a policy from a PGP Universal Server, the fields may be different from the fields shown above.

- 3 In the **Description** field, type a descriptive name for the policy you are creating.
- 4 In the **First Section (stating the policy conditions)**:
 - a In the **If** field, select:
 - **If any**. The policy applies when any condition is met.
 - **If all**. The policy only applies when all conditions are met.
 - **If none**. The policy only applies if none of the conditions are met.
 - b In the first condition field, select:
 - **Recipient**. The policy applies only to messages to the specified recipient.
 - **Recipient Domain**. The policy applies only to email messages in the specified recipient domain.
 - **Sender**. The policy applies only to messages with the specified sender address.
 - **Message**. The policy applies only to messages which have the specified signed and/or encrypted state.
 - **Message Subject**. The policy applies only to messages with the specified message subject.
 - **Message Header**. The policy applies only to messages for which the specified header meets the specified criterion. Note that the conditions described in the next section (is, is not, contains, and so on) apply to the text typed in the text box that appears when you select **Message Header**.



When searching message headers in MAPI email systems, you can search on the Subject, Sensitivity, Priority, and Importance headers only.

- **Message Body.** The policy applies only to messages with the specified message body.
 - **Message Size.** The policy applies only to messages of the specified size (in bytes).
 - **Message Priority.** The policy applies only to messages with the specified message priority.
 - **Message Sensitivity.** The policy applies only to messages with the specified message sensitivity.
- c** In the second condition field, select:
- **is.** The condition is met when text in the first condition field *matches* the text typed in the text box.
 - **is not.** The condition is met when text in the first condition field *does not match* the text typed in the text box.
 - **contains.** The condition is met when text in the first condition field *contains* the text typed in the text box.
 - **does not contain.** The condition is met when text in the first condition field *does not contain* the text typed in the text box.
 - **begins with.** The condition is met when text in the first condition field *begins with* the text typed in the text box.
 - **ends with.** The condition is met when text in the first condition field *ends with* the text typed in the text box.
 - **matches pattern.** The condition is met when text in the first condition field *matches the pattern* typed in the text box.
 - **greater than.** The condition is met when message size is *greater than* the text typed in the text box
 - **less than.** The condition is met when message size is *less than* the text typed in the text box
- d** In the third condition field, select:
- **text entry box.** Type text for the matching criteria.
 - **normal.** Matching criteria for Message Sensitivity is *normal*.
 - **personal.** Matching criteria for Message Sensitivity is *personal*.
 - **private.** Matching criteria for Message Sensitivity is *private*.
 - **confidential.** Matching criteria for Message Sensitivity is *confidential*.

- **signed**. Matching criteria for Message is signed.
 - **encrypted**. Matching criteria for Message is encrypted.
 - **encrypted to key ID**. Matching criteria for encrypted to key ID (you must then type a key ID in the resulting text box).
 - **low**. Matching criteria for Message Priority is *low*.
 - **normal**. Matching criteria for Message Priority is *normal*.
 - **high**. Matching criteria for Message Priority is *high*.
 - **is less than**. Matching criteria for Message Size is less than (you must then supply an integer representing a size).
 - **is greater than**. Matching criteria for Message Size is more than (you must then supply an integer representing a size).
- 5 In the **Perform the following actions on the message** section:
- a In the first action field, select:
 - **Send In Clear**. Specifies that the message should be sent in the clear; that is, not signed nor encrypted.
 - **Sign**. Specifies that the message should be signed.
 - **Encrypt to**. Specifies that the message should be encrypted.
 - b In the second action field, select:
 - **recipient's verified key**. Ensures the message can be encrypted only to a verified key of the intended recipient.
 - **recipient's unverified key**. Allows the message to be encrypted to an unverified key of the intended recipient.
 - **recipient's verified end-to-end key**. Ensures the message can be encrypted only to a verified end-to-end key of the intended recipient. An end-to-end key is a key in sole possession of the individual recipient. In a PGP Universal-managed environment, this is a Client Key Mode key as opposed to a Server Key Mode key, where the PGP Universal Server is in possession of the key. (Whether the key is end-to-end or not is shown on the **Key Properties** screen in the **Group** field—**No** means that it *is* end-to-end (is not part of a group), and **Yes** means that it *is not* end-to-end.)
 - **recipient's unverified end-to-end key**. Allows the message to be encrypted to an unverified end-to-end key of the intended recipient.
 - **a list of keys**. Specifies that the message can only be encrypted to keys on the list.
 - c In the prefer message encoding field, select:


- **automatic.** Lets PGP Desktop choose the message encoding format. This is almost always the best option unless you know exactly why you need to use one of the other message encoding formats explicitly.
 - **PGP Partitioned.** Sets PGP Partitioned as the preferred message encoding format. This format is the most backwards compatible with older PGP and OpenPGP products.
 - **PGP/MIME.** Sets PGP/MIME as the preferred message encoding format. PGP/MIME is able to encrypt and sign the entire message including attachments in one pass and is usually therefore faster and better able to reproduce the full message fidelity.
 - **S/MIME.** Sets S/MIME as the preferred message encoding format. Choose S/MIME if, for some reason, you need to force messages to be S/MIME even if the user has a PGP key.
- 6 In the **Recipient's key is not available** section:
- a In the first **Key Not Found** field, select:
 - **Search keys.domain and.** Specifies a search that includes both keys.domain as well as another server you specify.
 - **Search.** Allows for searching for an appropriate key if one is not found on the local keyring.
 - **Clear-sign message.** Specifies that the message should be sent in the clear, but signed.
 - **Send message unsecured.** Specifies that the message be sent in the clear.
 - **Block message.** Specifies that the message must not be sent if an appropriate key is not found.
 - b In the second Key Not Found field, select:
 - **All keyserver.** Allows all keyserver, including the PGP Global Directory, to be searched for an appropriate key.
 - **[configured keyserver].** Specifies that only the keyserver you choose from the list of currently configured keyserver is searched. Note that keyserver other than the PGP Global Directory may provide unverified keys that cannot be used if you require verified keys in the policy. Unless you know exactly why you need to search another keyserver and are prepared to find those keys manually to verify them when necessary, search only on the PGP Global Directory.
 - **Edit Keyserver List.** Lets you add keyserver to the list of currently configured keyserver.
 - c In the last Key Not Found field, specify:

- **temporarily cache found keys.** Specifies that a found key should be temporarily saved in memory. Keys in this cache will automatically be used when verifying signed messages, and will be used for encryption if they have been verified.
 - **ask to save found keys.** Specifies that PGP Desktop should ask if you want to save to your local keyring a particular found key.
 - **save found keys.** Specifies that found keys should automatically be saved to your local keyring.
- d In the If no result field, select:
- **Clear-sign message.** Allows messages for which an encryption key has not been found to be signed and sent in the clear.
 - **Send message unsecured.** Do not encrypt message.
 - **Block message.** Prevents message for which an encryption key has not been found from being sent.
- 7 Click **OK** when the policy settings are configured.
- The new policy appears in the list of security policies.

Wildcards and Regular Expressions in Policies


PGP Desktop supports the use of wildcards and regular expressions in security policies in text entry boxes.

Using wildcards and regular expressions lets you match multiple text strings using a single text string.

 In addition to the examples, PGP Desktop also supports broader regular expressions that adhere to standard formats. The "Matches Pattern" criteria actually means "matches regular expression."

Security Policy Information and Examples

When you create a service, four security policies are automatically created. This section describes how the four default security policies work (Opportunistic Encryption, Require Encryption: [PGP] Confidential, Mailing List Submissions, and Mailing List Admin Requests). It also describes two example situations for which you might want to create a security policy and explains how to configure them.

 If you make any changes to the default policies and want to restore the default settings, click **Revert to Default** in the Message Policy dialog box.

Opportunistic Encryption Default Policy

Opportunistic Encryption is one of the four default security policies that PGP Desktop automatically creates for a service.

The settings for **Opportunistic Encryption** are:

- **If:** any
- **Conditions:** Recipient Domain / is / *
- **Actions:** Sign / Encrypt to / recipient's verified key
- **Prefer message encoding:** automatic
- **Key Not Found:** Search keys.domain and / keyserver.pgp.com/ temporarily cache found keys
- **If no result:** Send message unsecured

Opportunistic Encryption causes those messages for which a verified key can be found to be sent signed and encrypted. Those messages for which a verified key cannot be found are delivered with no encryption (in the clear). This ensures your messages get sent, although some may be sent in the clear.

Opportunistic Encryption was designed to go last in your list of security policies, as it will match any message sent. If placed above a policy in the list, PGP Desktop will never reach that policy, thus rendering it useless.

Require Encryption: [PGP] Confidential Default Policy

Require Encryption: Confidential is one of the four default security policies that PGP Desktop automatically creates for a service.

The settings for Require Encryption: [PGP] Confidential are:

- **If:** any
- **Conditions:** Message Subject / contains / [PGP] Message Sensitivity / is / confidential
- **Actions:** Sign / Encrypt to / recipient's verified key
- **Prefer message encoding:** automatic
- **Key Not Found:** Search keys.domain and / All Keyserver / temporarily cache found keys
- **If no result:** Block message

Require Encryption: [PGP] Confidential causes those messages with subjects that contain [PGP] or are marked confidential in your email client to require encryption to a verified key in order to be sent. If a verified key cannot be found, the message is *not* sent.

Mailing List Submission Default Policy

Mailing List Submission is one of the four default security policies that PGP Desktop automatically creates for a service.

The settings for Mailing List Submission are:

- **If:** If any
- **Conditions:** Recipient / matches pattern/ .*-users@.* , .*-bugs@.* , .*-docs@.* , .*-help@.* , .*-news@.* , .*-digest@.* , .*-list@.* , .*-devel@.* , .*-announce@.* ,
- **Actions:** Sign
- **Prefer Encoding:** PGP Partitioned

Mailing List Admin Requests Default Policy

Mailing List Admin Requests is one of the four default security policies that PGP Desktop automatically creates for a service.

The settings for Mailing List Admin Requests are:

- **If:** If any
- **Conditions:** Recipient / matches pattern/ .*-subscribe@.* , .*-unsubscribe@.* , .*-report@.* , .*-request@.* , .*-bounce@.* ,
- **Actions:** Send in clear

Example of a Policy to Require Encryption to <Domain>

If you use Opportunistic Encryption with its default settings and you put it at the bottom of the list of policies, it will cause those messages for which a verified key cannot be found to be delivered in the clear. This ensures that your messages get sent, but it also means that some may be sent in the clear.

If there are specific domains to which sending in the clear is not an option, you can create a security policy that calls for encrypting and/or signing or the message is *not* sent. When you create this policy, make sure it is higher in the list than Opportunistic Encryption.

- **If:** any
- **Conditions:** Recipient Domain / is / example.com
- **Actions:** Encrypt to / recipient's verified key
- **Prefer message encoding:** automatic
- **Key Not Found:** Search keys.domain and / All Keyservers / temporarily cache found keys
- **If no result:** Block message

This security policy is similar to Require Encryption: [PGP] Confidential in that it requires a message be encrypted or the message is not sent, but the criteria is not whether the message is marked confidential but rather that the email domain of the recipient is example.com. Using this policy ensures all messages to example.com are encrypted with a verified key or they are not sent.

Example of a Policy to Sign and Send in the Clear to a Specific Domain

If you regularly send email to a domain for which you want to sign all messages but not encrypt them, you should set up a policy for that domain.

- **If:** any
- **Conditions:** Recipient Domain / is / example.com
- **Actions:** Sign
- **Prefer message encoding:** automatic

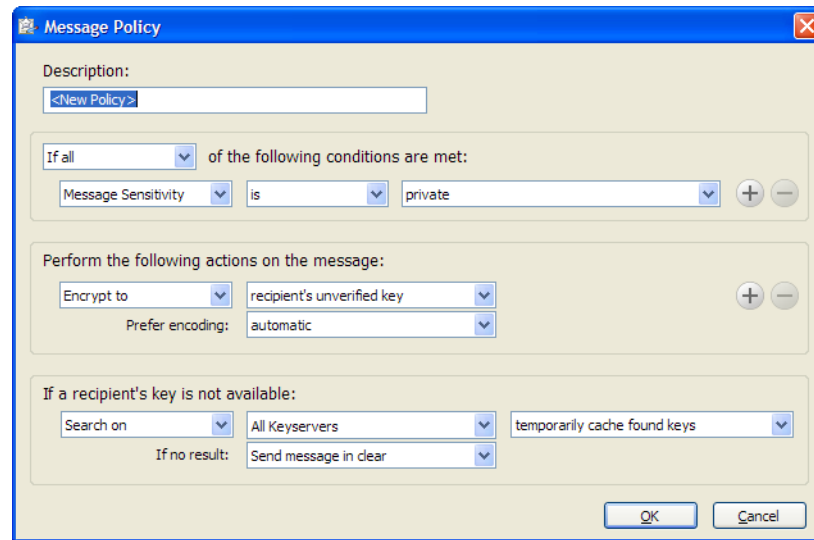
Working with the Security Policy List

There are several important things you can do to the security policies in the list of security policies, such as edit a policy, add a new policy (described in ["Creating a New Security Policy" on page 39](#)), delete a policy, and change the order of policies in the list.

Editing a Security Policy

To edit an existing security policy:

- 1 Open PGP Desktop and click the PGP Messaging Control box.
The PGP Messaging Control box highlights.
- 2 In the PGP Messaging Control box, click on the name of the service that has the security policy you want to edit.
The properties for the service you selected appear in the PGP Messaging Work area.
- 3 Click on the **Edit Policies** button.
- 4 In the list of security policies, click on the policy you want to edit.
The specified policy highlights.
- 5 Click **Edit Policy**.
The Message Policy dialog appears, displaying the current settings for the specified policy.



The default policies can be viewed, modified, and disabled, but not deleted.

- 6 Make the desired changes to the policy.

Refer to [“Creating a New Security Policy” on page 39](#) and [“Security Policy Information and Examples” on page 44](#) for information about the fields on the Message Policy dialog.

- 7 When you have made the desired changes, click **OK** to close the Message Policy dialog.

The specified security policy is changed.

- 8 Click **Done**.

Editing a Mailing List Policy

To edit a default Mailing List policy:

- 1 Open PGP Desktop and click the PGP Messaging Control box.

The PGP Messaging Control box highlights.

- 2 In the PGP Messaging Control box, click on the name of the service that has the security policy you want to edit.

The properties for the service you selected appear in the PGP Messaging Work area.

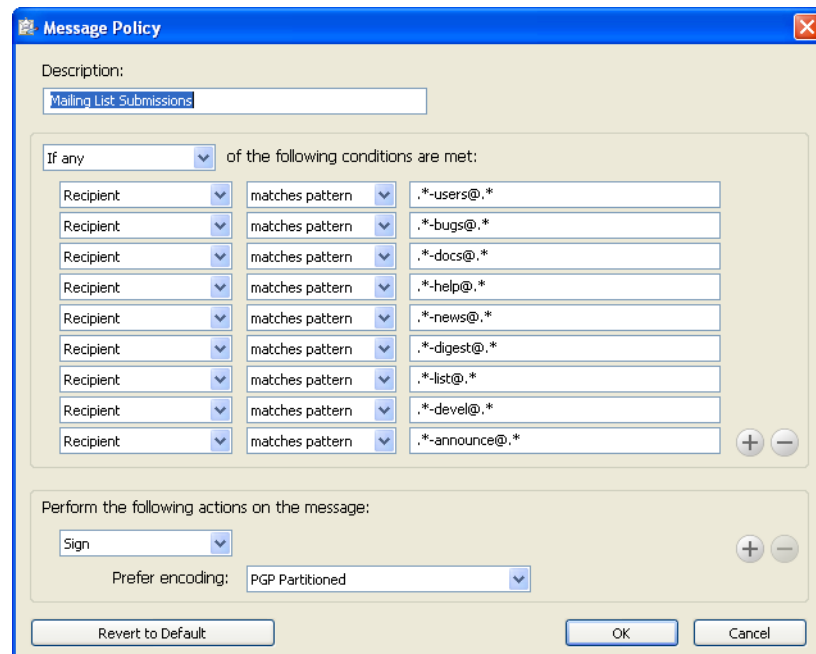
- 3 Click on the **Edit Policies** button.

- 4 In the list of security policies, click on the Mailing List policy you want to edit.

The selected policy highlights.

- 5 Click **Edit Policy**.

The Message Policy dialog appears, displaying the current settings for the specified policy.



The default policies can be viewed, modified, and disabled, but not deleted.

- 6 Make the desired changes to the policy:
 - a In the first field, select:
 - **If any.** The policy applies when any condition is met.
 - **If all.** The policy only applies when all conditions are met.
 - **If none.** The policy only applies if none of the conditions are met.
 - b In the first condition field, select:
 - **Recipient.** The policy applies only to messages to the specified recipient.
 - **Recipient Domain.** The policy applies only to email messages in the specified recipient domain.
 - **Sender.** The policy applies only to messages with the specified sender address.
 - **Message.** The policy applies only to messages which have the specified signed and/or encrypted state.
 - **Message Subject.** The policy applies only to messages with the specified message subject.

- **Message Header.** The policy applies only to messages for which the specified header meets the specified criterion. Note that the conditions described in the next section (is, is not, contains, and so on) apply to the text typed in the text box that appears when you select **Message Header**.



Searching message headers in Lotus Notes and MAPI email systems is not implemented, as messages in these systems do not include headers.

- **Message Body.** The policy applies only to messages with the specified message body.
 - **Message Size.** The policy applies only to messages of the specified size (in bytes).
 - **Message Priority.** The policy applies only to messages with the specified message priority.
 - **Message Sensitivity.** The policy applies only to messages with the specified message sensitivity.
- c** In the second condition field, select:
- **is.** The condition is met when text in the first condition field *matches* the text typed in the text box.
 - **is not.** The condition is met when text in the first condition field *does not match* the text typed in the text box.
 - **contains.** The condition is met when text in the first condition field *contains* the text typed in the text box.
 - **does not contain.** The condition is met when text in the first condition field *does not contain* the text typed in the text box.
 - **begins with.** The condition is met when text in the first condition field *begins with* the text typed in the text box.
 - **ends with.** The condition is met when text in the first condition field *ends with* the text typed in the text box.
 - **matches pattern.** The condition is met when text in the first condition field *matches the pattern* typed in the text box.
- d** In the third condition field, in the **text entry box**, type the text for the matching criteria.
- 7** In the **Perform the following actions on the message** section:
- a** In the first action field, select:
- **Send In Clear.** Specifies that the message should be sent in the clear; that is, not signed nor encrypted.
 - **Sign.** Specifies that the message should be signed.

- **Encrypt to.** Specifies that the message should be encrypted.
- b** In the second action field, select:
- **recipient's verified key.** Ensures the message can be encrypted only to a verified key of the intended recipient.
 - **recipient's unverified key.** Allows the message to be encrypted to an unverified key of the intended recipient.
 - **recipient's verified end-to-end key.** Ensures the message can be encrypted only to a verified end-to-end key of the intended recipient. An end-to-end key is a key in sole possession of the individual recipient. In a PGP Universal-managed environment, this is a Client Key Mode key as opposed to a Server Key Mode key, where the PGP Universal Server is in possession of the key. (Whether the key is end-to-end or not is shown on the **Key Properties** screen in the **Group** field—**No** means that it *is* end-to-end (is not part of a group), and **Yes** means that it *is not* end-to-end.)
 - **recipient's unverified end-to-end key.** Allows the message to be encrypted to an unverified end-to-end key of the intended recipient.
 - **a list of keys.** Specifies that the message can only be encrypted to keys on the list.
- c** In the prefer message encoding field, select:
- **automatic.** Lets PGP Desktop choose the message encoding format. This is almost always the best option unless you know exactly why you need to use one of the other message encoding formats explicitly.
 - **PGP Partitioned.** Sets PGP Partitioned as the preferred message encoding format. This format is the most backwards compatible with older PGP and OpenPGP products.
 - **PGP/MIME.** Sets PGP/MIME as the preferred message encoding format. PGP/MIME is able to encrypt and sign the entire message including attachments in one pass and is usually therefore faster and better able to reproduce the full message fidelity.
 - **S/MIME.** Sets S/MIME as the preferred message encoding format. Choose S/MIME if, for some reason, you need to force messages to be S/MIME even if the user has a PGP key.
- 8** In the **Recipient's key is not available** section:
- a** In the first **Key Not Found** field, select:
- **Search keys.domain and.** Specifies a search that includes both keys.domain as well as another server you specify.
 - **Search.** Allows for searching for an appropriate key if one is not found on the local keyring.
 - **Clear-sign message.** Specifies that the message should be sent in the clear, but signed.

- **Send message unsecured.** Specifies that the message be sent in the clear.
 - **Block message.** Specifies that the message must not be sent if an appropriate key is not found.
- b** In the second Key Not Found field, select:
- **All keyserver.** Allows all keyserver, including the PGP Global Directory, to be searched for an appropriate key.
 - **[configured keyserver].** Specifies that only the keyserver you choose from the list of currently configured keyserver is searched. Note that keyserver other than the PGP Global Directory may provide unverified keys that cannot be used if you require verified keys in the policy. Unless you know exactly why you need to search another keyserver and are prepared to find those keys manually to verify them when necessary, search only on the PGP Global Directory.
 - **Edit Keyserver List.** Lets you add keyserver to the list of currently configured keyserver.
- c** In the last Key Not Found field, specify:
- **temporarily cache found keys.** Specifies that a found key should be temporarily saved in memory. Keys in this cache will automatically be used when verifying signed messages, and will be used for encryption if they have been verified.
 - **ask to save found keys.** Specifies that PGP Desktop should ask if you want to save to your local keyring a particular found key.
 - **save found keys.** Specifies that found keys should automatically be saved to your local keyring.
- d** In the If no result field, select:
- **Clear-sign message.** Allows messages for which an encryption key has not been found to be signed and sent in the clear.
 - **Send message unsecured.** Do not encrypt message.
 - **Block message.** Prevents message for which an encryption key has not been found from being sent.
- 9** When you have made the desired changes, click **OK** to close the Message Policy dialog.

The specified security policy is changed.

Deleting a Security Policy

To delete an existing security policy:

- 1** In the PGP Messaging Control box, click on the name of the service that has the security policy you want to delete.

The properties for the service you selected appear in the PGP Messaging Work area.

- 2 Click on the **Edit Policies** button.
- 3 In the list of security policies, click on the policy you want to delete.

The specified policy highlights.

- 4 Click **Remove Policy**.

A PGP Desktop Confirmation dialog appears.

- 5 Click **Delete Policy** to delete the policy or **OK** to disable it.

The specified security policy is deleted or disabled.

- 6 Click **Done**.



Default policies can be disabled, but not deleted

Changing the Order of Policies in the List

To change the order of policies in the Security Policy list:

- 1 In the PGP Messaging Control box, click on the name of the service that has the security policy whose order you want to change.

The properties for the service you selected appear in the PGP Messaging Work area.

- 2 Click on the **Edit Policies** button.

- 3 In the list of security policies, click on the policy whose order in the list you want to change.

The specified policy highlights.

- 4 Click **Move Up** or **Move Down** until the policy is in the desired location in the list.

Make sure **Opportunistic Encryption** is at the bottom of the list. Any policy below it will not be implemented.

- 5 Click **Done**.

Key Modes

If you are using PGP Desktop in a PGP Universal-managed environment, PGP Desktop will have a key mode.



The information in this section applies *only* to users of PGP Desktop in an email domain protected by a PGP Universal Server.

Available key modes are:

- **Server Key Mode (SKM):** Keys are generated on and managed by the PGP Universal Server; they are only shared with the computer on which you are running PGP Desktop as needed. Your private key is stored only on the PGP Universal Server, which also handles all private key management. The PGP Universal administrator has complete access to your private key and can thus access all messages you encrypt. This key mode is **not** compatible with Smart Cards.



PGP Corporation recommends that PGP Desktop users **not** use SKM, as you will not have control over your private key, which is required for most other PGP Desktop features.

- **Client Key Mode (CKM):** Keys are generated on and managed by the computer on which you are running PGP Desktop; private keys are not shared with the PGP Universal Server. All cryptographic operations (encrypt, decrypt, sign, verify) are also handled by the computer on which you are running PGP Desktop. This key mode is compatible with Smart Cards.
- **Guarded Key Mode (GKM):** Very similar to CKM, except that an **encrypted** copy of the private key is stored on the PGP Universal Server, which you can access if you change computers. As the key is encrypted, the PGP Universal administrator cannot access this private key, only you can. This key mode is compatible with Smart Cards as long as the key is not generated directly on the Smart Card; that is, as long as the key is copied to the Smart Card.
- **Server Client Key Mode (SCKM):** Also very similar to CKM, except that a copy of the private *encryption* key is stored on the PGP Universal Server; private *signing* keys never leave the computer on which you are running PGP Desktop. This key mode ensures compliance with laws and corporate policies that require that the private signing key not leave the control of the user, while making sure that the private encryption key is stored in case of emergency. This key mode is compatible with Smart Cards as long as the key is not generated directly on the Smart Card. SCKM requires a key with a separate signing subkey, which can be created for a new key with PGP Desktop 9.5 or greater or added to an older PGP key using PGP Desktop 9.5 or greater.

Depending on how your PGP administrator configured your copy of PGP Desktop, you may or may not be able to choose your key mode. Also, you may or may not be able to change your key mode.

Please contact your PGP administrator if you have additional questions about your key mode.

Determining Key Mode

Remember that only PGP Desktop users in a PGP Universal-protected environment will have a key mode; standalone PGP Desktop users do not have a key mode.

To determine your key mode:

- 1 Open PGP Desktop and select the **PGP Messaging** service whose key mode you want to determine. The account properties and security policies for the selected service appear.

- 2 In the **Universal Server** field, the key mode for the selected service is shown in parentheses after the name of the PGP Universal Server.

For example: **keys.example.com (GKM)**

This tells you that the key mode for the selected service is Guarded Key Mode and that the associated PGP Universal Server is keys.example.com.

Changing Key Mode

Depending on how your PGP administrator configured your copy of PGP Desktop, you may not be able to change your key mode.

To change your key mode:

- 1 Open PGP Desktop and select the **PGP Messaging** service whose key mode you want to determine. The account properties and security policies for the selected service appear.
- 2 Click **Key Mode**. The PGP Universal Key Mode screen appears, describing your current key management mode.
- 3 Click **Reset Key**. The PGP Key Setup Assistant appears.
- 4 Read the text, then click **Next**. The Key Management Selection screen appears.
- 5 Select the desired key mode. Depending on how your PGP Universal administrator configured your copy of PGP Desktop, some key modes may not be available.
- 6 Click **Next**. The Key Source Selection screen appears.
- 7 Choose one of the following:
 - **New Key**. You will be prompted to create a new PGP key, which will be used to protect your messaging.
 - **PGP Desktop Key**. You will be prompted to specify an existing PGP key to use to protect your messaging.
 - **Import Key**. You will be prompted to import a PGP key, which will be used to protect your messaging.
- 8 Make the desired selection, then click **Next**.
- 9 If you selected **New Key**:
 - a Enter a passphrase for the key, then click **Next**.
 - b When the key is generated, click **Next**.
 - c Click **Finish**.
- 10 If you selected PGP Desktop Key:
 - a Select the key from the local keyring that you want to use, then click **Next**.
 - b Click **Finish**.

- 11 If you selected **Import Key**:
 - a Browse to file that holds the PGP key you want to import (it must contain a private key), then click **Next**.
 - b Click **Finish**.

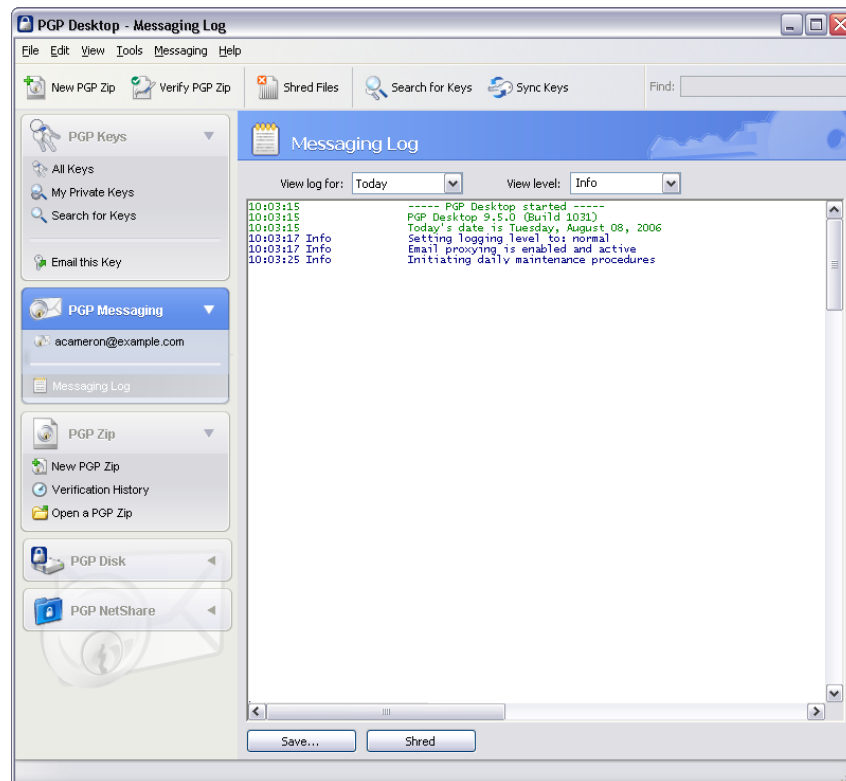
Viewing the PGP Messaging Log

The PGP Messaging Log is a handy way of seeing what actions the PGP Messaging feature is taking to secure your messaging.

To view the PGP Messaging Log:

- 1 Open PGP Desktop and click the PGP Messaging Control box.
The PGP Messaging Control box highlights.
- 2 Click **View Messaging Log** at the bottom of the PGP Messaging Control box or from the **Messaging** menu, select **View Log**.

The PGP Messaging Log appears.



- 3 **View log for** lets you select the day for the logs you wish to view.

- 4 **View level** lets you select the minimum severity of log entries you wish to view: **Error**, **Warn**, **Info**, or **Verbose**. Note that Verbose can result in some large log files.
- 5 Click **Save** to save a copy of the PGP Messaging Log.
- 6 Click **Shred** to clear the entries in the PGP Messaging Log.

5

Securing Instant Messaging

Using PGP Desktop to protect your instant messages

The following topics are available on how to use PGP Desktop to secure your instant messaging (IM) sessions:

- [“About PGP Desktop’s Instant Messaging Support”](#)
- [“Encrypting your IM Sessions” on page 60](#)

Refer to [“Messaging Options” on page 234](#) for information about **PGP Options** that affect IM sessions.


About PGP Desktop’s Instant Messaging Support


PGP Desktop automatically encrypts AOLstandard instant messaging sessions, direct connects, and file transfers if the following conditions are met:

- Both users in the IM session have PGP Desktop 9.0 or later up and running on the system on which they are doing the IM session. You can confirm that you are using PGP Desktop 9.0 or later by clicking the **PGP Tray** icon and selecting **About PGP** from the menu or by pulling down the **Help** menu and selecting **About PGP**.
- Both users have the **Use PGP AIM Proxy** setting enabled. To confirm that **Use PGP AIM Proxy** is enabled on your system, click the **PGP Tray** icon or select the **Tools** menu and verify that **Use PGP AIM Proxy** is selected.
- Both users are using supported IM clients.
- The AIM address of the initiator of the IM session **must** be on the Buddy List of the recipient of the session or the session will not be encrypted.

The secure IM feature is compatible with any IM client that supports AOL's OSCAR protocol for instant messaging, such as AOL Instant Messenger, Trillian Pro, iChat and Gaim. Refer to the [PGP Desktop Release Notes](#) for information about which specific versions of these IM clients are supported.

The file transfer and direct connect sessions require recent versions of these clients in order for PGP Desktop to encrypt them. In addition, PGP recommends that you set up the connection for both Direct IM and File Transfer to use the AOL Proxy, rather than allowing your buddy to connect directly to your computer.

 Audio and video connections are not encrypted by PGP Desktop.

 PGP Desktop’s secure IM feature uses Perfect Forward Secrecy for enhanced security. All keys used to secure your IM sessions are generated at the beginning of the connection and then destroyed when you disconnect; completely new sets of keys are used for every IM session. This adds an extra level of security to your IM sessions.

About the Keys Used for Encryption

A 1024-bit RSA key is generated each time you log onto your IM software, and is destroyed when you log out. This key is used to exchange randomly generated seed data with anyone with whom you communicate. The seed data is combined and hashed to allow each participant in the communication to generate a set of symmetric keys used for that particular communication (one for each direction). The symmetric keys are used to encrypt all the messages with AES256.

Some of that data is also used to generate keyed-hash message authentication code, or HMAC, for each message so that the message integrity can be checked.

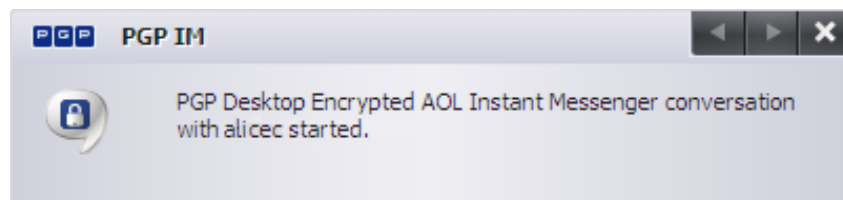
 The keys used for secure IM communication are not user configurable.

Encrypting your IM Sessions


Once you have met the conditions described above to support encrypted IM sessions, start your IM session as you normally would. Your IM sessions with any other PGP Desktop user with a supported IM client will be automatically and transparently protected.

There are multiple ways to verify that your IM session is being protected:

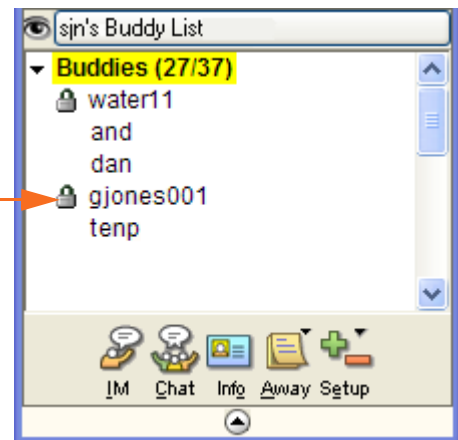
- When you start an IM session, the **PGP Notifier** appears, telling you that a secured IM session has begun.



- When the IM session begins, the first message you see from the other user in the session will have extra text below it that says: "Conversation encrypted by PGP Desktop."
- The padlock icon shown next to the names in the Buddy List indicate that the user is probably using PGP Desktop to secure their IM sessions.

 The padlock could also mean that the user is using AIM's built-in security.

The padlock icon indicates the user is probably using PGP Desktop to secure their IM sessions.



- If you open the Messaging Log after you have started your IM session, it will have an entry noting that the IM session is encrypted.

For example:

```
17:01:06 Info    Initiating PGP Desktop encrypted AIM session with  
breynolds using your key with id 0xEFDDCE3C.
```


6

Protecting Disks with PGP Whole Disk Encryption

Automatically secure your entire disk

PGP Whole Disk Encryption (WDE) locks down the entire contents of a laptop, desktop, external drive, or USB flash drive, including boot sectors, system files, and swap files. Encryption runs as a background process that is transparent to you, automatically protecting valuable data without requiring you to take additional steps.

About PGP Whole Disk Encryption

When you encrypt an entire disk or disk partition using the PGP Whole Disk Encryption feature, every sector is encrypted using a symmetric key. This includes all files: operating system files, application files, data files, swap files, free space, and temp files.

On subsequent reboots, PGP WDE prompts you for the correct passphrase. Then the encrypted data is decrypted as you access it. Before any data is written to the disk, PGP WDE encrypts it. As long as you are logged in to your PGP WDE-Encrypted disk, the files are available. When you log out, the disk is protected against use by others.

Before encrypting your disk with PGP WDE, it is important to understand the process of creating and using a PGP WDE-encrypted disk:

- 1 Make sure that your PGP Desktop license supports its use, as described in [“Licensing PGP Whole Disk Encryption”](#).
- 2 [“Prepare Your Disk for Encryption”](#) on page 64.
- 3 [“Determine the Authentication Method for the Disk”](#) on page 70.
- 4 [“Setting Encryption Options”](#) on page 71.
- 5 [“Encrypting a Disk or Partition”](#) on page 74.
- 6 [“Using a PGP WDE-Encrypted Disk”](#) on page 80.
- 7 [“Maintaining the Security of Your Disk”](#)
- 8 [“Decrypting a PGP WDE-Encrypted Disk”](#) on page 94
- 9 [“Special Security Precautions Taken by PGP Desktop”](#) on page 96

If you are a PGP Universal Administrator, or are using PGP WDE in a PGP Universal-managed environment, see [“Using PGP-WDE in a PGP Universal-Managed Environment”](#) for additional information.

Licensing PGP Whole Disk Encryption

To use the PGP Whole Disk Encryption feature, your copy of PGP Desktop must have a license that supports it.

Check to make sure your license supports PGP Whole Disk Encryption:

- 1 Open PGP Desktop.
- 2 From the **Help** menu, select **License**. If you see a green checkmark by PGP Whole Disk Encryption, your license supports its use.

If your license does not support PGP WDE, you can find more information about licensing PGP Desktop using one of the following methods:

- If you are using PGP Desktop in a PGP Universal-managed environment, contact your PGP administrator for more information about support for the PGP WDE feature in your license. Also, see [“Appendix C, PGP Desktop and PGP Universal”](#) for more information.
- If you are using PGP Desktop outside of a PGP Universal-managed environment, go to the PGP Corporation website (<http://www.pgp.com>) for more information about adding the PGP WDE feature to your license.

License Expiration

PGP WDE used under a subscription license basis provides a 90-day post-license expiration decryption feature for boot disks only. 90 days after the subscription license expires, the PGP WDE feature decrypts your data (after notifying you) so you can retrieve your files.

How does PGP WDE Differ from PGP Virtual Disk?

The PGP Virtual Disk feature differs from PGP WDE in that PGP Virtual Disks perform like additional volumes on your system that can be locked, even while you are using your computer. These volumes are like a vault where you can store files needing protection. There is no actual physical disk, only the virtual one that the PGP Virtual Disk feature creates and manages.

PGP WDE protects your entire physical hard disk—either individual partitions, if you have created them, or the entire disk.

Both products work independently of each other, so you can use them at the same time. For more information, see [Chapter 7, Using PGP Virtual Disks](#).

Prepare Your Disk for Encryption

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” on page 65](#).
- **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 66](#).

- **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. Also be sure to make regular backups of your disk.
- **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 ["Creating Recovery Disks"](#) on page 66.
- **Consider the time it will take to encrypt the disk** and prepare accordingly. See ["Calculate the Encryption Duration"](#) on page 68.
- **Be certain that you will have AC power** for the duration of the encryption process. See ["Maintain Power Throughout Encryption"](#) on page 69.
- **Run a pilot test to ensure software compatibility.** See ["Run a Pilot Test to Ensure Software Compatibility"](#) on page 69.

Supported Disk Types

The PGP WDE feature protects the contents of the following types of disks:

- Desktop or laptop disks (either partitions, or the entire disk).



Do not use PGP Whole Disk Encryption to encrypt server hardware. PGP WDE is not supported on Windows 2000 Server or Windows 2003 Server.

- External disks, excluding music devices and digital cameras.
- USB flash disks.

You can encrypt FAT16, FAT32, and NTFS formatted disks or partitions. If you use PGP Whole Disk Encryption with a FAT disk or partition, you can later convert it to NTFS. Floppy disks and CD-RW/DVD-RWs are not supported.

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 or Windows 2000) 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.

There is no minimum or maximum size for a PGP WDE-encrypted disk. If the disk or partition is supported by the operating system (or your hardware BIOS for the boot disk or partition), it should work with PGP Desktop.



Windows XP allows basic disks to be converted to dynamic disks, which support some features that basic disks do not. **Never perform this conversion on the boot drive of a system that has already been protected using PGP Whole Disk Encryption. This conversion, from a basic-type disk to a dynamic one, renders the drive unusable.**

All Windows power management modes (Hibernation, Standby, Suspend) are supported.

Encryption Algorithm Used by PGP WDE

The encryption algorithm used by PGP WDE is AES-256. The hashing algorithm is SHA-1. You cannot change these options.

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.

Best Practices Recommendation

As a best practice, 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.

Creating Recovery Disks

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. If it happens, it could prevent your system from booting.

Be safe: prepare for this highly unlikely event by creating a recovery CD or floppy disk—or both—**before** you encrypt a boot disk or partition using PGP Whole Disk Encryption.



Note that recovery disks work only with the version of PGP Desktop that created the recovery disk. For example, if you attempt to use a 9.0.x recovery disk to decrypt a disk protected with PGP WDE 9.5 software, it will render the PGP WDE 9.5 disk inoperable.

This section includes procedures for creating both a recovery compact disc and a floppy disk. It also discusses their use.

To create a recovery CD:

- 1 Make sure PGP Desktop for Windows and Roxio Easy Media Creator or Roxio Easy CD Creator (or other software that can create a CD from an ISO image) are installed on your system.
- 2 Open Roxio Easy Media Creator or Roxio Easy CD Creator and choose to create a Data CD Project.
- 3 From the **File** menu, select **Record CD from CD Image**.
The Record CD from Hard Disk Image screen appears.
- 4 From the **Files of Type** menu, select **ISO Image Files (ISO)**.
- 5 Navigate to the PGP directory.
The default is: **C:\Program Files\PGP Corporation\PGP Desktop**
- 6 Select **bootg.iso** and click **Open**.
The Record CD Setup screen appears.
- 7 Insert a blank, recordable CD into a CD drive on your system.
- 8 On the Record CD Setup screen, click **Start Recording**.
The Record CD from CD Image Progress screen appears as the ISO file is burned to the CD.
- 9 When the file is burned to the CD, click **OK**.
The PGP Whole Disk Encryption recovery CD is ready.
- 10 Remove the recovery CD from the drive and label it appropriately.

To create a recovery floppy disk:

- 1 Make sure PGP Desktop for Windows and an application that can create a recovery floppy disk (such as MagicISO) are installed on your system.
 - 2 Insert a blank floppy disk into the floppy disk drive.
 - 3 Open MagicISO.
 - 4 From the **Tools** menu, select **Write Floppy Disk Image**.
The Open dialog appears.
 - 5 Navigate to the PGP directory.
The default is: **C:\Program Files\PGP Corporation\PGP Desktop**
 - 6 Select **Bootg.img**, then click **Open**.
The file is written to the floppy disk.
 - 7 Remove the recovery floppy disk from the drive and label it appropriately.
-

8 Exit from MagicISO.

To use a recovery disk:

1 If the PGP Whole Disk Recovery log-in screen does not appear when you restart your system, or on restart you are prompted for a PGP Whole Disk Encryption recovery disk, insert the recovery CD into a CD drive on the system or the recovery floppy into the floppy disk drive.

2 Restart the system.

The PGP Whole Disk Encryption log-in screen from the recovery disk appears.

3 Type an appropriate passphrase for the boot drive or partition that is protected by PGP Whole Disk Encryption. You can:

- Press **Enter** to attempt to boot the system.
- Press **D** to decrypt the disk.

Calculate the Encryption Duration

Encryption is a time-consuming and CPU-intensive process. The larger the disk or partition 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 or partition
- 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 or partition takes approximately three hours to encrypt using PGP Whole Disk Encryption (when no other applications are running). A very fast system, on the other hand, can easily encrypt such a disk or partition 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.

If you will not be using the computer during encryption, you can speed up initial encryption using the **Maximum CPU Usage** option, described on [“Setting Encryption Options” on page 71](#). The extra speed during encryption comes primarily by taking priority over other operations that your computer is performing.

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 described in the section, “[Setting Encryption Options](#)” on page 71.



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

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.

Certain other disk protection software is incompatible with PGP WDE and can cause serious disk problems, up to and including loss of data. Please note the following known interoperability issues, and please review the PGP Desktop Release Notes for the latest updates to this list.

Software that is not compatible:

- **CompuTrace in MBR mode.** PGP Whole Disk Encryption is compatible only with the BIOS configuration of Absolute Software's CompuTrace laptop security and tracking product. Using CompuTrace in MBR mode is not compatible.
- **Utimaco Safeguard Easy 3.x** is incompatible with the PGP Whole Disk Encryption feature; do not install it on a system with PGP Desktop and do not install PGP Desktop on a system with Utimaco Safeguard Easy 3.x.

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

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

Determine the Authentication Method for the Disk

When you encrypt a disk or partition using PGP Whole Disk Encryption, you choose a method that determines how you will authenticate yourself to decrypt the disk.

You have the following options:

- [“Passphrase and Single Sign-On Authentication”](#)
- [“Public Key Authentication”](#)
- [“Token-Based Authentication”](#)



On a multi-user system, be sure to create separate authentication methods for each user.

Passphrase and Single Sign-On Authentication

With passphrase authentication, you specify a passphrase to use when you reboot a computer with an encrypted boot disk or partition, or if you attempt to access any other encrypted disk or partition. This method requires no additional files or hardware, and can be used with fixed as well as removable disks.

You have two options with passphrase authentication:

- You can choose a passphrase that you use only with PGP WDE.
- You can synchronize your PGP WDE passphrase with your Windows Account logon, so you only need to type your passphrase once to unlock your encrypted disk or partition and to log in to Windows. If synchronized with your Windows login, this option is known as **Single Sign-On (SSO)**.
- For instructions on setting up Single Sign-On, see [“Using PGP WDE Single Sign-On” on page 83](#).

Public Key Authentication

With public-key authentication, you specify a public key when encrypting a disk or partition using PGP Whole Disk Encryption. Only the holder of the corresponding private key can access the contents of the disk or partition. To do that, they must provide the passphrase of their private key.

Public key authentication is available only for removable disks you use with your system. Fixed disks, including boot disks, partitions, or disks in USB enclosures, can use either passphrase or token authentication—not public key authentication.

Token-Based Authentication

If you are using the PGP WDE feature to encrypt a fixed disk (including your boot disk or partition) and for authentication you want to use a PGP key on a token, you must use a PGP keypair on an **Aladdin eToken Pro USB token**. This is the only supported USB token for use with the PGP WDE feature.


Using a keypair on a token adds an extra level of security, as you can take the token away with you.

Note that you must install the Aladdin eToken drivers before you can proceed with disk encryption. See [“Preparing a Token to Use For Authentication” on page 72](#) for more information.


Setting Encryption Options

Once you have completed the tasks for getting your disk ready for encryption, you should review the process for starting initial encryption:

- 1 Choose whether to encrypt the entire disk or specific partitions.** See [“Partition-Level Encryption”](#).
- 2 Choose options to use during encryption,** such as power failure safety or greater encryption speed. See [“Using PGP Whole Disk Encryption Options” on page 73](#).
- 3 Select your choice of authentication.** See [“Determine the Authentication Method for the Disk” on page 70](#).

 If you are using token-based authentication, make sure your token is ready for use. See [“Preparing a Token to Use For Authentication” on page 72](#).

- 4 Encrypt the disk** as described in [“Encrypting a Disk or Partition” on page 74](#).

 If you are a PGP Universal-managed user, PGP WDE creates a Recovery Token to use to recover disks for which the passphrase has been forgotten. See [“Creating a Recovery Token” on page 93](#).


Partition-Level Encryption

If your disk is divided into partitions, you can choose to encrypt by partition, rather than encrypting the entire disk. You can use this flexibility to encrypt:

- One disk partition.
- All disk partitions except one.
- Any number of partitions in-between.

Only the files on the partition(s) that you have selected are encrypted.

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.

 Once a disk or any of its partitions have been encrypted, you cannot change the disk's partitioning (for example, adding or removing a partition, or resizing an existing partition). Make sure the disk is partitioned the way you want it **before** protecting it with PGP Whole Disk Encryption.

Preparing a Token to Use For Authentication

If you choose to authenticate with a token, please note that you must use an Aladdin eToken Pro USB token.


- Use the proper token model.
- Consider adding other users (a passphrase user, for example) to the encrypted disk in case the token is ever lost.
- Install the token's drivers on the system on which you will use the token *before* you use the token.

Supported Token Model

You can use the 32K or 64K model of the Aladdin eToken Pro. The 32K model supports keys up to 1,024 bits; the 64K model supports keys up to 2,048 bits.

Functional Requirements for Using Token-Based Authentication

Please review these requirements and ensure you meet them prior to encryption.

 Using a keypair on a token to authenticate to a disk or partition encrypted using PGP Whole Disk Encryption increases your security, **but if you lose the token you can no longer authenticate to the Bootguard login screen, and all the data on the disk or partition is lost.** For this reason, consider adding other users (passphrase, token, or both) to a disk or partition encrypted using PGP Whole Disk Encryption. If your token is lost or stolen, those additional users can authenticate and unlock the disk or partition for you.

- You can use only keypairs stored on the token. You must either create a keypair on the Aladdin eToken, or send an existing keypair to the token by choosing **Add To** from the right-click context menu.
- When you create a keypair on a token, or when you send an existing keypair to the token, the passphrase to the private key of that keypair changes to the PIN of the token. For an Aladdin eToken, the default PIN is 1234567890. Because this is a well-known default PIN, you should immediately change the PIN using Aladdin's configuration tools so that the security of the keypair is not severely reduced.

Required Drivers

Before you use the Aladdin eToken, install the latest software drivers on the system on which you will be using the token. Microsoft Windows may recognize the token generically if you do not install the software drivers, but PGP Desktop **requires** the appropriate software drivers to be installed. Software drivers for this token are included with the PGP Desktop installation package.

You can also get the latest software drivers from the Aladdin Support Web site:

www.aladdin.com/support/default.asp

Download the latest version of the **eToken PKI Client (RTE)** driver software (version 3.65 was the current version when this document was written), then install it on your system. When the installation of the eToken PKI client driver software on your system is complete, open PGP Desktop and click the PGP Keys control box; if the driver software was installed correctly, you see **Smartcard Keys** listed in the PGP Keys control box.

If you see `No suitable key available` in the **Select Key** field when you specify **Token Key User** as your method of authentication for the disk or partition you are encrypting using PGP Whole Disk Encryption, it means one of several things:

- Your Aladdin eToken is not inserted.
- The driver software is not the right version, or was not installed correctly.
- The keypair on the token cannot be used, or there is no key on the eToken (that is, the eToken is empty).

Using PGP Whole Disk Encryption Options

The PGP Whole Disk Encryption feature offers two options that you can select prior to protecting your disk or partition:

- **Maximum CPU Usage.** This is the fastest way to perform initial encryption on your disk using PGP Whole Disk Encryption, yet it is just as safe. This extra speed comes primarily by taking priority over other operations that your computer is performing. Consider this option for a time when you are away from your computer.
- **Power Failure Safety.** While you can pause the initial encryption process at any time by properly shutting down or restarting your computer, it is exceptionally important to avoid unexpected shutdowns (power failures, power cord gets pulled out, and so on). If this is a possibility for you—or if you do not have an uninterruptible power supply for your computer—consider choosing the **Power Failure Safety** option. When **Power Failure Safety** is selected, encrypting is journaled; if the power fails, the encryption process can safely and accurately resume where it was interrupted. However, this option can cause initial encryption to take several times longer to complete.

This is also useful for use when encrypting USB devices. Interrupting encryption by removing a USB device during encryption can corrupt the device and require that it be reformatted. Encrypting with Power Failure Safety mode permits you to remove the USB device during encryption and resume encryption once it is reinserted.

Use this table to help you decide which options are best for you:

Option Selected	Benefits	Things to consider
Neither Option (Normal)	<p>Encrypts the disk or partition with a good combination of speed and safety.</p> <p>You can use the computer while the disk or partition is being encrypted.</p> <p>Best for most users.</p>	<p>Encryption runs at the standard speed.</p> <p>You must make sure that the computer does not shut down unexpectedly, or data loss may occur.</p>
Maximum CPU Usage	<p>Encrypts the disk or partition more quickly than Normal mode.</p> <p>Despite additional speed, is as safe as encryption using Normal mode.</p>	<p>This option takes maximum computer power, so your system is much less responsive than usual while the disk or partition is being encrypted.</p>
Power Failure Safety	<p>Encrypts your disk or partition using a method with which it can safely resume encryption easily, even if power is interrupted.</p> <p>Good for locations where power loss is a risk.</p>	<p>Takes much longer than Normal mode.</p>
Both Options	<p>Protects the disk or partition with the extra safety of Power Failure Safety mode.</p> <p>Works faster than Power Failure Safety mode alone.</p>	<p>Is still considerably slower than Normal mode.</p>

Encrypting a Disk or Partition

Once you have prepared the disk and specified encryption options, you can encrypt the disk or partition. Note the following before you begin:

- If you are using a USB token for authentication to a fixed disk protected using PGP Whole Disk Encryption, make sure you have the correct token and you have installed the proper driver software. See [“Token-Based Authentication” on page 70](#) for more information.



Note that token-based authentication is not available for Single Sign-On.

- Your system is somewhat slower than usual during the encryption process, although it is fully usable. It returns to normal operation when the encryption process is complete.
- 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.

- You can minimize or close PGP Desktop during encryption. This does not affect the process, but it does improve the speed of the encryption process.
- To stop the encryption process for a short time, use the **Stop** button, then click **Pause** in the dialog box. Click **Resume** to restart. You may need to authenticate after you click **Resume**.
- To shut down the system before the encryption process is over, perform a normal shutdown. You do not need to pause the process. When you restart, the encryption process automatically resumes where it left off.
- You can only encrypt, decrypt, or re-encrypt one disk or partition at a time. Once you begin an operation on a disk or partition, you cannot start encrypting another one until the process is complete on the first. You cannot circumvent this by pausing the first operation.

Supported Characters for PGP WDE Passphrases

The PGP Whole Disk Encryption Single Sign-On feature supports alphanumeric characters, punctuation characters, and standard meta-characters. Tab and control characters are not supported. As you choose a passphrase, please note the following supported character set.

abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789`!@#\$%^&*()_+={}:;['"<>, .?/-

Encrypting the Disk

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.

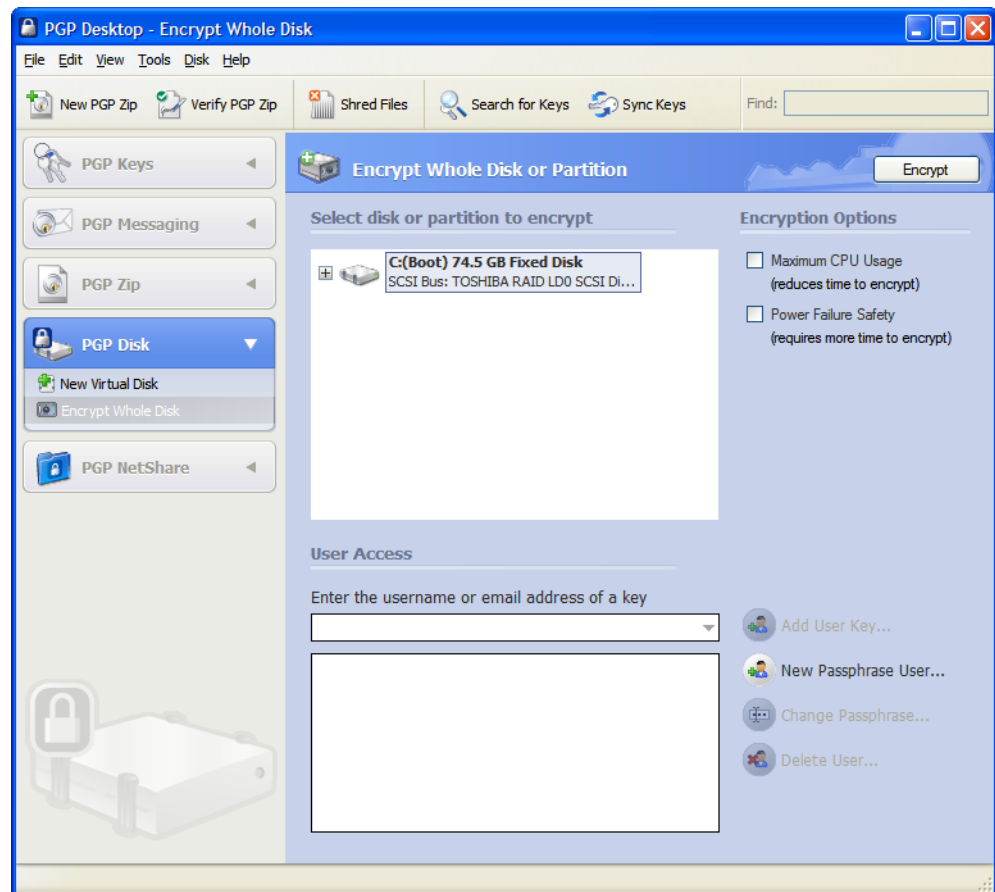
To protect a disk or partition using PGP Whole Disk Encryption:

- 1 Open PGP Desktop and click on the PGP Disk Control box.

The PGP Disk Control box highlights.

- 2 Click **Encrypt Whole Disk**.

The **Encrypt Whole Disk (Partition)** work area displays, and you see a listing of the disks on your system that can be protected by PGP Whole Disk Encryption: disks, disk partitions, removable media, and so on.



- 3 In the **Encrypt Whole Disk (Partition)** work area, in the **Select disk or partition to encrypt** section at the top, click to select the disk or partition on your computer that you want to protect using PGP Whole Disk Encryption.
- 4 Choose the **Encryption Options** that you would like, if any. For more information about your choices, see [“Using PGP Whole Disk Encryption Options” on page 73](#).
- 5 In the **User Access** section, specify how you want to access your protected disk or partition:
 - **Token-based Public Key User.** If you are protecting a fixed (non-removable) disk on your system:
 - a Do one of the following:
 - Type the user name or email address associated with the key, then press **Enter** to find the key.


- You can also select **Add User Key**. A list of the keypairs on your keyring appears.
 - b** From the key source box, select the public key or keys that you want to use.
 - c** Click **Add** to move the keys to the **Keys to add** box.
 - d** Click **OK**.
 - e** Click **Encrypt**.
- **Passphrase User.** If you want to protect your disk or partition with a passphrase:
- a** Select **New Passphrase User**.

The **PGP Whole Disk New User Assistant** appears.

- b** Choose the method that you would like to use to access the disk or partition that you are about to protect. If you are adding access for another user, choose a method for them.


If you would like to unlock your encrypted disk using your Windows Account Logon, select **Use Windows Password** then click **Next**. (This is the Single Sign-On feature. For more information, see [“Using PGP WDE Single Sign-On” on page 83.](#))

If you would like to unlock your encrypted disk or partition using a new passphrase, select **Create New Passphrase**, then click **Next**.

 If you choose the **Use Windows Password** option, after initial encryption, use your Windows password when the PGP Bootguard screen appears at the start of booting. The PGP Single Sign-On (SSO) feature logs into Windows for you—you only need to type your passphrase once.

- c** If you chose the **Use Windows Password** option, type your Windows log-in password in the **Password** field. Click **Finish**.

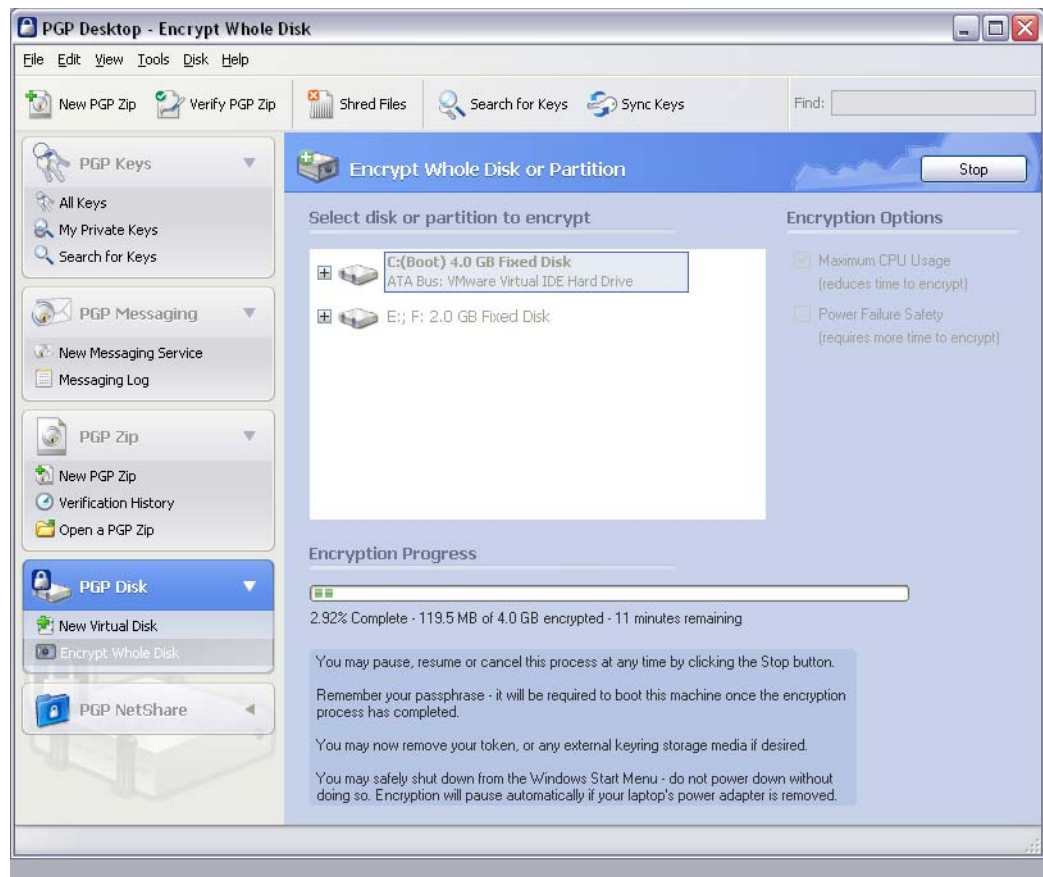
If you chose the **Create New Passphrase** option, type the new passphrase in the **Passphrase** field, and then type it again in the **Confirm** field. Click **Finish**.

 Normally, as an added level of security, the characters you type for the passphrase are not visible on the screen. However, if you are sure that no one is watching (either physically over your shoulder or scanning for the radio waves emitted by your monitor) and you would like to see the characters of your passphrase as you type, select the **Show Keystrokes** checkbox.

See [“The Passphrase Quality Bar” on page 250](#) for more information on the Passphrase Quality Bar.

- ! It is strongly recommended that you use a supported keyboard layout when you are creating a passphrase for your disk or partition protected with PGP Whole Disk Encryption. Supported keyboard layouts are English (United States), English (United Kingdom), German, and Japanese. The Whole Disk Encryption log-in screen assumes you are using one of these three keyboard layouts when you type your passphrase to authenticate. Using a different keyboard layout could result in problems authenticating. Refer to [“Authenticating at the PGP Bootguard Screen” on page 80](#) for more information.

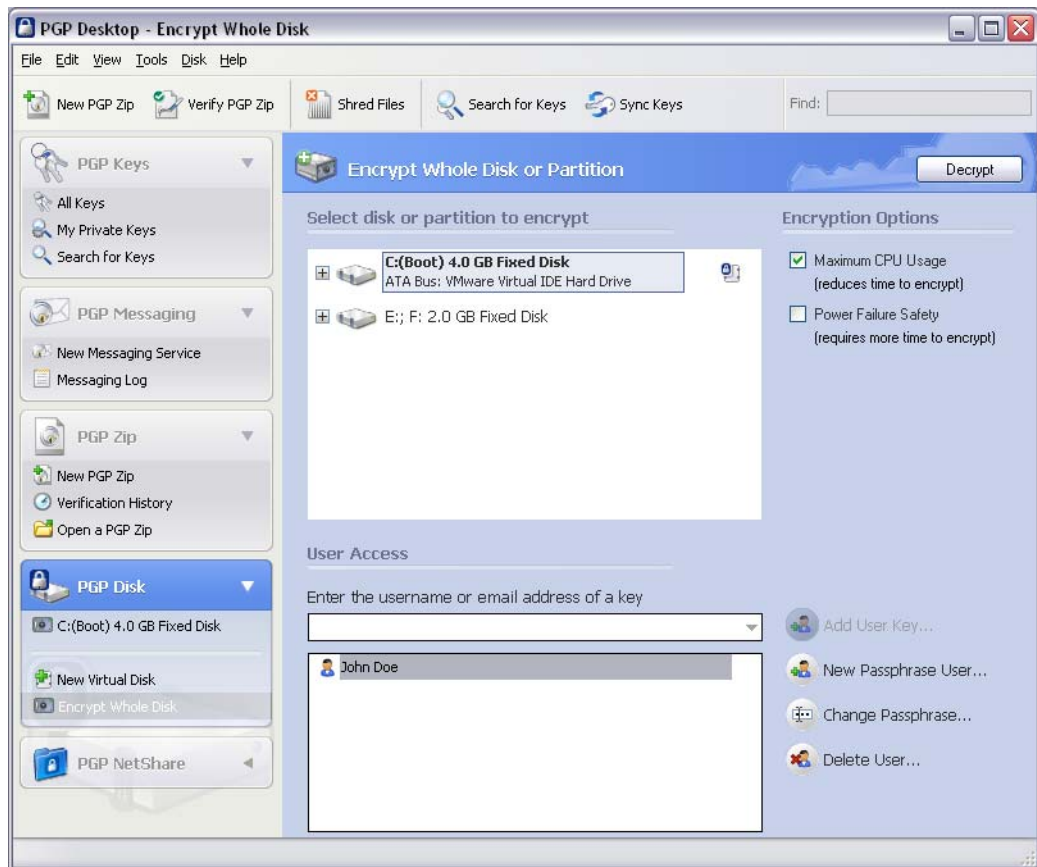
- 6 Confirm that you have the user access arrangement that you want, then click **Encrypt**.
- 7 Read the information in the dialog box, and then click **OK**.
- 8 Refer to the progress bar to see how much of the disk has been encrypted.



- 9 You can stop the encryption process temporarily by clicking **Stop**, then clicking **Pause** in the dialog box that appears. To resume, click **Resume**. You may be prompted for the appropriate passphrase.

- i 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 or partition during the encryption process. You can continue encryption or abort the process and fix the errors. See [“Encountering Disk Errors During Encryption” on page 79](#).

When the encryption process completes, the **User Access** section appears.



Encountering Disk Errors During Encryption

Many hard disks have bad sectors. If PGP WDE encounters bad disk sectors during encryption, encryption pauses. You are warned that PGP WDE has encountered disk errors. (Note that these errors are unrelated to encryption; they are an indication that your hard disk needs maintenance.)



You can do one of the following:

- Force encryption to continue by clicking **Yes**. Disk errors are frequently encountered and often harmless. Clicking **Yes** will continue the encryption process and PGP WDE will ignore further errors.

- Stop encryption by clicking **No**, completely decrypt the disk, and then repair the disk errors using a tool such as SpinRite or Norton Disk Doctor before making another attempt to encrypt the disk. If you know that your disk is seriously fragmented or has many bad sectors, you should immediately perform the maintenance that your hard disk needs before encrypting the disk.

Using a PGP WDE-Encrypted Disk

Your computer boots up in a different way once you use PGP Whole Disk Encryption to protect the boot disk—or a secondary fixed disk—on your system. On power-up, the first thing you see is the PGP Bootguard log-in screen asking for your passphrase.

PGP WDE then decrypts the disk. If you enabled the Single Sign-On feature (that is, you synchronized your PGP WDE passphrase with your Windows Account logon), you are also logged on to Windows.

When you use a PGP WDE-encrypted disk, it is decrypted and opened automatically as needed. With most modern computers, after the disk is completely encrypted, there is no noticeable slowdown of your activities.

Once you unlock a disk or partition, its files are available to you—as well as anyone else who can physically use your system. Your files are unlocked until you lock them again by shutting down your computer.



Because your files remain unlocked until you lock them again, you may want to use a PGP Virtual Disk volume for files that need to be secured even while your computer is in use. See [Chapter 7, Using PGP Virtual Disks](#).

When you shut down a system with an encrypted boot disk or partition, or if you remove an encrypted removable disk from the system, all files on the disk or partition remain encrypted and fully protected—data is never written to the disk or partition in an unencrypted form. Proper authentication (passphrase, token, or private key) is required to make the files accessible again.

Authenticating at the PGP Bootguard Screen

The PGP Bootguard log-in screen prompts you for the proper passphrase for protected disk or partition for one of two reasons:

- If your boot disk or partition is protected using PGP Whole Disk Encryption, you must authenticate correctly for your system to start up. This is required because the operating system files that control system startup are encrypted, and must be decrypted before they can be used to start up the system. The PGP Single Sign-On feature also logs into Windows for you, if you chose the SSO option when you first encrypted the boot disk or partition.
- If a secondary fixed disk or partition is protected using PGP Whole Disk Encryption, you can authenticate at startup so that you don't have to authenticate later when you need to use files on the secondary disk or partition. Because the files on the

secondary (non-boot) disk or partition are not required for startup, you are not required to authenticate at startup. You can use the Bypass feature to skip authentication at startup. You are then asked to authenticate later, when you try to use files on the secondary disk or partition.

i The PGP Bootguard log-in screen accepts the authentication information from any user configured for an encrypted disk or partition. For example, if you have two users configured for a boot disk or partition and two different users configured for a secondary fixed disk or partition on the same system, **any** of the four configured users can use their passphrase to authenticate on the PGP Bootguard log-in screen at startup, even the two users configured on the secondary disk or partition.

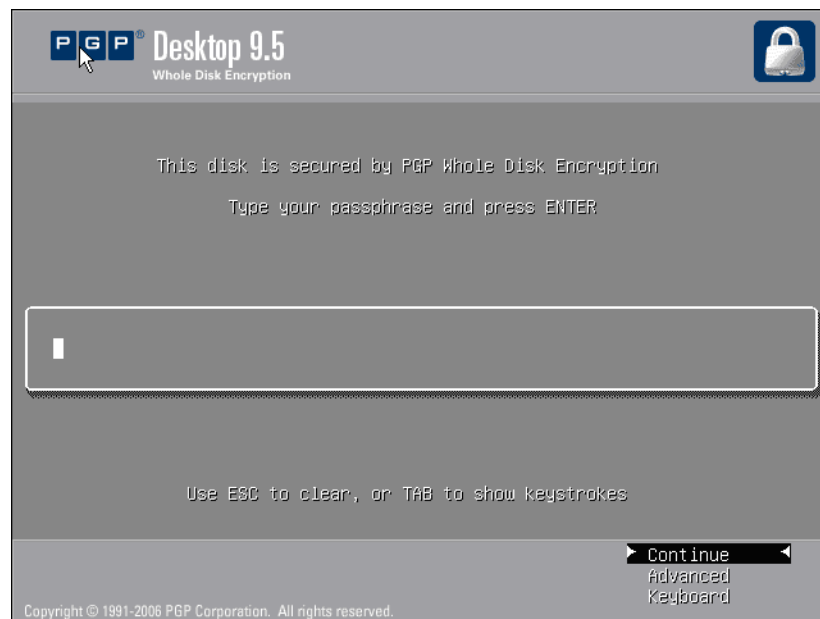
On the PGP Bootguard log-in screen you can:

- Authenticate an encrypted boot or secondary disk or partition on the system.
- View information about the disks or partitions on your system and access the Bypass feature.
- Choose your keyboard layout.

To authenticate using the PGP Bootguard log-in screen:

- 1 Start or restart the system that has a disk or partition protected by PGP Whole Disk Encryption.

On startup, the PGP Bootguard log-in screen appears.



- 2 Type a valid passphrase and press **Enter**.



The PGP Bootguard log-in screen assumes you are using one of the supported keyboard layouts when you type your passphrase. Supported keyboard layouts are English (United States), English (United Kingdom), German (Germany), and Japanese (Japan). If you use a different keyboard layout to create the passphrase for a disk or partition protected by PGP Whole Disk Encryption, you could have problems authenticating because the mappings between the keyboard layouts may be different. See [“Selecting Keyboard Layouts”](#).

To see the characters you type, press **Tab** before you begin typing.

If you make a typing error, or think you might have made a typing error, press **Esc** to clear all characters and start again.

- 3 If you typed a valid passphrase, the PGP Bootguard log-in screen goes away and the system boots normally.

When you first encrypted the boot disk, if you chose to use your Windows Account Logon to authenticate, the PGP Whole Disk Encryption feature logs into Windows for you. You only need to type your passphrase once.

- 4 If you typed an invalid passphrase, an error message appears. Try typing the passphrase again.

If you are having problems entering the PIN of an Aladdin eToken Pro USB token, the system may not “see” the token. Try removing it and re-inserting it. (If the text on the Main PGP Bootguard log-in screen says `Enter your PIN for the eToken Pro or your passphrase and press ENTER`, then the system sees the token.)

Selecting Keyboard Layouts

The PGP Whole Disk Encryption log-in screen supports four keyboard layouts: English (United States), English (United Kingdom), German (Germany), and Japanese (Japan).

Different keyboard layouts can have different mappings between characters, potentially causing problems when you enter your passphrase to authenticate. Select the keyboard layout that most closely maps to the keyboard you are using, then make sure to use that same layout each time you authenticate.

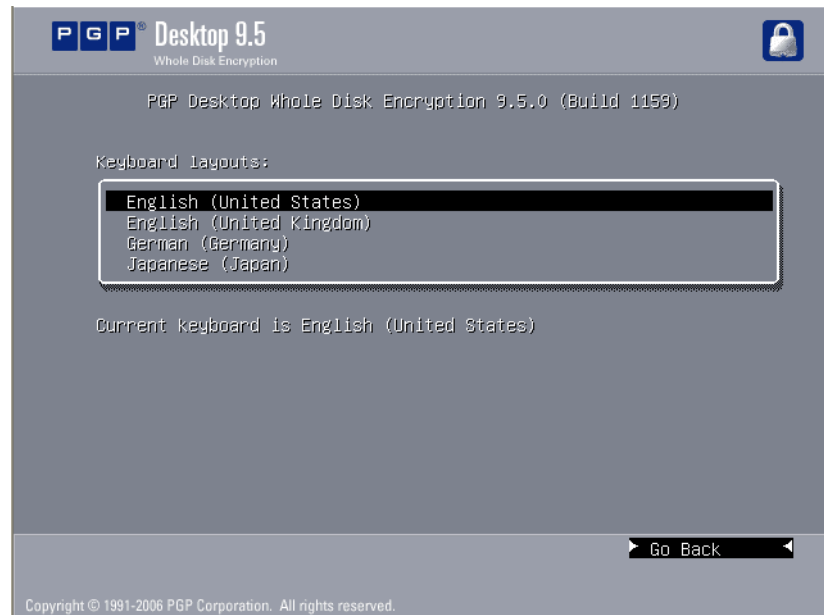
To select a keyboard layout:

- 1 Start or restart the system with the disk or partition protected by PGP Whole Disk Encryption.

On startup, the PGP Bootguard log-in screen appears.

- 2 Press the down arrow on your keyboard until **Keyboard** is highlighted.
- 3 Press **Enter**.

The Keyboard layouts screen appears.



- 4 Press **Tab** to move focus to the list of keyboard layouts, then use the up- and down arrows on your keyboard to select the desired keyboard layout.
- 5 Press **Tab** again.
The **Go Back** option highlights.
- 6 Press **Enter**.
The PGP Bootguard log-in screen appears again.

Using PGP WDE Single Sign-On

Single Sign-On allows you to use your existing Windows passphrase to both authenticate to your PGP WDE-encrypted drive and automatically log you into Windows.

How does Single Sign-On Work?

Single Sign-On utilizes one of the methods Microsoft Windows provides for customizing the Windows login experience. PGP WDE uses your configured authentication info to dynamically create specific registry entries when you attempt to log in.




Note that your Windows password is **never** stored in the registry, nor in any form on the disk—neither encrypted, nor as cleartext.

Prerequisites for Using Single Sign-On

- You must have PGP Whole Disk Encryption installed.

- You must ensure that the **Password Complexity** setting (**Password must meet complexity requirements**) is enabled.

 PGP administrators: If you are administering this feature for systems on a domain, ensure this setting is enabled on the Domain Controller. This setting is used by the Single Sign-On feature to synchronize password changes; if not set, Windows password changes will not be synchronized with PGP Single Sign-On.

Local users

If a computer is not a member of a domain, PGP Whole Disk Encryption automatically disables certain User Access features when a Single Sign On user is added to a disk, including 'Use Welcome Screen' and 'Fast User Switching' (which relies on the welcome screen), such that it then makes the Windows Security panel available when using the CTRL+ALT+DEL key combination.

These features are already automatically disabled if computers are members of a domain.

To enable the Password Complexity feature:

- 1 From the **Start** menu, select **Settings > Control Panel > Administrative Tools**.
- 2 Double-click **Local Security Policy**.
- 3 Double-click **Account Policies**.
- 4 Double-click **Password Policy**.
- 5 Enable **Password must meet complexity requirements**.
- 6 Once you have enabled this feature, you can set up Single Sign-On.

Encrypting the Disk to Use Single Sign-On

- 1 Click the PGP Disk control box, then select **Encrypt Whole Disk**.
- 2 Select the disk or partition that you would like to encrypt, and choose the PGP Whole Disk Encryption options that you would like, if any. For information on these options, see ["Setting Encryption Options" on page 71](#).
- 3 In the **User Access** section, select **New Passphrase User**.
- 4 Select **Use Windows Password**, and then click **Next**.
- 5 Type your Windows login password, and then click **Finish**.

PGP Whole Disk Encryption verifies that your name is correct across the domain, and that the Windows password is correct. PGP Whole Disk Encryption also checks your password to make sure that it contains only allowable characters. If your password does contain any such characters, you are not allowed to continue. See ["Supported Characters for PGP WDE Passphrases" on page 75](#) for information on allowable characters.

- 6 Click **Encrypt**, and then click **OK**.

Multiple Users and Single Sign-On

You can configure up to 28 users for Single Sign-On. PGP Corporation, however, recommends limiting the number of Single Sign-On users to the fewest possible persons who must share the system. While technically feasible to do so, a large number of users sharing a single, encrypted computer is not a secure solution, and PGP Corporation discourages this practice.



Note that the Single Sign-On feature is passphrase-only; you cannot utilize Single Sign-On with users' keys, nor is the feature compatible with smartcards or tokens.

Logging in with Single Sign-On

Once you have configured Single Sign-On, when you start up the system, the PGP BootGuard screen appears. If you provide the correct username and password PGP WDE logs you in to the Windows session and provides access to those disk partitions encrypted with PGP WDE.

Changing Your Passphrase With Single Sign-On

To synchronize your Windows password changes with PGP WDE, you must change your password for Single-Sign On using the **Change Password...** feature in the Windows Security dialog box, which you access by pressing CTRL+ALT+DEL.

To change your passphrase:

- 1 Press CTRL+ALT+DEL.
- 2 Type your old password.
- 3 Type and confirm your new password.
- 4 Click **OK**.

Single Sign-On automatically and transparently synchronizes with this new password. You can use the new password immediately, in your next login attempt.



If you change your password in any other manner—via Domain Controller, the Windows Control Panel, via the system administrator, or from another system—your next login attempt on the PGP BootGuard screen will fail. You must then supply your old Windows password. Successful login on the PGP BootGuard screen using your old Windows password then brings up the Windows Login username/password screen. You must then log in successfully using your new Windows password, at which time PGP WDE will synchronize with the new password.

If you cannot synchronize your password, check to ensure that the **Password Complexity** setting is enabled for your system as described in the section [“Prerequisites for Using Single Sign-On”](#) on page 83.

Maintaining the Security of Your Disk

The following sections describe how to work with your disk once you've encrypted it with PGP WDE.

Getting Disk or Partition Information

To see read-only disk or partition information on the Advanced PGP Bootguard log-in screen:

- 1 Start or restart the system that has a disk or partition protected using PGP Whole Disk Encryption.

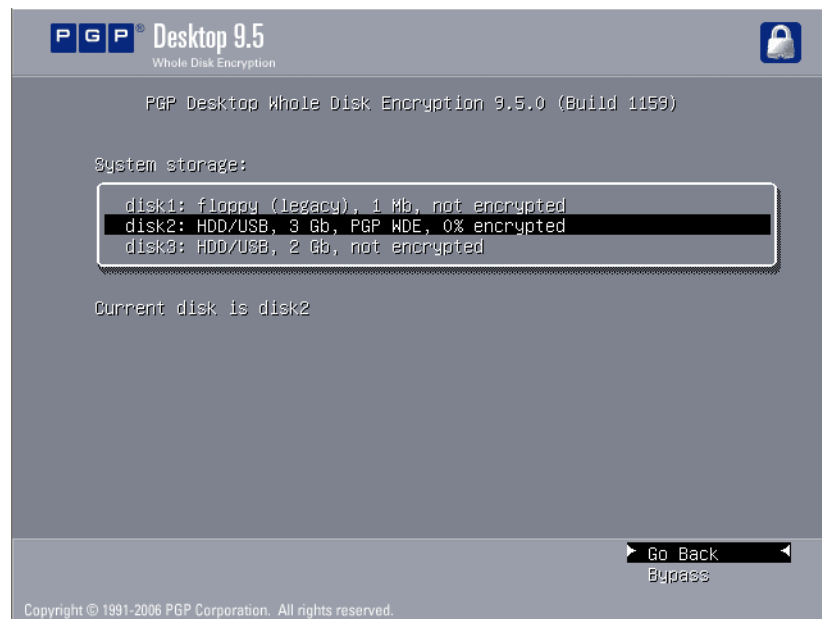
On startup, the PGP Bootguard log-in screen appears.

- 2 Press the down-facing arrow on your keyboard.

In the lower right corner, **Advanced** highlights.

- 3 Press **Enter**.

The Advanced PGP Bootguard log-in screen appears.



This screen shows:

- The version of PGP Desktop being used
- All disks or partitions on the system, including the encryption status of disks or partitions protected using PGP Whole Disk Encryption.
- The disk or partition that is currently selected, and whether the Bypass feature is available for the selected disk or partition.

- 4 To return to the PGP Bootguard log-in screen, highlight **Go Back** in the lower right corner of the screen, then press **Enter**.

Using the Bypass Feature

With the Bypass feature, you can skip authentication at startup. If your boot disk or partition is not protected using PGP Whole Disk Encryption, but a different fixed disk or partition on your system is, the PGP Bootguard log-in screen appears at startup. You can use the Bypass feature to skip authentication so the boot disk or partition can start up.



You can use the Bypass feature only if your boot disk or partition is **not** protected using PGP Whole Disk Encryption. If your boot disk or partition is protected and you do not authenticate, the operating system does not load and the computer does not boot.

To use the Bypass feature:

- 1 Start or restart the system with the disk or partition protected using PGP Whole Disk Encryption.
On startup, the PGP Bootguard log-in screen appears.
- 2 Press the down arrow on your keyboard.
In the lower right corner, **Advanced** highlights.
- 3 Press **Enter**.
The **Advanced** PGP Bootguard log-in screen appears.
- 4 Press the down arrow on your keyboard again.
In the lower right corner, **Bypass** highlights.
- 5 Press **Enter**.
The PGP Bootguard **Advanced** log-in screen stops displaying, and the system boots normally.

Deleting Users From an Encrypted Disk or Partition

At some point you may want to remove the ability of a user to access an encrypted disk or partition.

To remove a user from an encrypted disk or partition:

- 1 On the **Encrypt Whole Disk (Partition)** screen, select the appropriate disk or partition protected by PGP Whole Disk Encryption.
- 2 From the **User Access** list, select the name of the user you want to remove.
- 3 Click **Delete User**.

The Passphrase dialog box appears, prompting you to authenticate.

- 4 Type a valid passphrase, then click **OK**.

The alternate user is removed.

Changing User Passphrases

If you are using Single Sign-On, change your password as described in [“Changing Your Passphrase when the Single Sign-On Feature is Used”](#) on page 91.

To change user passphrases on an encrypted disk or partition:

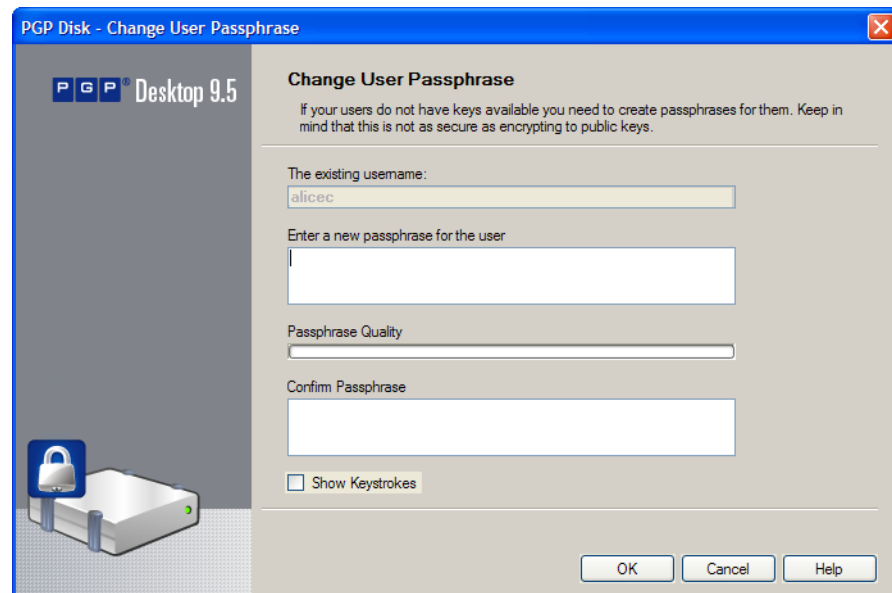
- 1 On the **Encrypt Whole Disk (Partition)** screen, select the appropriate disk or partition protected by PGP Whole Disk Encryption.
- 2 In the **User Access** list, select the name of the user whose passphrase you want to change.

- 3 Click **Change Passphrase**.

You are prompted to type the current passphrase.

- 4 Type the appropriate passphrase, then click **OK**.

The **Change User Passphrase** dialog appears.



- 5 Type a new passphrase.
- 6 In the **Confirm Passphrase** box, type the new passphrase again, then click **OK**.

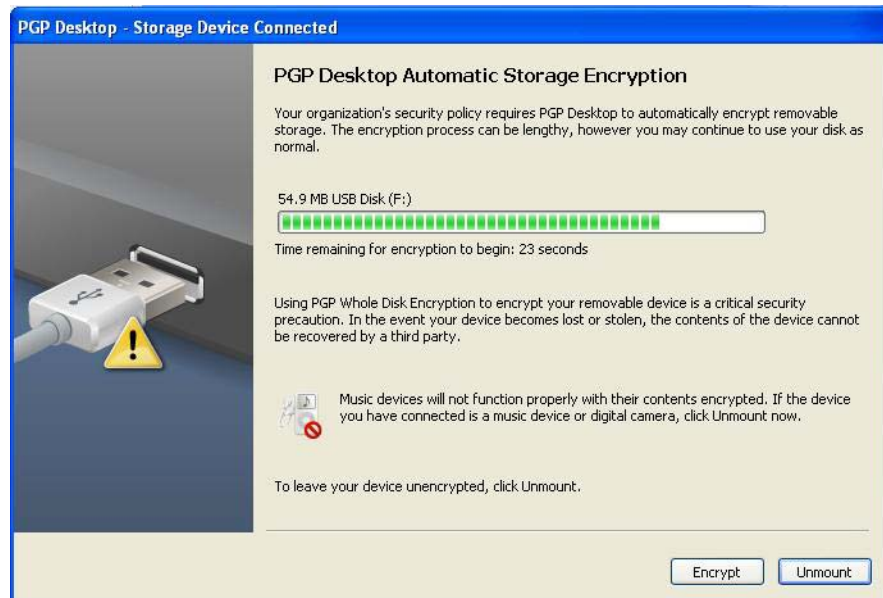
The passphrase is changed.

The Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating. Refer to [“The Passphrase Quality Bar”](#) on page 250 for more information.

Normally, as an added level of security, the characters you type for a passphrase are not visible on the screen. If you would like to see the characters of your passphrase as you type, select the **Show Keystrokes** checkbox.

Encrypting Removable Disks

If you are using PGP Whole Disk Encryption in a PGP Universal-managed environment, your security policy may require that removable disks be encrypted. When you insert the removable disk, the following dialog box appears:



Do one of the following:

- If the removable disk is an external drive, such as a USB flash disk or external hard drive, click **Encrypt**. The device is automatically encrypted to your key. Depending on the size of the disk, it may take some time for the encryption process to complete. While the disk is being encrypted you can continue to use the removable disk.
- If the removable disk is a music device or digital camera, click **Unmount**. These types of devices will not work if the contents of the device are encrypted.


If you accidentally encrypt a music device or digital camera, you will need to decrypt it. Depending on your corporate security policy you may need to contact your IT department or PGP administrator for help with decrypting this device.

If your security policy requires that all removable disks be encrypted and the PGP Universal Server is not available (for example, if you are on an airplane and not connected to your corporate network), the removable device cannot be encrypted. If this is the first time you have inserted the removable device and it has not previously been encrypted, the device will be "unmounted." This means that you cannot use the device until it has been encrypted (the next time you insert the device when you are connected to the PGP Universal Server).

Moving Removable Disks to Other Systems

If you use PGP Whole Disk Encryption to protect a removable disk—a USB flash disk, for example—you can move that disk to another Windows XP or Windows 2000 system that has PGP Desktop 9.5 installed, and access the encrypted files on that flash disk on the other system.

You will need to be able to authenticate to access the contents of the disk.

 Consider PGP Desktop licensing when moving an encrypted, removable disk. To protect a disk using the PGP Whole Disk Encryption feature, you must have the appropriate PGP Desktop license. However, if you have protected a removable disk with PGP Whole Disk Encryption, you can use that removable disk on another computer with PGP Desktop 9.5 installed—even if the other system does not have a PGP Desktop license that supports Whole Disk Encryption.

Uninstalling PGP Desktop from Encrypted Disks or Partitions


If you have any disks or partitions on your system that are protected by PGP Whole Disk Encryption, these disks or partitions become inaccessible once PGP Desktop is uninstalled. For that reason, a safety feature prevents you from uninstalling PGP Desktop if your system has any disks or partitions protected by PGP Whole Disk Encryption. In this instance you see an error message explaining that the uninstall is being terminated to protect the encrypted disk or partition.

If you want to uninstall PGP Desktop, first decrypt any disks or partitions on your system that are protected using PGP Whole Disk Encryption.

Re-Encrypting an Encrypted Disk or Partition

Consider re-encrypting a protected disk or partition that you suspect of having a passphrase or authentication token that has been compromised, or if users have been removed who previously had access.

To re-encrypt a disk or partition, the PGP Whole Disk Encryption feature uses the same encryption algorithm (AES256)—but a different underlying encryption key—to encrypt the disk or partition again. The result is as if you decrypted the disk or partition and encrypted it again, but much faster.

 Re-encryption applies to all partitions that are already encrypted. Selecting one partition to encrypt implies all partitions on the same disk that are already encrypted would be re-encrypted one by one.


To re-encrypt an encrypted disk or partition:

- 1 Select the appropriate encrypted disk or partition.
- 2 From the **Disk** menu, select **Re-Encrypt**.
You are prompted to authenticate.
- 3 Type the appropriate passphrase, then click **OK**.

The re-encryption process begins.

Adding Other Users to an Encrypted Disk or Partition

The user who creates an encrypted disk or partition can make it available to others. These additional users can access the encrypted disk or partition using their own unique passphrase, private key, or token.


 Having multiple users who can access a disk or partition protected by PGP Whole Disk Encryption serves as a backup in case one person forgets their passphrase or loses their authentication token. Users configured for an encrypted disk or partition can authenticate to the PGP Whole Disk Encryption log-in screen to unlock any protected disk or partition on that system.

To add additional users to a disk or partition protected by PGP Whole Disk Encryption:

- 1 Click the PGP Disk Control box on the left pane of the PGP Desktop main screen.
- 2 Select the encrypted disk or partition to which you want to add another user in the list of disks at the top of the PGP Disk Work area.
- 3 Click **New Passphrase User**.

The **Select User Type** dialog box appears.

- 4 Follow the instructions provided on page 76, [step 5](#).

 Public key encryption is the most secure protection method when adding other users to disks or partitions encrypted with PGP Whole Disk Encryption because: (1) There is no need to reveal passphrases to new users, so the risk of passphrases being intercepted or overheard is minimal. (2) Other users do not need to memorize another passphrase. (3) It is easier to manage lists of users if each uses their own private key to access the disk. If you are protecting a boot disk or partition with PGP Whole Disk Encryption, the public key must be on a token.

Using Automatic Backup Software on a PGP WDE-Encrypted Disk

You can automatically back up the disk or partition once protected with PGP WDE. Note, however, that any files the software backs up will be decrypted before being backed up.

Changing Your Passphrase when the Single Sign-On Feature is Used

If you opt for the PGP Whole Disk Encryption Single Sign-On feature, it is recommended that you change your passphrase using the **Change Password** feature in the Windows Security dialog box.

 You can access the Windows Security dialog box by pressing CTRL+ALT+DEL.

To change your passphrase while using the Single Sign-On feature:

- 1 Press **CTRL+ALT+DEL**.
The Windows Security dialog box appears.
- 2 Type your old passphrase.
- 3 Type and confirm your new passphrase.
- 4 Click **OK**.

Your Windows password and PGP Whole Disk Encryption passphrase are changed together. Use the new passphrase during your next login attempt.



If you change your passphrase in any manner other than the one described here, your next login attempt on the PGP BootGuard screen will fail. You must then supply your old passphrase. Successful login on the PGP BootGuard screen using your old passphrase then brings up the Windows Login username/password screen. You must then log in successfully using the Windows Login screen, at which time the PGP Whole Disk Encryption feature will synchronize with the new passphrase.

Local users and the PGP Whole Disk Encryption Single Sign-On Feature

If a computer is not a member of a domain, PGP Whole Disk Encryption automatically ensures that users must sign in using CTRL-ALT-DELETE. It does that by disabling certain Windows user access features, including the **Use Welcome Screen** and the **Fast User Switching** options after a Single Sign On user has been added.

These features are automatically disabled when a computer is member of a domain.

Using PGP-WDE in a PGP Universal-Managed Environment

The PGP Whole Disk Encryption feature can be administered for PGP Desktop for Windows users in a PGP Universal-managed environment. Administrators can use the Microsoft System Management Server (SMS) to deploy PGP Desktop installers to users throughout their enterprise.

PGP Whole Disk Encryption Administration

The PGP administrator can control:

- **Whether or not the PGP Whole Disk Encryption feature is available to users.** If you are in a PGP Universal-managed environment and the PGP Whole Disk Encryption feature is *not* available, check with your PGP administrator to see if the feature has been disabled by policy.

The PGP Whole Disk Encryption feature also requires an appropriate license from PGP Corporation. If the feature is disabled for you, even though it is enabled by policy, check with your PGP administrator to make sure you have an appropriate license.

- **Whether or not you can recover disks or partitions that are protected with PGP Whole Disk Encryption.** If you forget the passphrase to a disk or partition encrypted with PGP Whole Disk Encryption, or if you lose the authentication token, the disk or partition is not accessible. However, if you are using the PGP Whole Disk Encryption feature in a PGP Universal-managed environment, check with your PGP administrator to see if disk or partition recovery is an available option.
- **Whether or not your boot disk must be encrypted with PGP Whole Disk Encryption when you install PGP Desktop.**

If you are using PGP Desktop in a PGP Universal-managed environment, contact your PGP administrator for more information.

- **Whether or not your computer uses the PGP Whole Disk Encryption Single Sign-on (SSO) feature.**

For more information on this feature, see [“Using PGP WDE Single Sign-On” on page 83](#).

- **What modes you can use with the PGP Whole Disk Encryption feature.**

For more information on encryption modes, see [“Determine the Authentication Method for the Disk” on page 70](#).

If you are using PGP Desktop in a PGP Universal-managed environment, after installing PGP Desktop, you may be required to encrypt your boot disk or partition using the PGP WDE feature. Conversely, the PGP WDE feature may be disabled by your PGP administrator.

If you are using PGP Desktop in a PGP Universal-managed environment, you may be prompted to encrypt a removable disk when it is inserted. See [“Encrypting Removable Disks” on page 89](#) for more information.

If your policy should change from one to the other, specifically from having the ability to encrypt a disk to having that feature disabled, note that you are still able to use any drives that are already whole disk encrypted. You will not, however, be able to encrypt any more drives, re-encrypt existing encrypted drives, or add new users.

See [“Appendix C, PGP Desktop and PGP Universal”](#) for more information.

Creating a Recovery Token

If you are working within a PGP Universal-managed environment, and the policy that applies to you allows for the creation of whole disk recovery tokens, then PGP Desktop creates a recovery token whenever you encrypt a disk or partition using PGP Whole Disk Encryption. This recovery token can be used to access the disk or partition in case the passphrase or authentication token is lost.

If the policy that applies to you does not support it, or if you are not in a PGP Universal-managed environment with a pre-configured installation of PGP Desktop, you will not be able to use whole disk recovery tokens.

This recovery token is automatically sent to the PGP Universal Server managing security for the disk or partition protected by PGP Whole Disk Encryption.

If you are in a PGP Universal-managed environment, and you lose the passphrase or authentication token used to protect a disk or partition with PGP Whole Disk Encryption, you should contact your PGP administrator for assistance using the recovery token.

The recovery token can be used only once to access a disk or partition that has been protected using PGP Whole Disk Encryption. After a recovery token is used, a new one is generated automatically and sent to the PGP Universal server. The PGP Desktop user is given the option of creating a new user, or keeping the existing one(s) on the disk or partition.



Consider re-encrypting disks or partitions protected by PGP Whole Disk Encryption if security is compromised, by passphrase exposure for example, or loss of the authentication token. This process re-encrypts the disk or partition with the same encryption algorithm, but with a different underlying encryption key. The result is as if you decrypted the disk or partition and encrypted it again, but is much faster.

Decrypting a PGP WDE-Encrypted Disk

As a best practice, if you need to perform any disk recovery activities on a disk protected with PGP Whole Disk Encryption, PGP Corporation recommends that you first decrypt the disk. Decrypt a disk by doing one of the following:

- Use the PGP Desktop Disk > Decrypt option (see the following procedure for information on how to use this option to decrypt a disk).
- Use your prepared PGP WDE Recovery Disk (see [“Creating Recovery Disks” on page 66](#) for information on how to create a recovery disk).
- Connect the hard disk via a USB cable to a second system and decrypt from that system's PGP Desktop software.

Once the disk is decrypted, proceed with your recovery activities.

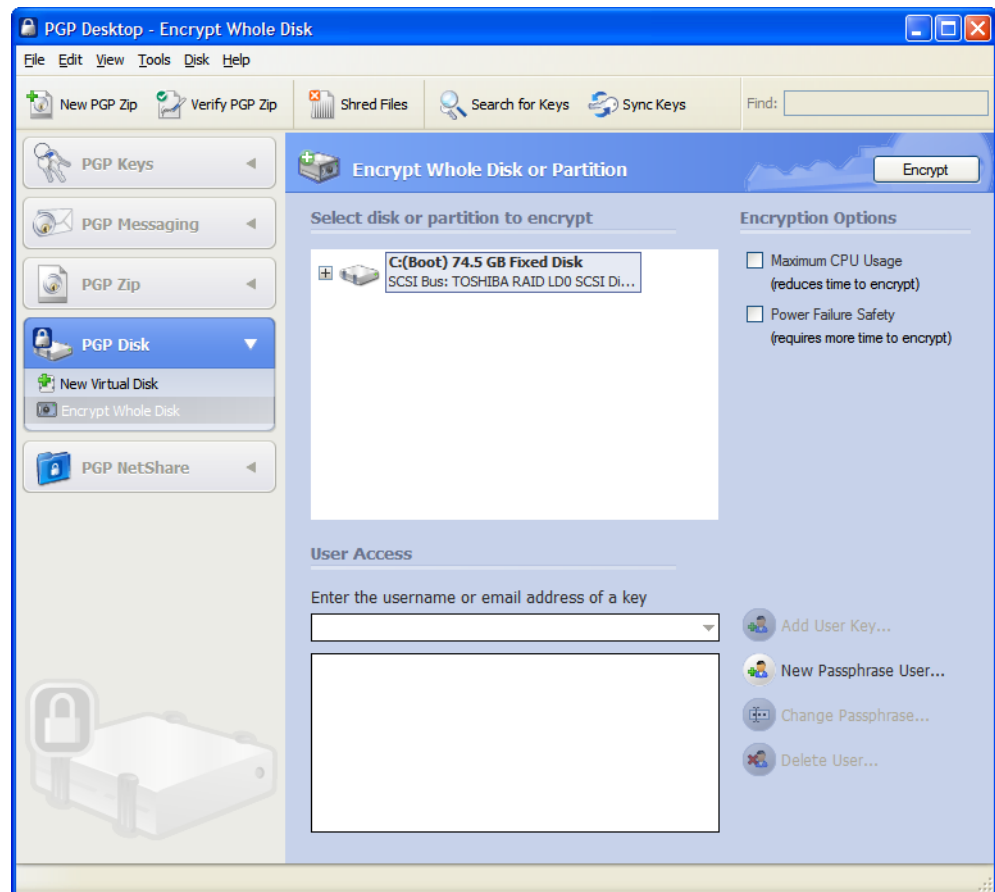
To use PGP Desktop to decrypt a disk:

- 1 Open PGP Desktop and click on the PGP Disk Control box.

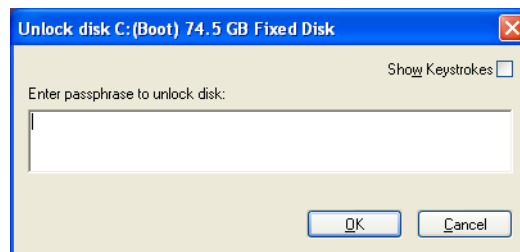
The PGP Disk Control box highlights.

- 2 Click **Encrypt Whole Disk or Partition**.

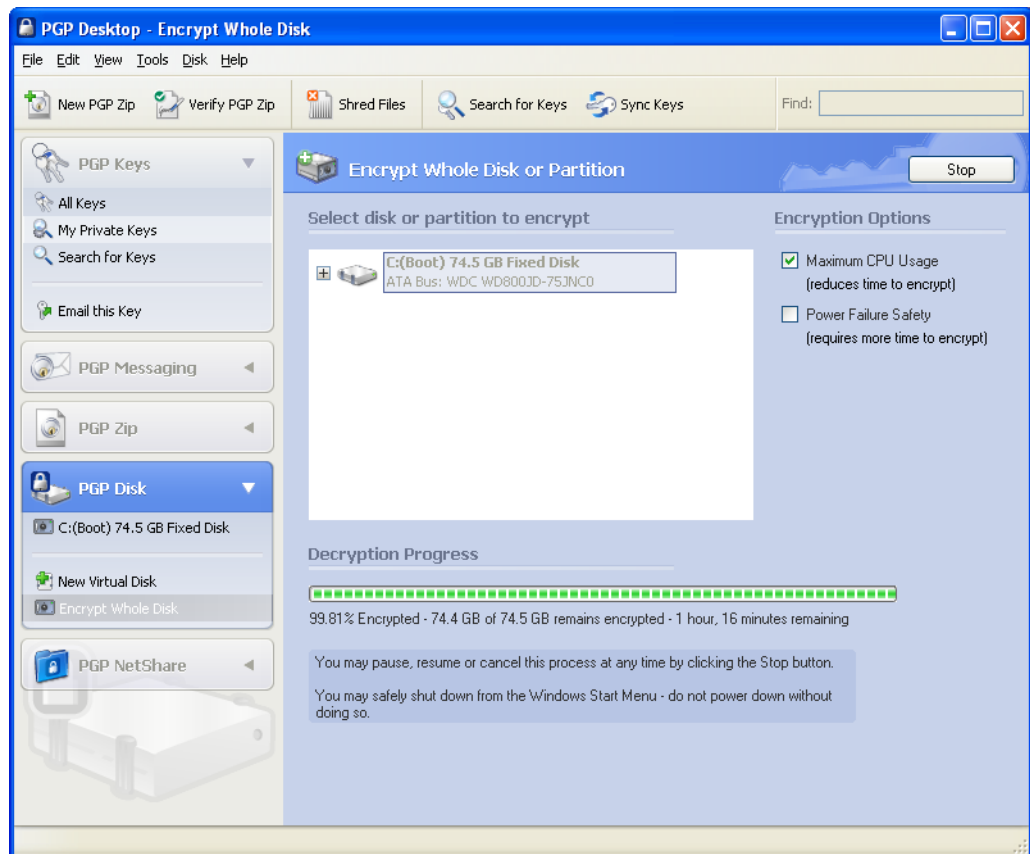
The **Encrypt Whole Disk (Partition)** work area displays, and you see a listing of the disks on your system that can be protected by PGP Whole Disk Encryption: disks, disk partitions, removable media, and so on.



- 3 In the **Encrypt Whole Disk (Partition)** work area, in the **Select disk or partition to encrypt** section at the top, click to select the disk or partition on your computer that you want to decrypt.
- 4 Choose **Disk > Decrypt** or click **Decrypt**. The Unlock Disk dialog box appears.



- 5 Enter the passphrase to unlock the disk. The Decryption Progress displays in the PGP Desktop window.



The time it will take to decrypt the disk is displayed in the PGP Desktop window. To pause or cancel the decryption process, click **Stop**. If necessary, you can shut down the computer by choosing **Start > Shut Down**. *Do not power down the system by depressing the power on/off button.*

To use another system to decrypt a PGP WDE-encrypted drive:

- 1 Remove the hard drive you want to decrypt from the computer and place it in a drive enclosure.
- 2 Connect a USB cable from the drive enclosure to a computer that has PGP Desktop installed on it.
- 3 On the computer that has PGP Desktop installed, at the prompt enter the passphrase to decrypt the drive that is located in the drive enclosure.

Special Security Precautions Taken by PGP Desktop

PGP Desktop has features that help avoid security problems with the PGP Whole Disk Encryption feature. These precautions also apply to PGP Virtual Disk volumes, a include:

- [“Passphrase Erasure” on page 112.](#)
- [“Virtual Memory Protection” on page 113.](#)

- [“Hibernation” on page 113.](#)
- [“Memory Static Ion Migration Protection” on page 113.](#)
- [“Other Security Considerations” on page 113.](#)

7

Using PGP Virtual Disks

Creating a protected area on your computer

This section describes the PGP Virtual Disk feature of PGP Desktop, and includes the following topics:

- [“About PGP Virtual Disks” on page 99](#)
- [“Creating a New PGP Virtual Disk” on page 100](#)
- [“Finding PGP Virtual Disks” on page 103](#)
- [“Mounting a PGP Virtual Disk” on page 104](#)
- [“Using a Mounted PGP Virtual Disk” on page 104](#)
- [“Unmounting a PGP Virtual Disk” on page 104](#)
- [“Adding Alternate User Accounts to a PGP Virtual Disk” on page 105](#)
- [“Deleting Alternate User Accounts From a PGP Virtual Disk” on page 106](#)
- [“Disabling Alternate User Accounts” on page 106](#)
- [“Toggling Read/Write Statuses” on page 107](#)
- [“Granting Administrator Status to an Alternate User” on page 107](#)
- [“Changing User Passphrases” on page 108](#)
- [“Re-Encrypting PGP Virtual Disks” on page 108](#)
- [“Deleting PGP Virtual Disks” on page 109](#)
- [“Maintaining PGP Virtual Disks” on page 110](#)
- [“About PGP Virtual Disk Volumes” on page 111](#)
- [“The PGP Virtual Disk Encryption Algorithms” on page 112](#)
- [“Special Security Precautions Taken by PGP Virtual Disk” on page 112](#)

About PGP Virtual Disks

A PGP Virtual Disk is an area of space, on any disk connected to your computer, that is set aside and encrypted. PGP Virtual Disks are much like a bank vault, and are very useful for protecting sensitive files while the rest of your computer is unlocked for work.



PGP Virtual Disks were called *PGP Disks* in previous versions of PGP Desktop. The phrase *PGP Disk* now includes both the PGP Virtual Disk and the PGP Whole Disk Encryption features.



If you are using PGP Desktop in a PGP Universal-managed environment, you may be required to create a PGP Virtual Disk after installing PGP Desktop. If so, the size, filesystem, and algorithm may have been specified. Refer to [Appendix C, PGP Desktop and PGP Universal](#) for more information.

A PGP Virtual Disk looks and acts like an additional hard disk, although it is actually a single file that can reside on any of your computer disks. It provides storage space for your files—you can even install applications, or save files to a PGP Virtual Disk—but it can also be locked at any time without affecting other parts of your computer. When you need to use the applications or files that are stored on a PGP Virtual Disk, you can unlock the disk and make the files accessible again.

PGP Virtual Disks are unlocked and locked by mounting and unmounting them from your computer. PGP Desktop helps manage this operation for you.

Although you specify a size for your PGP Virtual Disk, you can also create a dynamically-sizing disk, one that grows larger as needs require it. The size you specify when you are creating the disk is the maximum size the disk can become.

When a PGP Virtual Disk is mounted, you can:

- Move/copy files into or out of the mounted PGP Virtual Disk.
- Save files to the mounted PGP Virtual Disk.
- Install applications within the mounted PGP Virtual Disk.

Files and applications on a PGP Virtual Disk are stored encrypted. If your computer crashes while a PGP Virtual Disk is unmounted, the contents remain safely encrypted.

When a PGP Virtual Disk is unmounted, it does not appear within Windows Explorer, and it is inaccessible to anyone without proper authentication.

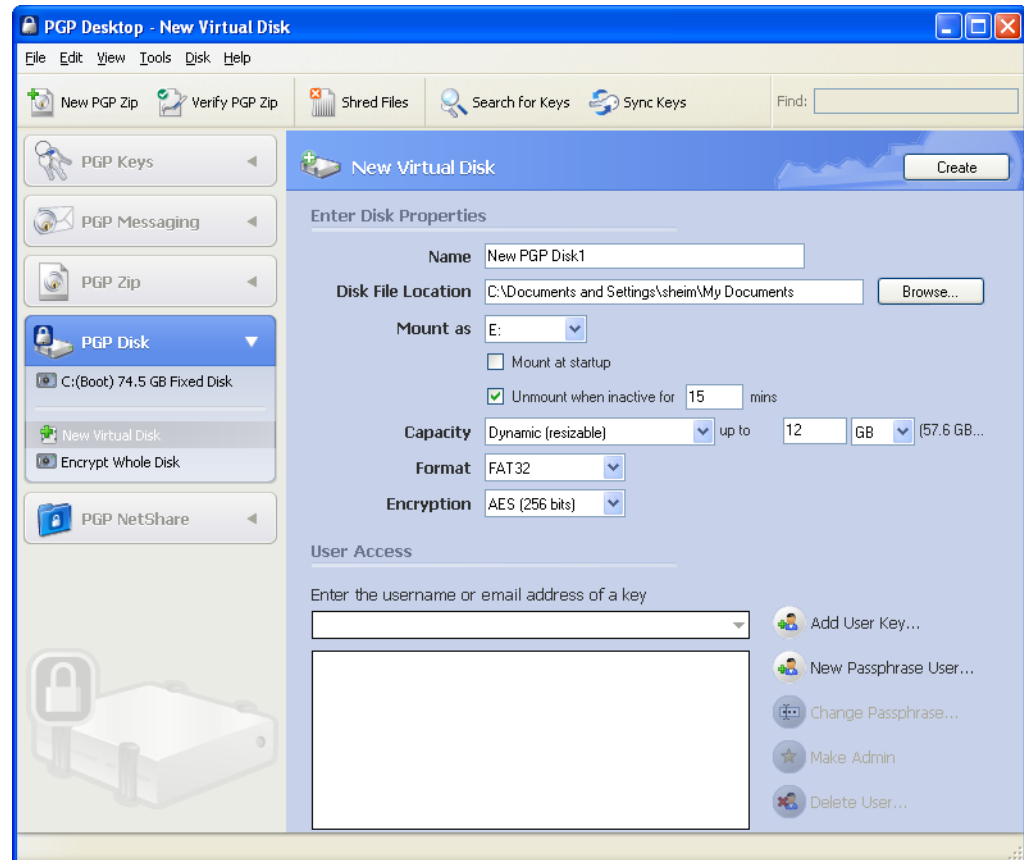
For information about the PGP Options that affect PGP Virtual Disk volumes, see page 242.

Creating a New PGP Virtual Disk

To create a new PGP Virtual Disk:

- 1 Open PGP Desktop.
- 2 Click the PGP Disk control box on the left pane of the PGP Desktop main screen, then click **New Virtual Disk**. Alternatively, from the **File** menu, select **New > PGP Virtual Disk**.

The New Virtual Disk screen appears in the right pane of the screen.



- 3 In the **Name** field, type the name that you would like for the new PGP Virtual Disk.
- 4 In the **Disk File Location** field, accept the default location for the PGP Virtual Disk volume you are creating, or click **Browse** to specify another location.
- 5 From the **Mount as** menu, select the drive letter that you would like for the new PGP Virtual Disk.

You can:

- Accept the drive letter that PGP Desktop suggests for you.
 - From the **Mount as** menu, select an available drive from the list.
 - From the **Mount as** menu, select **Folder**, if you would like to mount the new PGP Virtual Disk to a folder instead of a drive letter. If you do this, a field appears next to the **Mount as** menu, so you can specify a location for the folder.
- 6 Select **Mount at Startup** to have your new PGP Virtual Disk volume mount at startup automatically. When selected, you are prompted for your PGP Virtual Disk passphrase when you start your computer.

- 7 Select **Unmount when inactive for n mins** [where n is a number of minutes] to have the PGP Virtual Disk unmount if you have not used your computer for a specific time interval that you specify (in minutes). This is helpful if you often leave your computer unattended—it is an additional safeguard that locks your PGP Virtual Disk if you forget to.
- 8 From the **Capacity** menu, select the desired type of PGP Virtual Disk. Your choices are:
 - **Dynamic (resizeable)**. This type of disk grows in capacity as files are added to it, yet it stays small until the additional space is needed. PGP Desktop manages this process, you only need to set the maximum size that you would like the disk to be. You can also compress this disk later, if you choose.
 - **Fixed size**. This type of disk remains the same size, regardless of how many files are added to it.
- 9 From the **Capacity** menu, set the size (in the case of Dynamic disks, the maximum size) for your new PGP Virtual Disk. Use whole numbers; no decimal places. Choose **KB** (kilobytes), **MB** (megabytes), or **GB** (gigabytes) from the menu.

The maximum allowable size for a PGP Virtual Disk depends on the size and format of your hard disk.
- 10 Specify a filesystem format for the volume:
 - **FAT**. Volume must be 100 KB or larger.
 - **FAT32**. Volume must be 260 MB or larger.
 - **NTFS**. Volume must be 5 MB or larger.
- 11 Specify the encryption algorithm you want to use to protect your data:
 - **AES (256 bits)**. AES (Advanced Encryption Standard) is a block cipher that can be used at 128, 192, or 256 bits. The more secure 256-bit version is used for creating PGP Virtual Disk volumes by default.
 - **CAST5 (128 bits)**. CAST is a 128-bit block cipher. CAST is a strong, military-grade encryption algorithm that has a solid reputation for its ability to withstand unauthorized access.
 - **Twofish (256 bits)**. Twofish is a 256-bit block cipher, symmetric algorithm. It was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the AES (Rijndael was selected).
- 12 You must have at least one user who can access your new PGP Virtual Disk. In the **User Access** section, specify who you want to give access to, and what method they use for access:
 - a **User Key**. To add users who authenticate with public-key cryptography:
 - Click **Add User Key**. The **Add Key Users** box appears, displaying the keypairs currently on your keyring.

- From the **Add Key Users** box, select the key users you want by double-clicking the listing. Alternatively, you can drag the listing from the left side to the right, or select a listing and click Add. Click **OK** when you are finished.
- b** Passphrase. Click **New Passphrase User**. The **Create New User** box appears.
 - For each new passphrase user, type a name for that user, type a passphrase for them, then type the passphrase again to confirm. Click **OK** to create the passphrase user. If you want to authorize more passphrase users, repeat the process.
 - To modify the passphrase for a passphrase user, select that user, then click **Change Passphrase**.

For information on creating effective, high-quality passphrases, refer to page 250.

- 13** Click **Create** to start creating the new PGP Virtual Disk.

A progress bar indicates how much of the PGP Virtual Disk has been initialized and formatted. When complete, your new PGP Virtual Disk appears in the PGP Disk control area.

- 14** The first user you create is granted administrator status, and there can only be one administrator at a time. However, you can grant administrator status to any of your other users, regardless of whether they are public key or passphrase users. Click their name in the User Access list, then click **Make Admin**.
- 15** Delete any user, other than the Administrator, by selecting their name and clicking **Delete User**. To delete the Administrator, first grant administrator status to another user, then delete the former administrator.

Finding PGP Virtual Disks

If you created PGP Virtual Disks using previous installations of PGP Desktop, you can easily find these volumes using the PGP Disk Search Assistant.

To find PGP Virtual Disks on your system:

- 1** In PGP Desktop, click the **PGP Disk** Control box.

The PGP Disk main screen appears.
- 2** From the **File** menu, select **Scan for PGP Disks**.

The **PGP Disk Search Assistant** screen appears.
- 3** Follow the on-screen instructions.

Mounting a PGP Virtual Disk

When you create a new PGP Virtual Disk, it is automatically mounted so you can begin using it to store your files.

To secure the contents of a volume, you must unmount it. Once a volume is unmounted, its contents remain secured in an encrypted file where they are inaccessible until the volume is mounted once again.

There are several ways to mount a PGP Virtual Disk:

- During creation of the PGP Virtual Disk, select the **Mount at Startup** checkbox. The volume mounts automatically when you start Windows. If you do not select this during creation of the PGP Virtual Disk, you can set it as an option later.
- In PGP Desktop, click the PGP Disk control box. Select the PGP Virtual Disk you want to mount, then click **Mount** in the upper-right corner. You can also select **Mount** from the **Disk** menu.
- In Windows Explorer, right-click the PGP Virtual Disk file, and select **PGP > Mount PGP Virtual Disk** from the shortcut menu.

Mounted PGP Virtual Disk volumes appear as empty drives in Windows Explorer.

Using a Mounted PGP Virtual Disk

You can create, copy, move, and delete files and folders on a PGP Virtual Disk just as you normally do with any other disk on your system.


Anyone else who has access to the volume (either on the same computer or over the network) can also access the data stored there. It is not until you unmount the volume that the data is protected.



Although each PGP Virtual Disk file is encrypted and cannot be accessed by anyone without proper authorization, it can still be deleted from your system. Anyone with access your system could delete the encrypted file containing the PGP Virtual Disk. For this reason, keeping a backup copy of the encrypted file is an excellent safety measure, as is keeping your computer locked when you are not nearby.

Unmounting a PGP Virtual Disk

You lock a PGP Virtual Disk by unmounting it.

 You may lose data if you unmount a PGP Virtual Disk when some files that it contains are open. The **Disk** tab of **Tools > PGP Options** has some settings for the PGP Virtual Disk feature. One option is **Allow PGP Virtual Disks to unmount even while files are still open**. If that option is active, then it is also possible to select **Don't ask before unmounting**. **DO NOT USE THESE OPTIONS UNLESS YOU ARE FAMILIAR WITH THEM.** While these options can be useful for advanced users who protect their data with regular data backups, they are not recommended for most users.

There are several ways to unmount a PGP Virtual Disk volume:

- Click the PGP Disk control box on the left pane of the PGP Desktop main screen, then select the volume you want to unmount. Click **Unmount** in the upper-right corner, or select **Unmount** from the **Disk** menu.
- In Windows Explorer, right-click on the PGP Virtual Disk file, then select **PGP > Unmount PGP Virtual Disk** from the shortcut menu.
- Use the hotkey to unmount all PGP Virtual Disks. The default hotkey is Ctrl-Shift-U. The hotkey must be enabled first.

Once a PGP Virtual Disk is unmounted, its contents remain locked and inaccessible until the volume is mounted once again.

Adding Alternate User Accounts to a PGP Virtual Disk

The administrator of a PGP Virtual Disk can make it available to other users. Those users can access the volume using their passphrases or private keys.

To add alternate user accounts to a PGP Virtual Disk:

- 1 Click the PGP Disk Control box on the left pane of the PGP Desktop main screen, then select the volume to which you want to add an alternate user account.
- 2 Make sure the PGP Virtual Disk is **not** currently mounted, otherwise, you cannot add alternate user accounts.
- 3 Click **Add User Key**, or **New Passphrase User**, depending on what kind of alternate user account you want to add.

If you clicked **Add User Key**, the **Add Key Users** box appears.

If you clicked **New Passphrase User**, the **PGP Disk New User** box appears.

- 4 Do one of the following:
 - If you selected **Add User Key**, then select a public key from the list, then click **OK**.
 - If you selected **New Passphrase User**, type the user name, the passphrase for the PGP Virtual Disk you are adding the user to, then type the passphrase again in the **PGP Disk New User** box. Click **OK**.

The alternate user account is added.

Deleting Alternate User Accounts From a PGP Virtual Disk

At some point you may want to remove the ability of an alternate user to access a PGP Virtual Disk.

To remove an alternate user account from a PGP Virtual Disk:

- 1 Click the PGP Disk control box on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk for which you want to delete an alternate user account.
- 2 Make sure that the PGP Virtual Disk is **not** mounted. You cannot remove an alternate user account if the volume is mounted.
- 3 In the User Access list, select the name of the alternate user whose account you want to remove.
- 4 Click **Delete User**.

The Passphrase dialog box appears, prompting you for either the administrator passphrase or the passphrase for the user account being removed.

- 5 Type the passphrase, then click **OK**.

The alternate user account is removed.

Disabling Alternate User Accounts

To prevent access to a PGP Virtual Disk for an alternate user without deleting their account entirely, you can instead temporarily disable their access.

To disable an alternate user account from a PGP Virtual Disk:

- 1 Click the PGP Disk control box on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk with the alternate user account that you want to disable.
- 2 Make sure that the PGP Virtual Disk is **not** mounted. You cannot disable an alternate user account if the volume is mounted.
- 3 In the User Access list, right-click the name of the alternate user account you want to disable, then select **Disable User**.

The Passphrase dialog box appears, prompting you for either the administrator passphrase or the passphrase for the user account being disabled.

- 4 Type the passphrase, then click **OK**.

The alternate user account is disabled.

Toggling Read/Write Statuses

Users of a PGP Virtual Disk can have either full read/write privileges, or read privileges only. You can change these privileges for a user at any time.

To toggle privileges for a user on a PGP Virtual Disk:

- 1 Click the **PGP Disk** control box on the left pane of the PGP Desktop main screen, then select the appropriate PGP Virtual Disk.
- 2 Make sure the selected PGP Virtual Disk is **not** mounted. You cannot toggle privileges if the volume is mounted.
- 3 Right-click the name of the user whose status you want to change.
- 4 Do one of the following:
 - If the user's status is read/write, select **Read Only** from the contextual menu to change their status to read-only.
 - If the user's status is read-only, select **Read/Write** from the contextual menu to change their status to read/write.

A passphrase dialog appears.

- 5 Type the administrator passphrase for the PGP Virtual Disk, then click **OK**.

The privileges of the selected user are changed.

Granting Administrator Status to an Alternate User

You can change the status of a user account from alternate to administrator:

- 1 Click the PGP Disk control box on the left pane of the PGP Desktop main screen, then select the appropriate PGP Virtual Disk volume.
- 2 Make sure the selected PGP Virtual Disk is **not** mounted. You cannot make a user into an administrator if the volume is mounted.
- 3 Right-click the account and select **Make Admin**.

The selected user account is changed to administrator.



You can only grant Administrator status to one user account at a time. By granting Administrator status to one account, you also remove it from another.

Changing User Passphrases

To change a user's passphrase for a PGP Virtual Disk:

- 1 Click the PGP Disk control box on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk on which you are a user.
- 2 Make sure the selected PGP Virtual Disk is **not** mounted. You cannot change the passphrase if the volume is mounted.
- 3 Select the name of a passphrase user from the User Access list, then click **Change Passphrase**.

The **Enter Passphrase** box appears.

- 4 Type your current passphrase, then click **OK**.

The **PGP Enter Confirmed Passphrase** box appears.

- 5 Type a new passphrase, move to the **Confirmation** box and the same passphrase again, then click **OK**.

The passphrase is changed.

Re-Encrypting PGP Virtual Disks

You can re-encrypt all data stored on a PGP Virtual Disk. You might do this for either (or both) of two reasons:

- You want to change the encryption algorithm currently being used to protect the volume.
- You suspect there has been a security breach.

With re-encryption, you can encrypt your PGP Virtual Disk again, but with a different underlying encryption key.



Adept users may be able to search the memory of their computers for the underlying encryption key of a PGP Virtual Disk. They could use the key to access the volume even after being removed from the user list. Re-encrypting the disk changes this underlying key and prevents this kind of intrusion.

To re-encrypt a PGP Virtual Disk:

- 1 If the PGP Virtual Disk that you want to re-encrypt is mounted, unmount it.
- 2 Select the PGP Virtual Disk you want to re-encrypt.
- 3 From the **Disk** menu, select **Re-Encrypt**.
- 4 Type your passphrase for the volume.

The **PGP Re-Encryption Assistant** appears.

- 5 Read the introductory information, and then click **Next**.

A dialog box appears displaying:

- The current encryption algorithm protecting your PGP Virtual Disk.
- The available encryption algorithms other than the one you originally chose.

For example, if your PGP Virtual Disk is currently encrypted with AES, then CAST5 and Twofish appear in the New Algorithm list.

- 6 Choose from one of the following options:

- To re-encrypt the volume using the current algorithm, select the **Re-encrypt to the same algorithm** checkbox, then click **Next**.

The PGP Virtual Disk volume re-encrypts using the same encryption algorithm as before.

- To re-encrypt the volume using a different algorithm, select it from the **New Algorithm** menu, then click **Next**.

The PGP Virtual Disk volume re-encrypts using the new encryption algorithm you selected.

- 7 When the current status displays Done, click **Next**.

- 8 Click **Finish** to complete the re-encryption process.

Deleting PGP Virtual Disks

At some point you may decide you no longer need a particular PGP Virtual Disk.



When you delete a PGP Virtual Disk, all data on it is also deleted. **There is no way to retrieve the data once you delete a PGP Virtual Disk.** Make sure that you have copied any data that you wish to save to another location **before deleting a PGP Virtual Disk.**

To delete a PGP Virtual Disk:

- 1 Open PGP Desktop.

- 2 Click the PGP Disk Control box.

The PGP Disk screen appears in the Work area.

- 3 Select the PGP Virtual Disk you want to delete in the list at the top of the PGP Disk Work area.

The name of the PGP Virtual Disk you selected highlights.

- 4 From the **Disk** menu, select **Delete**.

A confirmation dialog appears.


- 5 Do either of these two things:
 - Click **OK** to delete the PGP Virtual Disk from the PGP Desktop listing. The virtual disk remains on your system.
 - Click **Delete PGP Disk** to remove the PGP Virtual Disk from the PGP Desktop listing, as well as deleting it from your hard drive.

Maintaining PGP Virtual Disks

This section describes how to take proper care of the PGP Virtual Disks that you use with your computer.

Mounting PGP Virtual Disk Volumes on a Remote Server

You can place PGP Virtual Disk volumes on any kind of server (Windows or UNIX). The volumes can then be mounted by anyone with a Windows computer and PGP Desktop.

 The first person to mount the PGP Virtual Disk volume locally has read-write access to the volume. No one else is then able to access the volume. If you want others to be able to access files within the volume, you must mount the volume in read-only mode (applies to FAT and FAT32 filesystem formats only). All users of the volume then have read-only access.

If the PGP Virtual Disk volume is stored on a Windows server, you can also mount the volume remotely on the server and allow people to share the mounted volume. However, this action provides no security for the files within the volume.

Backing up PGP Virtual Disk Volumes

Backing up the contents of your PGP Virtual Disk is the best way to safeguard your information from hardware failure or other loss.

It is not advisable to back up the contents of a mounted (and therefore, decrypted) PGP Virtual Disk just as you would any other volume. The contents are not encrypted, and are accessible to anyone who can restore the backup. Instead, instead make a backup copy of the encrypted volume.

To back up PGP Virtual Disks:

- 1 Unmount the PGP Virtual Disk.
- 2 Copy the unmounted encrypted file to a floppy disk, tape, or removable cartridge just as you would any other file.

Even if some unauthorized person has access to the backup, he or she will not be able to decipher its contents.

When making backups of the encrypted files, keep these issues in mind:


- Backing up encrypted files to a network drive gives others plenty of opportunity to guess at a weak passphrase. It is much safer to back up only to devices over which you have physical control.
- A lengthy, complicated passphrase helps further improve the security of your data.
- If you are on a network, make sure that any network back up system does not back up the files in your **mounted** PGP Virtual Disk. (You may need to discuss this with your System Administrator.) Once a PGP Virtual Disk is mounted, its files are decrypted and can be copied to a network backup system that way.

Exchanging PGP Virtual Disks

You can exchange PGP Virtual Disks with other users who have PGP Desktop installed on their computers. You do that by sending them a copy of the PGP Virtual Disk data file, which contains the volume data. Here are some of the ways you might exchange PGP Virtual Disks:

- As mail attachments
- On a removable disk or CD
- Over a network

Once the other user has the PGP Virtual Disk file, they can mount it on a system running PGP Desktop and use the correct passphrase to access it. If the volume was encrypted to their public key, they would use their private key for access.

 Public key is the most secure protection method when adding alternate users to a PGP Virtual Disk because: (1) You don't need to exchange a passphrase with the alternate user which, depending on your method, could be intercepted or overheard. (2) The alternate user doesn't need to memorize another passphrase which could be forgotten. (3) It is easier to manage a list of alternate users if each uses their own private key to unlock the volume.

About PGP Virtual Disk Volumes

You can use PGP Virtual Disk volumes to organize your work, keep similarly named files separate, or keep multiple versions of the same documents or programs separate.

Although the PGP Virtual Disk volumes you create with PGP Desktop function just as any other volume you are accustomed to working with, the data is actually stored in one large encrypted file. Only when you mount the file are its contents presented in the form of a volume.

It is important to realize that all your data remains secure in the encrypted file and is only deciphered when you access one of the files. Having the data for a volume stored in this manner makes it easy to manipulate and exchange PGP Virtual Disk volumes with others but it also makes it easier to lose data if the file is somehow deleted. It is wise to keep a back up copy of these encrypted files so that the data can be recovered if something happens to the original.

The PGP Virtual Disk Encryption Algorithms

Encryption employs a mathematical formula to scramble your data so that no one else can use it. When you apply the correct mathematical key, you unscramble the data. The PGP Virtual Disk volume encryption formula uses random data for part of the encryption process.

The PGP Desktop application offers strong algorithm options for protecting your PGP Virtual Disk volumes: AES-256, CAST, and Twofish.

The Advanced Encryption Standard (AES) is the NIST-approved encryption standard. The underlying cipher is Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen. The AES replaces the previous standard, the Data Encryption Standard (DES). PGP Virtual Disk volumes can be protected with the strongest variation of AES, AES-256 (that is, AES with a key size of 256 bits).

CAST is considered an excellent block cipher because it is fast and very difficult to break. Its name is derived from the initials of its designers, Carlisle Adams and Stafford Tavares of Northern Telecom (Nortel). Nortel has applied for a patent for CAST, but they have made a commitment to make CAST available to anyone on a royalty-free basis. CAST appears to be exceptionally well-designed by people with good reputations in the field.

The design is based on a very formal approach, with a number of formally provable assertions that give good reasons to believe that it probably requires key exhaustion to break its 128-bit key. CAST has no weak keys. There are strong arguments that CAST is immune to both linear and differential cryptanalysis, the two most powerful forms of cryptanalysis in the published literature, both of which have been effective in cracking the Data Encryption Standard (DES).

Twofish is a relatively new, but well regarded 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the new Advanced Encryption Standard (AES).

Special Security Precautions Taken by PGP Virtual Disk

PGP Desktop takes special care to avoid security problems with PGP Virtual Disk volumes that other programs may not. These precautions also apply to whole disk encrypted drives.

Passphrase Erasure

When you type a passphrase, PGP Desktop uses it only for a brief time, then erases it from memory. PGP Desktop also avoids making copies of the passphrase. The result is that your passphrase typically remains in memory for only a fraction of a second.

This feature is crucially important—if the passphrase remained in memory, someone could search for it in your computer memory while you were away from the computer. You would not know it, but they would then have full access to any PGP Virtual Disk volumes protected by this passphrase.

Virtual Memory Protection

Your passphrase or other keys could be written to disk as part of the virtual memory system swapping memory to disk. PGP Desktop takes care that the passphrases and keys are never written to disk. This feature is important because someone could scan the virtual memory file looking for passphrases.

Hibernation

In Windows, Hibernate mode writes an image of your computer's entire main memory storage, including PGP Virtual Disk information, to a file on your hard drive. If your PGP Virtual Disk is open when you invoke hibernation, sensitive data will be written to your hard drive, including the session key, but **not** your passphrase.

Because hibernation is inherently insecure, PGP Corporation recommends using the PGP Whole Disk Encryption feature if you use hibernation or make sure to **enable** the PGP Virtual Disk options "Unmount when computer goes to sleep" and "Prevent sleep if disk(s) cannot be unmounted," located on the Disk tab of the PGP Options.

Memory Static Ion Migration Protection

When you mount a PGP Virtual Disk volume, your passphrase is turned into a key. This key is used to encrypt and decrypt the data on your PGP Virtual Disk volume. While the passphrase is erased from memory immediately, the key (from which your passphrase cannot be derived) remains in memory while the disk is mounted.

This key is protected from virtual memory; however, if a certain section of memory stores the exact same data for extremely long periods of time without being turned off or reset, that memory tends to retain a static charge, which could be read by attackers. If your PGP Virtual Disk volume is mounted for long periods, over time, detectable traces of your key could be retained in memory. Devices exist that could recover the key. You won't find such devices at your neighborhood electronics shop, but major governments are likely to have a few.

PGP Desktop protects against this by keeping two copies of the key in RAM, one normal copy and one bit-inverted copy, and inverting both copies every few seconds.

Other Security Considerations

In general, the ability to protect your data depends on the precautions you take, and no encryption program can protect you from sloppy security practices. For instance, if you leave your computer running with sensitive files open when you leave your desk, anyone can access that information or even obtain the key used to access the data.

Here are some tips for maintaining optimal security:

- Unmount PGP Virtual Disk volumes when you leave your computer. This way, the contents will be safely stored in the encrypted file associated with the volume until you are ready to access it again.
- Use a screen saver with a password so that it is more difficult for someone to access your computer or view your screen when you are away from your desk.

- Make sure that your PGP Virtual Disk volumes cannot be seen by other computers on the network. You may need to talk to your network management people to guarantee this. The files in a mounted PGP Virtual Disk volume can be accessed by anyone who can see them on the network.
- Never write down your passphrases. Pick something you can remember. If you have trouble remembering your passphrase, use something to jog your memory, such as a poster, a song, a poem, a joke, but do not write down your passphrases.
- If you use PGP Desktop at home and share your computer with other people, they will probably be able to see your PGP Virtual Disk volume files. As long as you unmount the PGP Virtual Disk volumes when you finish using them, no one else will be able to read their contents.
- If another user has physical access to your computer, that person can delete your PGP Virtual Disk files as well as any other files or volumes. If physical access is an issue, try either backing up your PGP Virtual Disk files or keeping them on an external device over which only you have physical control.
- Be aware that copies of your PGP Virtual Disk volume use the same underlying encryption key as the original. If you exchange a copy of your volume with another and both change your master passwords, both of you are still using the same key to encrypt the data. While it is not a trivial operation to recover the key, it is not impossible.

You can change the underlying key by re-encrypting the volume.

8

PGP NetShare

Creating a secure shared workspace

PGP NetShare provides transparent, end-to-end encryption for shared file storage.

This section includes the following topics:

- [“About PGP NetShare” on page 115](#)
- [“Licensing PGP NetShare” on page 117](#)
- [“Authorized User Keys” on page 118](#)
- [“Establishing a PGP NetShare Coordinator” on page 119](#)
- [“Working with Protected Folders” on page 119](#)
- [“Working with Authorized Users” on page 131](#)
- [“Importing PGP NetShare Access Lists” on page 135](#)
- [“Working with Active Directory Groups” on page 136](#)
- [“Removing a Folder” on page 137](#)
- [“Re-Encrypting a Folder” on page 138](#)
- [“Clearing a Passphrase” on page 139](#)
- [“Protecting Files Outside of a Protected Folder” on page 140](#)
- [“Accessing PGP NetShare Features using the Context Menu” on page 141](#)
- [“Accessing PGP NetShare Features using the Context Menu” on page 141](#)
- [“The Properties Tab” on page 143](#)
- [“PGP Desktop Menus” on page 144](#)

About PGP NetShare

PGP NetShare enables specific users to share protected files in a shared space, such as on a corporate fileserver, in a shared folder, or on removable media such as a USB drive.



In circumstances where you do not have an easily accessible shared space, using a USB removable drive is one way to share your PGP NetShare files.

The files are protected by encryption, but continue to appear as normal application files—Notepad, Microsoft Word, HTML, Microsoft Excel, and so on. Applications can directly read from and write to the files; the fact that the files are protected is transparent to the applications. Anyone else with access to the shared space can see the files, but they cannot read/use them.

PGP NetShare is client-only software—there is nothing to install on the file server; it works with your existing storage infrastructure. Server backups will archive ciphertext, which is unreadable to anyone who is not authorized to view the files.

Those who have access to the protected files are called *Authorized Users*, and folders containing the protected files are called *Protected Folders*:

- **Authorized Users:** This is the set of users who are allowed to access the protected files in the shared space. The files in the Protected Folder are encrypted to the keys of the Authorized Users. You become an Authorized User by creating a Protected Folder and adding yourself as a member, or by being added by a member of an existing set of Authorized Users. All Authorized Users have equal privileges, including the creator of the Protected Folder. You can be a member of multiple Authorized User sets at one time.
- **Protected Folder:** The Protected Folder is any folder designated to hold protected files. Files that are in a folder converted to a Protected Folder are automatically encrypted; files moved into a Protected Folder after its creation are encrypted when they are added. You can also protect individual files by selecting **Protect Individual Files** in the **NetShare** tab of **Tools > PGP Options**.



PGP NetShare does *not* provide access control for the files in a Protected Folder. Anyone with access to the files in a Protected Folder can add new, unencrypted files and/or remove existing encrypted files. This makes it important that you establish your Protected Folder in a secure shared space; but it also means that your network administrator can back up the files in the Protected Folder without being able to read them.

PGP NetShare can be used with both the PGP Virtual Disk and PGP Whole Disk Encryption features of PGP Desktop. PGP NetShare protection is designed for files in a shared, collaborative environment, usually over a network. PGP Virtual Disk and PGP Whole Disk Encryption protect individual drives or portions of drives on a local system. All three are valuable security products that are designed for slightly different circumstances. In fact, you can use all three on the same system to provide strong security for your data.

Here is an example to help you understand how you might use PGP NetShare:

Suppose you are the VP of Finance for a small company with two major product lines. The company president calls you into her office and asks you to spearhead an initiative to see if adding another major product line would be successful.

She wants you and representatives from Marketing, Sales, Engineering, Manufacturing, and Support to examine the issue from all sides and make a recommendation. The whole project needs to be low profile.

Fortunately, everyone in the company uses PGP Desktop in a PGP Universal-managed environment, so the solution for creating, sharing, updating, and securely storing the files you need is already in place: PGP NetShare.

Because members of your project are physically dispersed, you need to set up the Protected Folder for the project in a location accessible to everyone; creating the Protected Folder on the corporate intranet, for example, would allow all project members to access it.

Once the Protected Folder is established, the project members can add new files, open and work on existing files, or removes files without worrying about the fact that they are protected by encryption; the encryption and decryption are totally transparent.

Another advantage of PGP NetShare is that the files appear normally to anyone who is not an Authorized User, thus allowing your network administrator to back up the files in the Protected Folder the same way they back up all the other files on the corporate network. The backups are also protected by encryption.

PGP NetShare provides complete security for files in a Protected Folder. Data is encrypted when a Protected Folder member finishes accessing it, it is encrypted while it is in transit from or to project members, and it is encrypted while it is stored in the Protected Folder.



If you do a Save As of a protected file, and save it *outside* the Protected Folder, the new version will **not** be protected.

Licensing PGP NetShare

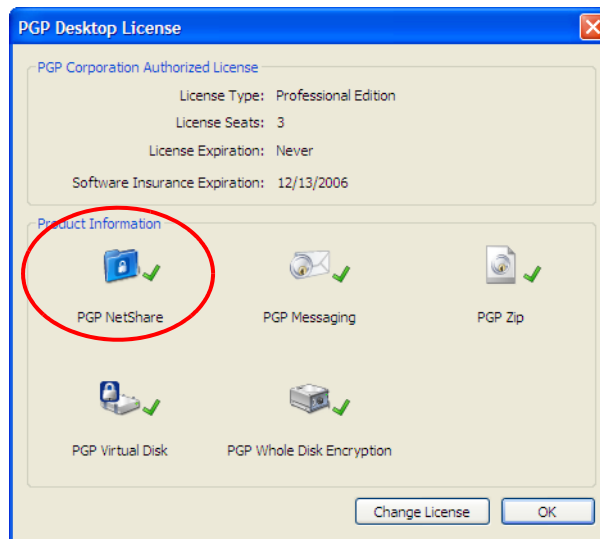
In order to use PGP NetShare, you must be running PGP Desktop 9.5 or greater and have a license that supports PGP NetShare.

To see if your copy of PGP Desktop supports PGP NetShare:

- 1 Open PGP Desktop.
- 2 From the **Help** menu, select **License**.

The PGP Desktop License window appears.

- 3 In the **Product Information** section, find the **PGP NetShare** icon:
 - If the PGP NetShare icon has a green check mark next to it, then PGP NetShare is supported.
 - If it does not have a green check mark, contact your PGP administrator about getting a license that supports PGP NetShare.




If you created one or more Protected Folders with a PGP NetShare license that has now expired, you will not be able to create any new Protected Folders, use the files currently in any Protected Folders, add files to existing Protected Folders, or be added as an Authorized User for a new Protected Folder.

In order to regain access to the decrypted versions of any files in an existing Protected Folder, you must either obtain a new PGP NetShare license or decrypt the files/folders in your Protected Folders using the **Remove <filename> from PGP NetShare** command (see ["Accessing PGP NetShare Features using the Context Menu"](#) on page 141 for more information).

Authorized User Keys

PGP NetShare uses the PGP keys of the Authorized Users you designate to control access to the decrypted files in the Protected Folder, and it uses the private keys of these Authorized Users to sign new files that are added to the Protected Folder.

 PGP NetShare does not support the use of passphrases to protect files. PGP keys must be used to protect files.

When a set of Authorized Users is created, the creator specifies the public keys of the users who will be able to use the files in the Protected Folder. To use those files, Authorized Users must have the corresponding private key on their system in order to gain decrypted access to the files.

Establishing a PGP NetShare Coordinator

While a PGP NetShare coordinator for a Protected Folder is not required, you may want to consider establishing one from among the Authorized Users. It would be the responsibility of this person to monitor the files and folders in the Protected Folder, and how the Authorized Users use them, to make sure that the activity in the Protected Folder is going as planned.

Because all Authorized Users can add or remove files, folders, and (in some cases) users, it is possible that, over time, files are inappropriately added or removed from the Protected Folder, or Authorized Users are inappropriately added or removed.

The Protected Folder coordinator should monitor Authorized Users and the Protected Folder for these problems and fix them if they occur.

Working with Protected Folders

Choosing the Location for a Protected Folder

PGP Corporation recommends that you create your PGP NetShare Protected Folder in a space that is accessible to all Authorized Users, but that is protected from everyone else.

While you can create the Protected Folder in a publicly accessible space, remember that PGP NetShare does *not* provide access control for the files in a Protected Folder.

What you do with the files in a Protected Folder and who can access them impacts the protection PGP NetShare can provide. You should take the following circumstances into consideration when choosing the location for a PGP NetShare Protected Folder.

- “Normal Usage”
- “File Access”
- “Direct Access to Ciphertext”
- “Protected Files Corrupted, Deleted, or Overwritten”
- ““Blacklisted” and Other Files You Cannot Protect”

Normal Usage

In normal usage by an Authorized User, PGP NetShare fully protects the files within a Protected Folder. Normal usage means opening a protected file, making changes, then saving it; creating a new file in a Protected Folder; or moving or copying a file into a Protected Folder.

When a file is moved or copied out of a PGP NetShare Protected Folder, PGP NetShare attempts to keep the file protected. This allows you to copy files from a Protected Folder to a USB drive, for example, and retain the file's protection. If you move or copy a file out of a Protected Folder, you should always verify that the destination file is still protected by looking for the visual lock indicator or examining the file properties.

File Access

Every application you use will have full access to the decrypted data of your PGP NetShare-protected files. This includes other PGP Corporation applications, such as PGP Zip. So, if you create a PGP Zip archive and include a PGP NetShare-protected file, the PGP Zip archive will contain a decrypted version of the file.

Be aware also that if you do a Save As of a protected file from within an application, you may be saving the contents of a protected file into an unprotected folder. The resulting file will therefore **not** be protected.

Direct Access to Ciphertext

There are some circumstances where PGP NetShare can be bypassed, providing direct access to the ciphertext of the encrypted file.

This allows the protected files on a fileserver, for example, to be backed up, moved, copied, or FTPed by a user (such as the network administrator) who has physical access to the protected files but who does not have PGP Desktop installed. In these cases, the ciphertext of the protected files would be backed up, moved, copied, or FTPed.

Protected Files Corrupted, Deleted, or Overwritten

PGP NetShare does **not** provide file access control. Even though users without proper authorization are unable to open files within Protected Folders, it is still possible for these users to access them. This means that even protecting files with PGP NetShare is no assurance that they cannot be corrupted, deleted, or overwritten by users who have access to them. PGP NetShare protects the contents of a file—it cannot protect the file itself.

It is highly recommended that you keep strong file access controls in place—in addition to the cryptographic access control and protection offered by PGP NetShare.

“Blacklisted” and Other Files You Cannot Protect

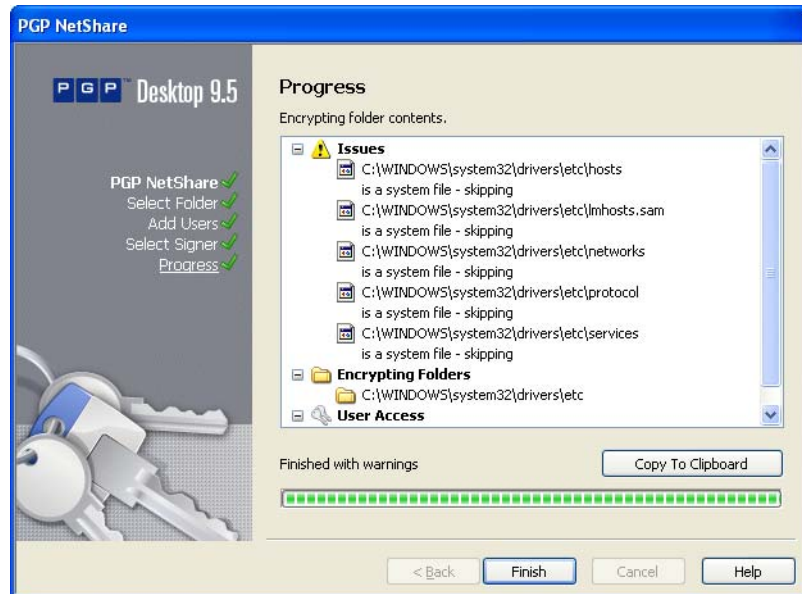
PGP NetShare does not allow you to protect certain files and folders. Before a file or folder is protected by PGP NetShare, it is checked against this list, known as the “blacklist.” If a file or folder is identified as being blacklisted, PGP NetShare continues with creating the Protected Folder, but the file and/or folder is skipped and a message is displayed in the PGP NetShare Assistant Progress screen that the item is a blacklisted.

Files that are blacklisted include:

- All files with the file extension *.skr, *.pkr, and *.pgd, to prevent you from encrypting your keys or PGP Virtual Disks.
- The PGP Desktop installation folder and all files within it (by default, the folder is located at C:\Program Files\PGP Corporation\PGP Desktop).
- The PGP Preferences folder and all files within it (by default, the folder is located in your user folder at C:\Documents and Settings\[your user name]\Application Data\PGP Corporation\PGP).

- The PGP default keyring folder (by default, the keyring is located in the My Documents folder).

Other files that PGP NetShare prevents from adding to Protected Folders are any files or folders that have the System attribute set, and all files and folders in the Windows installation directory (by default, C:\Windows and C:\Windows\System32). When system files or folders are added to PGP NetShare, the file and/or folder is skipped and a message is displayed in the PGP NetShare Assistant Progress screen that the item is a system file or folder.



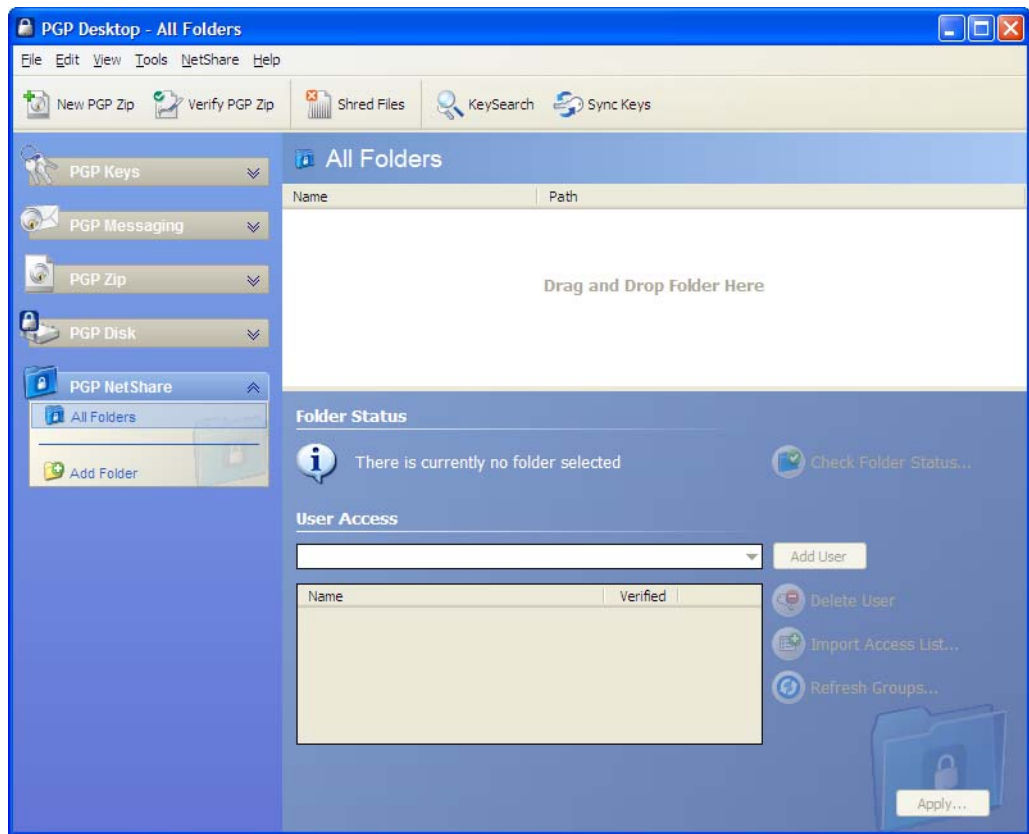
Creating a New PGP NetShare Protected Folder

The Protected Folder is the folder that holds the PGP NetShare-protected files.

To create a new PGP NetShare Protected Folder:

- 1 Open PGP Desktop and click on the PGP NetShare Control Box.

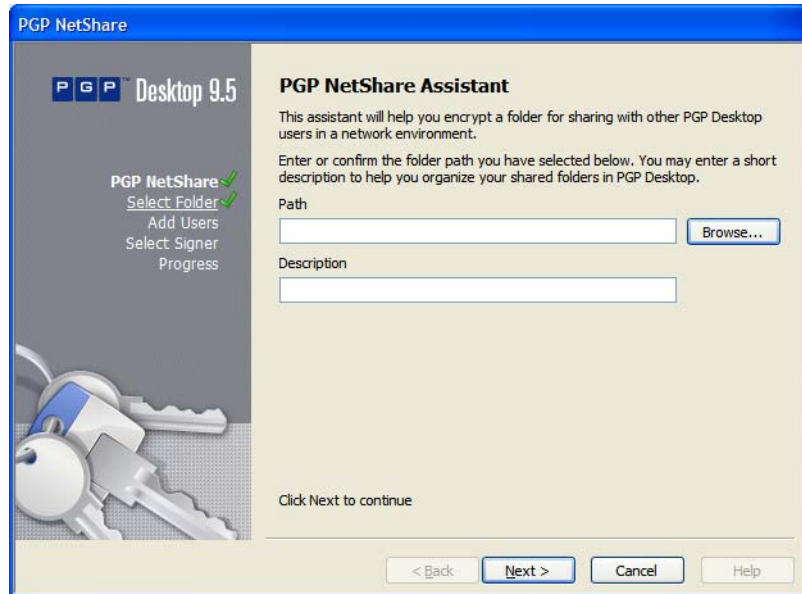
The PGP NetShare work area appears.



2 Do one of the following:

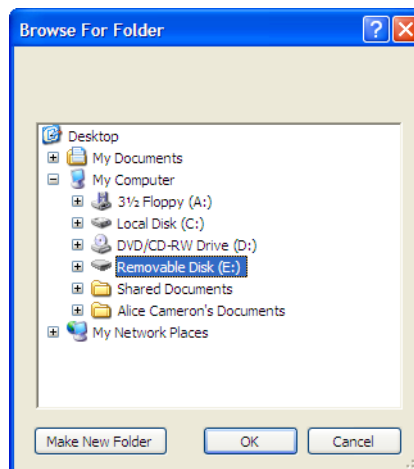
- Drag the folder you want to be the Protected Folder to the field labeled “Drag and Drop Folder Here,” which opens the PGP NetShare Assistant and skips the step of specifying the Protected Folder.
- Click **Add Folder** in the PGP NetShare Control Box or from the **NetShare** menu, select **Add Folder**.

The **Select Folder** screen of the PGP NetShare Assistant appears.



- a Click **Browse**.

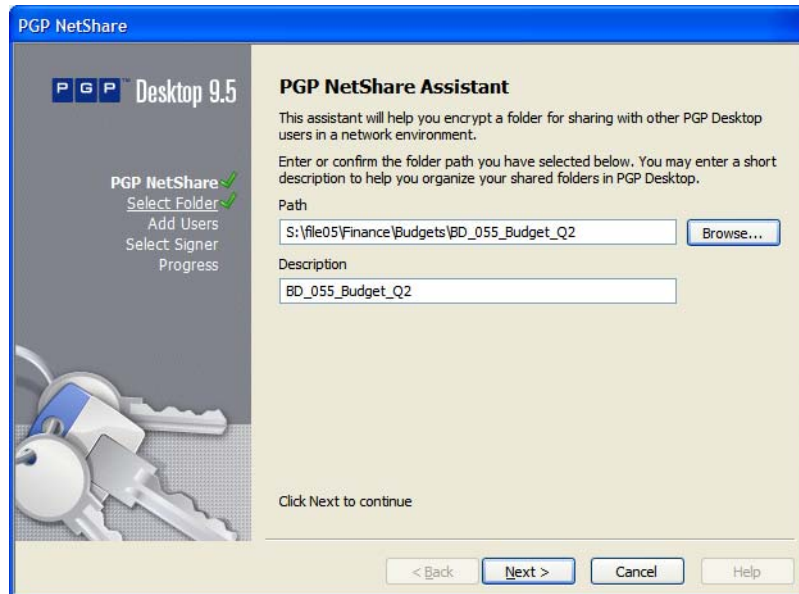
The **Browse For Folder** dialog appears.



- b Do one of the following:
- Navigate to the folder with the files you want to include in the Protected Folder you are creating.
 - Create an empty folder into which you will put the files you want to be part of the Protected Folder by clicking **Make New Folder** on the **Browse For Folder** dialog.
- c Click **OK** to close the **Browse For Folder** dialog.

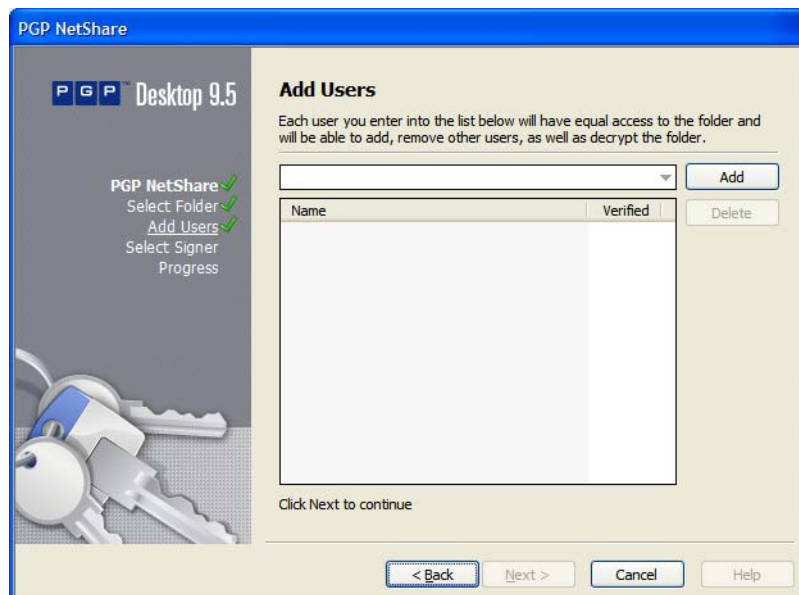
The **Select Folder** screen appears again.

- d (Optional) In the **Description** field, type a description for the Protected Folder you are creating.



- 3 Click **Next**.

The **Add Users** screen appears.



- 4 To add authorized users for the Protected Folder you are creating, click the down-facing triangle.

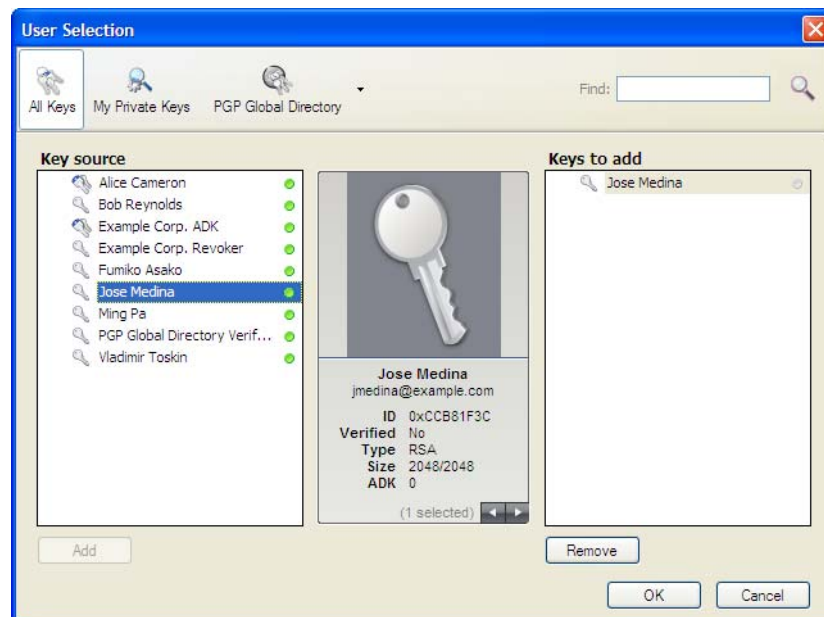
A list of the keys on your keyring appears.

- 5 Select a user, and then click **Add**.

i If you want to be an Authorized User, do not forget to add your own key. If you do not, you will not be able to use the files in the Protected Folder.

- 6 You can also add authorized users by clicking **Add**.

The **User Selection** dialog appears.



- 7 Do one of the following:

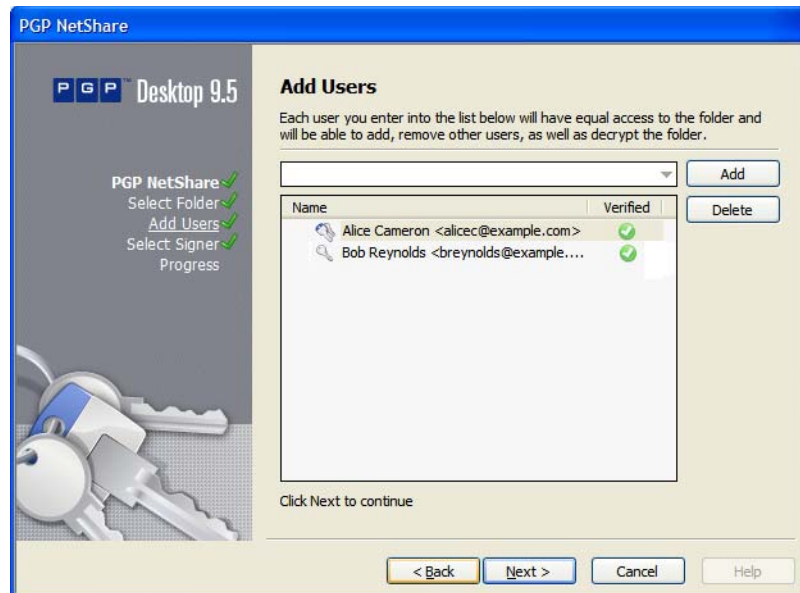
- Drag keys from the **Key source** column into the **Keys to add** column.
- Click on a key in the **Key source** column and click **Add**.
- Double-click on a key in the **Key source** column

- 8 To add keys from the PGP Global Directory, click the PGP Global Directory icon, type a search term in the **Search** field, then click the magnifying glass to start the search. The results of the search appear in the **Key source** column; from there, add them to the **Keys to add** column.

i PGP NetShare does not automatically notify newly added members that they have been added to a Protected Folder as authorized users. Generally speaking, it is the responsibility of the creator of a new Protected Folder to notify members that the Protected Folder has been created and that they are authorized users.

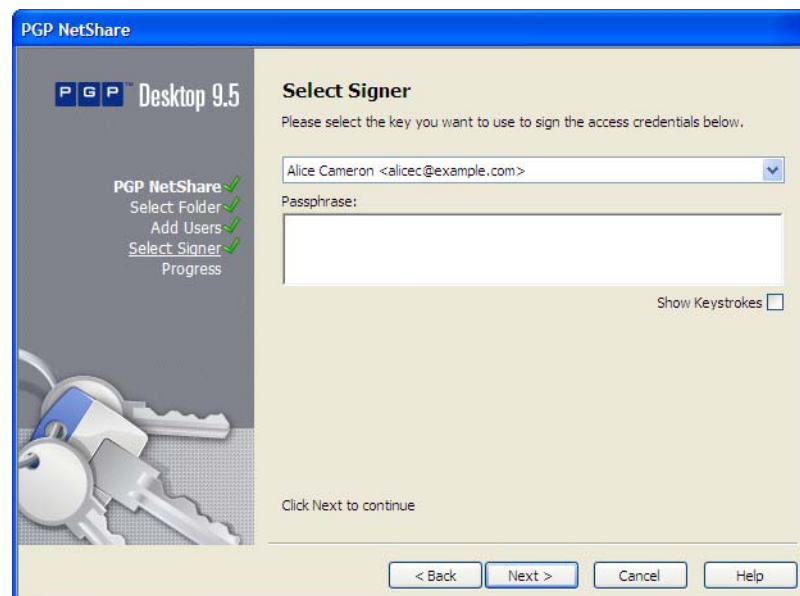
- 9 Click **OK** when you are finished with the User Selection screen.

The **Add Users** screen reappears.



- 10 Click **Next**.

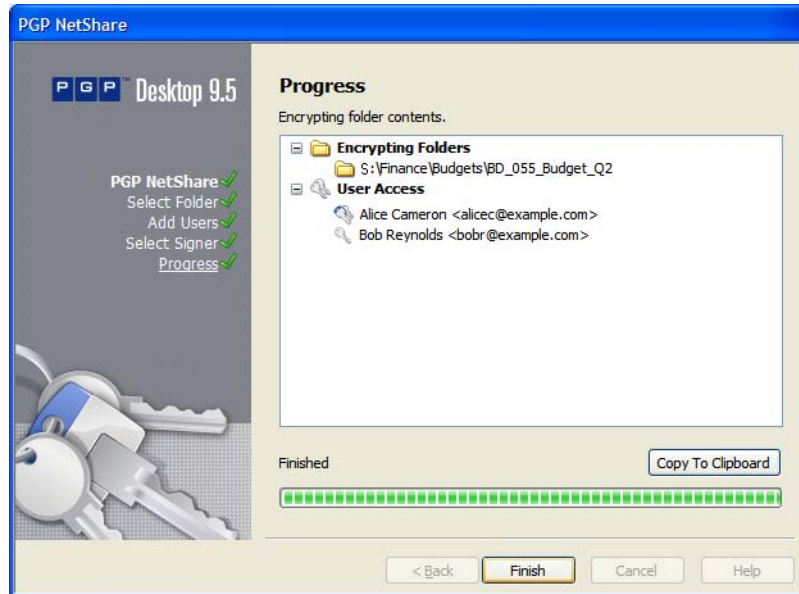
The **Select Signer** screen appears.



- 11 Select one private key from the private keys on the local keyring.
This key will be used to sign the files that are protected by encryption in the Protected Folder.
- 12 Type the **Passphrase** for the key.

13 Click **Next**.

The Progress screen appears.



The files in the specified Protected Folder are encrypted and the specified users are added as Authorized Users.

14 When the process is done, click **Finish**.

Using Files in a PGP NetShare Protected Folder

Once you are a PGP NetShare Authorized User, there are three ways to use the files in the Protected Folder:

- Double-click the Protected Folder folder to open it, then double-click the specific file you want to use.
- Open the file you want to use from within the application that created it.
- Open the Protected folder by clicking its path, which displays as a hypertext link; then double-click the specific file you want to use.

If the passphrase of the private key used for your membership in the PGP NetShare Protected File is cached on your system, you do not need to do anything else to open the files; they will open automatically.

If your passphrase is not cached, however, the Protected Folder is locked. You will need to authenticate before you can open the files in the Protected Folder. Refer to [“Unlocking a Protected Folder” on page 128](#) for more information.

Unlocking a Protected Folder

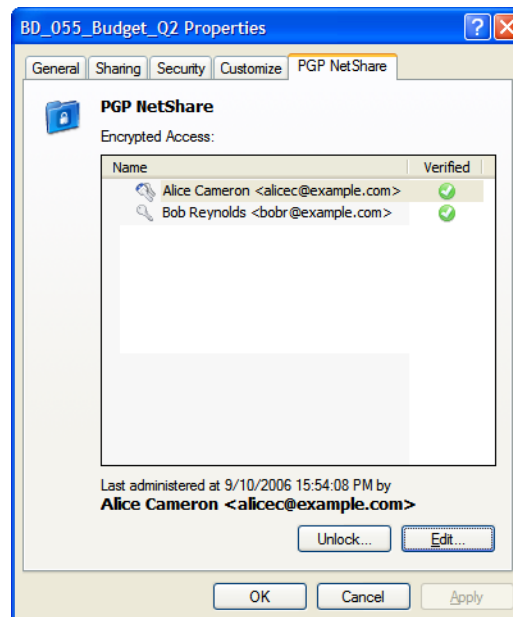
You can use the **Unlock** button to try to access a folder that you can't seem to access but believe you should be able to unlock, or in situations where a folder requires manual unlocking. You must manually unlock a Protected Folder when the folder is locked due to one of the following reasons:

- The timer in the Passphrase prompt dialog box expires.
- If you click **Cancel** in the Passphrase dialog box without entering a valid passphrase.

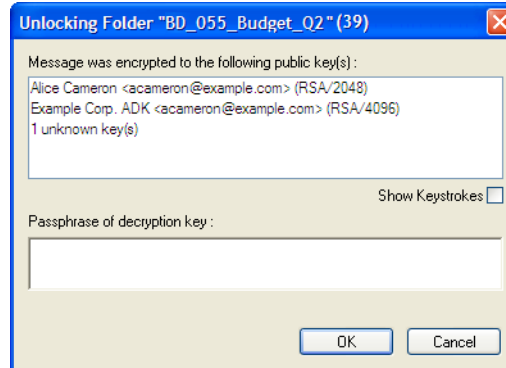
Any subsequent attempts to access the protected folder result in an "Access is denied" dialog box and you must unlock each Protected Folder before you can use the files in them.

To unlock a Protected Folder:

- 1 Right-click the Protected Folder and select **PGP Desktop > PGP NetShare Properties**.
- 2 The PGP NetShare Properties tab appears.



- 3 Click **Unlock**.
The **Unlocking** dialog appears.



- 4 Type the appropriate passphrase, then click **OK**.

The Unlocking dialog disappears. Your passphrase is cached and you have access to all files in the Protected Folder.

Determining the Files in a Protected Folder

Once you become an Authorized User, you have full access to all files in the Protected Folder. If you created the Protected Folder, you probably know what files are in it. If you were added to the Protected Folder by another member, however, it may not be immediately clear to you what files are available to you in the Protected Folder.

To determine what files are in a Protected Folder:

- 1 Open PGP Desktop and click on the **PGP NetShare** Control Box.
- 2 Click the path to the Protected Folder, which appears as a hypertext link.

The Protected Folder contents will appear in a new window, showing the files and folders that are in the Protected Folder.

If access is denied, it means the Protected Folder is locked. You will need to either go to the PGP NetShare tab of the Properties screen for the locked folder and unlock it or restart your system to gain access. Refer to [“Using Files in a PGP NetShare Protected Folder” on page 127](#) for more information about unlocking a Protected Folder.

Adding Subfolders to a Protected Folder

PGP NetShare supports adding both files and folders into a Protected Folder after it has been created.

All of the files in a folder you add into a Protected Folder will automatically be protected; once added to the Protected Folder, both the folder and the files in it will only be available to authorized users.

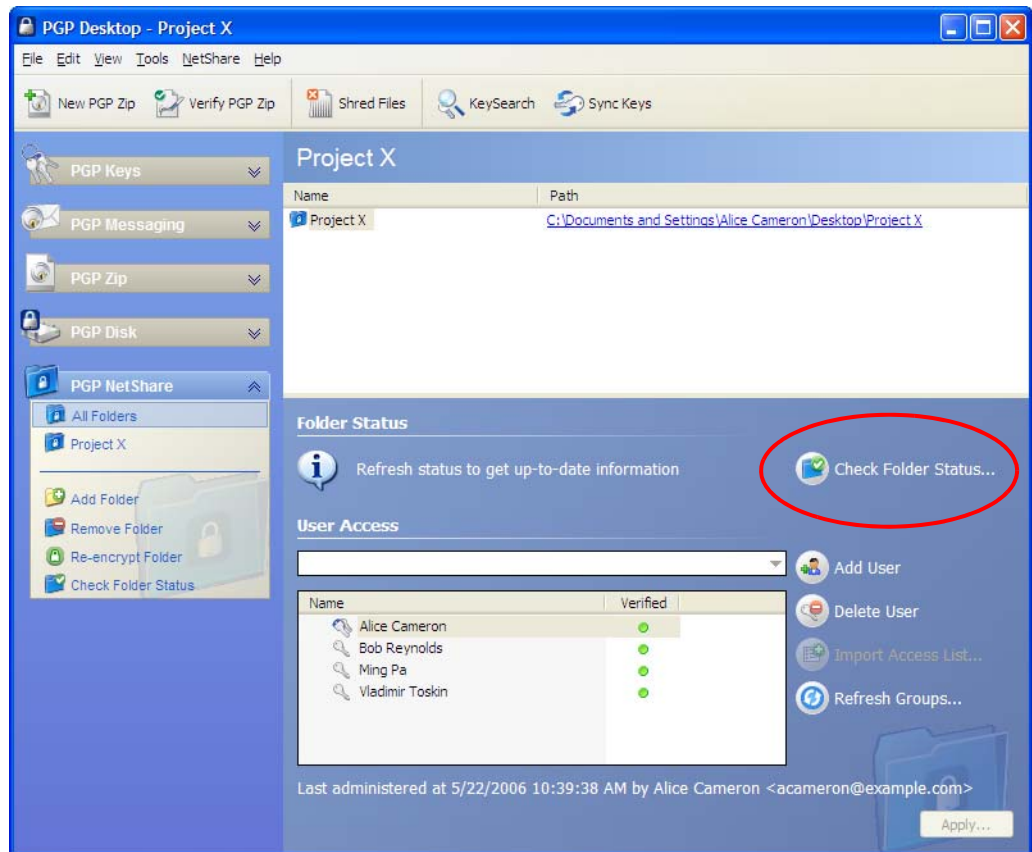
Be sure not to add a folder that is already a Protected Folder for a different set of authorized users. This would cause the new subdirectory to have a different set of authorized users from the parent folder.

Checking Folder Status

The **Check Folder Status** command, available from the NetShare Folder work area, the PGP NetShare Control Box, or from the NetShare menu, provides up-to-date information about the status of the specified PGP NetShare folder.

To check the status of a folder in a Protected Folder:

- 1 On the PGP NetShare work area, in the Folder Status section, click **Check Folder Status**.



You must have a PGP NetShare folder selected.

- 2 Read the text to the left of the **Check Folder Status** button for the status of the selected folder.

For example: "All folders and files are encrypted."

Copying Protected Folders to Other Locations

You will achieve greatest security if you always work within a protected folder; PGP Corporation recommends that when you need to copy a folder, you must first create a Protected Folder as your destination. Whenever you move files from a Protected Folder to another Protected Folder, your environment will remain protected.

PGP NetShare retains file encryption even when the Protected Folder is moved to another location. However, depending on how you copy the files, and where, you may discover that the process has caused the *folder* to lose its protection. The files in the folder retain their protected status, but the folder may lose its PGP NetShare information, and thus lose its PGP icon as well.

If you have copied a folder to an unprotected location, as a best practice, check the folder status as described in [“Checking Folder Status”](#) to ensure the folder and files are encrypted.

If the folder is not encrypted, do the following:

- 1 If your PGP NetShare permissions allow you to do so, create a new protected folder at the destination as described in [“Creating a New PGP NetShare Protected Folder”](#).
- 2 Copy the contents of the folder that has lost its protection into the new protected folder.
- 3 Import the access list of the old folder into the new folder as described in [“Importing PGP NetShare Access Lists”](#) on page 135.

Working with Authorized Users

Anyone with a PGP Desktop 9.5 or greater who has an appropriate keypair in PGP Desktop can be an Authorized User of a PGP NetShare Protected Folder.

Keypairs can be:

- Created in PGP Desktop
- Created by an OpenPGP application and imported into PGP Desktop
- An X.509 certificate that has been imported into PGP Desktop

There are two ways to become an Authorized User:

- You can create a Protected Folder using PGP Desktop and add yourself as an Authorized User.
- You can be added as an Authorized User by an existing member.

Once you become an Authorized User, you have the same rights as all other members. There is no hierarchy of rights for PGP NetShare Authorized Users.

Adding an Authorized User

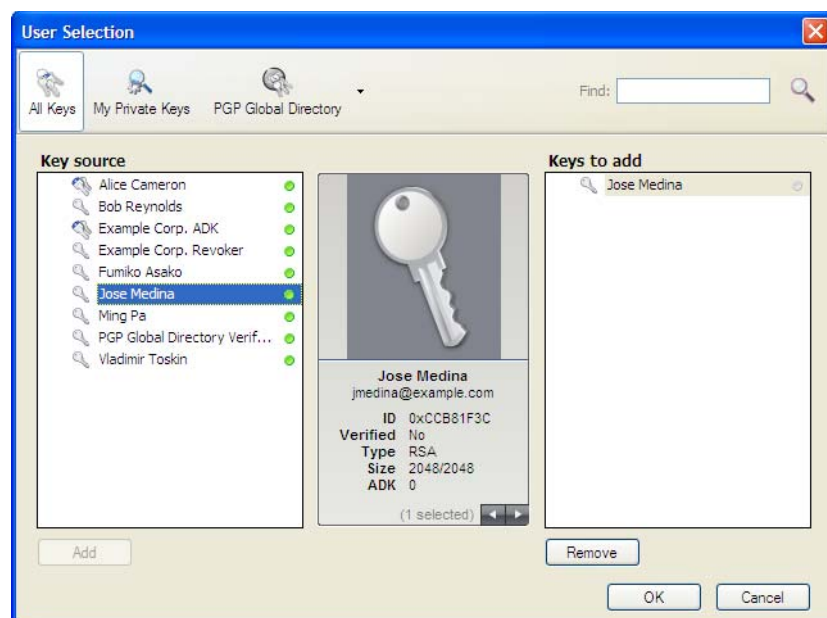
Most PGP NetShare Authorized Users are added when the Protected Folder is created, but you can add members at any time after creation—as long as you are an Authorized User of that Protected Folder.

- ! Be careful who you add as an Authorized User. Once a person is added, that person has all the rights and privileges as any other member. The new member can add new files to or remove existing files from the Protected Folder, and can remove other Authorized Users, including you.

To add a new PGP NetShare Authorized User:

- 1 Select the PGP NetShare folder to which you want to add a new member.
- 2 In the User Access section, click **Add User**.

The User Selection dialog appears.



- 3 Do one of the following:
 - Drag keys from the **Key source** column into the **Keys to add** column.
 - Click on a key in the **Key source** column and click **Add**.
- 4 To add keys from the PGP Global Directory, click the PGP Global Directory icon, type a search term in the **Search** field, then click the magnifying glass or press **Enter** to start the search. The results of the search appear in the **Key source** column; from there, add them to the **Keys to add** column.

- i PGP NetShare does not notify new members that they have been added as an Authorized User. Generally speaking, it is the responsibility of the person who adds a new user to tell them that they are now authorized.

- 5 Click **OK**.

The user is added to the list of Authorized Users.

- 6 Click **Apply**.

The Select Signer screen appears.

- 7 Select one private key from the private keys on the local keyring or accept the default key.

This key will be used to sign the files when they are re-encrypted.

Re-encryption of the files in a Protected Folder is done automatically as a security precaution when Authorized Users are added.

- 8 Type the passphrase for the selected key, if it is not cached, then click **Next**.

The Progress screen appears and the files in the specified Protected Folder are re-encrypted.

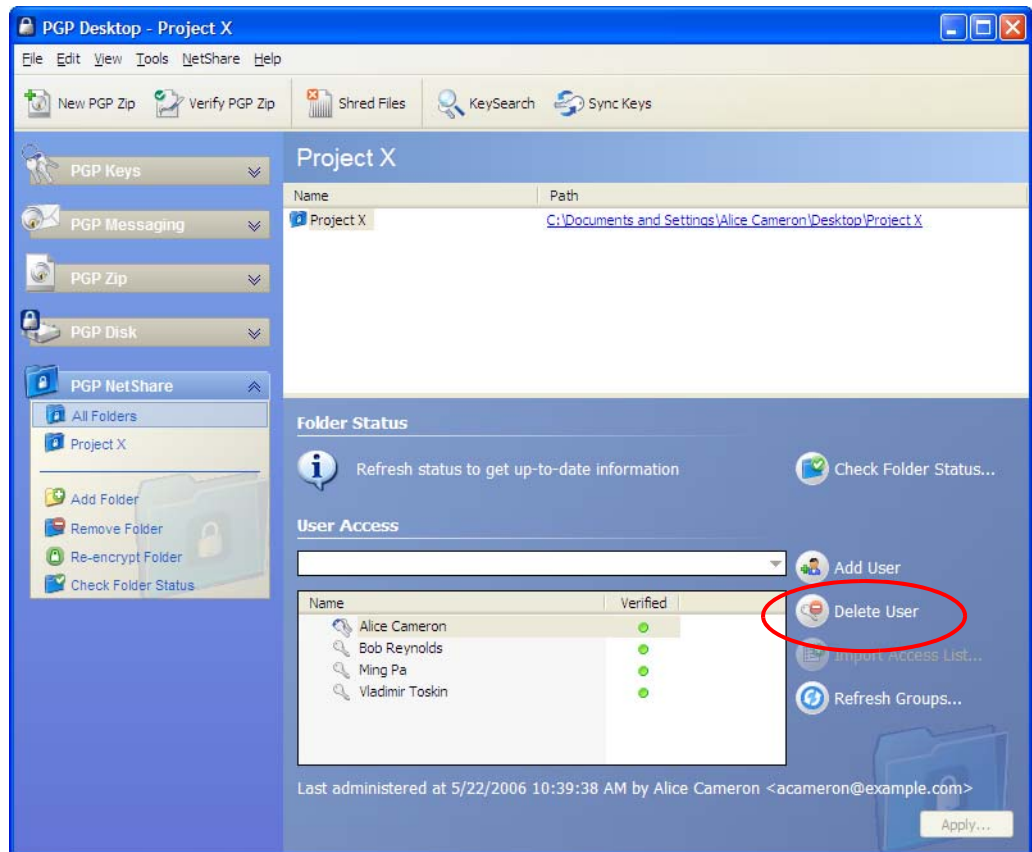
- 9 Click **Finish**.

Deleting a User from a Protected Folder

To remove a member of a PGP NetShare Protected Folder, you must delete that user.

To delete a user from a PGP NetShare Protected Folder:

- 1 On the PGP NetShare screen, select the Protected Folder from which you want to delete the user.



- 2 In the User Access list near the bottom of the screen, click on the name of the user you wish to delete, then click **Delete User**.

The user is deleted from the list.

- 3 Click **Apply**.

The Select Signer screen appears.

- 4 Select one private key from the private keys on the local keyring or accept the default key.

This key will be used to sign the files when they are re-encrypted.

PGP NetShare automatically re-encrypts files in a Protected Folder as a security precaution when a member is removed from the Protected Folder.

- 5 If you are prompted to do so, type the passphrase for the selected key, then click **Next**.

The Progress screen appears and the files in the specified Protected Folder are re-encrypted.

- 6 Click **Finish**.

The deleted user is no longer a member of the Protected Folder and will not be able to access the files in it.

Importing PGP NetShare Access Lists

Importing access lists lets you import the set of members and their keys from one set of Authorized Users of which you are a member to another set of Authorized Users of which you are a member.

This option is available only when you have more than one Protected Folder.

To import an access list:

- 1 On the PGP NetShare screen, select the Protected Folder into which you want to import the members of another Protected Folder.
- 2 In the **User Access** list near the bottom of the screen, click the **Import Access List** button.

The **PGP Import User Access List** screen appears.

- 3 Click the name of the existing Protected Folder whose members you wish to import, then click **Import**.

- 4 Click **Apply**.

The **Select Signer** screen appears.

- 5 Select one private key from the private keys on the local keyring or accept the default key.

This key will be used to sign the files when they are re-encrypted.

Re-encryption of the files in a Protected Folder is done automatically as a security precaution when membership in that folder is modified.

- 6 If you are prompted to do so, type the passphrase for the selected key, then click **Next**.

The Progress screen appears and the files in the specified Protected Folder are re-encrypted.

- 7 Click **Finish**.

The new members are added to the Protected Folder.

Working with Active Directory Groups

PGP NetShare integrates with Active Directory so you can easily assign users to Protected Folders an Active Directory group. PGP NetShare uses LDAP (Lightweight Directory Access Protocol) to retrieve group information from your organization's Active Directory.

Setting up PGP NetShare to Work with Groups

In order to retrieve group information, you must bind to your PGP Universal Server and then enable the Use for Group Expansion option. The following procedures describe these steps if you have installed PGP Desktop in a standalone environment. If PGP Desktop is installed and integrated with a PGP Universal Server environment, you do not need to follow this procedure, as LDAP integration is automatic.

To set up PGP NetShare to work with groups:

- 1 Add the PGP Universal Server to your list of Preferred Keyservers. To do this, create a new messaging service and specify the name of your PGP Universal Server. For more information, refer to ["Creating a Service and Editing Account Properties"](#) on page 29.
- 2 Bind to the PGP Universal Server. To do this, follow the instructions to manually bind to a PGP Universal server in ["Binding to a Universal Server"](#) on page 256.
- 3 In the PGP Key Generation assistant, select the key mode as GKM, CKM, or SCKM. Do not select SKM.
- 4 Verify that the key is available on the PGP Universal Server. To do this, in PGP Desktop, select the PGP Keys Control Box. Click **Search for Keys**, select the name of the PGP Universal Server, enter your name, and click **Search**.
- 5 Enable group expansion. To do this, in PGP Desktop, select the PGP Messaging Control Box.
- 6 Choose **Messaging > Use for Group Expansion**. A check appears next to the menu item to indicate it is enabled.

Refreshing Groups

If you are using PGP NetShare in a PGP Universal-managed environment, and your PGP administrator has established Active Directory groups, you can have PGP NetShare verify that group memberships are up to date.

To refresh Active Directory groups:

- 1 On the PGP NetShare screen, select the Protected Folder whose Active Directory groups you want to refresh.
- 2 In the **User Access** section, click the **Refresh Groups** button.

PGP NetShare checks the Active Directory group memberships and refreshes them if necessary.

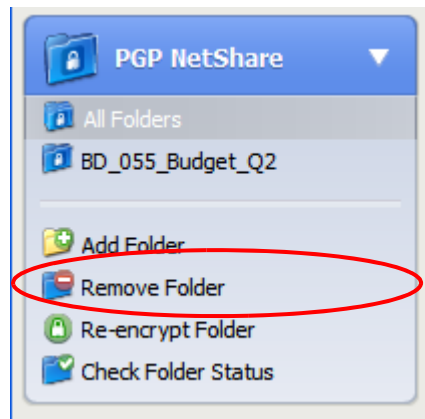
Removing a Folder

The Remove Folder command restores the files in a Protected Folder to their normal, decrypted state.

All folders and files that are part of the Protected Folder are decrypted; the PGP icon overlay on the files will be removed.

To remove protection from a PGP NetShare Protected Folder:

- 1 On the PGP NetShare screen, select the Protected Folder whose protection you wish to remove.
- 2 In the PGP NetShare Control Box, click **Remove Folder**.



The Confirm Decryption screen appears.

- 3 Verify that you are removing protection from the desired folder, then click **Next**.
The Unlocking Folder dialog appears, if your passphrase has not been cached.
- 4 Type the passphrase of one of the keys to which the files were encrypted, then click **OK**.

You must type an appropriate passphrase in the allotted time or the decryption process will be cancelled.

The Progress screen appears and the files are decrypted.

- 5 Click **Finish**.

The files in the Protected Folder folder are no longer protected by encryption, it is removed from the PGP NetShare Protected Folder list, and its lock icon disappears.

Re-Encrypting a Folder

Re-encrypting a folder re-encrypts the files in the specified Protected Folder. Re-encryption changes the underlying key, preventing access to anyone who might have been able to determine the current key.

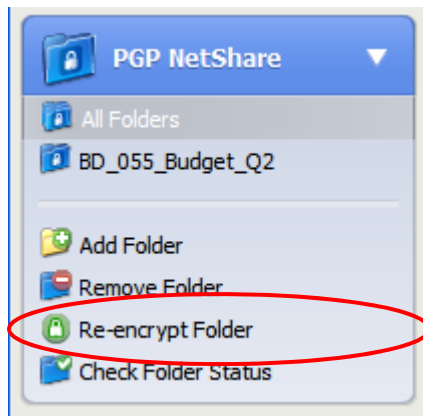
The Re-encrypt Folder command lets you re-encrypt whenever you want; for example, if you believe an unauthorized person has gained access to the files in the Protected Folder.

Examples of why you might want to re-encrypt:

- You are concerned some Protected Folder contents are not encrypted; for example, if someone who is not an Authorized User places a file in a Protected Folder.
- The key information of an Authorized User has been compromised.
- A new Authorized User is added, and needs access to the Protected Folder (this does not happen automatically).

To re-encrypt a Protected Folder:

- 6 On the PGP NetShare screen, select the Protected Folder you want to re-encrypt, then click **Re-encrypt Folder** in the PGP NetShare Control Box.



The Add Users screen appears.

- 7 You can add new members to or remove existing members from a Protected Folder that is being re-encrypted.

- 8 Click **Next** to continue.

The Select Signer screen appears.

- 9 Select one private key from the private keys on the local keyring or accept the default key.

This key will be used to sign the files when they are re-encrypted.

- 10 If you are prompted to do so, type the passphrase and then click **Next**.

The Progress screen appears and the files in the specified Protected Folder are re-encrypted.

- 11 Click **Finish**.

The re-encryption process is complete.

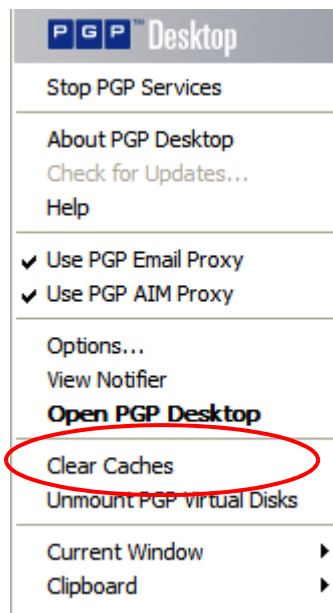
Clearing a Passphrase

By default, PGP NetShare caches passphrases according to the settings on the General tab of the PGP Desktop Options. This can make it easier to use PGP NetShare, as you do not need to type your passphrase to use the protected files in the Protected Folder.

However, if you are going to be leaving your system, you may not want to leave it with your passphrase cached, as this might let an unauthorized person perform actions without needing the passphrase.

To clear a passphrase:

- 1 In Windows, click the PGP icon in the System Tray.




- 2 Select **Clear Caches** from the list of commands that appears.

At least one passphrase must be cached for this command to be active.

Your cached passphrases are cleared.


Protecting Files Outside of a Protected Folder

PGP NetShare has an advanced option that lets you protect individual files that are **not** in a PGP NetShare Protected Folder. This option is disabled by default.

 You may be prevented from selecting this option by your PGP administrator if you are using PGP Desktop in a PGP Universal-managed environment.

To protect individual files outside of a PGP NetShare Protected Folder, you must first select the **Protect individual files** option on the NetShare tab of the PGP Options; refer to “[PGP NetShare Options](#)” on page 241 for more information. You cannot protect files that are outside of a PGP NetShare Protected Folder until this option is enabled.

Once you select the **Protect individual files** option, you can protect individual files that are outside of a Protected Folder using the PGP Desktop context menu in Windows Explorer. *Individually protected files do **not** appear in the PGP NetShare Work area of the PGP Desktop user interface.*

 PGP NetShare makes every effort to protect individually protected files, but some applications (Microsoft Word, for example) save modified files in such a way that it appears to PGP NetShare that the protected file has been deleted. Under such circumstances, PGP NetShare cannot continue to protect these files. Note that this applies only to individually protected files that are not in a Protected Folder, not files in a PGP NetShare Protected Folder. To avoid having protected files become unprotected, PGP Corporation strongly recommends that you keep files you want protected in a PGP NetShare Protected Folder.

To enable the Protect individual files option:

- 1 From the **Tools** menu in PGP Desktop, select **PGP Options**.
- 2 Click the **NetShare** tab.
- 3 On the NetShare tab, make sure the **Protect individual files** option is selected.
The default setting is *not* selected.

To protect individual files using PGP NetShare:

- 1 In Windows Explorer, right-click the file you would like to protect using PGP NetShare.
- 2 In the context menu that appears, select **PGP Desktop > Add [filename] to PGP NetShare**.
- 3 When the PGP NetShare Assistant appears, add Authorized Users and select a private key for signing.
- 4 When the encryption process is complete, click **Finish**.

The protected file displays a PGP NetShare icon in Windows Explorer.

You can also use the context menu to view the PGP NetShare properties of a protected file, re-encrypt individually protected files that are outside of a Protected Folder, and remove protection from them.

To view the PGP NetShare properties of a protected file using the context menu:

- 1 In Windows Explorer, right-click the protected file whose PGP NetShare properties you would like to view.
- 2 In the context menu that appears, select **PGP Desktop > PGP NetShare Properties**.
The Properties window for the selected file appears.
- 3 When done viewing properties, click **OK**.

To re-encrypt protected files using the context menu:

- 1 In Windows Explorer, right-click the protected file you would like to re-encrypt.
- 2 In the context menu that appears, select **PGP Desktop > Re-encrypt**.
- 3 When the PGP NetShare Assistant appears, add and/or remove Authorized Users and select a private key for signing.
- 4 When the re-encryption process is complete, click **Finish**.

To remove protection from individually protected files using the context menu:

- 1 In Windows Explorer, right-click the protected file whose protection you would like to remove.
- 2 In the context menu that appears, select **PGP Desktop > Remove [filename] from PGP NetShare**.
- 3 When the PGP NetShare Assistant appears, confirm that you want to remove protection from the file by clicking **Next**.
- 4 When the file has been decrypted, click **Finish**.

Accessing PGP NetShare Features using the Context Menu

Some PGP NetShare functionality is available from the right-click context menu in Windows Explorer.

You can protect folders (and files, if you have enabled the **Protect individual files** option) from Windows Explorer by right-clicking the item. Select **PGP Desktop > Add [name] to PGP NetShare** from the context menu that appears to begin the process of designating that item as protected by PGP NetShare.

Refer to [“Protecting Files Outside of a Protected Folder” on page 140](#) for more information about protecting individual files outside of a Protected Folder using PGP NetShare.

Once a folder or file is protected by PGP NetShare, there are three commands you can perform in Windows Explorer using the context menu:

- **PGP NetShare Properties.** This command opens the PGP NetShare tab of the Properties screen for the file or folder. On this tab, you can view who can use protected files, unlock a file/folder if locked, and add users who can use the protected files.
- **Re-encrypt.** This command re-encrypts the specified folder or file to a new underlying key.
- **Remove <filename> from PGP NetShare.** This command removes the PGP NetShare protection from the specified folder or file.

Refer to [“Protecting Files Outside of a Protected Folder” on page 140](#) for the applicable procedures.

PGP NetShare in a PGP Universal-Managed Environment

If you are using PGP NetShare in a PGP Universal-managed environment, your PGP administrator may have configured two settings that affect how PGP NetShare works on your system.

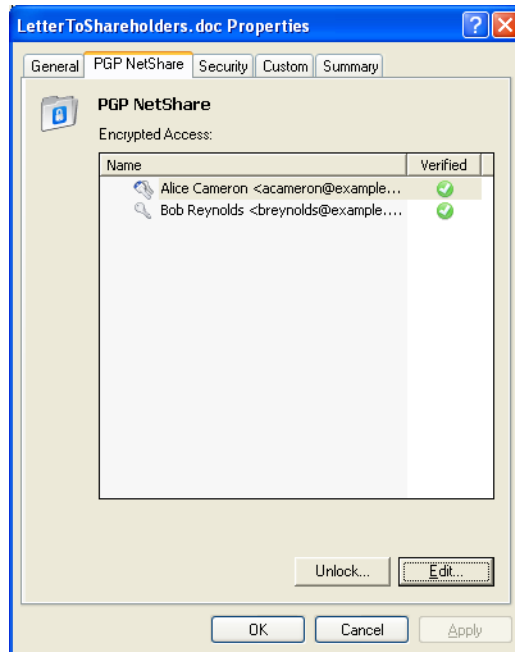
These settings are:

- **Allow the user to create and manage PGP NetShare folders.** When enabled, this setting allows you to create PGP NetShare Protected Folders. When disabled, you can use a Protected Folder that someone else has created, but you cannot create one yourself. This setting is enabled by default.
- **Allow the user to enable Advanced User mode.** When enabled, this setting allows you to enable Advanced User mode in your PGP Options, which means that you can protect individual files that are moved out of a Protected Folder. This setting is disabled by default.

Contact your PGP administrator if you would like to change these settings.

The Properties Tab

Any file that is protected by PGP NetShare has a PGP NetShare tab on its Properties screen, which shows information about the file.



To access the PGP NetShare tab on the Properties screen of a file:

- 1 In Windows Explorer, do one of the following:
 - Right-click the file and select **Properties** from the list.
 - From **File** menu, select **Properties** from the list.

The Properties screen for the specified file appears.

- 2 Click the **PGP NetShare** tab.

The PGP NetShare tab appears.

The PGP NetShare tab for a file shows you the names of those users who can use the encrypted file.

From here you can do one of the following:

- **Unlock.** Click to unlock a Protected Folder that has been locked.
- **Edit.** Click to display the Add Users screen, which lets you add/remove users who can use the selected file/folder. The file/folder will be re-encrypted if a user is added or removed.

To close the Properties dialog, click **OK**.

PGP Desktop Menus

There are three PGP Desktop menus that have commands that affect PGP NetShare: File, Edit, and NetShare.

The File Menu

When the PGP NetShare Control Box is selected, the **New PGP NetShare Folder** command under the **File** menu lets you create a new Protected Folder.

The process is the same as described in [“Creating a New PGP NetShare Protected Folder” on page 121](#).

The Edit Menu

When the PGP NetShare Control Box is selected, the **Rename** command under the PGP Desktop Edit menu lets you rename a Protected Folder.

To rename a PGP NetShare Protected Folder via the Edit menu:

- 1 Open PGP Desktop and click on the **PGP NetShare** Control Box.
- 2 If you have more than one Protected Folder, click on the name of the Protected Folder you want to rename.
- 3 From the **Edit** menu, select **Rename**.
- 4 Type a new name for the Protected Folder.
- 5 Press **Enter** or click outside the Protected Folder name.

The Protected Folder is renamed.

The **Show File in Explorer...** option in the Edit menu is equivalent to clicking a Protected Folder's path. Choosing this option opens a selected folder in Windows Explorer.

The NetShare Menu

You can select the following commands from the NetShare menu when the PGP NetShare Control Box is selected:

- **Add Folder:** Select the **Add Folder** command to create a new Protected Folder. The process is the same as described in [“Creating a New PGP NetShare Protected Folder” on page 121](#). You must select the PGP NetShare Control Box for this command to be active.
- **Remove Folder:** Select the **Remove Folder** command to begin the process of taking a Protected Folder and restoring it to its normal, decrypted state. All folders and files that are part of the Protected Folder will be decrypted; the PGP icon overlay on the files will be removed. You must select a Protected Folder for this command to be active.

- **Re-encrypt Folder:** Select the **Re-encrypt Folder** command to re-encrypt the files in a Protected Folder. Re-encryption changes the underlying key, preventing access to anyone who might have been able to determine the current key. Re-encryption is done automatically when a user is added to or removed from a Protected Folder. The **Re-encrypt Folder** command lets you re-encrypt whenever you want; for example, if you believe an unauthorized person has gained access to the files in the Protected Folder. You must select a Protected Folder for this command to be active.
- **Check Folder Status:** Select the **Check Folder Status** command to get up-to-date information about the status of the selected Protected Folder. You must select a Protected Folder for this command to be active.
- **Clear Recent Folder:** Select the **Clear Recent Folder** command to remove it from the list of Protected Folders. Unlike the **Remove Folder** command, however, this command does not decrypt the files in the Protected Folder. You must select a Protected Folder for this command to be active.

9

PGP Zip

Creating encrypted and compressed archives

You can use PGP Zip and the PGP Zip Assistant features of PGP Desktop to create, open, and edit encrypted and compressed packages. This section includes the following topics:

- [“About PGP Zip”](#)
- [“Creating PGP Zip Archives” on page 148](#)
- [“Opening a PGP Zip SDA” on page 167](#)
- [“Verifying Signed PGP Zip Archives” on page 168](#)
- [“Opening and Editing a PGP Zip Archive” on page 169](#)

About PGP Zip

A PGP Zip Archive package is a single file that is encrypted and compressed for convenient transport or backup. These archive files can hold any combination of files and/or folders, and are especially convenient for secure transport or backup.

The PGP Zip Assistant is a feature within PGP Desktop that helps you create new PGP Zip Archive packages. The Assistant guides you through the process of selecting the files and/or folders for your archive, then it helps you select the best way of creating your archive file:

- Encrypting and packaging your files and/or folders using the PGP keys of one or more recipients (they must have PGP Desktop on their computers);
- Encrypting and packaging your files and/or folders using a passphrase (recipients must have PGP Desktop on their computers);
- Encrypting and packaging your files and/or folders into a self-decrypting archive (PGP Zip SDA) that is protected by a passphrase (recipients do not need PGP Desktop, but their computer must be running Microsoft Windows);
- No encryption, no packaging, but a file is created that you can send to your recipients to verify that you are the person who sent the file.

When you are using the PGP Zip Assistant to create a PGP Zip Archive file, you have the option of automatically sending the original files to the PGP Shredder, so they can be removed securely and permanently from your computer.

When you receive a PGP Zip Archive file, you can edit it in just about every way. You can:

- Extract all of the files and/or folders in the archive.
- Extract only some of the files and/or folders in the archive.
- Add new files and/or folders to the archive.
- Extract some files and/or folders in the archive while adding others.

- Edit the archive by:
 - Changing the type of encryption.
 - Changing the signing key.
 - Changing the recipients.

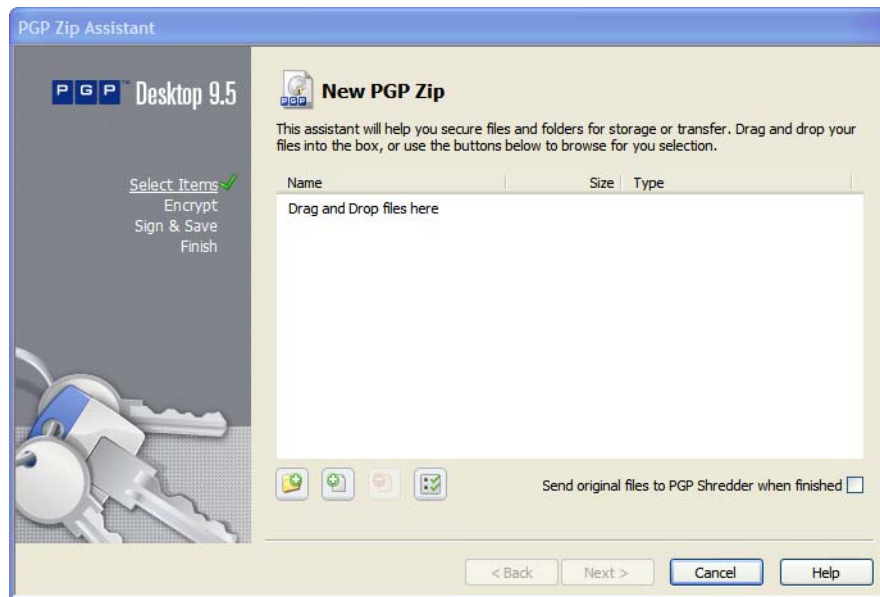
PGP Zip archives are encrypted to the preferred cipher for your copy of PGP Desktop (if configured by a PGP administrator) or to AES256.




Creating PGP Zip Archives


To create a PGP Zip archive:

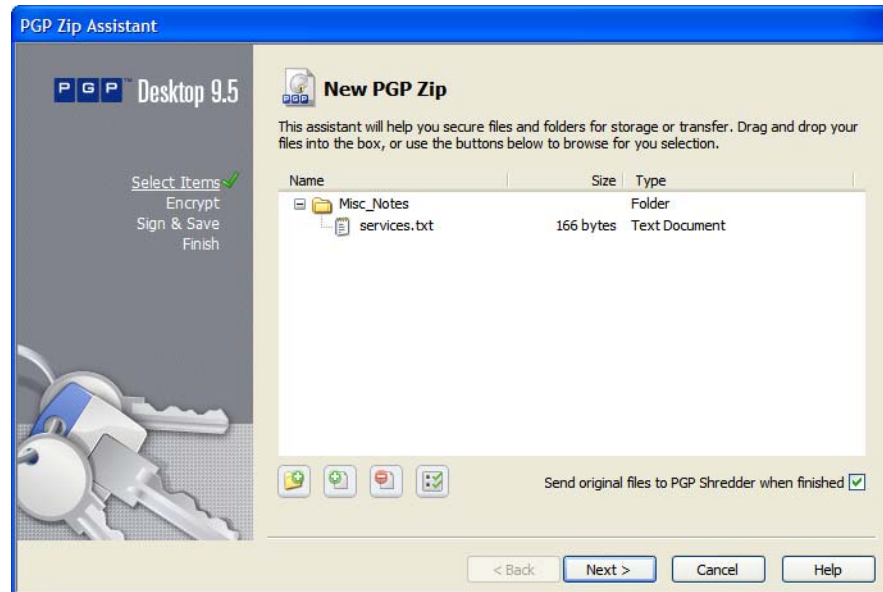
- 1 On the PGP Desktop Toolbar, click **New PGP Zip** (you can also click New PGP Zip on the PGP Zip Control box).




To cancel the creation of a new PGP Zip archive, click **Cancel**.




- 2 Click:
 - **Add directory**  to add an entire directory to the PGP Zip archive you are creating.
 - **Add files**  to add a file to the PGP Zip archive you are creating.
 - **Remove selected files**  to remove a file or directory from the PGP Zip archive you are creating.


- **PGP Zip advanced options**  to select additional options for the PGP Zip file that you are creating. The default settings are fine for most users.

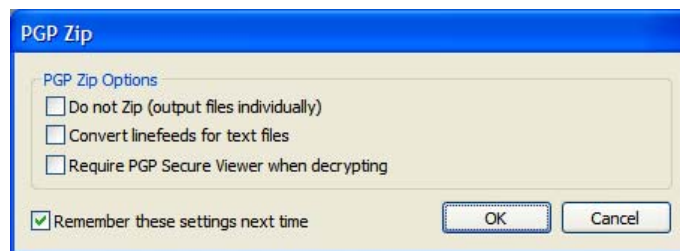


-  To add a combination of files and folders, use a combination of the  and the  buttons. When you add a directory to the file list, the PGP Zip Assistant displays all files separately, making it easy to see all of them. If you need to add many files to your Zip Archive, you might save time if you add an entire directory to the Zip Archive file list first, then remove the files that you do not want included. **If you do this, before proceeding, make sure that you have completely removed any files that are not intended for the Zip Archive.**

- 3 If you want to securely delete the original files once the PGP Zip Archive is created, select **Send original files to PGP Shredder when finished**.

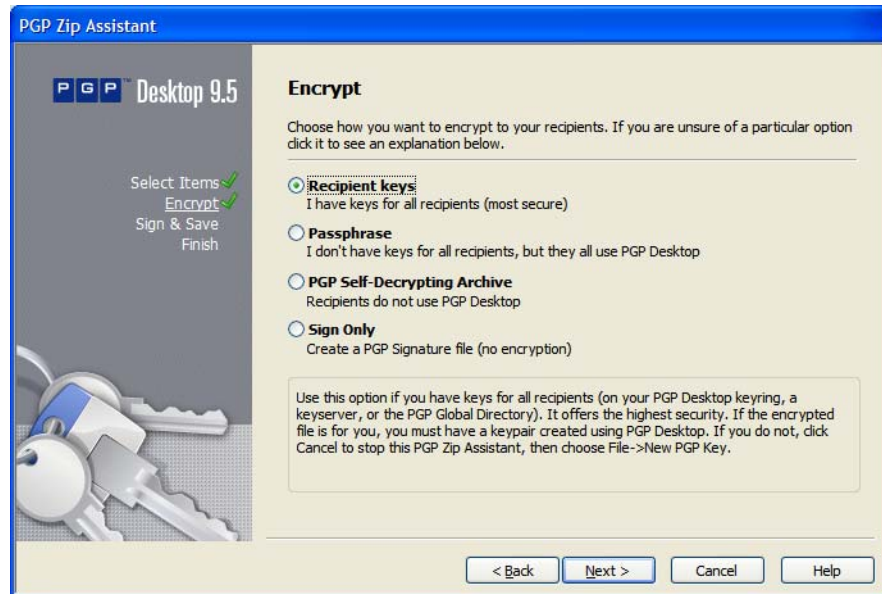
-  If you choose to send the original files to PGP Shredder once the PGP Zip Archive is created, you cannot retrieve your files later—not even with a file recovery utility. Your files are permanently and irrecoverably deleted. Use care when selecting this option.

- 4 Click **PGP Zip advanced options**  if you want special PGP Zip options:
 - a Select **Do not Zip (output files individually)** if you want separate encrypted files rather than one PGP Zip Archive package that contains all files in a single encrypted file.
 - b Select **Convert linefeeds for text files** if you are creating zip archives of only text files.
 - c Select **Require PGP Secure Viewer when decrypting** if your organization's security policies call for that requirement. If you have selected this mode, when the file is decrypted it is displayed in a PGP Secure Viewer window. Using this option protects against outdated radiation capturing attacks.
 - d Select the checkbox for **Remember these settings next time** if you want to use these advanced options settings again.
 - e Click **OK** when you are done selecting special options. Click **Cancel** if you choose not to change any of these options.



The New PGP Zip screen displays once again.

- 5 When you have finished selecting files for your PGP Zip Archive, click **Next**.
- 6 Select the desired type of encryption. (You can move your mouse over each choice to see more details in the information box below the option list):



- **Recipient keys.** Creates a PGP Zip Archive by encrypting the files to the public keys of the recipient(s), ensuring that only those recipients can use PGP Desktop to open the archive. This is the most secure option. See [“Encrypting to Recipient Keys” on page 151](#).
- **Passphrase.** Creates a PGP Zip Archive by encrypting the files with a passphrase you specify when saving the archive. Only those persons who know the passphrase, and who are using PGP Desktop, can open the archive. See [“Encrypting with a Passphrase” on page 156](#).

i If you are using PGP Desktop in a PGP Universal-managed environment, passphrase (conventional) encryption may be disabled.

- **PGP Self-Decrypting Archive.** Creates a PGP Self-Decrypting Archive with a passphrase you specify when saving the archive. PGP Desktop is not required when decrypting a PGP Self-Decrypting Archive—**but recipients must be using a computer running the Microsoft Windows operating system**. See [“Creating a PGP Self-Decrypting Archive \(SDA\)” on page 161](#).
- **Sign Only.** Adds your PGP signature to an unencrypted zip file. Your recipient(s) can then open the zip archive using PGP Desktop, and the included signature verifies that the zip archive came from you and has not been modified in transit. For more information, see [“Sign Only” on page 165](#).

Encrypting to Recipient Keys

The **Recipient keys** option:

- Offers the highest possible security for your files.
- Requires that each of your recipients have PGP Desktop installed on their computers (Windows or Mac OS X).

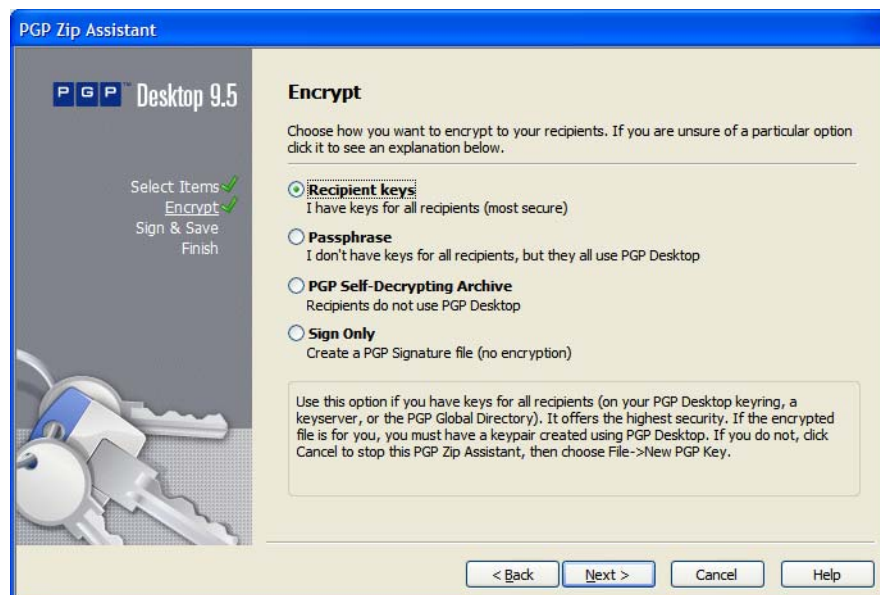
- Requires that you have a public key for each recipient (from your Keyring or a PGP Keyserver).
- Does not require you to reveal a passphrase to file recipients.

Encrypting your PGP Zip Archive by using the public keys of all of your recipients is the most secure option, and should be the first choice if you need top security and have the necessary requirements available.

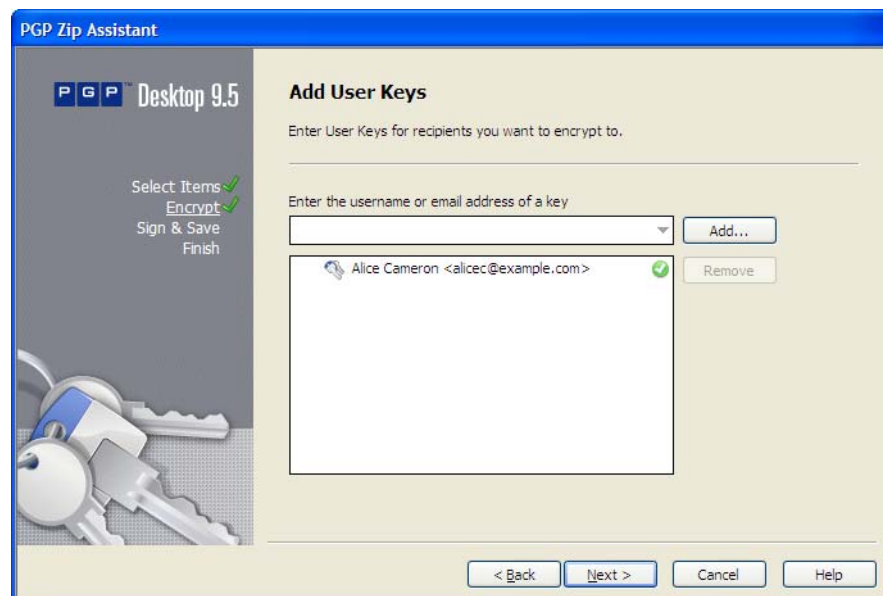
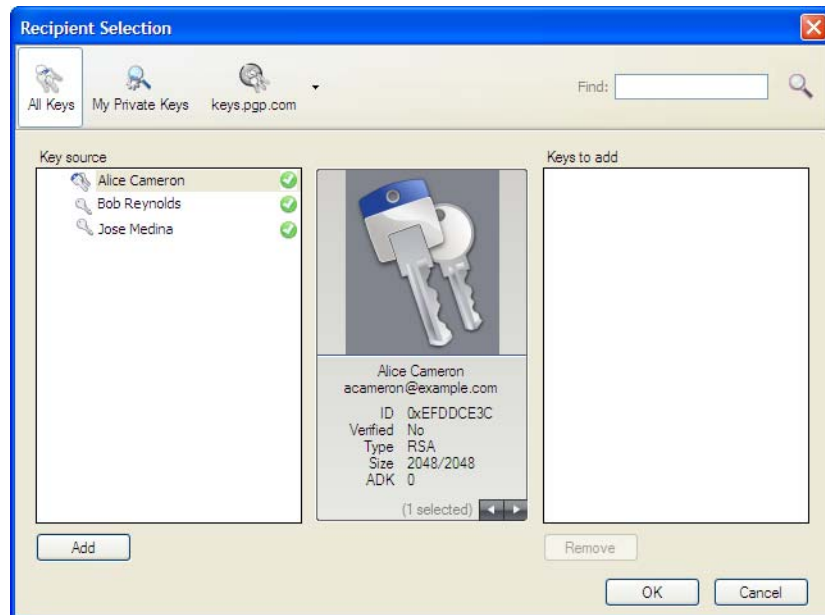
Once your files are secured, you send the resulting PGP Zip Archive file to your recipients however you choose. Your recipients then use PGP Desktop to open the PGP Zip Archive file. Anyone whose key you included when you encrypted the file can open the resulting PGP Zip Archive file, and everyone sees the same items. If you need to have some recipients only see some items, you must create separate PGP Zip Archive files for each.

To encrypt to recipient keys:

- 1 If you haven't already, begin the process of creating a PGP Zip Archive as described in ["Creating PGP Zip Archives" on page 148](#).
- 2 In the Encrypt window, click **Recipient keys**.



- 3 Click **Next**. The **Add Users** window appears.



- 4 Select the recipients of your PGP Zip Archive. Click the drop-down menu and select from the list of keys that are on your keyring.
- 5 If there are any recipients you would like to remove, click to select their names, then click **Remove**.
- 6 If you would like to send the file to a recipient not listed in the drop-down list, click **Add**.

The Recipient Selection dialog box appears.

- 7 From the **Key Source** panel on the left, click to select the key(s) you would like to use. You can select a range of names by Shift-clicking, or you can select discontinuous names by Ctrl-clicking.



To select keys, you can also drag 'n drop keys from the **Key Source** panel, or double-click keys in the **Key Source** panel.

When the names are selected, click **Add** to move the key to the **Keys to add** panel on the right. You can also drag-and-drop them with your mouse.

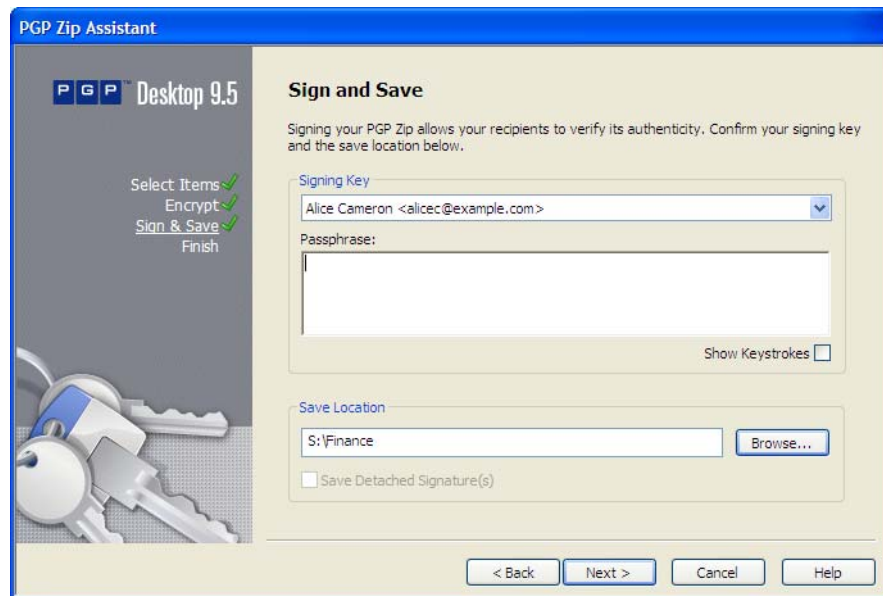
- 8 If a key is not available, you can search for it. Do either or both of these until you find the keys you want:
 - Narrow down the available keys from those PGP Desktop is managing for you in PGP Keys, by clicking **All keys** or **My private Keys**, depending on which contains the key you want. You can type all or part of the name or email address that you would like to find in the Find box on the right, and then press **Enter** to filter the results.
 - Find keys that you do not have available by clicking PGP Global Directory. Type all or part of the name or email address that you would like to find in the **Search** box on the right, and then press **Enter** or click the magnifying glass icon.

As you type, the results of your search appear in **Results** in the panel on the left.

- 9 Click to select one or more of the found names, then click **Add** to move the names to the **Keys to add** panel on the right. You can remove the names from the **Keys to add** panel by clicking to select them, then clicking **Remove**.
- 10 When you are finished selecting additional names, click **OK** to return to the **Add User Keys** panel.

The keys that you have found are already in the list of file recipients. If you would like to remove any of them, click to select them and click **Remove**.

- 11 Click **Next**. If you chose to encrypt to **Recipient's Keys** or **Sign Only**, the **Sign and Save** window appears.



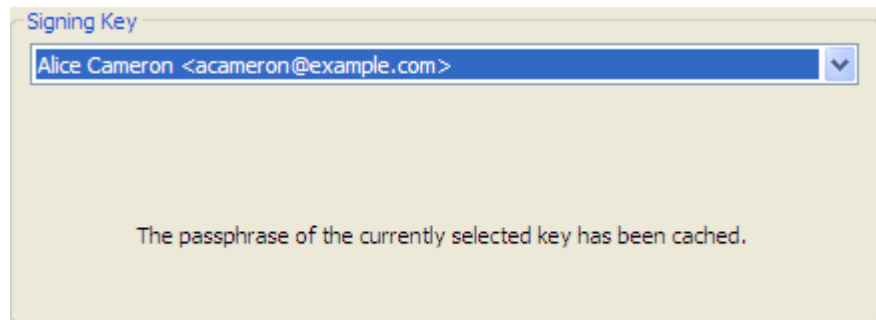
- 12** If desired, specify a private key on your keyring as a Signing Key for the PGP Zip archive being created.

This specified Signing Key is used to digitally sign the PGP Zip archive. The recipient(s) will be able to verify who the archive is from by verifying the digital signature using the corresponding public key.

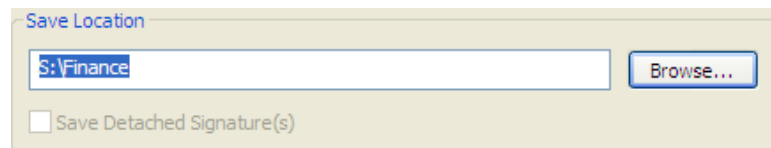
- a** If you do not need to sign the file, or prefer not to, choose **None** from the Signing Key drop-down list.
- b** If you choose to sign your PGP Zip Archive, choose your key from the Signing Key drop-down menu, and then enter the passphrase of the key selected for signing (not the passphrase used to secure the zip). To see keystrokes as you type the passphrase, select the checkbox for **Show Keystrokes**.



If you have already typed your passphrase during this session using PGP Desktop, your passphrase might be cached, depending on your **Options** settings. You see a message stating that the passphrase is cached, if this is the case. Even if your passphrase is cached, you can still choose not to sign the PGP Zip Archive file.



- 13 Confirm that the PGP Zip Archive is being saved in the location that you prefer. You can:
 - a Click **Browse** and choose a location from the Windows File dialog
 - b Manually type the location where you would like to save the PGP Zip Archive
 - c Accept the file save location as it currently appears.




- 14 If you chose the **Sign Only** option, click to select **Save Detached Signatures**.
- 15 Click **Next**. The PGP Zip Archive is created.
- 16 Click **Finish**. Your PGP Zip Archive is ready to be sent to the recipients whose keys you encrypted it to. If your key was one of the keys you used for encryption, the file is ready for storage wherever you wish.

Encrypting with a Passphrase

The **Passphrase** option:

- Can be potentially less secure than encrypting with recipients' keys (although still highly secure).
- Requires that your recipients have PGP Desktop software installed on their computers (Windows or Mac OS X).
- Requires that you reveal the passphrase to your recipients.
- Does not require you to have any of your recipients' public keys.

 Encrypting with a passphrase is also referred to as *conventional encryption*.

Encrypting your PGP Zip Archive with a passphrase can be extremely secure, especially with a strong passphrase. However, encrypting to recipient keys does offer even higher security. When you encrypt to your recipients' keys, those who possess the PGP Zip Archive need both their private keys and passphrases to decrypt the file (and each recipient's private key has its own passphrase).

When encrypting with a passphrase, everyone opens the file using the same passphrase, and no private keys required. Anyone who possesses the file, uses PGP Desktop, and knows the passphrase can decrypt the file.



Take every possible precaution to ensure that the passphrase to your PGP Zip Archive is revealed to no one but the file recipients. If the passphrase is revealed to unauthorized persons, you can create a new PGP Zip Archive with a different passphrase, but you can do nothing to re-secure the original archive file and whatever it contains.

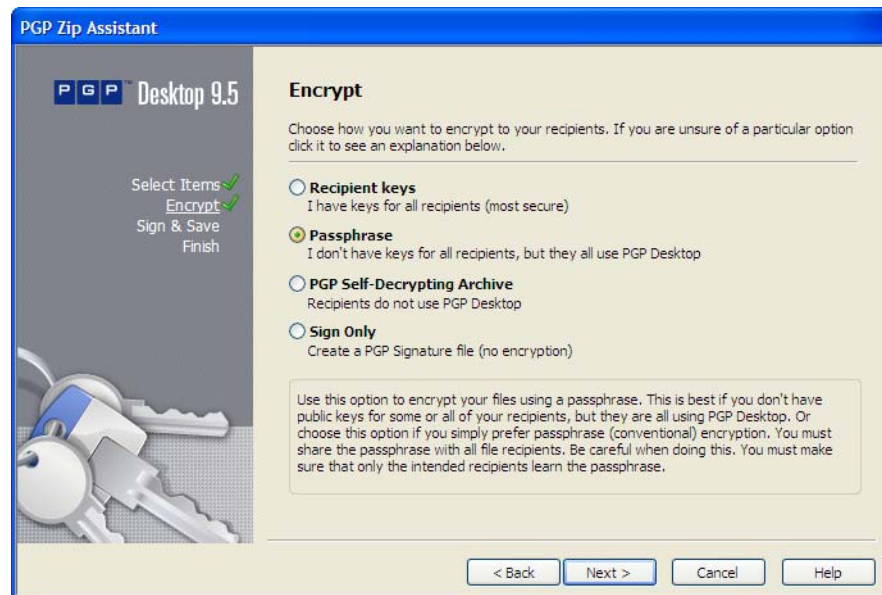
Once your files are secured, you send the resulting PGP Zip Archive file to your recipients however you choose. Your recipients then use PGP Desktop to open the PGP Zip Archive file. *Anyone who has the file and the passphrase can open the resulting PGP Zip Archive file*, and everyone sees the same items. If you need to have different recipients see different items, you must create separate PGP Zip Archive files for each.



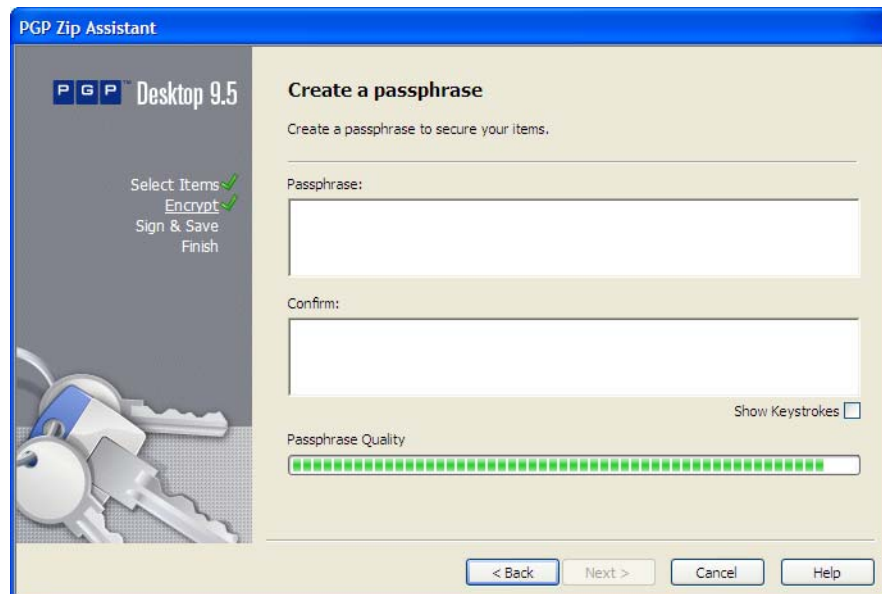
If you are using PGP Desktop in a PGP Universal-managed environment, encrypting with a passphrase may be disabled.

To encrypt using a passphrase:


- 1 If you haven't already, begin the process of creating a PGP Zip Archive as described in ["Creating PGP Zip Archives" on page 148](#). Follow the instructions to Step 6 Once that is completed, return to this section.
- 2 In the Encrypt window, click **Passphrase**.



- 3 Click **Next**. The **Create a passphrase** window appears.




- 4 If you would like your password to be visible to you as you type it, click to select **Show Keystrokes**.

 PGP Desktop is designed to offer the maximum possible security. A fundamental part of high security is preventing anyone else from learning your passphrase. For this reason, PGP Desktop is designed by default to hide your passphrase completely—it does not even show dots to represent characters as you type. Displaying dots as you type reveals the number of characters in your passphrase, useful information for breaking a passphrase via computer. Ultra-secure environments require invisible passphrase typing because it is possible to detect monitor images remotely by intercepting radio-frequency signals.

- 5 In the **Passphrase** box, type the passphrase that you would like to use.

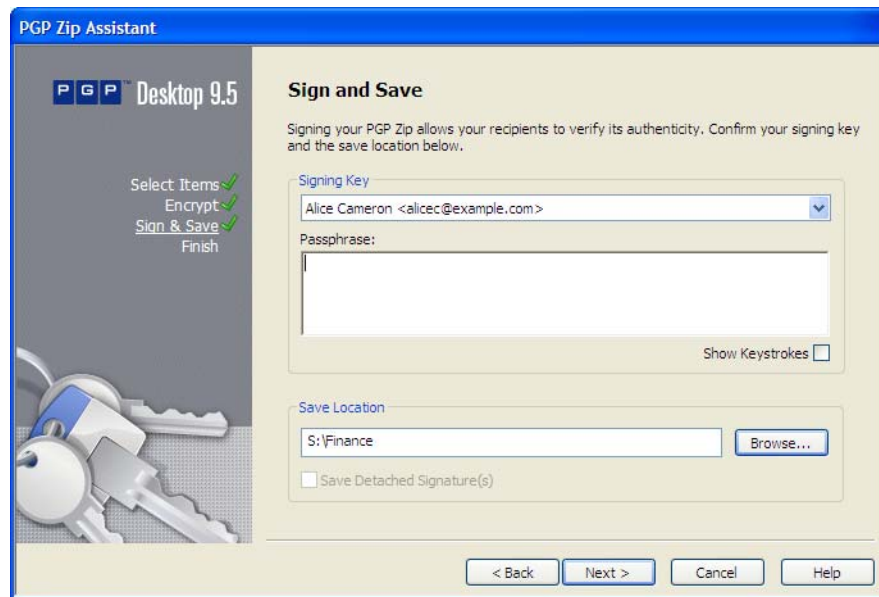
The stronger your passphrase is, the more secure your files are. The **Passphrase Quality** bar indicates passphrase strength by comparing the amount of entropy in your passphrase against a true 128-bit random string (the same amount of entropy in an AES128 key). You can fill the Passphrase Quality bar by:

- a Typing a longer rather than a shorter passphrase
- b Avoiding words found in the dictionary
- c Using mixed-case in a non-standard way (“dKmPgp” instead of “dkmPGP”)
- d Including numerals in your passphrase
- e Including symbols in your passphrase
- f Including spaces in your passphrase

 While you do not have to entirely fill the bar to generate a high-quality passphrase, filling the Passphrase Quality bar gives you a passphrase so strong that it could take literally *billions* of years to break. Refer to [“The Passphrase Quality Bar” on page 250](#) for more information.

- 6 Type your passphrase again in the **Confirm** box to make sure there are no typographical errors.
- 7 Click **Next**.

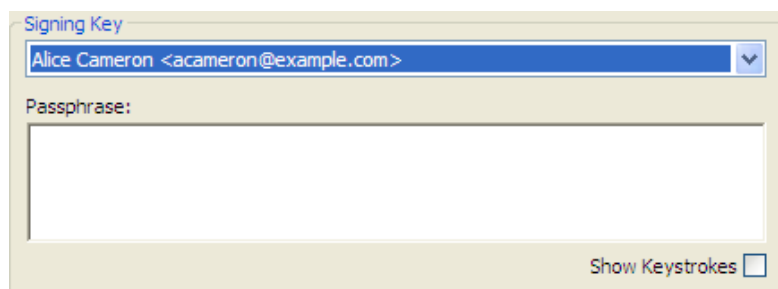
The **Sign and Save** panel appears.



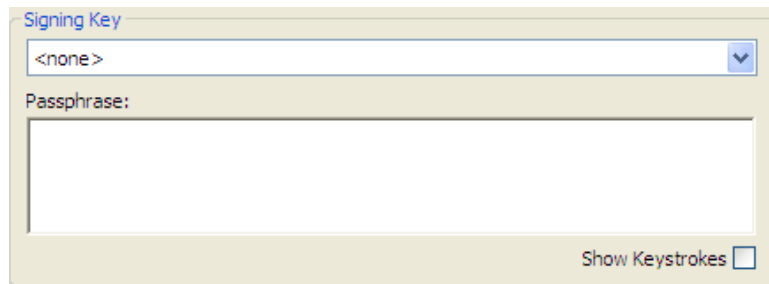
- 8** If desired, specify a *private* key on your keyring as a Signing Key for the PGP Zip archive being created.

This specified Signing Key is used to digitally sign the PGP Zip archive. The recipient(s) will be able to verify who the archive is from by verifying the digital signature using the corresponding public key.

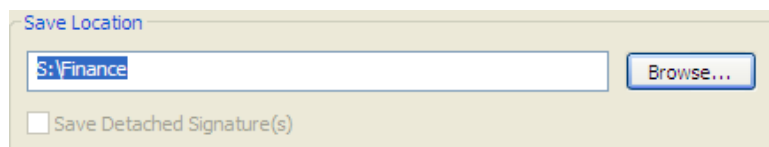
- a** If you do not need to sign the file, or prefer not to, choose **None** from the Signing Key drop-down list.
- b** If you choose to sign your passphrase-encrypted PGP Zip Archive, choose your key from the drop-down menu, then type your passphrase in the box.



- c** If you choose not to sign your passphrase-encrypted PGP Zip Archive, select **None** from the drop-down menu.



- i** If you have already typed your passphrase during this session using PGP Desktop, your passphrase might be cached, depending on your Options settings. You see a message stating that the passphrase is cached, if this is the case. Even if your passphrase is cached, you can still choose not to sign the PGP Zip Archive file.
- 9** Confirm that the PGP Zip Archive is being saved in the location—and with the filename—that you prefer. You can:
- change where the file is saved by clicking Browse and choosing a location from the Windows File dialog;
 - change where the file is saved by manually typing the location where you would like to save the PGP Zip Archive;
 - change the PGP Zip Archive filename by manually typing it at the end of the file location text string.



- 10** Click **Next**. The PGP Zip Archive is created.
- 11** Click **Finish**.

- i** The default filename for a PGP Zip Archive containing a single file, directory, or drive is the name of that item with **.pgp** appended. If the PGP Zip Archive contains more than one item, its filename is one of the items with **.pgp** appended. You can change the PGP Zip Archive filename in Step 9.

Creating a PGP Self-Decrypting Archive (SDA)

The **PGP Self-Decrypting Archive** option:

- Potentially less secure than encrypting with recipients' keys (although still highly secure).
- Requires that your recipients are using Windows computers.

- Requires that you reveal the passphrase to your recipients.
- Does not require that your recipients have PGP Desktop software installed on their computers.
- Does not require you to have any of your recipients' public keys.

A PGP Self-Decrypting Archive (SDA) is a PGP Zip Archive that can be opened on any Windows computer, even those that do not have PGP Desktop installed. SDA files are standard Windows executable (.exe) files that you can open simply by double-clicking them.

SDA files are slightly larger than regular PGP Zip Archives because the SDA self-decrypting "mechanism" requires a certain amount of extra space (usually about 100 K).



If you are using PGP Desktop in a PGP Universal-managed environment, SDA creation may be disabled.

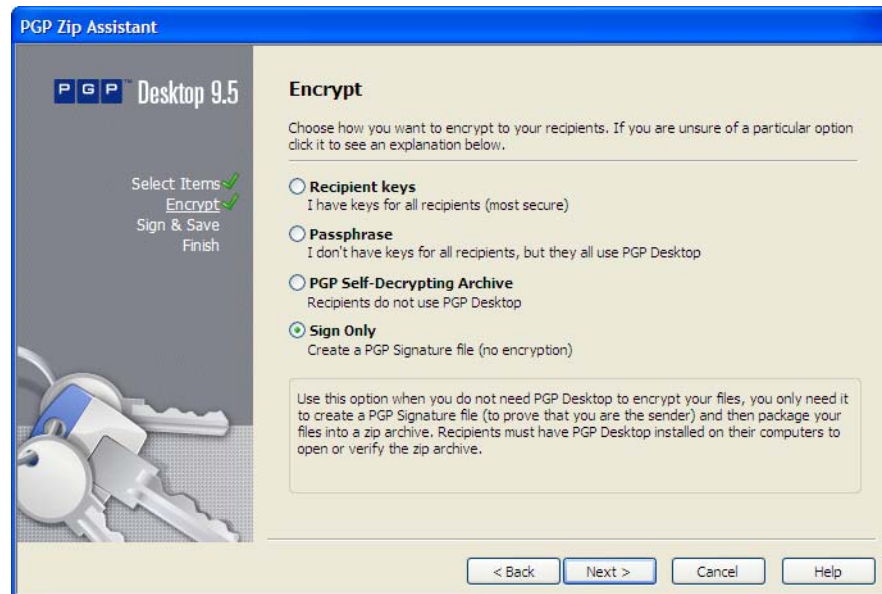
Once you have created your PGP Zip SDA, you can send it to your recipients however you choose. *Anyone who has the file and the passphrase can open the resulting PGP Zip Archive file*, and everyone sees the same items. If you need to have different recipients see different items, you must create separate PGP Zip Archive files for each.



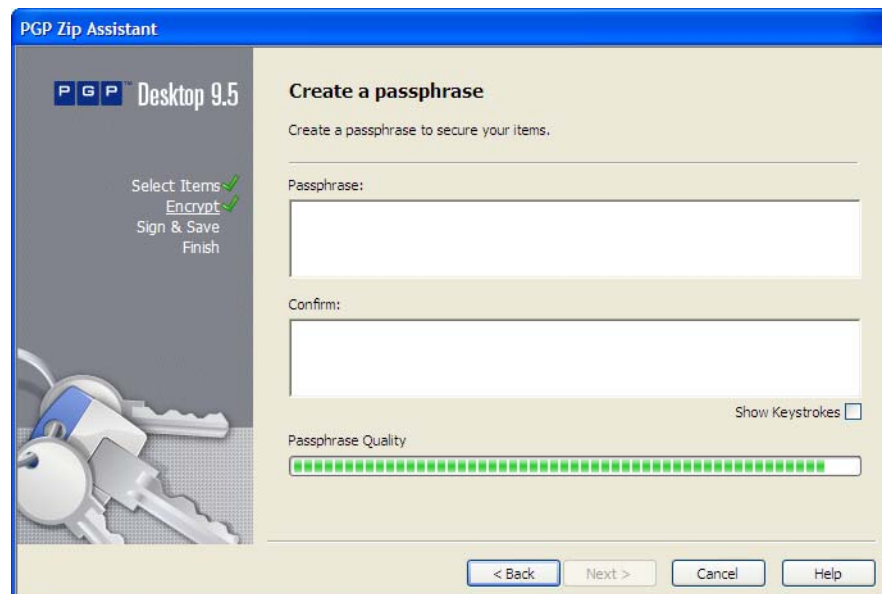
Take every possible precaution to ensure that the passphrase to your PGP Zip SDA is revealed to no one but the file recipients. If the passphrase is revealed to unauthorized persons, you can create a new PGP Zip SDA with a different passphrase, but you can do nothing to re-secure the original archive file and whatever it contains.

To create a PGP Zip SDA:


- 1 If you haven't already, begin the process of creating a PGP Zip Archive as described in ["Creating PGP Zip Archives" on page 148](#). Follow the instructions to Step 6 Once that is completed, return to this section.
- 2 In the Encrypt window, click **PGP Self-Decrypting Archive**.



- 3 Click **Next**. The **Create a passphrase** window appears.




- 4 If you would like your password to be visible to you as you type it, click to select **Show Keystrokes**.

 PGP Desktop is designed to offer the maximum possible security. A fundamental part of high security is preventing anyone else from learning your passphrase. For this reason, PGP Desktop is designed by default to hide your passphrase completely—it does not even show dots to represent characters as you type. Displaying dots as you type reveals the number of characters in your passphrase, useful information for breaking a passphrase via computer. Ultra-secure environments require invisible passphrase typing because it is possible to detect monitor images remotely by intercepting radio-frequency signals.

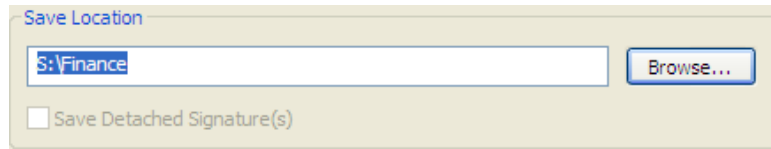
- 5** In the **Passphrase** box, type the passphrase that you would like to use.

The stronger your passphrase is, the more secure your files are. The **Passphrase Quality** bar indicates passphrase strength by comparing the amount of entropy in your passphrase against a true 128-bit random string (the same amount of entropy in an AES128 key). You can fill the Passphrase Quality bar by:

- a** Typing a longer rather than a shorter passphrase
- b** Avoiding words found in the dictionary
- c** Using mixed-case in a non-standard way (“dKmPgp” instead of “dkmPGP”)
- d** Including numerals in your passphrase
- e** Including symbols in your passphrase
- f** Including spaces in your passphrase

 While you do not have to entirely fill the bar to generate a high-quality passphrase, filling the Passphrase Quality bar gives you a passphrase so strong that it could take literally *billions* of years to break. Refer to [“The Passphrase Quality Bar” on page 250](#) for more information.

- 6** Type your passphrase again in the **Confirm** box to make sure there are no typographical errors.
- 7** Click **Next**.
- 8** Confirm that the PGP Zip SDA is being saved in the location—and with the filename—that you prefer. You can do any of the following:
- Change where the file is saved by clicking Browse and choosing a location from the Windows File dialog;
 - Change where the file is saved by manually typing the location where you would like to save the PGP Zip SDA;
 - Change the PGP Zip SDA filename by manually typing it at the end of the file location text string.



9 Click **Next**. The PGP Zip SDA is created.

10 Click **Finish**.

i The default filename for a PGP Zip SDA containing a single file, directory, or drive is the name of that item with **.exe** appended. If the PGP Zip SDA contains more than one item, its filename is one of the items with **.exe** appended. You can change the PGP Zip SDA filename in Step 8.

Sign Only

The **Sign Only** option:

- DOES NOT ENCRYPT your files, and thus requires no passphrase to reveal to recipients.
- Processes each file individually and makes a separate detached sig for every file.
- Is used to generate a signature file that your recipients can use to confirm the PGP Zip Archive came from you.
- Requires that your recipients have PGP Desktop software installed on their computers (Windows or Mac OS X).
- Does not require you to have any of your recipients' public keys.

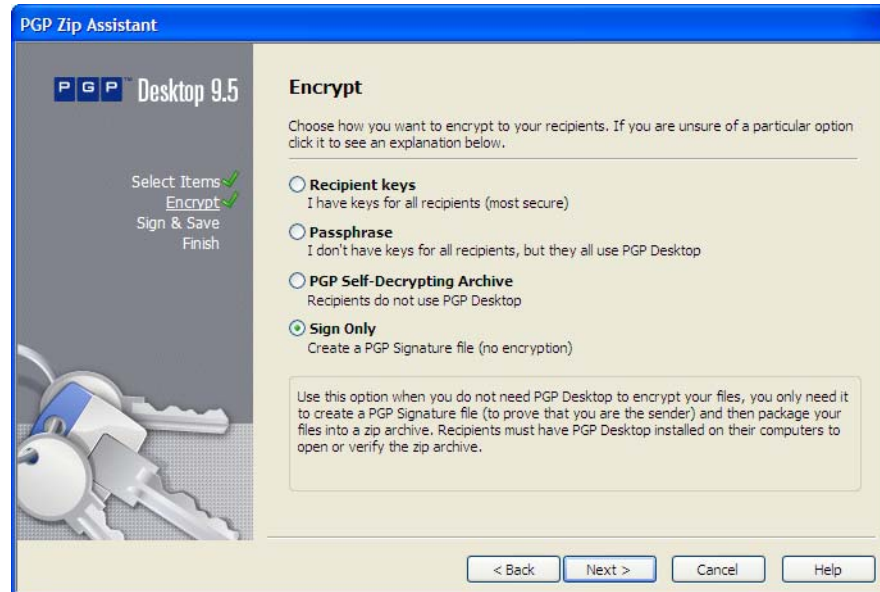
For times when you do not need to encrypt file(s) for your recipients, you can choose the Sign Only option. Instead of encrypting your files and zipping them into one PGP Zip Archive, this option zips them only.

To encrypt using the Sign Only option:

1 If you haven't already, begin the process of creating a PGP Zip Archive as described in ["Creating PGP Zip Archives" on page 148](#). Follow the instructions to Step 6. Once that is completed, return to this section.

i When you are selecting the files to be zipped and signed, the **Send original files to PGP Shredder** option is ignored, even if you select it.

2 In the Encrypt window, click **Sign Only**.



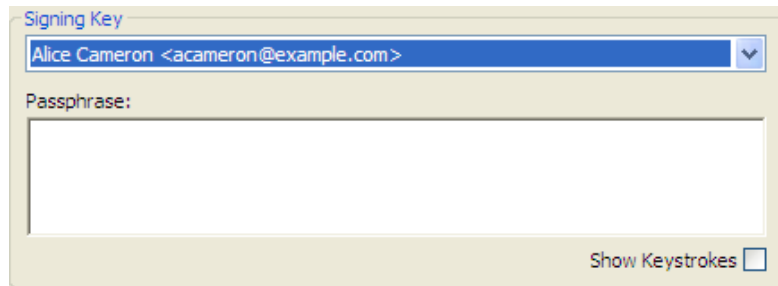
- 3 Click **Next**. The **Sign and Save** panel appears.



- 4 Specify a *private* key on your keyring as a Signing Key for the PGP Zip archive being created.

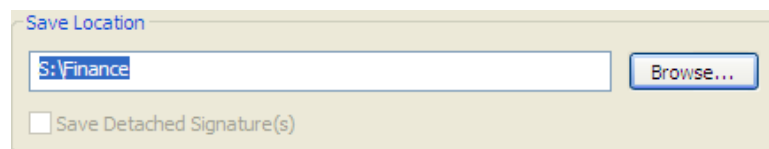
This specified Signing Key is used to digitally sign the PGP Zip archive. The recipient(s) will be able to verify who the archive is from by verifying the digital signature using the corresponding public key.

Choose your key from the drop-down menu, then type your passphrase in the box.



i If you have already typed your passphrase during this session using PGP Desktop, your passphrase might be cached, depending on your Options settings. You see a message stating that the passphrase is cached, if this is the case.

- 5 Confirm that the PGP Zip Archive is being saved in the location that you prefer. You can do any of the following:
 - Click **Browse** and choose a location from the Windows File dialog
 - Manually type the location where you would like to save the PGP Zip Archive
 - Accept the file save location as it currently appears.



- 6 If you would prefer to have a separate signature file, along with your PGP Zip Archive, click to select **Save Detached Signatures**.
- 7 Click **Next**. The PGP Zip Archive is created.
Click **Finish**.

Opening a PGP Zip SDA

To open a PGP Zip SDA:

- 1 Double click the SDA file. (It should have an extension of **.exe**.)
The **PGP Self Decrypting Archive - Enter Passphrase** screen displays.
- 2 Confirm that the output is going into the desired location. If not, click **Browse** to correct the location, or type it in the field manually.

- i** If you direct the decrypted files from the PGP Zip SDA into the same location from which they originally came, the original files are overwritten. To prevent this, for each file, you are prompted to select a different location. You can also type a different filename. If you click **Save** without doing this, a warning dialog box displays. If you bypass it, the file from the PGP Zip SDA overwrites the original.
- 3** Type the passphrase for the PGP Zip SDA, then click **OK**.
The SDA decrypts.

Verifying Signed PGP Zip Archives

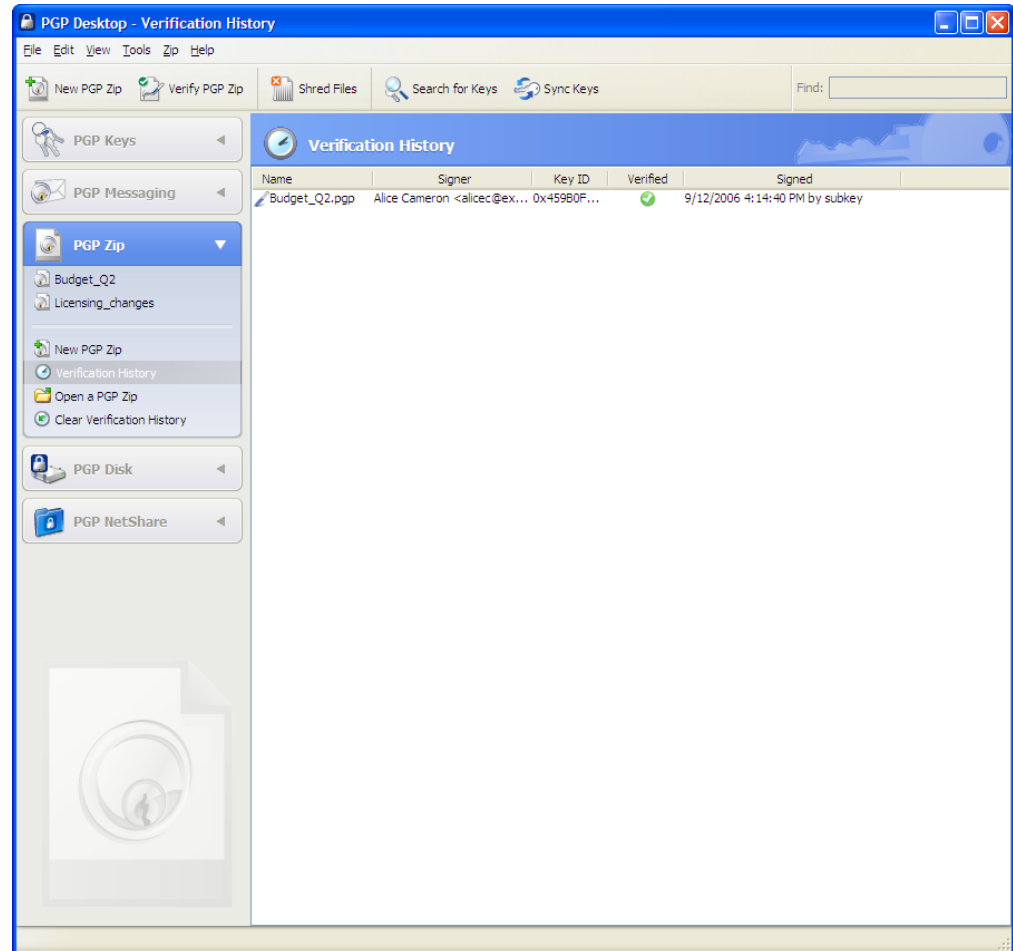
If you received a signed PGP Zip Archive, you should verify the signature so that you know who it came from—and that the archive was not tampered with before you got it.

To verify a PGP Zip Archive:

- 1** In PGP Desktop, click **Verify PGP Zip** on the PGP Desktop Toolbar.
The **Open** dialog appears.
- 2** Navigate to the signed .pgp file you want to verify, click to select it, then click **Open**.
If the message was encrypted (in addition to being signed), you are prompted for the passphrase of your private key, or whichever private key it is that corresponds to the public key to which the message was encrypted.
If the private key is not on your keyring, PGP Desktop will tell you it is not possible to decrypt the message. Unfortunately, this also means you cannot verify the archive. Click **Cancel** to end the verification.
- 3** Type the passphrase of the private key, then click **OK**.

- i** If the passphrase of the private key is cached, then you are not prompted for the passphrase.

The contents of the archive are saved to the same location as the PGP Zip archive, and the Verification History screen shows the information about the archive you are verifying.



- 4 To clear the list of verified archives, click **Clear Verification History**.
All listings on the Verification History screen are removed.

Opening and Editing a PGP Zip Archive

PGP Zip Archives are not static. At any time, you can:

- Extract files from them.
- Add files to them.
- Edit the settings of the archive itself.

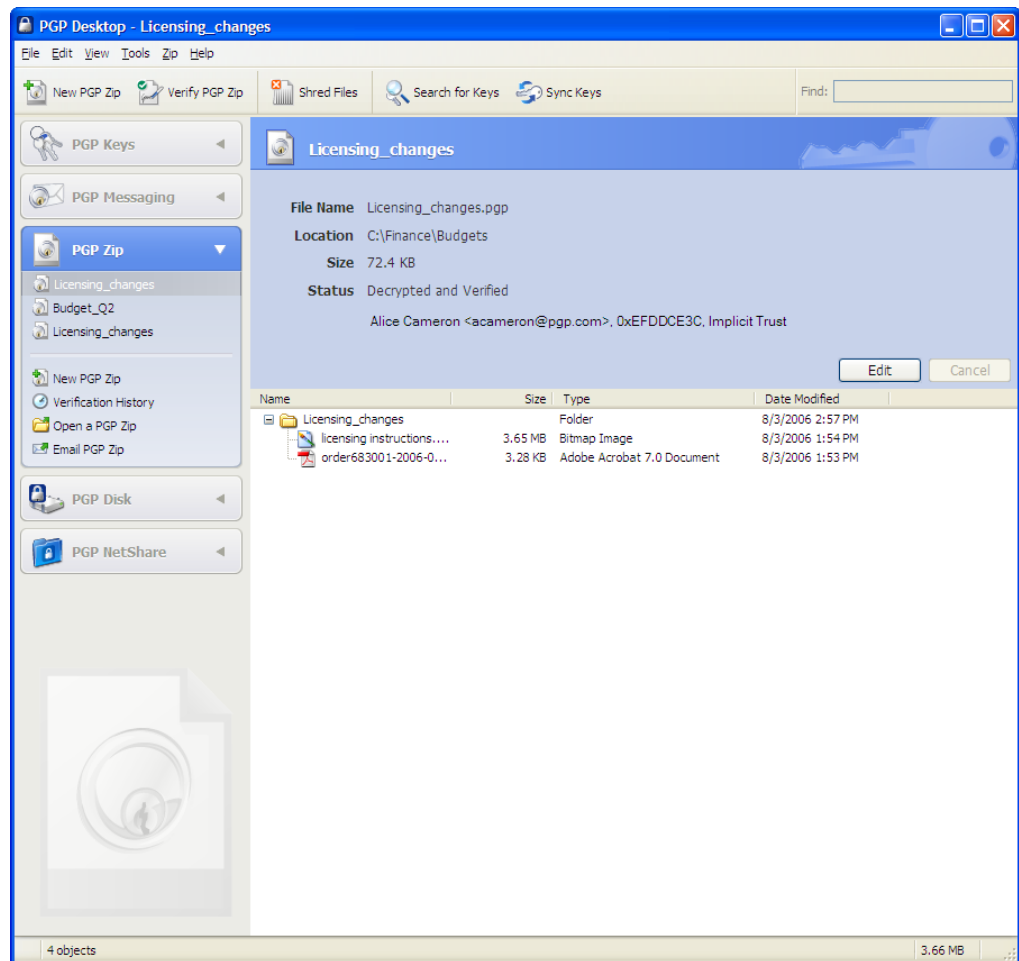
To open and edit a PGP Zip archive:

- 1 In PGP Desktop, click the PGP Zip Control box.
The PGP Zip Control box highlights.

- 2 Click the name of the PGP Zip archive you would like to open and/or edit in the list of PGP Zip archives at the top of the PGP Zip Control box.

(If the PGP Zip archive you want to open is not listed, click **Open a PGP Zip**, navigate to the .pgp file, select it, then click **Open**.)

The settings for the archive and the files and/or folders in the archive appear.



- 3 To edit the settings of the PGP Zip archive, click **Edit**, make the desired changes, then click **Save**. You can either overwrite the PGP Zip archive to which you made the changes or save the modified archive using a different name.
- 4 Edit a PGP Zip Archive this way:
 - a **To add a file to a PGP Zip archive**, click **Add Files** in the PGP Zip Control box, select the file or files you want to add, then click **Open**.

The files are added to the archive.

- b To add a folder in the archive and put files into that folder**, click **New Folder**, type a descriptive name for the new folder (if desired), click on the new folder to select it, click **Add Files** in the PGP Zip Control box, select the file or files you want to add to the folder, then click **Open**.

The files are added to the archive in the folder.

- c To extract a file from an archive**, right click the file you want to extract, select **Extract** from the context menu that appears, specify a location for the file, then click **OK**.

A copy of the file is created in the specified location; the original remains in the PGP Zip Archive.

- d To delete a file or folder from an archive**, select the items you want to delete, then press the **Delete** key on your keyboard. You can also select **Edit > Delete**.

The specified items are deleted.

- e To save changes to a PGP Zip archive that you have modified**, click the **Save** button in the upper right corner or **Save PGP Zip** in the PGP Zip Control box. Specify a location and a name. If the name you select already exists at the location, you will be asked if you want to overwrite the existing file. Type the passphrase that protects the archive, then click **OK**.

- f To change the signing key**, select the PGP Zip file you want to change in the PGP Zip Control Box, click **Edit**, and then select a new **Signing Key**. Click **Save** when you have finished.

- g To change the type of encryption** (Key or Conventional), select the PGP Zip file you want to change in the PGP Zip Control Box, click **Edit**, and then select the type of encryption (**Key** or **Conventional**). Click **Save** when you have finished.

- h To add recipients to the PGP Zip archive**, select the PGP Zip file you want to change in the PGP Zip Control Box, click **Edit**, and then click **Add Recipients**. In the Add Recipients dialog box, select the recipients you want to add and click **OK**. Click **Save** when you have finished.

- i To delete recipients from the archive**, select the PGP Zip file you want to change in the PGP Zip Control Box, click **Edit**, select the recipient you want to remove, and click **Delete Recipients**. Click **Save** when you have finished.

10

PGP Keys

Creating and working with PGP keys

This section describes how to create and manage PGP keys. PGP Keys is the feature of PGP Desktop you use to create and maintain your keypair(s) and the public keys of other PGP Desktop users. Topics include:

- [“Viewing Keys” on page 173](#)
- [“Creating a Keypair” on page 174](#)
- [“Protecting Your Private Key” on page 177](#)
- [“Distributing Your Public Key” on page 178](#)
- [“Getting the Public Keys of Others” on page 180](#)
- [“Working with Keyservers” on page 182](#)

Viewing Keys

To view all of the keys on the local keyring, open PGP Desktop and click on the PGP Keys Control box, then click **All Keys**.

The traditional view of PGP keys on a system showed both your private key(s) and the public keys of other PGP Desktop users, which you use to send them protected email.

While PGP Desktop has been improved so that there are many ways to see the keys on your system, the traditional view, called All Keys, is still available.

Behind the scenes, however, PGP Desktop 9.5 now gives you new ways of looking at sets of keys on your system. By default, there are at least three views:

- **All Keys.** Shows all PGP keys on your keyrings.
- **My Private Keys.** Shows only the private keys on your keyrings.
- **Search for Keys.** Lets you search for keys on your keyrings based on criteria you specify.

If you have a smartcard on your system, you also have a view called **Smartcard Keys**.

PGP Desktop 9.5 has also increased the usability of the view of PGP keys on your keyrings by making common functions easily available in the PGP Keys Control box, based on what is showing or selected in the PGP Keys Work area. For example:

- If a public key is selected in any view of the PGP Keys on your keyrings, the option to Email this Recipient appears in the PGP Keys Control box.
- If you perform a search, and you select a public key found in the search that is not on your local keyrings, the option Add to my Keyring appears in the PGP Keys Control box.

(PGP Desktop makes it easy to see the properties of any key being shown in the PGP Keys Work area; just double-click any part of the key listing to display the Properties dialog for that key.)

- When you perform a search, the option Save this KeySearch appears in the PGP Keys Control box, letting you easily save the results for later access.

These are just a few of the usability improvements built in to the PGP Keys Control box and Work area. Be sure to check the PGP Keys Control box for other available options as you work.

Creating a Keypair

You probably already created a PGP keypair for yourself — using the PGP Desktop Setup Assistant or with a previous version of PGP Desktop — but if you haven't, you need to now. Most of the things you do with PGP Desktop require a keypair.

To create a PGP keypair:

- 1 Make sure the PGP Keys Control box is selected.

- 2 From the **File** menu, select **New PGP Key** or press **Ctrl+N**.

The first screen of the PGP Key Generation Assistant appears.

- 3 Read the information on this screen.

- 4 If you want to generate your new PGP keypair on a token or smartcard, make sure the token or smartcard is connected to the system and then select the box labeled **Generate Key on Token: [name of smartcard or token on system]**.

Refer to [Chapter 13, Storing Keys on Smartcards and Tokens](#) for more information about smartcards and tokens.

- 5 Click **Next**.

The Name and Email Assignment screen appears.

- 6 Type your real name in the **Full Name** field and your correct email address in the **Primary Email** field.

It is not absolutely necessary to type your real name or even your email address. However, using your real name makes it easier for others to identify you as the owner of your public key. Also, when you upload your public key to the PGP Global Directory (which makes it easily available to other PGP Desktop users), your real email address is required.

- 7 If you would like to add more email addresses to the key you are creating, click **More** and type them in the fields that appear.

- 8 If you would like to specify advanced settings for the key you are creating, click **Advanced**.

The Advanced Key Settings dialog appears.

- 9 Select settings for the following:
 - **Key type.** Choose between Diffie-Hellman/DSS and RSA.
 - **Generate separate signing subkey.** Select this box if you need a separate subkey for signing. A separate Signing Subkey is created along with the new keypair. You can also create additional signing or encryption subkeys any time after the new key has been created.

Refer to [“Working with Subkeys” on page 196](#) for more information about separate Signing and Encryption Subkeys.
 - **Key size.** Type from 1024 bits to 4096 bits. The larger the key, the more secure it is, but the longer it will take to generate. Some smartcards and tokens limit key size to 1024 bits.
 - **Expiration.** Select **Never** or specify a date on which the keypair you are creating will expire.
 - **Allowed Ciphers.** Deselect any cipher you do not want the keypair you are creating to support.
 - **Preferred Cipher.** Select the cipher you want to be used in those cases where no algorithm is specified. Only a cipher that is allowed can be selected as preferred.
 - **Allowed Hashes.** Deselect any hash you do not want the keypair you are creating to support.
 - **Preferred Hash.** Select the hash you want to be used in those cases where no hash is specified. Only a hash that is allowed can be selected as preferred.

10 Click **OK** to close the **Advanced Key Settings** dialog.

11 Click **Next**.

12 If you are part of a PGP-Universal managed environment, you may see the Organization Settings screen, which displays keys your PGP administrator has configured to add to your copy of PGP Desktop. (Your organization's Additional Decryption Key (ADK) or Organization Key, for example.)

The **Passphrase Assignment** screen appears.

13 Type the passphrase you want to use to maintain exclusive access to the private key of the keypair being created.

14 To confirm your entry, press **Tab** to advance to the Confirmation field, then type the same passphrase again.

For information on the Passphrase Quality Bar, see [“The Passphrase Quality Bar” on page 250](#).



Normally, as an added level of security, the characters you type for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, select the **Show Keystrokes** checkbox.

- 15 Click **Next** to begin the key generation process.

PGP Desktop generates your new keypair.

This process can take several minutes.

- 16 When the key generation process indicates that it is done, click **Next**.

You are prompted to add the public key portion of the key you just created to the PGP Global Directory.

- 17 Read the text on the screen and click **Next** to add your new key to the PGP Global Directory (recommended). Click **Skip** if you want to prevent the public key from being posted to the PGP Global Directory.

- 18 Click **Finish**.

Your new PGP keypair has been generated. It should be visible in the PGP Keys Work area. If you don't see it listed, make sure **All Keys** or **My Private Keys** is selected in the PGP Keys Control box.



Consider backing up your private key to a safe location at this point. Your private key is very important, and losing it could have catastrophic consequences once you have data that is encrypted to it. See the section "[Protecting Your Private Key](#)" on page 177.

Passwords and Passphrases

Encrypting a file and then finding yourself unable to decrypt it is a painful lesson in learning how to choose a passphrase you will remember.

Most applications require a password between three and eight letters. Using a single-word passphrase is generally a bad practice, and is discouraged. A single word password is vulnerable to a dictionary attack, which consists of having a computer try all the words in the dictionary until it finds your password. You can imagine simple enhancements to dictionary attacks which manage to find broad arrays of passwords even when slightly modified from dictionary terms.

To protect against this manner of attack, it is widely recommended that you create a word that includes a combination of upper and lowercase alphabetic letters, numbers, punctuation marks, and spaces. This results in a stronger password, but an obscure one that you are unlikely to remember easily.

Trying to thwart a dictionary attack by arbitrarily inserting a lot of non-alphabetic characters into a passphrase makes your passphrase too easy to forget and could lead to a disastrous loss of information because you can't decrypt your own files. A multiple word passphrase is less vulnerable to a dictionary attack. However, unless the passphrase you choose is something that is easily committed to long-term memory, you are unlikely to remember it verbatim.

Picking a phrase on the spur of the moment is likely to result in forgetting it entirely. Choose something that is already residing in your long-term memory. It should not be something that you have repeated to others recently, nor a famous quotation, because you want it to be hard for a sophisticated attacker to guess. If it's already deeply

embedded in your long-term memory, you probably won't forget it. Of course, if you are reckless enough to write your passphrase down and tape it to your monitor or put it in your desk drawer, it won't matter what you choose.

Refer to [Appendix B, Passwords and Passphrases](#) for more information.

Protecting Your Private Key

PGP Corporation recommends that you take these actions immediately after you create your keypair:



Failure to take these actions could result in a devastating loss of data some time in the future.

- Back up a copy of your private key file to another, safe location, in case your primary copy is ever damaged or lost. See [“Backing up Your Private Key”](#).
- Reflect on your chosen passphrase to ensure that you chose something that you will not forget. If you are concerned that you chose a passphrase during the key creation process that you will not remember, change it RIGHT NOW to something you will not forget. For information on changing your passphrase, see [“Changing Your Passphrase” on page 191](#).

Your private key file is very important because once you have encrypted data to your public key, only the corresponding private key can be used to decrypt the data. This holds true for your passphrase as well; losing your private key or the passphrase means that you will not be able to decrypt data encrypted to the corresponding public key. When you encrypt information, it is encrypted to both your passphrase and your private key. You need both to decrypt the encrypted data. Once the data is encrypted, no one—not even PGP Corporation—can decrypt the data without your private key file and your passphrase.

Consider a situation where you have important encrypted data, and then either forget your passphrase or lose your private key. The encrypted data would be inaccessible, unusable, and unrecoverable.

Backing up Your Private Key

To back up your private key:

- 1 In the **PGP Keys** control box, click **My Private Keys**.
- 2 Select the icon representing your keypair.
- 3 From the **File** menu, select **Export**.
- 4 Type a name for the file.
- 5 Select the **Include Private Key(s)** checkbox. This is important, because if you do not do this, only your public key will be exported.
- 6 Click **Save**.

- 7 Copy the file (which has a .asc extension) to a secure location. This may be a CD which you carefully archive, another personal computer, or a USB flash drive that you keep in a safe location. Please remember not to distribute this file to others, as it contains both your private key and your public key.

Distributing Your Public Key

After you create your PGP Desktop keypair, you need to get your public key to those with whom you intend to exchange encrypted messages.

You make your public key available to others so they can send you encrypted information and verify your digital signature; you need their public key to send encrypted messages to them.

You can distribute your public key in various ways:

- Publish your key on the PGP Global Directory. Generally none of the other methods are necessary once your key is published to this directory
- Include your public key in an email message
- Export your public key or copy it to a text file

Placing Your Public Key on a Keyserver

The best method for making your public key available is to place it on a public keyserver, which is a large database of keys, where anyone can access it. That way, people can send you encrypted email without having to explicitly request a copy of your key. It also relieves you and others from having to maintain a large number of public keys that you rarely use.

There are a number of keyservers worldwide, including the PGP Global Directory, where you can make your key available for anyone to access. If you are using PGP Desktop in a domain protected by a PGP Universal Server, your PGP administrator will have preconfigured PGP Desktop with appropriate settings.

When you're working with a public keyserver, keep these things in mind before you send your key:

- Is this the key you intend to use? Others attempting to communicate with you might encrypt important information to that key. For this reason, we strongly recommend you only put keys on a keyserver that you intend for others to use.
- Will you remember your passphrase for this key so you can retrieve data encrypted to it or, if you don't want to use the key, so you can revoke it?
- Other than the PGP Global Directory, once a key is up there, it's up there. Some public keyservers have a policy against deleting keys. Others have replication features that replicate keys between keyservers, so even if you are able to delete your key on one server, it could reappear later.

Most people post their public key to the PGP Global Directory right after they create their keypair. If you have already posted your key to the PGP Global Directory, you do not need to do it again. Under most circumstances, there is no need to publish your key to any

other keyserver. Note also that other keyservers may not verify keys, and thus keys found on other keyservers may require significantly more work on your part to contact the key owner for fingerprint verification.

To manually send your public key to a keyserver:

- 1 Open PGP Desktop.
- 2 Make sure the PGP Keys Control box is selected.
- 3 Right-click the keypair whose public key you want to send to the keyserver.
- 4 Select **Send To**, then select the keyserver you want to send the public key to from the list.

Refer to [“Working with Keyservers” on page 182](#) if the keyserver you want to send your public key to is not on the list.

PGP Desktop lets you know when the public key is successfully copied to the keyserver.

Once you place a copy of your public key on a keyserver, it's available to people who want to send you encrypted data or to verify your digital signature. Even if you don't explicitly point people to your public key, they can get a copy by searching the keyserver for your name or email address.

Many people include the Web address for their public key at the end of their email messages. In most cases, the recipient can just double-click the address to access a copy of your key on the server. Some people even put their PGP fingerprint on their business cards for easier verification.

Including Your Public Key in an Email Message

Another convenient method of delivering your public key to someone is to include it with an email message.

When you send someone your public key, be sure to sign the email. That way, the recipient can verify your signature and be sure no one has tampered with the information along the way. Of course, if your key has not yet been signed by any trusted introducers, recipients of your signature can only truly be sure the signature is from you by verifying the fingerprint on your key.

To include your public key in an email message:

- 1 In PGP Desktop, make sure the PGP Keys Control box is selected.
- 2 Right-click the keypair whose public key you want to include in an email message.
- 3 Select **Send To**, then select **Mail Recipient**.

Your email application opens with your key information already in place.

- 4 Address the message and send it.

Exporting Your Public Key to a File

Another method of distributing your public key is to copy it to a file and then make this file available to the person with whom you want to communicate securely.

There are three ways to export or save your public key to a file:

- Select the icon representing your keypair, then from the **File** menu, select **Export**. Type a name for the file, then click **Save**. Be sure not to save your private key along with your public key if you plan on giving this file to others.
- Right-click the key you want to save to a file, select **Export** from the list, type a name for the file, then click **Save**. Be sure not to save your private key along with your public key if you plan on giving this file to others.
- Select the icon representing your keypair, choose **Copy** from the **Edit** menu, then open a text editor and choose **Paste** to insert the key information into the text file.

Copying from a Smartcard Directly to Someone's Keyring

Another method of distributing your public key—if you have it on a smartcard—is to copy it from the smartcard directly to someone's keyring.

Refer to [“Copying your Public Key from a Smartcard to a Keyring” on page 220](#) for more information about how to do this.

Getting the Public Keys of Others

Just as you need to distribute your public key to those who want to send you encrypted mail or verify your digital signature, you need to obtain the public keys of others to send them encrypted mail or verify their digital signatures.

There are multiple ways to obtain someone's public key:

- Automatically retrieve the verified key from the PGP Global Directory
- Find the key manually on a public keyserver
- Automatically add the public key to your keyring directly from an email message
- Import the public key from an exported file
- Get the key from your organization's PGP Universal Server

Public keys are just blocks of text, so they are easy to add to your keyring by importing them from a file or by copying them from an email message and then pasting them into your public keyring.

Getting Public Keys from a Keyserver

If the person to whom you want to send encrypted mail is an experienced PGP Desktop user, it is likely that a copy of his or her public key is on the PGP Global Directory or another public keyserver. This makes it very convenient for you to get a copy of the most up-to-date key whenever you want to send him or her mail and also relieves you from having to store a lot of keys on your public keyring.

If you are in a domain protected by a PGP Universal Server, then your PGP administrator may direct you to use the keyserver built into the PGP Universal Server. In this case, your PGP Desktop software is probably already configured to access the appropriate PGP Universal Server.

Similarly, the PGP Universal Server is configured by default to communicate with the PGP Global Directory. Thus, the PGP ecosystem distributes the load of key lookup and verification.

There are a number of public keyservers, such as the PGP Global Directory maintained by PGP Corporation, where you can locate the keys of most PGP users. If the recipient has not pointed you to the Web address where his or her public key is stored, you can access any keyserver and do a search for the user's name or email address. This may or may not work, as not all public keyservers are regularly updated to include the keys stored on all the other servers.

To get someone's public key from a keyserver:

- 1 Open PGP Desktop and highlight the PGP Keys Control box.
- 2 Choose **Search for Keys** from the PGP Keys Control box.

The Search for Keys screen appears in the Work area.

- 3 Specify your search criteria, then click **Search**.

If you want to search only a specific keyserver, click the **Search** drop-down button and specify the keyserver. If the keyserver you want to search isn't currently on the list, select **Edit Keyserver List** and add it.

You can search for keys on a keyserver by specifying values for multiple key characteristics. The inverse of most operations is also available. For example, you may search using "User ID is not Charles" as your criteria.

The results of the search appear.

- 4 If the search found a public key you want to add to your keyring, click **Add to My Keying** in the PGP Keys Control box.

The selected key is added to your keyring.

Getting Public Keys from Email Messages

A convenient way to get a copy of someone's public key is to have that person attach it to an email message.

To add a public key attached to an email message:

- 1 Open the email message.
- 2 Double-click the **.asc** file that includes the public key.
PGP Desktop recognizes the file format and open the **Select key(s)** dialog.
- 3 If asked, specify to open the file.
- 4 Select the public key(s) you want to add to your keyring and click **Import**.

Working with Keyserver

PGP Desktop understands three kinds of keyserver:

- **PGP Universal keyserver.** If you are using PGP Desktop in a domain protected by a PGP Universal Server, PGP Desktop is preconfigured to only communicate with the keyserver built into the PGP Universal Server with which it has a relationship. To PGP Desktop, this is a trusted keyserver, and PGP Desktop will automatically trust any key it finds on this keyserver unless the PGP Universal Server tells PGP Desktop that the key is not trusted—this can happen, for instance, when verifying signatures from remote keys.
- **The PGP Global Directory.** If you are using PGP Desktop outside of a domain protected by a PGP Universal Server, PGP Desktop is preconfigured to communicate with the PGP Global Directory.

The PGP Global Directory is a free, public keyserver hosted by PGP Corporation. It provides quick and easy access to the universe of PGP keys. It uses next-generation keyserver technology that verifies the key associated with each email address (so that the keyserver doesn't get clogged with unused keys, multiple keys per email address, forged keys, and other problems that plagued older keyserver) and it lets you manage your own keys, including replacing your key, deleting your key, and adding email addresses to your key. Using the PGP Global Directory significantly enhances your chances of finding the public key of someone with whom you want to send secured messages.

To PGP Desktop, the PGP Global Directory is a trusted keyserver, and PGP Desktop will automatically trust any key it finds there. During the initial connection to the PGP Global Directory, the PGP Global Directory Verification Key is downloaded, signed, and trusted by the key you publish to the directory. All of the keys verified by the PGP Global Directory are thus considered valid by your PGP Desktop.

- **Other keyserver.** In most cases, other keyserver are other public keyserver. However, you may have access, through your company or some other means, to a private keyserver.

Refer to [“Keys Options” on page 229](#) for more information about working with keyserver.

11

Managing PGP Keys

Using PGP keys effectively

This section tells you how to manage PGP keys. Topics include:

- [“Examining and Setting Key Properties” on page 183](#)
- [“Adding and Removing Photographic IDs” on page 188](#)
- [“Adding a New User Name and Email Address to a Key” on page 189](#)
- [“Importing Keys and X.509 Certificates” on page 190](#)
- [“Changing Your Passphrase” on page 191](#)
- [“Deleting Keys, User IDs, and Signatures” on page 192](#)
- [“Disabling and Enabling Public Keys” on page 192](#)
- [“Verifying a Public Key” on page 193](#)
- [“Signing a Public Key” on page 194](#)
- [“Granting Trust for Key Validations” on page 195](#)
- [“Granting Trust for Key Validations” on page 195](#)
- [“Working with Subkeys” on page 196](#)
- [“Working with ADKs” on page 200](#)
- [“Working with Revokers” on page 201](#)
- [“Splitting and Rejoining Keys” on page 203](#)
- [“PGP Key Reconstruction” on page 205](#)
- [“Protecting Your Keys” on page 207](#)

Examining and Setting Key Properties

The PGP Keys Work Area can display these important details about your keys:

- Name
- Email address
- Validity
- Size
- KeyID
- Trust

- Creation date
- Expiration date
- ADK
- Status
- Key description

You can choose how many or how few details are displayed by clicking the **Keys** item, then choosing columns to display by selecting **View > Columns**.

You can, however, see more information about a key and you can modify certain information about a key, by examining its key properties.

To view a key's properties:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **All Keys** in the Control box.

All keys on your keyring appear.

- 2 Double-click the key whose properties you want to view.

The Key Properties dialog for the key you selected appears.

The Key Properties dialog shows the following information about a key. Those attributes that can be changed are noted, as are the settings available for the specific attribute:

- **Key Properties Toolbar.** Click **Add Email Address** to add an email address to this key, click **Request Certificate** to create a certificate request to add a certificate to this key, click **Change Passphrase** to change the key's passphrase. The Key Properties Toolbar is only available for private keys, as you cannot make these changes on other people's public keys.
- **Photo ID.** If a photograph has been added to the key, it displays in the upper left corner of the Key Properties dialog. If no photograph has been added, one key appears for public keys, two keys for private keys.

Refer to ["Adding and Removing Photographic IDs" on page 188](#) for instructions how to add a photo ID to a key.

- **Name.** The user name entered when the key was created is shown at the top of the screen. This should be the real name of the key owner, as this helps others find the right key to use to send encrypted mail to the owner, but it is **not necessarily** the real name of the key owner.

Clicking on the user name shows all of the name/email address combinations currently associated with the key. To make another name/email address combination display, click the current name, select the desired name from the list, type the passphrase for the key, then click **OK**.

- **Email address.** The primary email address for this key.
- **ID.** The 32-bit key ID of this key. To copy the ID to the Clipboard, click it and select **Copy**.

- **Type.** The key type of this key. RSA and Diffie-Hellman are the most common. You may see older RSA Legacy keys that have been imported, but you cannot use PGP Desktop to create these keys.
- **Size.** The size of the key, in bits. The larger the size, the more secure, but it can also take longer to create the key and to use it. The first shown is the number of bits of the encryption subkey, the second is the number of bits of the signing key.
- **Trust.** Indicates how much you trust the owner of this key to act as an introducer for others, whose keys you may get in the future.

Refer to *An Introduction to Cryptography* for more information about trust.

Public keys can be **None**, **Marginal**, or **Trusted**. Your private keys can be **None** or **Implicit** (meaning it's your own key and thus you trust it completely). The **None** setting only occurs if you import your key from a file; **Implicit** is set automatically when you create a keypair.

If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change the trust setting of keypairs you import to Implicit.

If you import a key from a file into PGP Desktop, it will be imported in an unverified state; PGP Desktop knows it's a PGP key, but it doesn't know whether to trust it or not. If you import your own keypair that you saved to a file, set the **Trust** setting to **Implicit**. If you import someone else's public key, set the **Trust** setting to **Marginal** (if you are not certain of how responsible that person is when signing keys) or **Trusted** (you trust that the person signs keys only after they are sure the key can be trusted), then **Sign** the key **if you are certain that it belongs to the claimed owner**.

- **Verified.** A measure of the level to which you can be certain that this key really belongs to the claimed owner (it is a value calculated by PGP Desktop). If you obtained a key from a trustworthy source, such as a PGP Universal Server or the PGP Global Directory, PGP Desktop shows the key as verified.

If the verification of a key is **Unknown**, you can verify it by signing the key, indicating that you believe the claimed key owner is the actual key owner. This is done for the public keys of others that you put onto your keyring, or by setting the **Trust** field to **Implicit**. This means that it is your own key, so you trust that the claimed key owner, you, is in fact the actual key owner. This is done when you import your own key into PGP Desktop for some reason—because you are restoring it from a backup or moving it to another computer, for example.

- **Enabled.** Status of this key. Yes means the key is enabled, No means the key is disabled. An enabled key can be used for encrypting, signing, decrypting, and verifying. A disabled key cannot be used.

You can change the enabled/disabled status for a public key. Your private keys are always enabled.

- **Keyserver.** The preferred keyserver for this key, if specified. If a key has a preferred keyserver, that keyserver will be checked first when PGP Desktop synchronizes the key.

To specify a preferred keyserver for a key, click a listed keyserver or **None**, enter the information for the keyserver, click **OK**, type the passphrase for the key, then click **OK**.

You can only set a preferred keyserver for your private keys. A key can have only one preferred keyserver.

- **Created.** The date the key was created.
- **Expires.** The date the key will expire or **Never**. To change the expiration date for a private key, click on the current setting and select **Never** or specify an expiration date by selecting **Select Date**.

You can only change the expiration date for a private key.

- **Group.** Group status of this key, **Yes** or **No**. Yes means that more than one person or entity (such as a PGP Universal Server) has a copy of the private key together with the passphrase.

If your PGP Universal administrator has required that some keys are generated by the server, you may encounter keys with this set to **Yes**. When PGP Desktop is managed by a PGP Universal Server, it is not possible for this to occur. However, PGP Universal Satellite users may be provided with such keys if the administrator configures the server as such.

You can only change the Group status for your private keys.

- **Cipher.** Shows the preferred cipher for this key.

If you think a cipher doesn't meet your needs, you can disable it on this key. To do this, click the current cipher, select **Edit**, deselect the ciphers you don't want supported by this key, click **OK**, type the passphrase for the key, then click **OK** again. The selected ciphers are disabled for this key. Disabled ciphers display grayed out in the list.

You can only disable a cipher for your private keys.

- **Hash.** Shows the type of hash being used for this key. Click to see the allowed hashes. Hashes are used by PGP Desktop to detect changes in a signed document.

If you prefer a particular hash algorithm not be used, you can prevent PGP Desktop from using it for this key: click on **Hash**, select **Edit**, deselect any hash algorithm you do not want PGP Desktop to use, click **OK**, type the passphrase for the key, then click **OK** again. The specified hash is disabled for the key. Disabled hashes display grayed out in the list.

If you deselect **all** hash algorithms, SHA-1 will be used for version 4 keys and MD5 will be used for version 3 (older) keys.

You can only disable a hash for your private keys.

- **Compression.** The type of compression used by this key. Options are BZip2, ZLIB, and Zip.

If you don't care for a particular compression type, you can disable it on this key. To do this, click the current compression type, select **Edit**, deselect the compression types you don't want supported by this key, click **OK**, type the passphrase for the key, then click **OK** again. The selected compression types are disabled for this key.

- **Fingerprint.** A unique identifying string of numbers and characters used to identify a specific public key. No two PGP Desktop keys ever created have the same fingerprint. You cannot change a key's fingerprint.

Fingerprints are used to verify that you have the right key. For example, you can telephone the owner of a public key you got from a keyserver and have him or her read the fingerprint associated with their key so you can compare it with the fingerprint on your copy of their public key to see if they match. If the fingerprint does *not* match, you know you do not have their real key. And since you have them on the phone, you can ask them to email it to you.

Fingerprints can be displayed in either hexadecimal format (10 sets of four characters per set) or word list format (four columns with five unique words per column). Click Hexadecimal to view the fingerprint in hexadecimal format; click Biometric to view the fingerprint's biometric word list.

What is a biometric word list? PGP Desktop uses a special list of words to convey binary information in an authenticated manner over a voice channel, such as a telephone, via biometric signatures. The human voice that speaks the words, if recognized by the listener, serves as a means of biometric authentication of the data carried by the words. The word list serves the same purpose as the military alphabet, which is used to transmit letters over a noisy radio voice channel. The list contains 256 phonetically distinct words to represent the 256 possible byte values of 0 to 255.

This list enables users to read PGP public key fingerprints over the phone to authenticate the public key. The fingerprint is 20 bytes long, thus requiring 20 words to be read aloud. Experience has shown it to be fairly tedious and error prone to read that many bytes in hexadecimal, thus PGP Corporation has provided the word list as well to represent each byte using a word. Click the Copy icon to copy the fingerprint of a key.

- **Subkeys list.** Shows the subkeys currently configured on this key. The master key on a PGP key is for signing only; you can add subkeys for encrypting or for signing. Creating additional encryption subkeys, with specific expiration dates, can help keep your data secure (because the encryption subkey changes regularly). Creating additional signing subkeys for specific uses is helpful for file verification (and is required in some areas). Subkeys can be revoked, removed, or added to a PGP key without affecting the master key and the signatures on it.

To revoke a subkey, select the subkey to be revoked, click the backslash circle icon, click **Yes** on the confirmation dialog, type the passphrase for the key, then click **OK** again. The subkey is revoked.

To remove a subkey, select the subkey to be removed, click the minus sign icon, then click **Yes** on the confirmation dialog. The subkey is removed. **If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change your Subkey settings.**

To add a subkey, click the plus sign icon, configure the new subkey, click **OK**, type the passphrase for the key, then click **OK** again. The subkey is added.

You can only modify subkeys on your private keys.

- **ADK (Additional Decryption Key) list.** Shows the ADKs currently configured on this key. Messages encrypted by a key with an ADK are encrypted to the public key of the recipient and to the ADK, which means the holder of the ADK can also decrypt the message. Generally, ADKs are used as a corporate security measure if an employee is unable or unwilling to decrypt a message.

To update an ADK, select the ADK to be updated and then click the down-facing arrow icon. The ADK is updated.

To remove an ADK, select the ADK to be removed, click the minus sign icon, then click **Yes** on the confirmation dialog. The ADK is removed.

If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change your ADK settings.

To add an ADK, click the plus-sign icon, select the key to use as the ADK, click **OK**, click **Yes** on the confirmation dialog, type the passphrase for the key, click **OK** again, then click **OK** on the information dialog. The ADK is added.

You can only modify ADKs on your private keys.

- **Revoker list.** Shows the Revoker keys currently configured on this key. A Revoker key can be used to revoke a key if the key itself or the passphrase to the key is ever lost.

To update a Revoker key, select the Revoker key to be updated and then click the down-facing arrow icon. The Revoker key is updated.

To remove a Revoker key, select the Revoker key to be removed, click the minus sign icon, click **Yes** on the confirmation dialog, type the passphrase for the key, then click **OK** again. The Revoker key is removed. **If you are using PGP Desktop in a PGP Universal-managed environment, you may not be able to change your Revoker settings.**

To add a Revoker key, click the plus-sign icon, select the key to use as the Revoker key, click **OK**, click **Yes** on the confirmation dialog, type the passphrase for the key, click **OK** again, then click **OK** on the information dialog. The Revoker key is added.

You can only modify Revoker keys on your private keys.

Adding and Removing Photographic IDs

You can include a photographic ID on your Diffie-Hellman/DSS and RSA keys.

To add your photograph to your key:

- 1 Open PGP Desktop, click the PGP Keys Control box, and select **My Private Keys**.
- 2 In the PGP Keys Work area, double-click the private key to which you are adding the photo ID.

The Key Properties dialog for the selected key appears.

- 3 Right-click the placeholder key and silhouette icon and select **Add Photo ID**.

The Add Photo screen opens.

- 4 Drag or paste your photograph onto the Add Photo screen or browse to it by clicking **Select File**.

- 5 Click **OK**.

The **Passphrase** dialog box opens.

- 6 Type your passphrase for the key you are modifying, then click **OK**.

Your photo ID is added to your public key.

To delete a photo ID:

- 1 Right-click the existing photo on the Key Properties dialog and select **Remove Photo ID**.

The photo is removed from the key.

Adding a New User Name and Email Address to a Key

PGP Desktop supports multiple user names and email addresses on your keypair. These names and email addresses help others find your key so that they can send you encrypted messages.

To add a new user name or address to your keypair:

- 1 Open PGP Desktop, click the PGP Keys Control box, and select **My Private Keys**.
- 2 In the PGP Keys Work area, double-click the private key to which you are adding a user name or email address.

The Key Properties dialog for the key you double-clicked appears.

- 3 Click **Add Email Address**.

The PGP New User Name screen appears.

- 4 Type the new name and email address in the appropriate fields, then click **OK**.

The **PGP Enter Passphrase** screen appears.

- 5 Type the private key passphrase of the key you are modifying, then click **OK**.

The new name is added to the end of the user name list associated with the key.

- 6 If you want to set the new user name and address as the primary identifier for your key, right-click the new name and address and then choose **Set as Primary Name** from the list of commands that appears.

Importing Keys and X.509 Certificates

You can import PGP public keys and PKCS-12 X.509 certificates (a digital certificate format used by most Web browsers) to your PGP Desktop keyring. You can also import Privacy Enhanced Mail (PEM) format X.509 certificates from your browser by copying and pasting into your public keyring.

PGP Desktop provides an **Import Certificate Assistant** to help you with this task.

Using the Import Certificate Assistant

Before you begin: make sure that you know the passphrase for the certificate that you are importing.

To import a certificate using the Import Certificate Assistant:

- 1 Start the Assistant by:
 - Choosing **Open** from the **File** menu
 - Choosing **Import** from the **File** menu
 - Dragging the file containing the public key into the PGP Keys window
 - 2 Choose the way that you would like to import the certificate:
 - **Onto an existing key**—the certificate is added to a key that is already in your keyring.
 - **By creating a new PGP key**—a new PGP key is created using the imported certificate.
 - **By importing as a PGP X.509 wrapper key**—a new PGP key is created using the imported certificate. PGP Desktop treats the new key as an X.509 certificate.
 - 3 After you make your selection, click **Next**.

Either the **Certificate Passphrase Entry** screen or the **PGP Enter Passphrase** box displays.
 - 4 Provide the password for the certificate, then click **Next**.
 - If you are importing the certificate using the **Onto an existing key** option, the **Select Key** screen displays. Go to step 5
 - If you are importing the certificate using the **By creating a new PGP key** option, the key is generated. Click **Finish**. The process is complete.
 - If you are importing the certificate using the **By importing as a PGP X.509 wrapper** option, the **Select key(s)** dialog box displays. Click to select the key, click **Import**, and the PGP X.509 wrapper key is generated. The process is complete.
 - 5 To complete importing the certificate using the **Onto an existing key** option, from the **Select Key** dialog box, select the key onto which you would like to import the certificate, then type the password for the key.
-

Click **Next**.

- 6 The **Key Generation Progress** screen displays, and the certificate is imported onto the key.
- 7 Click **Finish**. The process is complete.

Changing Your Passphrase

It's a good practice to change your passphrase at regular intervals, perhaps every three months. More importantly, you should change your passphrase the moment you think it has been compromised, for example, by someone looking over your shoulder at the keyboard as you typed it in.

To change the passphrase for a split key, you must rejoin it first.

To change your private key passphrase:

- 1 Open PGP Desktop, click the PGP Keys Control box, and select **My Private Keys**.
- 2 In the PGP Keys Work area, double-click the private key for which you are changing the passphrase.

The Key Properties dialog for the key you double-clicked appears.

- 3 Click **Change Passphrase**.

The **PGP Enter Passphrase for Key** dialog appears.

- 4 Type your current passphrase for the private key, then click **OK**.

The **PGP Enter Confirmed Passphrase** screen appears.

- 5 Type your new passphrase in the first text box.
- 6 Press **Tab** to advance to the Confirmation box and confirm the new passphrase by typing it again.

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). Filling the Passphrase Quality bar gives you a strong passphrase that could take in the billions (billions with a 'b') of years to brute-force decrypt. Refer to ["The Passphrase Quality Bar" on page 250](#) for more information.

- 7 Click **OK**.

An information dialog appears.

- 8 Click **OK**.

The passphrase is changed.

Deleting Keys, User IDs, and Signatures

PGP Desktop gives you control over the keys on your keyrings, as well as the user IDs and signatures on those keys.

With public keys on your keyrings, you can delete entire keys, any or all user IDs on a key, and any or all signatures on a key.

With your keypairs, you can delete entire keypairs or any or all signatures; you cannot delete user IDs from a keypair.

To delete a key, user ID, or signature from your PGP keyring:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **All Keys** in the Control box.

All keys on your keyring appear.
- 2 To delete a key, right-click on the key, select Delete from the list of commands that appears, then click **OK** on the Confirmation dialog. The key is deleted from your keyring.
- 3 To delete a user ID (from a public key) or signature, click the plus sign on the left side of the key to display the user IDs and signatures. When you see the user ID or signature you wish to delete, right-click it, select **Delete** from the list of commands that appears, then click **OK** on the Confirmation dialog. The user ID or signature is deleted.

Disabling and Enabling Public Keys

Sometimes you may want to temporarily disable a public key on your keyring, which can be useful when you want to retain a public key for future use, but you don't want it cluttering up your recipient list every time you send mail.

You cannot disable your keypairs.

To disable a public key:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **All Keys** in the Control box.

All keys on your keyring appear.
 - 2 Double-click the public key you want to disable.

The Key Properties dialog for the key you selected appears.
 - 3 Locate the **Enabled** field.
 - 4 If the current Enabled setting is **No**, you don't have to do anything; the key is already disabled.
 - 5 If the current **Enabled** setting is **Yes**, click **Yes** once.
-

Yes changes to **No**; the key is disabled.

A disabled key cannot be used to encrypt, sign, decrypt, or verify.

To enable a disabled public key:

- 1 Repeat the process describe above.
- 2 When you locate the **Enabled** field, click **No** once.

No turns to **Yes**; the key is enabled.

Verifying a Public Key

It is difficult to know for certain whether a public key belongs to a particular individual unless that person physically hands the key to you on a removable media or you get the key from the PGP Global Directory. Exchanging keys on removable media is not usually practical, especially for users who are located many miles apart.

So the question remains: how can I make sure the public key I got from a public keyserver (not the PGP Global Directory) is really the public key of the person listed on the key? The answer is: you have to check the key's fingerprint.

There are several ways to check a key's fingerprint, but the safest is to call the person and have them read the fingerprint to you over the phone. Unless the person is the target of an attack, it is highly unlikely that someone would be able to intercept this random call and imitate the person you expect to hear on the other end. You can also compare the fingerprint on your copy of someone's public key to the fingerprint on their original key on a public server.

The fingerprint can be viewed in two ways: in a unique list of words or in its hexadecimal format.

To check a public key with its digital fingerprint:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **All Keys** in the Control box.

All keys on your keyring appear.

- 2 Double-click the public key whose fingerprint you want to check.

The Key Properties dialog for the key you selected appears. The fingerprint of the key is shown under the name and email address, in either hexadecimal format (10 sets of four characters per set) or word list format (four columns with five unique words per column).

- 3 Compare the fingerprint on the key with the original fingerprint.

If the two are the same, then you have the real key. If not, then you do **not** have the real key.

The word list is made up of special authentication words that PGP Desktop uses and are carefully selected to be phonetically distinct and easy to understand without phonetic ambiguity.

The word list serves a similar purpose as the military alphabet, which allows pilots to convey information distinctly over a noisy radio channel.

- 4 If you have a forged key, delete it.
- 5 Open your Web browser, point it at <https://keyserver.pgp.com/>, and search the PGP Global Directory for the real public key.

Signing a Public Key

When you create a keypair, the keys are automatically signed. Similarly, once you are *sure* a key belongs to someone, you can sign that person's public key, indicating you are sure it is valid. When you sign someone's public key, a signature icon along with your user name is shown attached to that key.

If you are using PGP Desktop in a PGP Universal-managed environment, key signing may be disabled.

If you import a keypair from a backup or from a different computer, that keypair will also need to be signed.

To sign someone's key:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **All Keys** in the Control box.

All keys on your keyring appear.

- 2 From the **Keys** menu, select **Sign** or right-click on the key you want to sign and select **Sign** from the list of commands that appears.

The PGP Sign Key dialog appears with the user name/email address and hexadecimal fingerprint displayed in the text box.

(The example below shows the PGP Sign Key dialog after the **More Choices** button was clicked. This is not the way the dialog first appears.)

- 3 Select the **Allow signature to be exported** checkbox, to allow your signature to be exported with this key.

An exportable signature is one that is allowed to be sent to servers and travels with the key whenever it is exported, such as by dragging it to an email message. The checkbox provides a shorthand means of indicating that you wish to export your signature.

- 4 Click the **More Choices** button to configure options such as signature type and signature expiration.

Choose a signature type to sign the public key with. Your choices are:

- **Non-exportable.** Use this signature when you believe the key is valid, but you don't want others to rely on your certification. This signature type cannot be sent with the associated key to a key server or exported in any way.
 - **Exportable.** Use exportable signatures in situations where your signature is sent with the key to the key server, so that others can rely on your signature and trust your keys as a result. This is equivalent to selecting the **Allow signature to be exported** checkbox on the **Sign Keys** menu.
 - **Meta-Introducer Non-Exportable.** Certifies that this key and any keys signed by this key with a Trusted Introducer Validity Assertion are fully trusted introducers to you. This signature type is non-exportable.
 - **Trusted Introducer Exportable.** Use this signature in situations where you certify that this key is valid, and that the owner of the key should be completely trusted to vouch for other keys. This signature type is exportable. You can restrict the validation capabilities of the trusted introducer to a particular email domain.
 - The **Maximum Trust Depth** option enables you to identify how many levels deep you can nest trusted-introducers. For example, if you set this to 1, there can only be one layer of introducers below the meta-introducer key.
 - If you want to limit the trusted introducer's key validation capabilities to a single domain, type the domain name in the **Domain Restriction** text box.
 - In the **Expiration** field, select **Never** if you don't want this signature to expire or select a date on which it does expire.
- 5 Click **OK**.
- The **PGP Enter Passphrase for Key** dialog appears.
- 6 Select the key you want to sign with from the drop-down list, then type the passphrase of the signing key, if required. (If the passphrase is already cached, you don't need to type it again.)
- 7 Click **OK**.
- The key is signed.

Granting Trust for Key Validations

Besides certifying that a key belongs to someone, you can assign a level of trust to the owner of the keys indicating how well you trust them to act as an introducer for others, whose keys you may get in the future.

Refer to *An Introduction to Cryptography* for more information about trusting keys.

This means that if you ever get a key from someone that has been signed by an individual whom you have designated as trustworthy, the key is considered valid even though you have not done the check yourself.

You must sign a key before you can set a trust level for it.

Public keys can be **None**, **Marginal**, or **Trusted**. Your keypairs can be **None** or **Implicit** (meaning it's your own key and thus you trust it completely). You shouldn't have anyone else's keypairs.

To grant trust to a key:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **All Keys** in the Control box.

All keys on your keyring appear.

- 2 Double-click the key for which you are granting trust.

The Key Properties dialog for the key you selected appears.

- 3 Locate the **Trust** field.

- 4 Click the current setting and select the desired setting from the list.

If you are granting trust for a public key, you can select **None**, **Marginal**, or **Trusted**. None means you don't trust the owner to act as an introducer, Marginal means you partially trust them, Trusted means you fully trust them.

If you are granting trust for a keypair, you can select **None** or **Implicit**. Only keypairs that you are importing from backup or from another computer of yours need to have their trust set to Implicit; when you create a keypair, its trust is automatically set to Implicit.

Working with Subkeys

A PGP Desktop keypair consists of these elements:



- the **Master Key**, for signing only;
- one mandatory **Subkey** for encryption;
- one or more *optional* **Separate Subkey(s)** for signing, encryption, or signing/encryption.

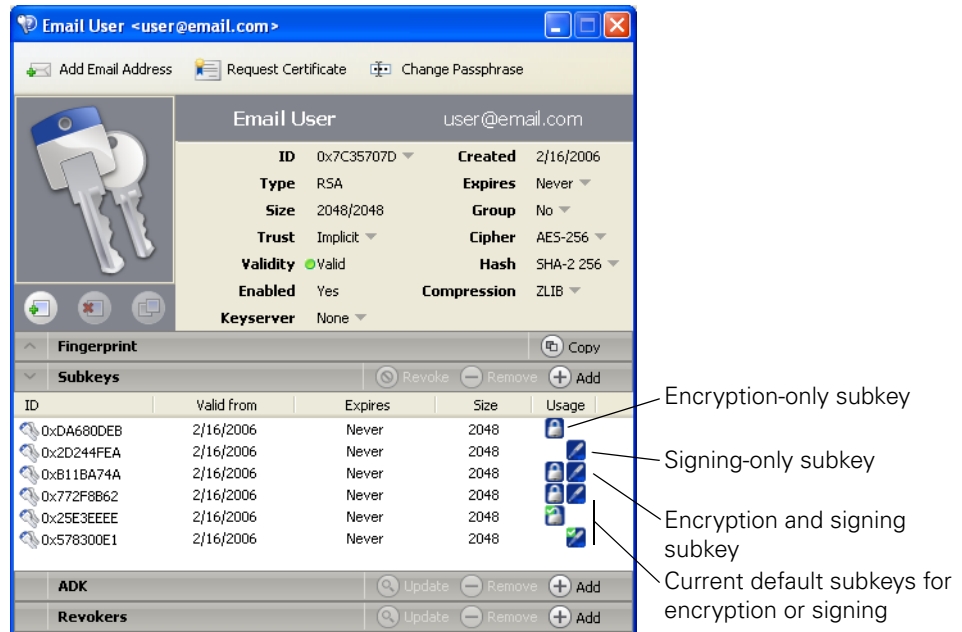
The Master Key is used by default for signing, while a subkey is always used for encryption. This can improve the security of a PGP Desktop keypair, as a separate encryption subkey can be revoked, removed, or added to the PGP Desktop keypair without affecting the Master Key or the signatures on it.

In addition to the Master Key and the mandatory encryption subkey, you have the option of creating one or more additional subkeys for your PGP Desktop keypair. You can create any combination of subkeys that can be used for encryption only, for signing only, or for both encryption and signing.

You can view the subkeys of a keypair from the Key Properties dialog. The Usage column indicates the function that a subkey performs:


- Encryption subkeys display a blue padlock symbol. 

- Signing subkeys display a blue pen symbol. 
- Subkeys used for both encryption and signing display both symbols. 



Using Separate Subkeys

Here are some examples of how additional separate subkeys can be useful:

- **Multiple encryption subkeys** that are valid during different portions of the keypair's lifetime can increase security. You can create encryption subkeys that have the Start and Expiration dates set so that only one encryption subkey at a time is valid. For example, you could create several encryption subkeys that are valid only during one future year (make sure you specify correct dates). The Encryption Subkey in use then changes with the new year. This can be a useful security measure, as it provides an automatic way to switch to a new encryption key periodically without having to recreate and distribute a new public key. Expired subkeys display a key icon with a red clock .
- **Separate signing subkeys** are needed in regions where separate subkeys for signing are required for legally-binding digital signatures.

The separate subkeys that you can create depend on the type of keypair that you are working with:

- For RSA keypairs, you can create subkeys for encryption, signing, and encryption/signing.
- For Diffie-Hellman/DSS keypairs, you can create subkeys for encryption or signing, but you cannot create subkeys that both encrypt and sign.
- For older PGP Legacy keypairs, subkeys are not supported.

Viewing Subkeys

You can view and change the subkey information on your own keypairs. The subkey information on your keyring's public keypairs can be viewed, but not changed.

To see what subkeys are on a keypair:

- 1 Open PGP Desktop, click the PGP Keys control box, then click **All Keys**.
All keys on your Keyring appear.
- 2 View the properties of a key by:
 - a Double-clicking the key you want to view, or
 - b Right-clicking on the key, then selecting **Key Properties** from the context menu, or
 - c Clicking to select the key in the Keyring, then choosing **Key Properties...** from the **Keys** menu.

The Key Properties dialog for the key you selected appears.

- 3 Click the **Subkeys** heading in the Key Properties dialog.
The Subkeys information for this key appears.

Creating New Subkeys

Most likely you will create new subkeys in the manner described in this section. However, you can also create subkeys when you first install PGP Desktop and are using the New Key wizard. For more information, see ["Using PGP Desktop for the First Time" on page 4](#).

To create new subkeys:

- 1 In the Subkeys section of the Key Properties dialog, click the **Add** button.
The New Subkey dialog appears.
- 2 In the **Use this subkey for** area, select **Encryption, Signing**, or **Encryption and Signing**, depending on how you want to use the new subkey.
- 3 In the **Key Size** field, choose a key size from 1024 to 3072 bits, or type a custom key size from 1024 to 4096 bits.
- 4 In the **Start Date** field, type a date on which the subkey you are creating becomes effective or choose a date from the drop-down calendar.
- 5 In the **Expiration** area, select **Never**, or select **Date** and specify a date or select a date from the drop-down calendar. This information controls when the subkey expires.
- 6 Click **OK**.
The Passphrase dialog appears.
- 7 Type your passphrase and then click **OK**.

The subkey is created.

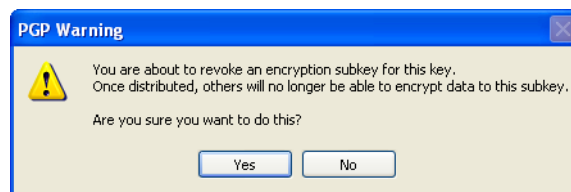
Using Subkeys with Smartcards

Revoking Subkeys

To revoke a subkey:

- 1 In the **Subkeys** section of the **Key Properties** dialog, select the subkey you want to revoke, then click **Revoke** (above the subkey list).

A **PGP Warning** dialog appears, informing you that once you revoke the subkey, other user's will not be able to encrypt data to it.



- 2 Click **Yes** to revoke the subkey or click **No** to cancel.

The Passphrase screen appears.

- 3 Type your passphrase, then click **OK**.

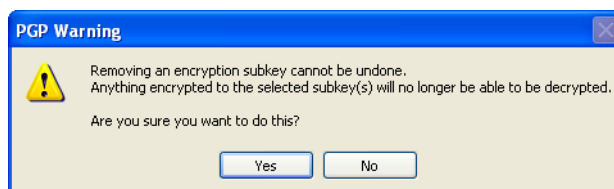
The subkey is revoked and the icon changes 🗑️.

Removing Subkeys

To remove a subkey:

- 1 In the **Subkeys** section of the **Key Properties** dialog, select the subkey you want to remove, then click **Remove** (above the subkey list).

A **PGP Warning** dialog appears, informing you that once you remove the subkey, you will not be able to decrypt information encrypted to it.



- 2 Click **Yes** to remove the subkey or click **No** to cancel.

The subkey is removed.

Working with ADKs

An additional decryption key (ADK) is a key generally used by security officers of an organization to decrypt messages that have been sent to or from employees within the organization.

Messages encrypted by a key with an ADK are encrypted to the public key of the recipient and to the ADK, which means the holder of the ADK can also decrypt the message.

You can only modify ADKs on your personal keypairs.

Adding an ADK

To add an ADK:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **My Private Keys** in the Control box.

The private keys on your keyring appear.

- 2 Double-click the key to which you are adding an ADK.

The Key Properties dialog for the key you selected appears.

- 3 Click the up-arrow to the left of **ADK**, if applicable (only those keys that already have at least one ADK already assigned will have the up-arrow).

The ADK information for this key appears, if configured.

- 4 Click the plus-sign icon on the right side of the ADK section.

The Select key(s) dialog appears.

- 5 Select the key you want to use as the ADK, then click **OK**.

- 6 A PGP Warning dialog appears, asking if you are sure you would like to add the selected key as an ADK.

- 7 Click **Yes**.

The **PGP Enter Passphrase for Key** dialog appears.

- 8 Type the passphrase for the key to which you are adding the ADK, then click **OK**.

A PGP Information dialog appears, telling you the ADK was added to the key.

- 9 Click **OK**.

Updating an ADK

To update an ADK:

- 1 Select the ADK you want to update from the list of ADKs.

The selected ADK highlights.

- 2 Click the down-facing arrow icon.

The ADK is updated.

To remove an ADK:

- 1 Select the ADK you want to remove from the list of ADKs.

The selected ADK highlights.

- 2 Click the minus-sign icon.

A PGP Warning dialog appears, asking if you are sure you want to remove the ADK.

- 3 Click **Yes** to remove the ADK.

The ADK is removed.

Working with Revokers

It is possible that one day you might forget your passphrase or lose your keypair (your laptop is stolen or your hard drive crashes, for example).

Unless you are also using Key Reconstruction and can reconstruct your private key, you would be unable to use your key again, and you would have no way of revoking it to show others not to encrypt to it. To safeguard against this possibility, you can appoint a third-party key revoker. The third-party you designate is then able to revoke your key just as if you had revoked it yourself.

This feature is available for both Diffie-Hellman/DSS and RSA keys.

You can only change revoker information on your keypairs. If a public key on your keyring has a revoker, you can see that information but you cannot change it.

Appointing a Designated Revoker

To add a designated revoker to your key:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **My Private Keys** in the Control box.

The private keys on your keyring appear.

- 2 Double-click the key to which you are adding a revoker.

The Key Properties dialog for the key you selected appears.

- 3 Click the plus sign to the left of **Revokers**, if applicable (only those keys that already have at least one revoker configured will have the plus sign).

The Revokers information for this key appears, if configured.

- 4 Click the plus-sign icon on the right side of the Revokers section.

The Select key(s) dialog appears.

- 5 Select the key you want to use as the Revoker key, then click **OK**.
A PGP Warning dialog appears, asking if you are certain that you want to grant revoker privileges to the selected key(s).
- 6 Click **Yes** to continue or **No** to cancel.
The **PGP Enter Passphrase for Key** dialog appears.
- 7 Type the passphrase for the keypair to which you are adding the revoker, then click **OK**.
A PGP Information dialog appears.
- 8 Click **OK**.
The selected key(s) is now authorized to revoke your key. For effective key management, distribute a current copy of your key to the revoker(s) or upload your key to the keyserver.

Revoking a Key

If the situation ever arises that you no longer trust your personal keypair, you can revoke your key, which tells everyone to stop using your public key.

The best way to circulate a revoked key is to place it on a public keyserver.

To revoke a key:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **My Private Keys** in the Control box.
The private keys on your keyring appear.
- 2 Right-click the key you want to revoke, then select **Revoke** from the list of commands that appears.
A PGP Warning dialog appears, asking if you are sure you want to revoke this key.
- 3 Click **Yes** to confirm your intent to revoke the selected key or **No** to cancel.
The **PGP Enter Passphrase for Key** dialog appears.
- 4 Type the passphrase for the keypair you are revoking, then click **OK**.
When you revoke a key, it is marked out with a red X to indicate that it is no longer valid.
- 5 Synchronize the revoked key so everyone will know not to use the now revoked public key.

Splitting and Rejoining Keys

Any private key can be split into shares among multiple “shareholders” using a cryptographic process known as Blakely-Shamir key splitting. This technique is recommended for extremely high security keys.

For example, PGP Corporation keeps a corporate key split between multiple individuals. Whenever we need to sign with that key, the shares of the key are rejoined temporarily.

Creating a Split Key

When you split a key, the shares are saved as files either encrypted to the public key of a shareholder or encrypted conventionally if the shareholder has no public key. After the key has been split, attempting to sign with it or decrypt with it will automatically attempt to rejoin the key.

To create a split key with multiple shares:

- 1 Open PGP Desktop, click the PGP Keys Control box, and then click **My Private Keys** in the Control box.

The private keys on your keyring appear.

- 2 Click on the keypair you want to split.

The selected keypair highlights.

- 3 From the **Keys** menu, select **Share Key > Make Shared**.

The Split PGP Key dialog appears.

- 4 Add shareholders for the split key by dragging and dropping their keys in the **Shareholder** list.

To add a shareholder that does not have a public key, click **Add**, type the person's name, then allow the person to type in their passphrase. (The shareholder needs to be physically present in order to type their own passphrase.)

- 5 When all of the shareholders are listed, you can specify the number of key shares that are necessary to decrypt or sign with this key.

By default, each shareholder is responsible for one share. To increase the number of shares a shareholder controls, click the name in the shareholder's list and then use the arrows to adjust the number of shares.

- 6 Click **Split Key**.

You are prompted to select a directory in which to store the shares.

- 7 Select a location to store the key shares, then click **OK**.

The Passphrase screen appears.

- 8 Type the passphrase for the key you want to split, then click **OK**.

A confirmation dialog box opens.

- 9 Click **Yes** to split the key.

The key is split and the shares are saved in the location you specified. Each key share is saved with the shareholder's name as the file name and an SHF extension.

- 10 Distribute the key shares to the owners, then delete the local copies.

Once a key is split among multiple shareholders, attempting to sign or decrypt with it will cause PGP Desktop to automatically attempt to rejoin the key.

Rejoining Split Keys

Once a key is split among multiple shareholders, attempting to sign or decrypt with it will cause PGP Desktop to automatically attempt to rejoin the key. There are two ways to rejoin the key, locally and remotely.

Rejoining key shares locally requires the shareholder's presence at the rejoining computer. Each shareholder is required to type the passphrase for their key share.

Rejoining key shares remotely requires the remote shareholders to authenticate and decrypt their keys before sending them over the network. PGP Desktop's Transport Layer Security (TLS) provides a secure link to transmit key shares which allows multiple individuals in distant locations to securely sign or decrypt with their key share.

To rejoin a split key:

- 1 Contact each shareholder of the split key. To rejoin key shares locally, the shareholders of the key must be present.

To collect key shares over the network, make sure the remote shareholders have PGP Desktop installed and are prepared to send their key share file. Remote shareholders must have:

- their key share files and passwords
- a keypair (for authentication to the computer that is collecting the key shares)
- a network connection
- the IP address or Fully Qualified Domain Name of the computer that is collecting the key shares

- 2 At the rejoining computer, use Windows Explorer to select the file(s) that you want to sign or decrypt with the split key.

- 3 Right-click on the file(s) and select **Sign or Decrypt** from the PGP context menu.

The **PGP Enter Passphrase for Selected Key** screen appears with the split key selected.

- 4 Click **OK** to reconstitute the selected key.

The Key Share Collection screen appears.

- 5 Do one of the following:

- If you are collecting the key shares locally, click **Select Share File** and then locate the share files associated with the split key. The share files can be collected from the hard drive, a floppy disk, or a mounted drive. Continue with [Step 6](#).
- If you are collecting key shares over the network, click **Start Network**.

The Passphrase dialog box opens. In the Signing Key box, select the keypair that you want to use for authentication to the remote system and type the passphrase. Click **OK** to prepare the computer to receive the key shares.

The status of the transaction is displayed in the Network Shares box. When the status changes to "Listening," the PGP application is ready to receive the key shares.

At this time, the shareholders must send their key shares.

When a share is received, the Remote Authentication screen appears. If you have not signed the key that is being used to authenticate the remote system, the key will be considered invalid. Although you can rejoin the split key with an invalid authenticating key, it is not recommended. You should verify each shareholder's fingerprint and sign each shareholder's public key to ensure that the authenticating key is legitimate.

- 6** Click **Confirm** to accept the share file.
- 7** Continue collecting key shares until the value for Total Shares Collected matches the value for Total Shares Needed on the Key Shares Collection screen.
- 8** Click **OK**.

The file is signed or decrypted with the split key.

PGP Key Reconstruction

This section only applies to PGP Desktop users in a PGP Universal-managed environment whose PGP administrator has configured key reconstruction support for their copy of PGP Desktop.

If you lose your key or forget your passphrase and do not have a backed up copy from which to restore your key, you will never again be able to decrypt any information encrypted to your key. You can, however, reconstruct your key if your PGP administrator has implemented a PGP key reconstruction policy for you, in which your key is encrypted and stored on a PGP Universal Server in such a way that only you can retrieve it.

The PGP Universal Server holding the key reconstruction data stores your key in such a way that only you can access it. Not even the PGP administrator has the ability to decrypt your key.

If your PGP administrator has configured support for key reconstruction, you will be prompted to enter additional "secret" information when you install PGP Desktop.

Once your key is on the server, you can restore it at anytime by selecting Reconstruct Key from the Keys menu in PGP Desktop.

Sending key reconstruction data

To send key reconstruction data to your company's PGP Universal Server:

- 1 Begin the installation normally.
- 2 When the Key Reconstruction screen appears, type five questions that only you can answer in the Prompt boxes (the default questions are examples only).

Choose obscure personal questions with answers that you are not likely to forget. Your questions can be up to 95 characters in length.

An example of a good question might be, "Who took me to the beach?" or "Why did Fred leave?"

An example of a bad question would be, "What is my mother's maiden name?" or "Where did I go to high school?"

- 3 In the Answer boxes, type the answers to the corresponding questions. Your answers are case sensitive and can be up to 255 characters.

Use the Hide Answers checkbox to view or hide your answers.

- 4 Click **OK** to continue.

If the **PGP Enter Passphrase for Key** screen appears, type the passphrase for your key, then click **OK**.

- 5 Click **OK**.

Your private key is split into five pieces, using Blakely-Shamir key splitting. Three of the five pieces are needed to reconstruct the key. Each piece is then encrypted with the hash, the uniquely identifying number, of one answer. If you know any three answers, you can successfully reconstruct the whole key.

To reconstruct your key:

- 1 In PGP Desktop, click the PGP Keys Control box.
- 2 From the **Keys** menu, select **Reconstruct Key**.

- 3 Answer the questions you established earlier, then click OK.

You are prompted to create a new passphrase. Your old passphrase will no longer work once your key is reconstructed.

- 4 Type a new passphrase, then click **OK**.

Your key is reconstructed.

Protecting Your Keys

Besides making backup copies of your keys, you should be especially careful about where you store your private key. Even though your private key is protected by a passphrase that only you should know, it is possible that someone could discover your passphrase and then use your private key to decipher your email or forge your digital signature. For instance, somebody could look over your shoulder and watch the keystrokes you enter or intercept them on the network or even over the Internet.

To prevent anyone who might happen to intercept your passphrase from using your private key, store your private key only on your own computer. If your computer is attached to a network, make sure that your files are not automatically included in a system-wide backup where others might gain access to your private key. Given the ease with which computers are accessible over networks, if you are working with extremely sensitive information, you may want to keep your private key on a flash drive, which you can insert like an old-fashioned key whenever you want to read or sign private information.

As another security precaution, consider assigning a different name to your private keyring file and then storing it somewhere other than in the default location.

Your private and public keys are stored in separate keyring files. You can copy them to another location on your hard drive or to a floppy disk. By default, the private keyring (secring.skr) and the public keyring (pubring.pkr) are stored along with the other program files in your "PGP" folder; you can save your backups in any location you like.

You can configure PGP Desktop to back up your keyrings automatically after you close PGP Desktop. Your keyring backup options can be set in the Keys tab of the Options screen.

12

PGP Shred

Secure file and folder deletion

If you want to completely destroy sensitive files without leaving fragments of their data behind, use the PGP Shred utility. This section includes the following topics:

- [“About Shredding Data with PGP Shred” on page 209](#)
- [“Using PGP Shredder to Permanently Delete Files and Folders” on page 209](#)
- [“Using the PGP Shred Free Space Assistant” on page 210](#)
- [“Scheduling Free Space Shredding” on page 212](#)

About Shredding Data with PGP Shred

When you delete a file using Shred, the file is immediately overwritten (even on systems with virtual memory) and all traces of the file are removed so that it cannot be retrieved even by using disk recovery software. Note that the PGP Shred utility does not shred Windows system files.

There are multiple ways to use Shred: via the PGP Shredder icon on your desktop, via the Shred Files icon on the PGP Toolbar, via the Shred Files command under the Tools menu, and in Windows Explorer (see [“Using PGP Shredder to Permanently Delete Files and Folders” on page 209](#) for more information).

You can also use PGP Desktop to erase free disk space that could contain data from previously deleted files and programs using the PGP Shred Free Space Assistant.

It is especially important to use the PGP Shred Free Space Assistant on Journaling file systems such as NTFS, as such file systems make a second copy of everything written to disk in a fleshiest journal. This helps the disk recover from damage, but requires extra work when removing sensitive data. Shredding a file does not remove any potential journal entries that may have been created. NTFS in particular can also store small (less than 1K) files in internal data structures that cannot be removed properly without using the PGP Shred Free Space Assistant with the “Wipe NTFS internal data structures” option.

You can set file shredding options on the Shred tab of the PGP Options screen. See [“Setting PGP Desktop Options” on page 227](#) for more information.

Using PGP Shredder to Permanently Delete Files and Folders

Use the PGP Shredder utility to permanently erase sensitive files and folders.

There are multiple ways to shred files using PGP Desktop:

- Using the PGP Shredder icon on your desktop.

- In Windows Explorer by right-clicking the files or folder you wish to shred, selecting PGP from the commands that appear, and then selecting Shred.
- Using the Shred Files icon on the PGP Toolbar.
- Using the Shred Files command under the Tools menu

To shred files using the PGP Shredder icon or right-clicking in Windows Explorer:

- 1 Drop the files/folders you want to shred on the PGP Shredder icon on the desktop or right-click in Windows Explorer on the files/folders you want to shred.

A confirmation dialog appears, 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.

To shred files using the Shred Files icon on the PGP Toolbar or the Tools > Shred Files command.

- 1 On the PGP Desktop screen, do one of the following:

- Click the **Shred Files** icon on the PGP Toolbar.
- From the **Tools** menu, select the **Shred Files** command.

The **Open** dialog appears.

- 2 Select the files on your system you want to shred, then click **Open**.

A confirmation dialog appears, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.

- 3 Click **Yes**.

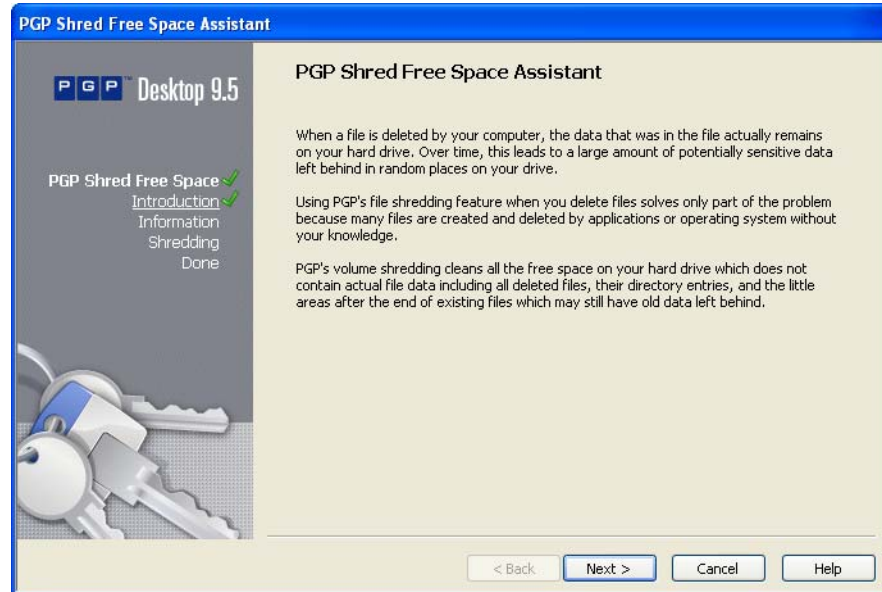
The files are securely deleted from your system.

Using the PGP Shred Free Space Assistant

To shred free space on your disks:

- 1 With PGP Desktop open, from the **Tools** menu, select **PGP Shred Free Space**.

The Introduction screen of the PGP Shred Free Space Assistant appears



- 2 Read the information, then click **Next**.

The **Gathering Information** screen appears.

- 3 In the Shred drive box, select the disk or volume you want shredded and the number of passes you want PGP Shred Free Space to perform.

The recommended guidelines for number of passes are:

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

- 4 Choose whether to shred internal NTFS data structures.

This option is not available on all systems.

If the selected partition is **not** your boot partition, you may perform an intensive shred operation that overwrites internal NTFS data structures that may hold residual data. The partition will be completely filled during this process, and as such you should not use the disk for anything else while this operation is in progress. Some of these structures are not generally considered free space on your drive, but the techniques employed by this option will cause them to be shredded. This option does not increase the risk of anything negative happening to your disk as a result of the shredding operation.

- 5 Click **Next**.

The Perform Shred screen opens and displays statistical information about the drive or volume you selected.

6 Click **Begin Shred**.

The PGP Free Space Wipe Assistant scans and then shreds leftover fragments from the specified disk or volume.

When the shred session is complete, a message appears near the bottom of the Perform Shred screen telling you the selected drive has been shredded.

7 Click **Next**.

The Completing screen appears.

8 Click **Finish**.

Scheduling Free Space Shredding

You can use the Windows Task Scheduler to schedule periodic shredding of free space on your system.

To schedule free space shredding:

1 With PGP Desktop open, from the **Tools** menu, select **Shred Free Space**.

The Introduction screen of the PGP Free Space Wipe Assistant appears.

2 Read the information, then click **Next**.

The Gathering Information screen appears.

3 In the Wipe drive box, select the disk or volume you want shredded and the number of passes you want PGP Free Space Wipe to perform.

The recommended guidelines for number of passes are:

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

4 Click **Next** to continue.**5** When the Perform Wipe screen opens, click the **Schedule** button.**6** When the Schedule screen appears, click **OK** to continue.

If you are running Windows NT, the Windows NT Confirm Password dialog box appears.

Enter your Windows NT login password in the first text box. Press **Tab** to advance to the next text box and confirm your entry by entering your password again. Click **OK**.

The Windows Task Schedule screen appears.

- 7 Choose how often you want the task to run from the Schedule Task area. Your choices are:
 - **Daily.** This option runs your task once at the time you specify on the days you indicate. Click **OK** to close the dialog box, then enter the time you want to run the task each day in the Start Time text box.
 - **Weekly.** This option runs your task on a weekly basis at the date and time you specify. Enter the number of weeks you want between each disk shred in the text box provided, then choose a day from the Schedule Task Weekly list.
 - **Monthly.** This option runs your task once each month on the day and at the time you specify. Enter the time in the text box provided, then enter the day of the month on which you want the task to run. Click **Select Months** to specify which months the task will run.
 - **Once.** This option runs your task exactly once on the date and at the time you specify. Enter the time in the text box provided, then select a month and a date from the lists Run On text box.
 - **At System Start up.** This option runs your task only upon system start up.
 - **At Logon.** This option runs your task when you log on to your computer.
 - **When Idle.** This option runs your task when your system is idle for the amount of time you specify in the minutes text box.
- 8 Enter the time of day that you want the task to start in the Start Time box.
- 9 Specify how often you want the task to run in the Schedule Task Daily box.
- 10 Click **Advanced** to open a dialog box where you can select additional scheduling options, such as the start date, the end date, and the duration of the task.
- 11 Click **OK**.

A confirmation screen appears.

Your new PGP folder or free space task is now scheduled. To edit or delete your PGP tasks, use the Windows Task Scheduler.

13

Storing Keys on Smartcards and Tokens

How PGP Desktop works with smartcards

Smartcards and tokens are portable devices that include a computer chip, which lets them store data and perform computations. Smartcards are plastic cards about the size of a credit card you insert into a smartcard reader attached to a computer. Tokens are keychain fobs with USB connectors that connect directly to a USB port on a computer.

This section describes how to use smartcards and tokens with PGP Desktop. Topics include:

- [“About Smartcards and Tokens” on page 215](#)
- [“Supported Smartcards” on page 216](#)
- [“Recognizing Smartcards” on page 217](#)
- [“Examining Smartcard Properties” on page 218](#)
- [“Generating a PGP Keypair on a Smartcard” on page 218](#)
- [“Copying your Public Key from a Smartcard to a Keyring” on page 220](#)
- [“Wiping Keys from Your Smartcard” on page 220](#)
- [“Copying a Keypair from Your Keyring to a Smartcard” on page 221](#)
- [“Using Multiple Smartcards” on page 223](#)
- [“Special-Use Tokens” on page 223](#)

About Smartcards and Tokens

You can use PGP Desktop to create a PGP keypair on a smartcard or token, or to copy a PGP keypair to a smartcard or token. Both options give you an extra layer of security in that you can keep your PGP keypair with you, on your smartcard or token, instead of leaving it on your system: a PGP keypair on a smartcard or token is less vulnerable than the same keypair stored on your computer because you can keep the smartcard or token with you.

In order to use PGP Desktop with a smartcard or token from a particular vendor, you must have a supported smartcard reader (if you are using a smartcard) and the appropriate software drivers installed on your system (for both smartcards and tokens). The drivers *must* include the PKCS-11 (the cryptographic token interface standard) library.

PGP Corporation strongly recommends using software drivers from the vendor who makes your smartcard or token.

PGP Desktop recognizes and works with a wide variety of smartcards, including those from Athena, AET SafeSign, Axalto (formerly Schlumberger), SafeNet (formerly Rainbow), Aladdin, and GemPlus, for example. PGP Desktop also works with Department of Defense Common Access Cards with the ActivCard Gold 2.0 profile.

In addition to these vendors, PGP Desktop recognizes and works with smartcards from vendors that include a standards-based PKCS-11 library in their software drivers. If the PKCS-11 library from a vendor is installed on your system and works with other PKCS-11 applications, such as Mozilla Firefox or Thunderbird, chances are high that PGP Desktop will recognize and work with smartcards from this vendor.

When you create and store a PGP keypair on a smartcard, you access the private key using the smartcard's PIN rather than a passphrase. If you have a smartcard that handles its own authentication (for example, on its own keypad or via a biometric device, PGP Desktop works with these smartcards; when PGP Desktop displays a passphrase dialog, do not enter a passphrase, just click OK. The device should then bring up its own authentication method.

The private portion of your keypair that is generated on a smartcard never leaves the device—it's not exportable. Decryption and signing operations take place directly on the device. The exception to this is if you generate a keypair on your computer, rather than on the smartcard, and then afterwards *copy* the keypair to your smartcard; because it was copied to the smartcard instead of created on it, the private portion *is* exportable.

Department of Defense Common Access Cards (CACs) work somewhat differently than other smartcards. They are read only, and they include two separate certificates, one for signing and one for encrypting. PGP Desktop filters the two certificates based on the intended usage; for example, only the signing certificate of a CAC is presented when you are prompted to select a key to sign a file.

Axalto smartcards are JavaCards. A small Java module, called a Java applet, runs on the card. The card can be configured to execute different applets that change the behavior or configuration of the smartcard, a process called personalization. In order for JavaCards to be used with PGP Desktop, only a few of the available personalization profiles are appropriate.

Additionally, all of the personalization profiles currently available require minor changes to their configurations to work with PGP Desktop. Specifically:

- The profile must enable PKCS-11 support. In most cases, the name "Netscape" or "Entrust" appear in the titles of profiles that support PKCS-11.
- One PGP Desktop key uses at least two PKCS-11 private keys. In order to work with PGP Desktop, a profile must have a value of 2 or greater in the maximum number of private keys allowed.

Refer to the documentation for the JavaCard you are using for more information.

Supported Smartcards

PGP Desktop can recognize and work with:

- DoD Common Access Cards (CACs) with the **ActivCard** Gold 2.0 profile. For more information about the ActivCard Gold 2.0 profile, refer to www.activcard.com.
- **Athena Smartcard Solutions** smartcards, including the ASEKey USB token. For more information about smartcards from Athena Smartcard Solutions, refer to www.athena-scs.com.

- **AET SafeSign** smartcards, including ASEKey 1.0. For more information about smartcards from AET SafeSign, refer to www.cryptoshop.com.
- **Axalto** (formerly Schlumberger) smartcards, including the Cryptoflex 32K. For more information about smartcards from Axalto, refer to www.axalto.com.
- **SafeNet** smartcards, including iKey 2032. (PGP Desktop no longer supports the SafeNet iKey 1000.) For more information about smartcards and USB tokens from SafeNet, refer to www.safenet-inc.com/products/tokens/index.asp.
- **Aladdin** smartcards, including eToken PRO USB 16K, 32K, and 64K. For more information about Aladdin eToken products, refer to www.aladdin.com/eToken/default.asp.
- **GemPlus** smartcards, including SafesITe and GemXpresso Pro. For more information about smartcards from GemPlus, refer to www.gemplus.com.

As mentioned previously, PGP Desktop also recognizes and works with smartcards from other vendors, as long as they include a standards-based PKCS-11 library in their software drivers. In those rare cases where a non-standard smartcard doesn't work with PGP Desktop, "Smartcard Keys" does *not* appear in the PGP Keys Control box when the smartcard is installed on the system.

Recognizing Smartcards

Before you can examine the properties of a smartcard you want to use with PGP Desktop or create a PGP keypair on a smartcard, you need to make sure that PGP Desktop recognizes that the smartcard you want to work with is available on the system.

The general requirements for this are:

- The smartcard software drivers, with PKCS-11 support, must be installed on the system.
- The smartcard must be installed on the system. For a USB token, this generally means it's inserted into a free USB port. For a smartcard, it generally means it's inserted into the appropriate smartcard reader.

So if you have done these two things, how can you tell that PGP Desktop recognizes that the smartcard is on the system?

There are two ways:

- The easiest way to tell if PGP Desktop "sees" a smartcard is to open PGP Desktop and click on the PGP Keys Control box. If "Smartcard Keys" is listed below "All Keys" in the PGP Keys Control box, then PGP Desktop sees the smartcard on the system.
- A slightly more complicated way is to open PGP Desktop, click the PGP Keys Control box, and then from the **File** menu, select **New PGP Key**. When the PGP Key Generation Assistant screen appears, look towards the bottom. If the **Generate Key on Token: <smartcard information>** checkbox is active, then PGP Desktop sees the

smartcard on the system. This method has a slight advantage over the previous method in that PGP Desktop shows you information about the particular smartcard that it sees on the system.

Examining Smartcard Properties

A PGP key stored on a smartcard is noted on the PGP Desktop screen with a special key-on-a-card icon. By viewing its properties, you can find information regarding the smartcard itself, such as the manufacturer, serial number, and key types it supports.

To view the properties of a smartcard:

- 1 Open PGP Desktop.
- 2 Put your smartcard in your smartcard reader or token in a USB port.
The key appears in the Smartcard Keys section of the PGP Keys Control box.

- 3 Highlight the key whose properties you want to view.

- 4 From the **Keys** menu, select **Smartcard Properties**.

The PGP Smartcard Properties screen appears.

This screen displays information about the smartcard on which the key resides, including:

- The name of the manufacturer.
- The smartcard model.
- The serial number associated with the smartcard.
- The smartcard's capabilities, including the type of PGP key that the card can store and the number of characters your PIN may contain.
- The total number of private keys you currently have on the smartcard, including subkeys.

- 5 Click **OK**.

Generating a PGP Keypair on a Smartcard

To generate a PGP keypair on a smartcard:

- 1 Put your smartcard in the smartcard reader or your token into a free USB port.
- 2 Open PGP Desktop.
- 3 Click on the PGP Keys Control box.

If the smartcard is detected, "Smartcard Keys" appears in the PGP Keys Control box.

- 4 From the **File** menu, select **New PGP Key**.

The PGP Key Generation Assistant Introduction screen appears.

PGP Desktop will only recognize the software drivers from one smartcard vendor at a time. If you have the software drivers from more than one smartcard vendor installed on your system, you need to tell PGP Desktop which vendor's smartcards you want to use; refer to ["Using Multiple Smartcards"](#) on page 223 for more information.

- 5 Select the box labeled **Generate Key on Token: [name of smartcard on system]**, then click **Next**.

The Name and Email Assignment screen appears.

- 6 Enter your name in the **Full Name** box and your email address in the **Primary Email** box. If you want to enter more email addresses for this key, click **More** and enter the email address(es) in the **Other Addresses** fields.

It is not absolutely necessary to enter your real name or email address. However, using your real name and email address makes it easier for others to identify you as the owner of your public key.

- 7 Click **Advanced** to set advanced key settings.

The Advanced Key Settings dialog appears.

- 8 Establish settings for:

- **Key type:** RSA (Diffie-Hellman/DSS keys are not supported)
- **Key size:** From 1028 to 2048
- **Expiration:** Never or a date you specify
- **Allowed algorithms:** AES, CAST, TripleDes, IDEA, and Twofish
- **Preferred algorithm:** Choose one of the allowed algorithms
- **Allowed hash:** SHA-2-256, SHA-2-384, SHA-2-512, RIPEMD-160, SHA-1, MD-5
- **Preferred hash:** Choose one of the allowed hashes

Some settings may be not be available if the smartcard you are using does not support them.

- 9 Click **OK**.

The Advanced Key Settings dialog goes away.

- 10 Click **Next**.

- 11 On the Passphrase Assignment screen, enter the PIN that corresponds to the smartcard. The PIN acts as passphrase for the key.

Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, select the **Show Keystrokes** checkbox.

- 12** Click **Next** to begin the key generation process.

PGP Desktop generates your new keypair directly on your smartcard.

This process can take several minutes.

- 13** When the key generation process indicates that it is done, click **Next**.

You are prompted to add the public key portion of the key you just created to the PGP Global Directory.

- 14** Read the text on the screen and click **Next**. Click **Skip** to prevent the public key from being posted to the PGP Global Directory.

The public key is posted to the PGP Global Directory.

- 15** Click **Done**.

Your new keypair is generated and stored directly on your smartcard.

Because the private portion of your keypair stays only on your smartcard, when you remove the smartcard from the system, the key icon changes to a single key to reflect that the public portion is left on the keyring and the private portion has been removed with the smartcard.

Copying your Public Key from a Smartcard to a Keyring

Storing your keys on a smartcard enables you to physically walk to a computer—a computer with a compatible smartcard reader or a free USB port, and PGP Desktop and the appropriate drivers installed—and automatically copy the *public* portion of your keypair to the PGP Desktop keyring on that system.

To copy your *public* key from your smartcard to another user's keyring:

- 1** Open PGP Desktop on the other system.
- 2** Put your smartcard into the smartcard reader or token into a USB port.
- 3** Wait for your key to display in PGP Desktop.

When you see your key display, it means that your public key has been copied onto the system.

- 4** Remove your smartcard from the system.

Your public key remains on the system.

Wiping Keys from Your Smartcard

You can delete all the data stored on a smartcard by using the **Wipe Contents** feature in the Smartcard properties window.

To wipe a smartcard:

- 1** Open PGP Desktop.
- 2** Put the smartcard you want to wipe in the smartcard reader or the token into a USB port.
- 3** In the PGP Keys box, select **Smartcard Keys**.
The PGP keys on the smartcard appear.
- 4** Select the smartcards or tokens you want to wipe.
- 5** From the **Keys** menu, select **Wipe Smartcard**.
PGP Desktop asks for confirmation you want to delete all keys currently on the smartcard or token.
- 6** Click **OK**.
The PGP Enter Passphrase screen appears.
- 7** Enter the PIN for this smartcard.
Normally, as an added level of security, the characters you enter for the passphrase do not appear on the screen. However, if you are sure that no one is watching, and you would like to see the characters of your passphrase as you type, select the **Show Keystrokes** checkbox.
- 8** Click **OK**.
PGP Desktop deletes all keys stored on the smartcard.

Copying a Keypair from Your Keyring to a Smartcard

PGP Desktop also lets you copy an existing keypair from your system to a smartcard. This is a good way to make a backup of your keypair and/or to distribute your public key. Only RSA keys can be copied to a smartcard.

Copying your keypair to a smartcard is different from creating a keypair directly on the smartcard (which is not supported by all smartcards). When you create a keypair directly on a smartcard, you *must* have the smartcard on the system to use your private key.

When you have a keypair on your desktop and copy it to a smartcard, things work slightly differently. In this case, the private portion of your keypair resides on the smartcard **and on your system** (unless you choose to delete the private portion of your keypair from your system).

There are two main reasons to copy an existing keypair to a smartcard:

- To use it as a backup for the keypair on your system and to copy your public key from the smartcard to other people's keyrings. In this case, you would have two copies of the same private key: one on the system where you originally created it and one on the smartcard.

- To use it as your only copy of your private key, just as if you'd created it directly onto the smartcard. In this case, you would need to delete the private key from your system (PGP Desktop gives you the option to do this). You would select this option if you started using smartcards after you had already created your PGP keypair and wanted to have the advantages of having your keypair on your smartcard but don't want to create a new keypair.

Finally, when you copy your PGP keypair to a smartcard, the passphrase for the keypair that's on the smartcard is automatically changed from whatever it was to the PIN of the smartcard. However, the passphrase for the keypair that was already on your system, the keypair you copied to the smartcard, *doesn't change*. You end up with two copies of the same keypair, each with its own passphrase.

If you decide to delete the private key from your system and just keep the private key on your smartcard, this isn't a problem; you use the PIN of the smartcard as the passphrase for your private key.

To copy an existing PGP keypair to your smartcard:

- 1 Put your smartcard in the smartcard reader or your token in a USB port.
- 2 Open PGP Desktop.
- 3 Select the keypair you want to copy to your smartcard.

You cannot copy Diffie-Hellman/DSS keys to a smartcard.

- 4 Right-click the keypair you want to copy and choose **Add To -> Smartcard Keys**.

A warning appears informing you that once the keypair is copied to the smartcard, your PGP passphrase for this keypair will automatically change to the PIN of the smartcard.

- 5 Click **OK** to continue.

The PGP Enter Passphrase screen appears.

- 6 Enter the passphrase for your key, then click **OK**.

The PGP Enter Passphrase screen appears.

- 7 Enter the PIN for the smartcard, then click **OK**.

The keypair is copied to the smartcard.

PGP Desktop asks if you want to remove the private portion of the keypair from your keyring so that it only resides on the smartcard.

- 8 Click **Yes** to remove the private portion of your keypair from your keyring; click **No** to leave the private portion of your keypair on your keyring.

If you clicked Yes, the private portion of your keypair is deleted from the keyring on your system and exists only on your smartcard.

If you clicked No, the private portion is not deleted; you now have two copies of the same keypair, one on your system and the other on your smartcard.

Using Multiple Smartcards

PGP Desktop supports smartcards from a wide variety of vendors. At the same time, PGP Desktop only works with the smartcards from one vendor at a time.

On startup, PGP Desktop automatically searches your system for software drivers that support the use of smartcards from a particular vendor. When it finds those software drivers, it loads them, assuming you have smartcards from that vendor and want to use them.

If you have the software drivers from a single vendor installed on your system, this works perfectly; PGP Desktop automatically finds the software drivers and lets you use the smartcards from that vendor. You don't have to do anything; it just works.

However, there may be some occasions when you need to use the smartcards from more than one vendor. When this happens, and you have the software drivers from more than one vendor on a system, you need to tell PGP Desktop whose smartcards you want to use. Otherwise, PGP Desktop won't know which software drivers to use, and may not select the ones you want.

To specify which smartcard software drivers on your system to use:

- 1 Open PGP Desktop.
- 2 From the **Tools** menu, select **PGP Options** (or press CTRL-T).

The PGP Options screen appears, showing the General tab.

- 3 Click on the **Keys** tab.
- 4 In the **Synchronization** section, from the **Synchronize with smartcards and tokens** list, select the vendor whose software drivers you want to use.

(**Automatically** is the default setting; it is appropriate for when you have the software drivers from only one vendor on your system. Select **None** to prevent PGP Desktop from using the smartcards from any vendor.)

PGP Desktop will now expect you to use smartcards from the selected vendor; if you add a smartcard from a different vendor to your system, PGP Desktop will not recognize it.

- 5 If your vendor is *not* on the drop-down list, select **Other**. On the Select Smartcard Driver screen, navigate to the DLL file of the software drivers of your smartcard vendor, select it, then click **Open**.

You will now be able to use smartcards supported by the software driver file you selected.

Special-Use Tokens

Both PGP Desktop and PGP Universal Server use tokens for special uses:

- PGP Desktop uses the Aladdin eToken Pro USB token for authentication at startup if the system's *boot* drive has been whole disk encrypted (refer to [Chapter 6, Protecting Disks with PGP Whole Disk Encryption](#) for more information protecting a boot drive with PGP Whole Disk Encryption). Only the Aladdin eToken Pro USB token can be used for this purpose.
- PGP Universal Servers use the Athena ASEKey USB token as a hardware Ignition Key (refer to the *PGP Universal Administrator's Guide* for more information). Only the Athena ASEKey USB token can be used for this purpose.

How to configure these tokens for these special uses is described below.

Configuring the Aladdin eToken

You need an Aladdin eToken Pro USB token with a PGP keypair on it to use with the PGP Whole Disk Encryption feature of PGP Desktop for Windows.

To create a PGP keypair on an Aladdin eToken Pro USB token for use with the PGP Whole Disk Encryption feature:

- 1 Obtain an Aladdin eToken Pro USB token.

This is the only token that can be used with the Whole Disk Encryption feature. You can use any of the three models: 16K, 32K, or 64K.

The 16K and 32K models support 1024-bit keys; the 64K mode supports up to 2048-bit keys.

- 2 Make sure the appropriate driver software from Aladdin is installed on your system.

If you don't already have it, and don't have the PGP distribution, you can get the driver software from the Aladdin website. Go to the Aladdin website (www.aladdin.com), select Support & Downloads from the top of the main screen, select eToken from the drop-down list, select PKI Solutions from the next drop-down list, register (if necessary), download the file RTE_3_65.msi to your system, then double-click the msi file to begin the installation.

Note that a new version may be available by the time you read this.

When the driver software is installed, PGP Desktop will display "Smartcard Keys" in the PGP Keys Control box.

- 3 Open PGP Desktop for Windows.
- 4 Create a keypair on the Aladdin eToken (refer to ["Generating a PGP Keypair on a Smartcard" on page 218](#) for instructions) or use the **Add To** context menu to copy an existing keypair to the token (refer to ["Copying a Keypair from Your Keyring to a Smartcard" on page 221](#) for instructions).

(If you want to send an existing keypair to the token, it must be a 1024- or 2048-bit RSA key; the Aladdin eToken Pro token does not support any other key sizes or DH/DSS keys at this time.)

When you create a keypair on the token or send an existing keypair to the token, the passphrase of the keypair changes to the PIN of the token. The default PIN for the Aladdin eToken Pro token is 1234567890; as that is a well-known PIN, be sure to change it using the Aladdin software.

- 5 You can now use the PGP keypair on the Aladdin eToken with the PGP Whole Disk Encryption feature.

Configuring the Athena ASEKey USB Token

PGP Universal 2.5 requires a PGP keypair on an Athena ASEKey USB token for use as a hardware Ignition Key.

To create a PGP keypair on an Athena ASEKey USB token:

- 1 Obtain an Athena ASEKey USB token.

This is the only token that can be used as a hardware Ignition Key with PGP Universal Server 2.5.
- 2 Make sure the appropriate Athena driver software is installed on your system.

The Athena driver software was included with your PGP Universal installation CDs. The filename is ASECard Crypto Toolkit 3.1b.msi; it includes the ASEKey drivers and the PKCS-11 library. However, if you do not have access to the installation CDs, you can get the driver software from the Athena website.
- 3 Once the Windows system has both PGP Desktop for Windows 9.5 and the Athena driver software installed, open PGP Desktop.
- 4 Insert the Athena ASEKey token into an available USB port on the Windows system.
- 5 You have two options for getting a PGP keypair onto your Athena ASEKey token: you can create a new PGP keypair directly on the token or you can use the Send To context menu to send an existing PGP keypair to the token.
- 6 To create a new PGP keypair on your Athena ASEKey token, from the **File** menu, select **New PGP Key**. When the PGP Key Generation Assistant appears, make sure to check the **Generate Key on Token: [name of smartcard on system]**, option, then click **Next**.
- 7 On the Name and Email Assignment screen, enter a name and an email address. (If you plan on using this PGP keypair only as an Ignition Key for PGP Universal, you can leave the **Primary Email** field empty; no email address on a keypair means no messages will be encrypted to the key nor can it be uploaded to the PGP Global Directory. You will be asked if you want to continue without an email address; click **Yes**.) Click **Next**.
- 8 On the Passphrase Assignment screen, enter the PIN of your Athena ASEKey token (which will now also be used as the passphrase for keypair); the default for Athena tokens is eight 1s (11111111); click **Next**.
- 9 PGP Desktop generates the key on the token. When the process completes, click **Next**.

- 10** On the PGP Global Directory Assistant screen, click **Skip** so that the public key is not sent to the PGP Global Directory. When PGP Desktop reappears, click **Smartcard Keys** in the PGP Keys Control box; the PGP keypair you just created appears.
 - 11** To copy an existing PGP keypair to your Athena ASEKey token, click **All Keys** in the PGP Keys Control box. Right-click the keypair you want to send to the token (it must be a 1024- or 2048-bit RSA keypair, not just a public key).
 - 12** On the context menu that appears, select **Send To > Smartcard** (if **Smartcard** is grayed out, the selected key doesn't meet the requirements to be on the token).
 - 13** A warning message explains that the passphrase for the selected keypair will change to the PIN of the token; click **OK**.
 - 14** Enter the current passphrase for the selected keypair, then click **OK**.
 - 15** Enter the PIN of the Athena ASEKey token, then click **OK**.
- The keypair is copied to the token.
- 16** As the default PIN for Athena tokens is well known, you should change it immediately.

The Athena ASEKey token now has a PGP keypair on it. It can be used as a hardware Ignition Key with a PGP Universal Server.



Setting PGP Desktop Options

Adjusting settings to suit your needs

PGP Desktop is configured to accommodate the needs of most users, but you can adjust some settings to suit your requirements. You specify these settings on the PGP Options dialog.

- [“Accessing the PGP Options dialog box” on page 227](#)
- [“General Options” on page 228](#)
- [“Keys Options” on page 229](#)
- [“Master Keys Options” on page 233](#)
- [“Messaging Options” on page 234](#)
- [“PGP NetShare Options” on page 241](#)
- [“Disk Options” on page 242](#)
- [“Notifier Options” on page 243](#)
- [“Advanced Options” on page 245](#)

Accessing the PGP Options dialog box

To access the PGP Options dialog, do one of the following:

- Click the **PGP Tray** icon in the Windows System Tray, and then select **Options...**
- Open PGP Desktop, and then from the **Tools** menu, select **PGP Options**.

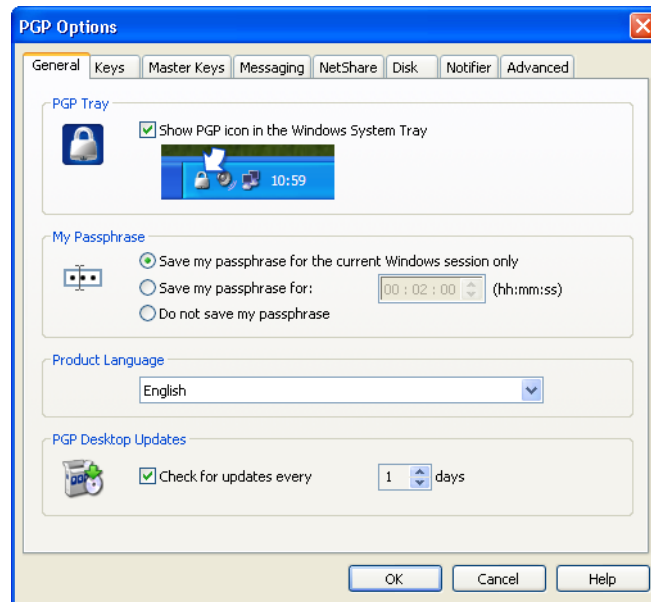
When you are finished with a particular tab, you can select another tab or click **OK** to save your changes and exit.

To cancel any changes you have made, click **Cancel**.

To get help for the fields on any tab, click **Help**.

General Options

The General tab contains a variety of PGP Desktop settings.



The options on the **General** tab are:

- **Show PGP icon in the Windows Tray.** When enabled, the PGP icon appears in the Windows Tray while PGP Desktop is active on the system. The PGP Tray icon provides easy access to PGP Desktop functions. Deselect the checkbox to remove the PGP icon from the Windows Tray. To restore the PGP icon, launch PGP Desktop, then from the **Tools** menu select **PGP Options**. Access the **General** tab, and select the checkbox.

i If you are using PGP Desktop in a PGP Universal-managed environment, this option may be required.

Removing the **PGP Tray** icon from the Windows System Tray does not shut down PGP Desktop services. PGP Desktop services continue running when the **PGP Tray** icon is removed from the Windows System Tray.

To stop PGP Services:

- Click the PGP Tray icon.
- Select **Stop PGP Services** from the list of commands that appears. A warning dialog box appears; you must confirm that this is what you intend to do.

i As a general rule, you are strongly encouraged not to stop PGP services.

- **Save my passphrase for the current Windows session only.** Automatically saves your passphrase in memory until you log off your computer. This is called **caching** your passphrase. If you enable this option, you are prompted for your passphrase once per private key. You are not prompted to type it again for the same key until you log off your computer.



When this option is enabled, it is very important that you log off your computer before leaving it unattended. Your passphrase can remain cached for weeks if you never log off, allowing anyone to read your encrypted messages, or encrypt messages with your key, while you are away from your computer. If you normally remain logged on to your computer for long periods of time, consider choosing one of the other passphrase caching options.

- **Save my passphrase for X (hh:mm:ss).** Automatically saves your passphrase in memory for the specified duration of time. If you enable this option, you are prompted for your passphrase once for the initial signing or decrypting task. You are not prompted to type it again until the specified time has elapsed. The default setting is 00:02:00 (2 minutes).
- **Do not save my passphrase.** Prevents your passphrase from being stored in memory. If you enable this option, you must type your passphrase each time it is needed.
- **Product Language.** Use this option to select the language in which the PGP Desktop user interface is presented. The options are: English (the default), German, and Japanese.



You must log off and log back in to your system if you change to a different language.

- **Check for updates every X days.** When enabled, PGP Desktop checks for software updates automatically at the specified interval. The default is one day. If a newer version of PGP Desktop is available for download, a notification screen appears that lets you download the new version.



This option requires an active Internet connection.

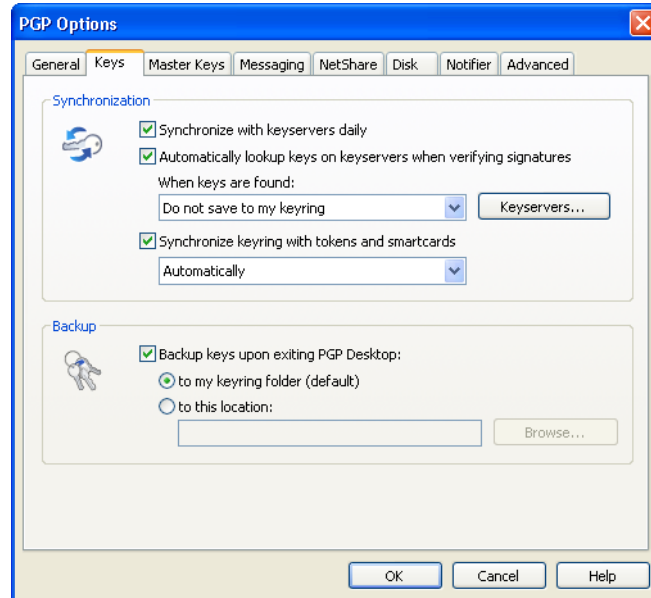
When disabled, PGP Desktop does not automatically check for software updates.



If you are using PGP Desktop in a PGP Universal-managed environment, this option may be required.

Keys Options

The Keys tab contains settings that apply to PGP Desktop keys.



The options on the Keys tab are:

- **Synchronize with key servers daily.** When selected, PGP Desktop performs a daily synchronization of the public keys on your Keyring with your list of key servers. This list includes the PGP Global Directory.

i If you are using PGP Desktop in a PGP Universal-managed environment, this option may be required.

If changed versions of the keys are available, they are downloaded automatically. If the key server notifies PGP Desktop that a key is removed from the key server, PGP Desktop disables that key on the local keyring.

If you use PGP Desktop to make a change to a keypair on your Keyring, that change is not automatically uploaded from your computer to any key server. You must manually upload the changed key to the desired key server. PGP Desktop prompts you to upload changed keys when you quit PGP Desktop. Otherwise, to send the key to the key server, right-click the changed key, select **Send To** from the shortcut menu that appears, and then select the desired key server from the list.

- **Automatically lookup keys on key servers when verifying signatures.** When this option is enabled, you can specify that PGP Desktop should search the configured key servers for a verified key if the public keys are not available in your local keyring.

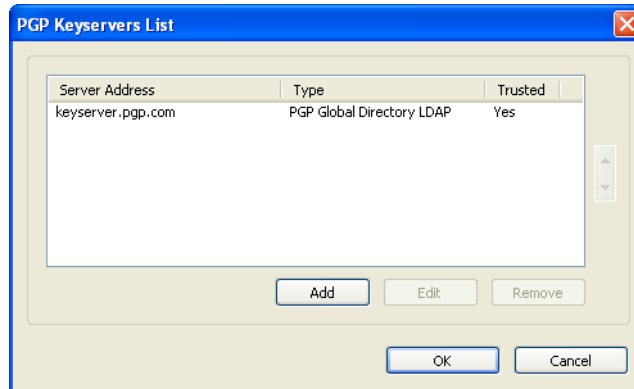
i If you are using PGP Desktop in a PGP Universal-managed environment, this option is not used. Your PGP Universal Server defines whether keys are looked up and, if found, if they are cached. Keys found in a PGP Universal-managed environment are never saved to your keyring.

If the public key is found, there are three options:

-
- **Do not save to my keyring.** Any key(s) found on the configured keyserver are used only once, to verify the signature with which you are currently working. The key is then not saved to your keyring.
 - **Ask to save to my keyring.** Specifies that PGP Desktop should ask if you want to save found keys to your local keyring.
 - **Save keys to my keyring.** Specifies that found keys are automatically saved to your local keyring.
 - **Synchronize keyring with tokens and smartcards.** Lets you specify how PGP Desktop synchronizes with smartcards and tokens:
 - **Automatically.** PGP Desktop automatically loads and uses the PKCS-11 driver from the first smartcard/token vendor it finds on your system. If you have the PKCS-11 driver from just one smartcard/token vendor installed on your system, choose this setting; PGP Desktop will automatically recognize and use smartcards/tokens from that vendor.
 - **Listed vendor.** PGP Desktop loads and uses the PKCS-11 driver from the smartcard/token vendor you select from the list. If you have the PKCS-11 drivers of more than one smartcard/token vendor on your system, use this setting to tell PGP Desktop which vendor's smartcards/tokens you want to use.
 - **Other.** Lets you select a PKCS-11 driver using the **Select Smart Card Driver** dialog that appears. When selected, PGP Desktop recognizes and uses the smartcards/tokens from the vendor whose PKCS-11 driver you select. Use this setting if you want to use the smartcards/tokens from a vendor not listed.

If the PKCS-11 library from a smartcard vendor is installed on your system and works with other PKCS-11 applications, such as Mozilla Firefox or Thunderbird, chances are high that PGP Desktop will recognize and work with smartcards from this vendor.

In those rare cases where a non-standard smartcard doesn't work with PGP Desktop, "Smart Card Keys" does not appear in the PGP Keys Control box when the smartcard is installed on the system.
 - **None.** PGP Desktop will not recognize or use any smartcard or token on your system.
 - **Keyserver.** Click to display the **PGP Keyserver List** dialog box. Use this dialog box to add, edit, or remove the list of keyserver you want to use when automatically looking up keys.
-



The PGP Keyservers List performs several functions:

- A way to add, remove, and edit keyserver settings. For more information on how to perform these tasks, see the following procedures.
 - A keyserver list that PGP Desktop uses when automatically synchronizing the keypairs on your keyring with keys listed on available keyservers.
 - Provides PGP Desktop with a list of keyservers whenever a feature needs to display a list of them—for example, the keyserver list that displays when you choose the **Send To** function for a public key.
 - Provides a list of keyservers that can be used in a PGP Messaging policy. This list is used for searching keyservers when an appropriate public key is not found on the local keyring.
- **Backup keys when exiting PGP.** When enabled, PGP Desktop automatically backs up your keys to the location you specify:
- **To my keyring folder (default).** When selected, your keys are backed up to the default keyring folder on your system. The default location is the My Documents folder.
 - **To this location.** When selected, your keys are backed up to the location on your computer that you specify. Click the **Browse** button to set a location.

To add a keyserver to the PGP Keyservers List:

- Click **Add**, type the appropriate information on the **New Server** dialog, and then click **OK**.

To edit a keyserver already on the PGP Keyservers List:

- Select the keyserver you want to edit, click **Edit**, make the desired changes on the Edit Server dialog, then click **OK**.

To remove a keyserver from the PGP Keyservers List:

- Select the keyserver you want to remove, click **Remove**, then click **OK**.
- Click **OK** on the **PGP Keyservers List** dialog to return to the **Keys** tab.

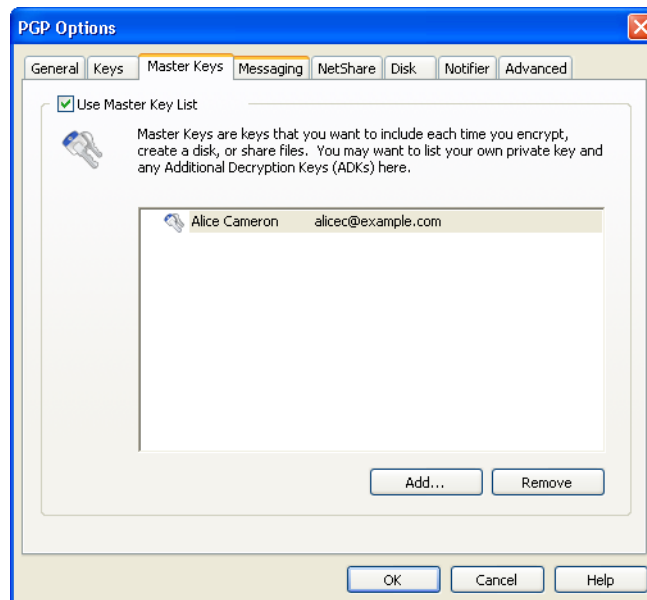
- the Edit Server dialog, then click **OK**.

To change the order in which key servers are searched when looking up keys:

- Select the keyserver you want to move and then click the up or down arrows.
- Click **OK** on the **PGP Key Servers List** dialog to return to the **Keys** tab.

Master Keys Options

The Master Key List is a set of keys that you want added by default any time you are selecting keys for messaging, disk encryption, NetShare, and PGP Zip. This saves you the step of dragging the keys that you regularly use into the **Recipients** box.



To use the Master Key List:

- Select the **Use Master Key List** checkbox. You cannot add or remove keys from the Master Key List unless this box is selected.

i If you generated your key using the Setup Assistant, the key is automatically added to the Master Key list. If you skipped key generation and imported your key, the key is not automatically added to the list.

To add keys to the Master Key List:

- 1 Click **Add**.

The **Select Master Keys** box appears.

- 2 From the **Key Source** list on the left, select the key(s) that you want to use. You can Shift-click or Ctrl-click to select multiple keys.
- 3 After selecting the keys you want, click **Add**.
- 4 If there are any keys in the **Keys to Add** list on the right that you do not want to include, select them and click **Remove**.
- 5 When you have finished selecting keys, click **OK**.

The keys you have selected appear in the Master Key List.

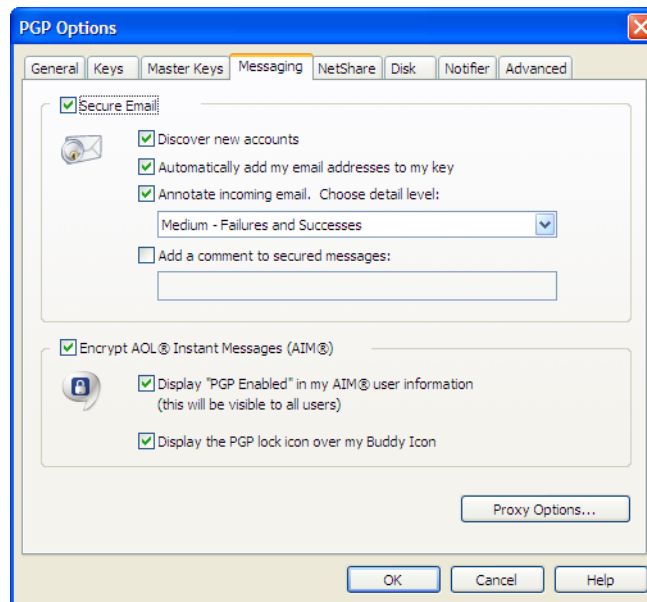
To remove keys from the Master Key List:

- 1 Select the key(s) that you want to remove. You can Shift-click or Ctrl-click to select multiple keys.
- 2 Click **Remove**.

The key(s) are removed.

Messaging Options

The Messaging tab contains settings that apply to email and IM messaging.



The options on the Messaging tab are:

- **Secure Email.** Select the **Secure Email** checkbox if you want PGP Desktop to secure all your email accounts automatically. When enabled, PGP Desktop intercepts both incoming and outgoing email messages and secures them based on the appropriate policies.

Deselect the **Secure Email** checkbox to stop PGP Desktop from securing your email accounts.

If you select the **Secure Email** checkbox, you can choose these additional options:

- **Discover new accounts.** Select this checkbox if you want PGP Desktop to monitor your email activity and automatically discover new email accounts that you are using. When a new account is discovered, PGP Desktop asks if you want to secure messages sent using that account.
- **Automatically add my email addresses to my key.** If you select this checkbox, PGP Desktop automatically adds to your key the email addresses that you use to send messages. This option is enabled by default. If you are using PGP Desktop in a PGP Universal-managed environment, this option may be disabled.

Deselect this checkbox to prevent email addresses from being automatically added to your key. This has privacy value; for example, if you wish to prevent someone from finding your email address.

- **Annotate incoming email.** Select this checkbox if you want incoming email messages to be annotated with explanatory text detailing the actions that PGP Desktop took when processing your incoming messages. You can choose three annotation levels:

Maximum: Verbose Annotation. Adds annotations to your incoming email detailing every action that PGP Desktop has taken during message processing.

Medium: Failures and Successes [this option is the default]. Provides annotations when there has been a processing failure, such as unknown key, or unknown signer. The Medium setting adds annotation when incoming email has been successfully decrypted and/or signed.

Minimum: Failures Only. Only provides annotations when there has been a processing failure.

- **Add a comment to secured messages.** When enabled, the text you type here is always included in messages you encrypt or sign. Comments typed in this field appear below the `--BEGIN PGP MESSAGE BLOCK--` text header and PGP Desktop version number of each secured message. These comments are not visible in decrypted email.



If you are using PGP Desktop in a PGP Universal-managed environment, there may already be text in this field.

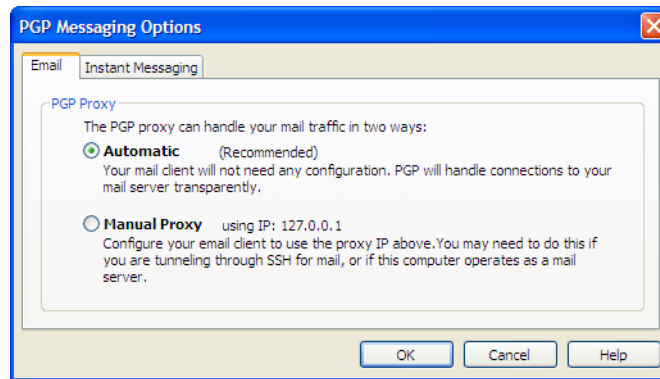
- **Encrypt AOL® Instant Messages (AIM®).** Enable if you want PGP Desktop to encrypt instant message sessions with supported instant messaging software.
AOL® Instant Messenger™ and compatible software applications are supported.
- **Display “PGP Enabled” in my AIM user information.** When selected, `PGP Enabled` is added to your screen name in such places as the AIM Buddy List and the Get Buddy Info command. When disabled, your screen name appears without `PGP Enabled`. The appearance of this text may vary depending on your instant messaging client.

- **Display the PGP lock icon over my buddy icon.** When selected, the PGP stylized lock icon appears with your buddy icon, so others can see that the IM session is protected. When disabled, your icon appears normally.

Proxy Options

Click the **Proxy Options** button to access advanced messaging options.

Email options



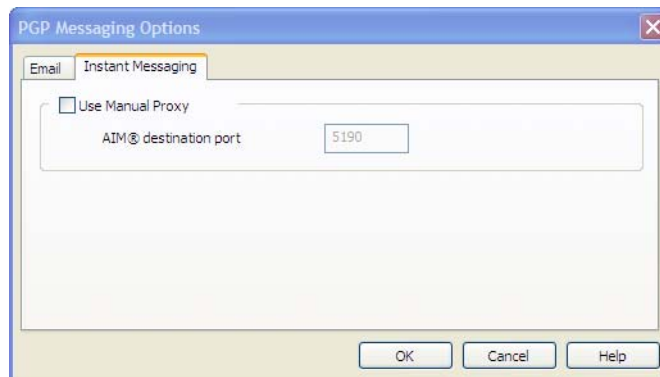
If your computer needs to have a proxy manually configured so that you can send and receive email, you would use this tab.

PGP Desktop “resides” between your email application and the mail server that provides your mail. This configuration enables PGP Desktop to filter, or *proxy*, your email traffic for you automatically. PGP Desktop can protect your messages, based on the applicable policy, without interrupting your work.

Normally, you do not need to change the PGP Proxy settings. However, some users must specify proxy settings manually. Choose the setting that your network administrator recommends:

- **Automatic.** The default, recommended setting. Your email is protected automatically and transparently. PGP Corporation recommends that you leave this option selected unless you are instructed to use the manual proxy setting.
- **Manual Proxy.** This option is needed if your computer is “tunneling” through SSH to your mail server, or if the computer on which you are running PGP Desktop also functions as a mail server. Refer to [“Configuring Manual Mode” on page 238](#) for more information.

Instant Messaging tab



If your computer is behind a network firewall, you may need to change the network port that AIM uses for your IM chat sessions. Most users do not need to change this setting.

- **Use Manual Proxy.** Select this checkbox to change the port that AIM uses for your IM sessions. Change the value to one other than the default (5190). Your network administrator can tell you if you need to change this setting, and if so, what the correct port number is.

Configuring Manual Mode

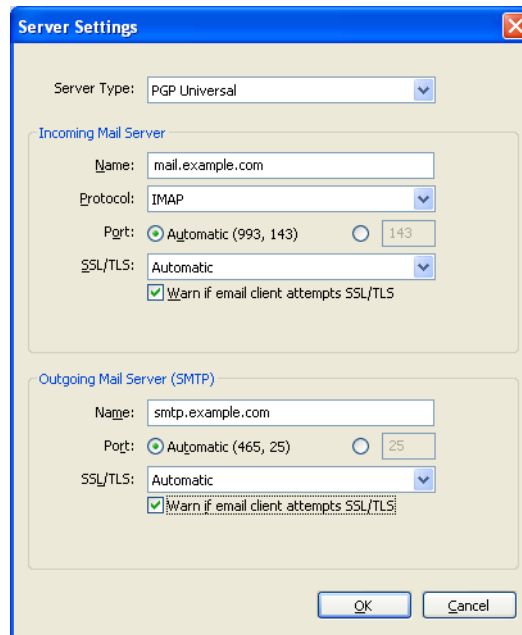
If you specify **Manual** for the email proxy, you must also configure the PGP Messaging settings, as well as some settings within your email client (ask your system administrator for the values that you should use):

- 1 In the PGP Messaging Control box, select the service for which you want to use Manual mode.

The **New Service** panel appears.

- 2 Click **Server Settings**.

The Server Settings screen for the specified service appears.



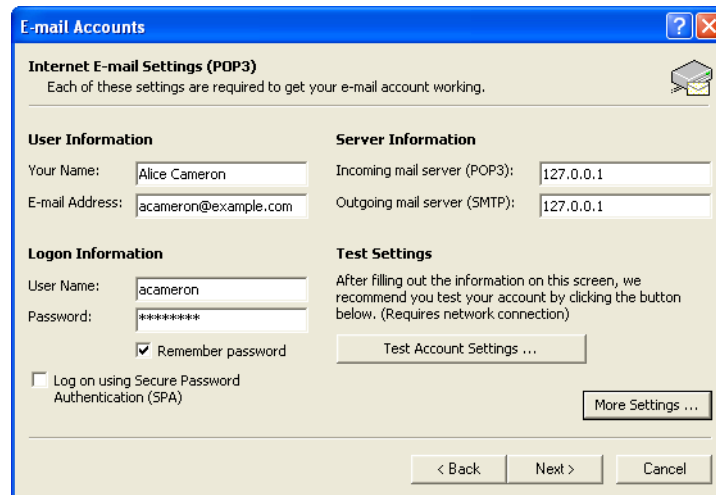
- 3 Select the type of server that the new service will be using:
 - **Internet Mail**—for standalone PGP Desktop users who have a POP or IMAP mail connections.
 - **PGP Universal**—for PGP Desktop users who are in a PGP Universal-managed environment. Contact your PGP Universal administrator for more details on correct settings.
 - **MAPI/Exchange**—for PGP Desktop users who are using Microsoft Outlook as a client on a Microsoft Exchange/MAPI server. Contact your mail administrator for more information on correct settings.
 - **Lotus Notes**—for PGP Desktop users who are using Lotus Notes as their email client with a Lotus Domino server. Contact your email administrator for more information on correct settings.
- 4 In the **Incoming Mail Server** section, type a value in the **Redirect local port X to this server** field.

PGP Desktop will monitor this port for email messages going from your mail server to your mail client.
- 5 In the **Outgoing Mail Server (SMTP)** section, type a value in the **Redirect local port X to this server** field.

PGP Desktop will monitor this port for email messages going from your mail client to your mail server.
- 6 Click **OK**.

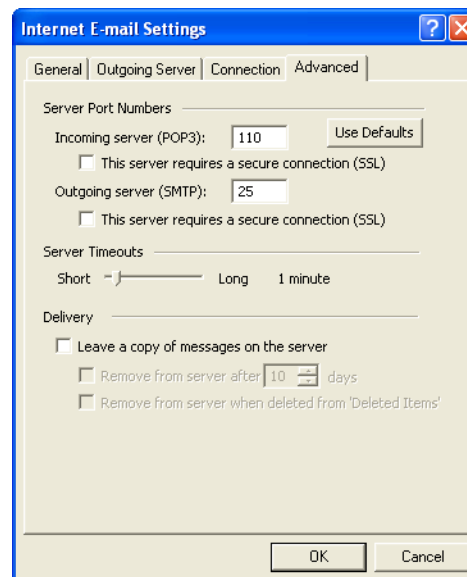
The **Server Settings** screen closes.

- 7 Open your email client and navigate to the settings for your email account (if you have multiple accounts, you will need to configure each account separately).



- 8 For both the *Incoming mail server* (POP3 or IMAP) and **Outgoing mail server (SMTP)** settings in Microsoft Outlook, type **127.0.0.1**.
- 9 Click **More Settings**.
- 10 On the Internet E-mail Settings dialog, click **Advanced**.

The **Advanced** tab of the Internet E-mail Settings dialog appears.



- 11 In the **Incoming server** (POP3 or IMAP) box, type the same value you established for the *incoming* mail server in the Redirect local port X to this server field; Step 7 of this procedure.

12 In the **Outgoing server (SMTP)** box, type the same value you established for the *outgoing* mail server in the Redirect local port X to this server field; Step 8 of this procedure.

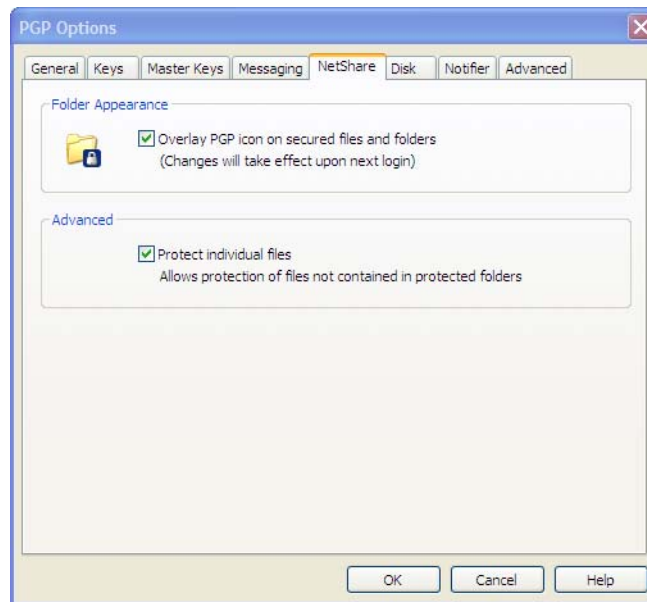
13 Click **OK**, then finish configuring the account settings.

Manual mode is configured for the selected service.


When you are done configuring Manual mode for the services, restart your computer.

PGP NetShare Options

Use the NetShare options tab to change settings when you protect shared network files.



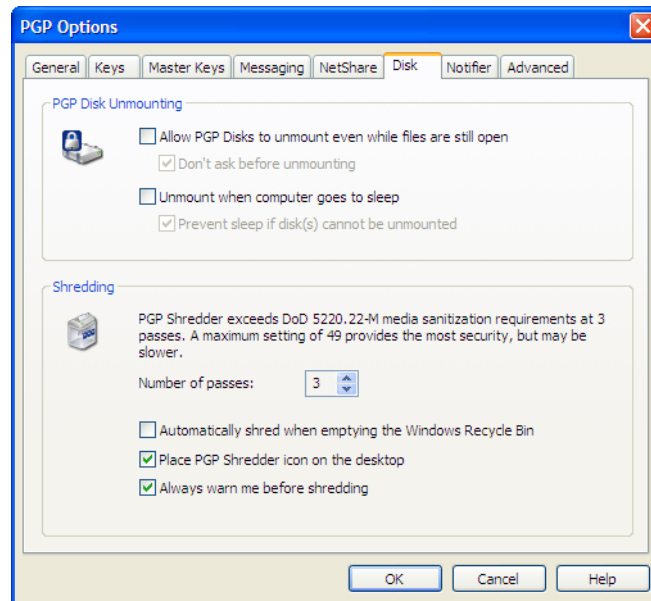
- **Folder Appearance.** Select **Overlay PGP icon on secured files and folders** if you want a small PGP lock icon to appear on files and folders that are protected using PGP NetShare.
- **Advanced.** Select **Protect individual files** to protect individual files that are outside of a Protected Folder using PGP NetShare.

 You may be prevented from selecting this option by your PGP administrator if you are using PGP Desktop in a PGP Universal-managed environment.

Refer to [“Protecting Files Outside of a Protected Folder”](#) on page 140 for more information about protecting individual files that are outside of Protected Folder using PGP NetShare.

Disk Options

The Disk tab contains settings that apply to volumes protected using the PGP Virtual Disk feature. The Disk tab also shows options for PGP Shredder.



i If you are using PGP Desktop in a PGP Universal-managed environment, these options may already be configured.

PGP Virtual Disk Options

The options for PGP Virtual Disk are:

- **Allow PGP Virtual Disks to unmount even while files are still open.** Normally, you cannot automatically unmount a PGP Virtual Disk volume if any of the files in that volume are open. Enabling this option allows unmounting even with open files (called a forcible unmount).
 - **Don't ask before unmounting** allows PGP Desktop to forcibly unmount a PGP Virtual Disk volume *without* first warning you of any files that may be open.

! You may lose data if you forcibly unmount a PGP Virtual Disk volume with open files.

- **Unmount when computer goes to sleep.** When enabled, PGP Desktop will automatically unmount any mounted PGP Virtual Disk volumes when your computer goes into any sleep modes; Standby or Hibernate, for example.
 - Enable **Prevent sleep if disk(s) cannot be unmounted** to prevent your computer from sleeping if a PGP Virtual Disk could not be unmounted.



The Windows Hibernate mode is inherently insecure, because Windows writes sensitive data to disk if your PGP Virtual Disk is open when hibernation is invoked. PGP Corporation recommends using the PGP Whole Disk Encryption feature if you use Hibernation; otherwise be sure to enable the **Unmount when computer goes to sleep** and **Prevent sleep if disk(s) cannot be unmounted** options.

PGP Shredder Options

The PGP Shredder feature offers a secure way for you to delete sensitive files. You can adjust the level of security the PGP Shredder feature offers, as well as other settings.

The options for the PGP Shredder feature are:

- **Number of passes.** The PGP Shredder feature removes your file(s) securely by deleting them normally, then using numerous "0" characters to overwrite the disk space that had been occupied by the files you just deleted.

Using this method, your files can be deleted very securely with only a few overwriting "passes." For this reason, a setting of **3** is the default, and offers an extremely high level of security, but you can adjust this setting to reflect the level of security that you desire by changing this setting.

Be aware that the cost of added security is increased time needed to shred your file(s), depending on several factors, particularly the speed of your computer's processor.

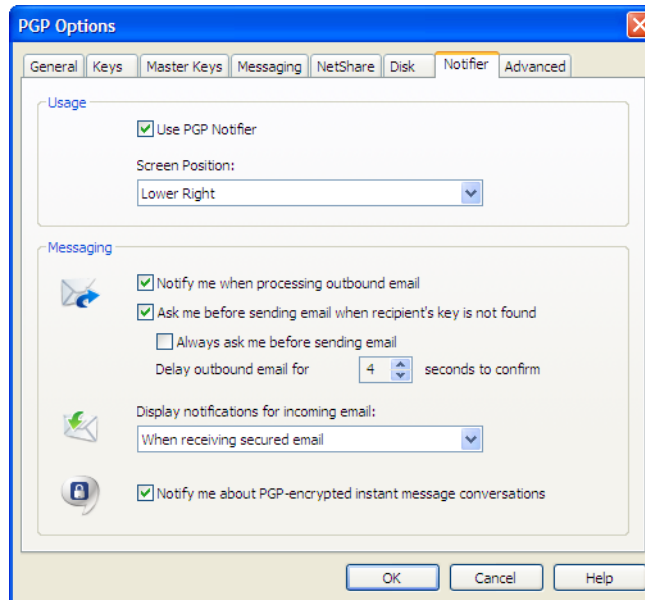
- **Automatically shred when emptying the recycle bin.** Select this checkbox to set the PGP Shredder feature to shred the contents of the Windows Recycle Bin whenever it is emptied. Use this option with care, as the PGP Shredder feature shreds all files in the Recycle Bin, whether sensitive or not, which can take time with very large files.

This automatic shredding provision uses the PGP Shredder feature settings that you have chosen, just like it does when you shred files manually.

- **Place PGP Shredder icon on the Desktop.** Select this checkbox if you would like to place an icon for the PGP Shredder feature conveniently on your computer's Desktop. Use this icon just as you do the Windows Recycle Bin icon: drag files into it. This option is selected by default.
- **Always warn me before shredding.** Select this checkbox if you would like a confirmation dialog box to appear before any shredding takes place. This gives you a chance to double-check that only the files you intended are the ones that are shredded. This option is selected by default.

Notifier Options

The **Notifier** tab contains settings that apply to the PGP Desktop Notifier feature, which displays status messages in a corner of your screen when you send or receive email messages. It also displays status messages when you use the PGP Whole Disk Encryption and the PGP NetShare features.



For more information on the PGP Desktop Notifier feature, see [“PGP Desktop Notifier alerts” on page 19](#).

Usage Options

To enable notifiers, select **Use PGP Notifier**.

Determine where you want Notifiers to appear.

- **Screen Position:** PGP Desktop Notifications can appear at any of the four corners of your screen. Select the corner that you would like PGP Desktop Notifications to appear.

Messaging Options

The settings for the PGP Desktop Notifier feature are:

- **Notify when processing outbound email:** Select this checkbox if you want PGP Desktop Notifiers to appear, informing you of encryption and/or signing status when you send mail. Deselect this checkbox to stop PGP Desktop Notifiers from appearing when you send mail.
- **Ask me before sending email when the recipient's key is not found:** PGP Desktop looks for a public key for every recipient of the email messages that you send. By default, if it cannot find a public key for a recipient, it sends that email in the clear (without encryption). If you select this Notifier option, you are notified that this is the case, and given a chance to block the email so that it is not sent.

(For more information on the PGP Desktop default policy settings, see [“Services and Policies” on page 27](#).)

- **Always ask me before sending email:** You can select this checkbox if you would prefer approving every email that you send. You can review the encryption status in the Notifier, and either send or block the email.
- **Delay outbound email for n second(s) to confirm** (where n is a number from 1-30). To change the amount of time that outbound messages are delayed, and a PGP Desktop Notifier is displayed, click the up or down arrows. Use the delay period to review the PGP Desktop Notifier message.

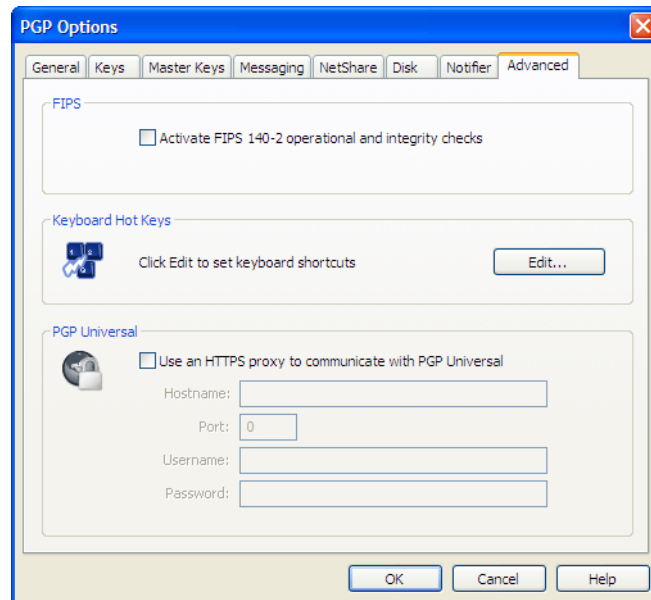
If you want the message to be sent, do nothing. The message is sent as soon as the delay period is met.

If you want a closer look at the notification, move your cursor over it. The PGP Desktop Notifier changes from translucent to opaque in appearance, and the outbound message is delayed while your cursor is over the notification message. Click **More** to view information on the encrypted/signed status of the message. If recipient's keys are not found, two additional buttons are available: **Block** and **Send**. Click **Block** if you want to stop the message from being sent. Click **Send** if you want to send the message unencrypted.

- **Display notifications for incoming mail:** For incoming email, you can choose the extent to which you are notified of its status upon arrival. Your choices are:
 - **When receiving secured email**—A Notifier appears whenever you receive secured email. The box displays who the email is from, its subject, its encryption and verification status, and the email address of the person sending it.
 - **Only when message verification fails**—For incoming email, you see a Notifier only when PGP Desktop is unable to verify the signature of the incoming email.
 - **Never**—If you do not need or want to see a Notifier as you receive email, select this option. This option does not affect Notifiers for outgoing mail.
- **Notify for status of PGP Encrypted IM sessions**—Select this checkbox if you want a PGP Desktop Notifier to appear briefly when you begin a secure instant message chat, and appear briefly again when the chat ends.

Advanced Options

The PGP Options Advanced settings tab provides settings that are very specific. Most users do not need to change these settings.



FIPS

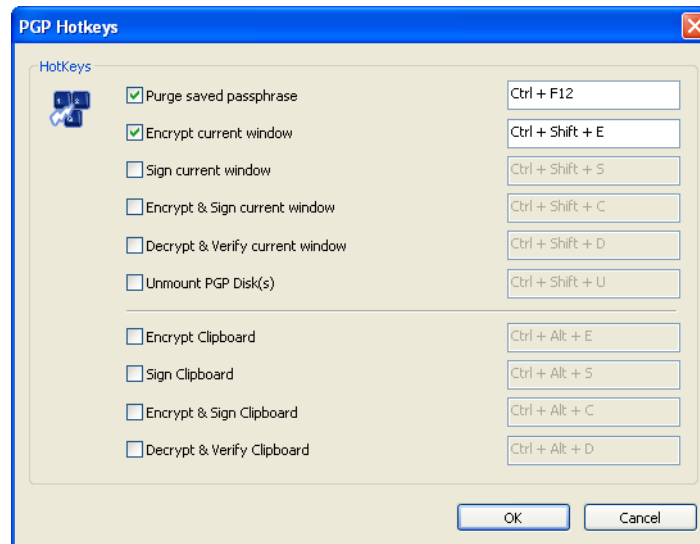
- **Activate FIPS 140-2 operational and integrity checks.** Select this option if you or your organization require FIPS 140-2 checks, but be aware that it slows down your computer's performance. You must reboot your computer for this setting to take effect.

Keyboard Hot Keys

- PGP Desktop offers many ways you can create custom hot keys to help you work faster and more easily. A set of hot keys comes pre-configured with PGP Desktop, but you can change these hot key assignments to suit your needs.

To change keyboard hot key assignments:

- Click **Edit** to display the PGP Hotkeys dialog.



- Select the check box next to the hotkey you want to edit and then make any changes in the edit field.

PGP Universal

- **Use an HTTPS proxy to communicate with PGP Universal.** Do not change these settings unless you are instructed to by your network administrator.

If your PGP Universal installation requires a secure client/server connection via a proxy, you can use these option settings to specify that. Your administrator can supply you with the server name, the correct communications port, your user ID, and your password, so you can configure this section correctly.

B

Passwords and Passphrases

This appendix describes the differences between passwords and passphrases, tells you about the **Passphrase Quality Bar** in PGP Desktop, and provides some guidelines for creating strong passphrases.

Passwords and Passphrases

Passwords and passphrases are used to protect things. In general, passphrases are longer and use a wider variety of characters than do passwords.

For example, a simple password might be four-letter two words concatenated: "whenjobs" without the quotes. A stronger password could use uppercase characters as well: WhenJobs. A stronger yet password could add numbers: When9Jobs4.

Passphrases, in comparison, are longer and use a wider variety of characters. For example, a simple passphrase might be: "Mb&1a>ttA." without the quotes, but including the period. This passphrase might seem difficult to remember easily, but in fact it's based on a simple phrase that is much easier to remember.

Passphrases can also be simple phrases, perhaps from a familiar book, that include the punctuation and capitalization: "Because that's not golf, I replied" including the quotes. Although this may not seem like a strong passphrase, it is in fact at least twice as strong as any of the other examples.

Choosing whether to use a password or passphrase

So how do you know whether to choose a password or a passphrase? It depends on what you are trying to protect. The more valuable the information you are protecting, the stronger the protection should be.

Most Word documents are not protected at all; the content is not valuable. When you access your bank account online, some banks require only a four-letter PIN; depending on the amount of money in that account, this very well may be very poor security. You may use a free Hotmail email account for unimportant correspondence; a simple password is adequate security. With your corporate email account you send and receive proprietary product, customer, or financial information.

With PGP Desktop, for example, you create passphrases for both your PGP keypair and for your PGP Virtual Disk volumes. If you create a weak passphrase for your PGP keypair, and an attacker managed to get physical control of your private key file, all they would need to do to be able to read your messages and send messages that appear to be coming from you would be to figure out that passphrase.

The Passphrase Quality Bar

When you create passphrases in PGP Desktop, the Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating. Nevertheless, it is a much better guideline than just number of characters.

In general, the longer the bar, the stronger the passphrase. But what does the length of the Passphrase Quality bar actually mean?

The Passphrase Quality bar compares the amount of randomness (entropy) in the passphrase you enter against a true 128-bit random string (the same amount of entropy in an AES128 key). This is called 128 bits of entropy.

(Entropy is a measure of the difficulty in determining a password or key.)

So if the passphrase you create fills up approximately half the Passphrase Quality bar, then that passphrase has approximately 64 bits of entropy. And if your passphrase fills the Passphrase Quality bar, then that passphrase has approximately 128 bits of entropy.

So how strong is 128 bits of entropy? In the late 1990s, specialized "DES cracker" computers were built that could recover a DES key in a few hours by trying all possible key values.

Assuming you could build a computer that could recover a DES key in one second (the computer would have to be able to try 2^{55} keys per second), then it would take that computer approximately 149 trillion (thousand billion) years to crack one 128-bit AES key. In comparison, the universe is believed to be less than 20 billion years old.

How is the entropy of a particular character measured? The answer is, the bigger the pool of characters there is to choose from when picking a particular character, the more entropy is assigned to the chosen character.

For example, if you are told to choose a numeric PIN, you are restricted to the numbers zero through nine; a total of 10 characters. This is a rather small pool, so the entropy for a chosen character is relatively low.

When you are choosing a passphrase using the English version of PGP Desktop, however, things are different. You have three pools of characters to choose from: uppercase and lowercase letters (52 characters), numbers zero through nine (10 characters), and the punctuation characters on a standard keyboard (32 characters).

When you enter a character, PGP Desktop determines the entropy value for that character based on the pool it is in and applies that value to the Passphrase Quality bar.

The same concept applies to the character sets of other languages; the larger the pool, the more entropy per character. So if you were using an Asian or Arabic character set, for example, some of which have hundreds of characters in the set, the amount of entropy for a selected character would be correspondingly higher, and thus fill up the Passphrase Quality bar that much faster.

Creating Strong Passphrases

Creating a good passphrase is a trade-off between ease of use and strength of the passphrase. Longer passphrases, with a mixture of uppercase and lowercase letters, numbers, and punctuation characters, are stronger, but they are also harder to remember.

Studies have shown that passphrases that are harder to remember are more frequently written down, which defeats the purpose of having a strong passphrase. It's better to have a somewhat shorter strong passphrase that you will remember than a longer strong passphrase that you will write down or forget.

One common system for generating strong passphrases takes a phrase and reduce it to individual characters. For example, the phrase:

My brother and I are greater together than apart.

becomes the passphrase:

Mb&1a>ttA.

This passphrase has 10 characters, and is a mix of uppercase and lowercase letters, numbers, and punctuation characters. At 10 characters, this is a relatively short passphrase. If you think 10 characters is not enough, consider either creating another passphrase using the same method and then use both together or simply use a longer phrase to start with.

Another approach is to use simple phrases that include punctuation and capitalization. For example:

"Edited by John Doe (not John Doe, Editor)"

While not overly long or complicated, this is a strong passphrase. If you decide to use a phrase from a familiar book, make sure not to lose the book.

When creating a passphrase in PGP Desktop, you can use up to 255 characters, including spaces.

Another approach is to concatenate many short, common words. A method called Diceware™ uses dice to select words at random from a special list called the Diceware Word List, which contains 7776 short English words, abbreviations, and easy-to-remember character strings. If you put together enough of these, you can create a strong passphrase. The Diceware FAQ states you may achieve 128 bits of entropy using a 10-word Diceware passphrase.

Refer to <http://world.std.com/~reinhold/diceware.html> for more information about Diceware.

When it comes to creating passphrases, here are some things you should do:

- Use a phrase that is in your long-term memory. You are less likely to forget it that way.
- Make your passphrase at least eight characters long. Length is not the best indicator of strength, but it's still better than shorter.

- Use a mixture of uppercase and lowercase letters, numbers, and punctuation characters.



Try to use only ASCII characters, if possible. This is particularly important when using international keyboards, as some special characters are not supported (for example, “\$”) in passphrases.

- Change your passphrase on a regular basis; every three months is a good rule of thumb. The longer you use the same passphrase, the more time there is for someone to figure it out.

Here are some things you should **not** do when creating passphrases:


- Don't write down your passphrase.
- Don't give your passphrase to anyone.
- Don't let anyone see you entering your passphrase.
- Don't use “password” or “passphrase.”
- Don't use patterns. Not “abcdefgh” or “12345678” or “qwertyui” or “88888888” or “AAAAAAAA.”
- Don't use common words. Almost any skilled attacker is using a password-cracking dictionary that tries regular words. Don't put two common words together, don't use the plural of a common word, don't use a common word with the first letter capitalized.
- Don't use numbers that pertain to you. If anyone knows these numbers, then an attacker could find out. Don't use your birthday, your phone number, your social security number, or your street address.
- Don't use names. Not the names of people, not the names of fictional characters, not your pet's name. Not where you vacationed last winter, not your login name, not your company's name. Not your favorite team's name, not a body part, not a name from any book, especially the Bible.
- Don't use any of the above backwards, or with a preceding or following single digit.



PGP Desktop and PGP Universal

Using PGP Desktop in a PGP-Universal Managed Environment

This appendix describes how using PGP Desktop is different in a PGP Universal-managed email domain.


 If you are using PGP Desktop outside of a PGP Universal-managed email domain, this appendix does not apply to you.

PGP Universal allows enterprises to automatically and transparently (to end users) protect email messages based on configurable policies the PGP administrator establishes to enforce the organization's security policies. PGP Universal also lets PGP administrators manage PGP Desktop deployments to users in their organization. Refer to www.pgp.com/products/universal/index.html for more information about PGP Universal.

Using PGP Desktop in a PGP Universal-managed environment gives you proven PGP encryption technology all the way to your desktop, plus the other security features in PGP Desktop: PGP Whole Disk Encryption, PGP Virtual Disk volumes, PGP Zip archives, and PGP Shred, among others.

Overview

To use PGP Desktop in a PGP Universal-managed environment, you must install PGP Desktop using an installer application you receive from your PGP administrator.

 If you obtained your PGP Desktop installer from a different source, you should check with your PGP administrator **before** installing or using that version of PGP Desktop.

Your PGP Desktop installer will have been configured by your PGP administrator in one of the following ways:

- **No policy settings.** Your copy of PGP Desktop will not have any built-in settings; you can use any feature your license supports.
- **Auto-detect policy settings.** Your copy of PGP Desktop will contact the PGP Universal Server that created the installer and download the appropriate settings. The settings it receives may require you to use PGP Desktop features in specific ways.
- **Preset policy settings.** Your copy of PGP Desktop will have the appropriate settings built in. These settings may require you to use PGP Desktop features in specific ways.

The result of your copy of PGP Desktop receiving settings from a PGP Universal Server means you may have to use PGP Desktop features in specific ways. This includes:

- You may have to take certain actions when you install PGP Desktop: you may have to whole disk encrypt your boot drive or create a PGP Virtual Disk volume, for example.
- You may be allowed or required to use PGP Desktop features in certain ways: you may be required to encrypt your AIM instant messaging sessions or you may be allowed to automatically shred files when deleting them, for example.
- You may be prevented from using certain PGP Desktop features: you may be prevented from using conventional encryption and creating self-decrypting archives (SDAs), for example.
- You may be required to use to certain messaging policies: you may have to encrypt and sign messages to certain email domains, for example.

Those features of PGP Desktop that can be managed by a PGP administrator in a PGP Universal-managed environment are noted in their descriptions throughout this User's Guide.

Contact your PGP administrator for more information about the differences when using PGP Desktop in a PGP Universal-managed environment.

For PGP Administrators

If you are a PGP administrator managing the rollout of PGP Desktop to some or all users in your organization, PGP Corporation recommends you allow your PGP Desktop users to manage their own keys, called Client Key Mode.

When you are preparing to create the PGP Desktop installers on your PGP Universal Server, you can control whether your PGP Desktop users are able to manage their own keys, Client Key Mode, or whether the PGP Universal Server will manage their keys, called Server Key Mode.

These settings are established in the Key Management section of the Key Setup: Default screen, which is part of the configuration of the default user group policy for internal users (**User Group > Policy Options > Key Setup: Default** in the PGP Universal Server's administrative interface).

For PGP Desktop users, Client Key Mode is the better choice because:

- Many PGP Desktop features require the user to have control of their private key. If the PGP Universal Server is managing that private key, those features will be unavailable to your PGP Desktop users.
- If you specify Server Key Mode, certain options you pre-configure for your PGP Desktop users will not be available. For example, the automatic creation of PGP Virtual Disks is not possible.

D

Messaging with Lotus Notes and MAPI

This appendix describes how to configure PGP Desktop messaging policies to support Lotus Notes and MAPI email clients in a PGP Universal-protected environment.

Topics in this chapter include:

- [“About Lotus Notes and MAPI Support” on page 255](#)
- [“Using PGP Desktop with Lotus Notes” on page 255](#)
- [“Binding to a Universal Server” on page 256](#)
- [“Notes IDs” on page 258](#)
- [“Notes Client Settings” on page 258](#)

About Lotus Notes and MAPI Support

Once set up correctly, PGP Desktop messaging with Lotus Notes and MAPI email clients in a PGP Universal-protected environment works the same as with POP or IMAP email clients, as described in [Chapter 4, Securing Email Messages](#). The information in this appendix supplements the information in that chapter.

Lotus Notes is a groupware application that supports messaging, calendaring, and scheduling capabilities. Lotus Notes email clients version 5.x and above are supported by PGP Desktop.

MAPI (Messaging Application Programming Interface) is a messaging architecture and a client interface used in Microsoft Exchange environments.

Lotus Notes and MAPI support in PGP Desktop means you get your messaging protected by PGP technology while using your existing email client, plus the other features Lotus Notes and MAPI make available to you.

Using PGP Desktop with Lotus Notes

This section provides an overview of the interoperability of PGP Desktop and PGP Universal in a Lotus Notes environment.

Sending email to recipients inside your Lotus Notes organization

Within the Lotus Notes environment PGP Desktop supports the use of both SMTP and Notes ID addressing.

Using Notes ID Addresses

Lotus Notes clients using PGP Desktop can use Notes IDs for key lookup. When a Lotus Notes email client sends an email, the PGP Desktop client recognizes this and automatically adds the Notes ID to the key. This key is then synchronized with PGP Universal to facilitate the lookup of keys by Notes ID.

All PGP Universal Server keys have an SMTP email address associated with them (for example, josem@example.com). The keys of internal Lotus Notes email client users have their Notes ID on their key in addition to a SMTP email address: CN=josem/O=notes6@notes6, for example. (External users will never have a Notes ID on their key, as contact with external users is always using their SMTP email addresses.) The keys of internal Lotus Notes email client users have both addresses, the SMTP email address and the Notes ID, because requests for the key from PGP Universal Satellite for Windows could specify either address.

Using SMTP Addresses to a recipient with PGP Desktop

Lotus Notes clients using PGP Desktop can use SMTP IDs for key lookup inside the organization. Some Lotus Notes enterprises utilize SMTP IDs for all internal communication, while others offer their employees a choice. PGP Desktop interoperates within both configurations. In this scenario Lotus Notes typically constructs the email in MIME and the PGP Desktop Proxy performs S/MIME.

Sending email to recipients outside your Lotus Notes organization

Lotus Notes clients using PGP Desktop will use SMTP IDs for email routing and key lookup outside the organization. PGP Desktop interoperates within both configurations. In this scenario Notes constructs the email in MIME and the PGP Desktop proxy performs S/MIME. The recipient receives and decrypts the email.

Binding to a Universal Server

When using Lotus Notes or MAPI email clients with PGP Desktop *in a PGP Universal-protected environment*, there may be an extra setup step required because both Lotus Notes and MAPI email clients must directly connect to their Domino or Exchange mail servers, respectively.

This section does not apply if you are using PGP Desktop standalone; that is, outside of a PGP Universal-protected environment.

In addition to communicating with their mail servers, they must also have a relationship with their PGP Universal Server. Both requirements are met by having a policy for the respective mail server and a second policy that includes both the mail server and the PGP Universal Server.

This is called binding, and it allows your email client to access its mail server to send and receive mail and its PGP Universal Server to get keys and policies. As mentioned, binding is achieved through PGP Desktop messaging policies.

There are two ways the necessary PGP Desktop messaging policies can be created to support binding: pre-binding and manual binding.

Pre-Binding

With pre-binding, the PGP administrator configures the PGP Desktop installer with the information needed to create the binding in the PGP Desktop messaging policies. So with pre-binding, the right policies come configured in PGP Desktop.

Manual Binding

With manual binding, the PGP administrator does not configure the PGP Desktop installer with the information needed to create the binding in the PGP Desktop messaging policies; you have to create these policies yourself.

To manually bind a mail server and a PGP Universal Server, you must first create a service for the PGP Universal Server and then create another service for the mail server that includes a reference to the PGP Universal Server.

To manually bind a mail server and a PGP Universal Server using PGP Desktop messaging policies:

- 1 Open PGP Desktop.
- 2 Click the PGP Messaging Control Box.
- 3 Under existing standalone service, click **Universal Server <none>** and select **Create new**.
- 4 In the New PGP Universal Service menu, type your Universal Server name and click **OK**.
- 5 Using your email client, send yourself a message. For MAPI users, doing this may not be necessary. If not, go to step 8.
- 6 Click **OK** in the **Operation stopped by your request** dialog box.
- 7 From your in-box, read the email from "PGP Universal."
A PGP Key Generation Wizard dialog box appears.
- 8 Click **Next**.
- 9 Choose a **Key Mode** from the **Key Management Selection**, then click **Next**.
- 10 In **Key Source Selection**, choose **PGP Desktop key**, if you are using PGP Desktop as a standalone application. Otherwise, select **New key** or **Import Key**.
- 11 Click **Next**.
- 12 Select the key set and click **Next**.
- 13 Click **Finish**.

Notes IDs

PGP Desktop keys generally have at least one SMTP email address associated with them: **josem@example.com**, for example.

The PGP Desktop keys of Lotus Notes email client users in a PGP Universal-managed environment have their Notes ID on their key in addition to a SMTP email address: **CN=josem/O=notes6@notes6**, for example. (Standalone PGP Desktop users do not have a Notes ID on their key; they always use their SMTP email addresses.)

If you are using PGP Desktop and a Lotus Notes email client in a PGP Universal-managed environment and want to know more information, contact your PGP administrator.

Notes Client Settings

If you are using PGP Desktop with a Lotus Notes email client, you need to make sure that on the Home/Mail Server Setting field of your email client's location record, the Servers tab has the full Notes name (host/orgName), and not just the WINS host.

If you're composing email in Rich Text Format in Lotus Notes, note that PGP Desktop will not use S/MIME encryption to secure the message, even if your policy requires S/MIME encryption. Instead, it will use another encryption method, such as PGP/MIME or PGP-Partitioned.

Glossary

AES (Advanced Encryption Standard)	The NIST-approved encryption standard. The underlying cipher is Rijndael, a block cipher designed by Joan Daemen and Vincent Rijmen. The AES replaces the previous standard, the Data Encryption Standard (DES).
algorithm (encryption)	A set of mathematical rules (logic) used in the processes of encryption and decryption.
algorithm (hash)	A set of mathematical rules (logic) used in the processes of message digest creation and key/signature generation.
anonymity	Of unknown or undeclared origin or authorship, concealing an entity's identification.
ANSI (American National Standards Institute)	Develops standards through various Accredited Standards Committees (ASC). The X9 committee focuses on security standards for the financial services industry.
ASCII-armored text	Binary information that has been encoded using a standard, printable, 7-bit ASCII character set, for convenience in transporting the information through communication systems. In the PGP program, ASCII armored text files are given the default filename extension, and they are encoded and decoded in the ASCII radix-64 format.
asymmetric keys	A separate but integrated user key-pair, comprised of one public key and one private key. Each key is one way, meaning that a key used to encrypt information can not be used to decrypt the same data.
authentication	The determination of the origin of encrypted information through the verification of someone's digital signature or someone's public key by checking its unique fingerprint.
authorization certificate	An electronic document to prove one's access or privilege rights, also to prove one is who they say they are.
authorization	To convey official sanction, access or legal power to an entity.
backdoor	A cipher design fault, planned or accidental, which allows the apparent strength of the design to be easily avoided by those who know the trick. When the design background of a cipher is kept secret, a back door is often suspected.
blind signature	Ability to sign documents without knowledge of content, similar to a notary public.
block cipher	A symmetric cipher operating on blocks of plain text and cipher text, usually 64 bits.
CA (Certificate Authority)	A trusted third party (TTP) who creates certificates that consist of assertions on various attributes and binds them to an entity and/or to their public key.

CAST	A 64-bit block cipher using 64-bit key, six S-boxes with 8-bit input and 32-bit output, developed in Canada by Carlisle Adams and Stafford Tavares.
certificate (digital)	An electronic document attached to a public key by a trusted third party, which provides proof that the public key belongs to a legitimate owner and has not been compromised.
certification	Endorsement of information by a trusted entity.
certify	To sign another person's public key.
certifying authority	One or more trusted individuals who are assigned the responsibility of certifying the origin of keys and adding them to a common database.
ciphertext	Plaintext converted into a secretive format through the use of an encryption algorithm. An encryption key can unlock the original plaintext from ciphertext.
clear-signed message	Messages that are digitally signed but not encrypted.
clear text	Characters in a human readable form or bits in a machine-readable form (also called plain text).
common access cards (CACs)	Read-only smartcards used by the U.S. Department of Defense. CACs include two separate certificates, one for signing and one for encrypting. PGP Desktop filters the two certificates based on intended usage; for example, only the signing certificate is presented on the file signing dialog.
compression function	A compression function takes a fixed-sized input and returns a shorter, fixed sized output.
conventional encryption	Encryption that relies on a common passphrase instead of public-key cryptography. The file is encrypted using a session key, which encrypts using a passphrase you will be asked to choose.
corporate signing key	A public key that is designated by the security officer of a corporation as the system-wide key that all corporate users trust to sign other keys.
cryptanalysis	The art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.
cryptography	The art and science of creating messages that have some combination of being private, signed, unmodified with non-repudiation.
cryptosystem	A system comprised of cryptographic algorithms, all possible plain text, cipher text, and keys.
data integrity	A method of ensuring information has not been altered by unauthorized or unknown means.
decryption	A method of unscrambling encrypted information so that it becomes legible again. The recipient's private key is used for decryption.
DES (Data Encryption Standard)	A 64-bit block cipher, symmetric algorithm also known as Data Encryption Algorithm (DEA) by ANSI and DEA-1 by ISO. Widely used for over 20 years, adopted in 1976 as FIPS 46.

dictionary attack	A calculated brute force attack to reveal a password by trying obvious and logical combinations of words.
Diffie-Hellman	The first public key algorithm, invented in 1976, using discrete logarithms in a finite field.
direct trust	An establishment of peer-to-peer confidence.
digital signature	See signature.
encryption	A method of scrambling information to render it unreadable to anyone except the intended recipient, who must decrypt it to read it.
entropy	In cryptography, a measure of randomness. It specifically relates to the difficulty in determining a passphrase or key. The greater the amount of entropy, the more difficult something is to determine. For example, if you were to pick a number from zero to 9, you would have a one in 10 chance, which works out to certain amount of entropy. If you were to pick a letter in the English alphabet, from A to Z, then you would have a one in 26 chance, a far greater amount of entropy.
fingerprint	A uniquely identifying string of numbers and characters used to authenticate public keys. This is the primary means for checking the authenticity of a key. See Key Fingerprint.
FIPS (Federal Information Processing Standard)	A U.S. government standard published by NIST.
firewall	A combination of hardware and software that protects the perimeter of the public/private network against certain attacks to ensure some degree of security.
hash function	A one way function that takes an input message of arbitrary length and produces a fixed length digest.
hierarchical trust	A graded series of entities that distribute trust in an organized fashion, commonly used in ANSI X.509 issuing certifying authorities.
HTTP (HyperText Transfer Protocol)	A common protocol used to transfer documents between servers or from a server to a client.
hexadecimal	Hexadecimal describes a base-16 number system. That is, it describes a numbering system containing 16 sequential numbers as base units (including 0) before adding a new position for the next number. (Note that we're using "16" here as a decimal number to explain a number that would be "10" in hexadecimal.) The hexadecimal numbers are 0-9 and then use the letters A-F.
IDEA (International Data Encryption Standard)	A 64-bit block symmetric cipher using 128-bit keys based on mixing operations from different algebraic groups. Considered one of the strongest algorithms.
implicit trust	Implicit trust is reserved for keypairs located on your local keyring. If the private portion of a keypair is found on your keyring, PGP Desktop assumes that you are the owner of the keypair and that you implicitly trust yourself.

integrity	Assurance that data is not modified (by unauthorized persons) during storage or transmittal.
introducer	A person or organization who is allowed to vouch for the authenticity of someone's public key. You designate an introducer by signing their public key.
ISO (International Organization for Standardization)	Responsible for a wide range of standards, like the OSI model and international relationship with ANSI on X.509.
key	A digital code used to encrypt and sign and decrypt and verify messages and files. Keys come in keypairs and are stored on keyrings.
key escrow/recovery	A practice where a user of a public key encryption system surrenders their private key to a third party thus permitting them to monitor encrypted communications.
key exchange	A scheme for two or more nodes to transfer a secret session key across an unsecured channel.
key fingerprint	A uniquely identifying string of numbers and characters used to authenticate public keys. For example, you can telephone the owner of a public key and have him or her read the fingerprint associated with their key so you can compare it with the fingerprint on your copy of their public key to see if they match. If the fingerprint does not match, then you know you have a bogus key.
key ID	A legible code that uniquely identifies a keypair. Two keypairs may have the same user ID, but they will have different Key IDs.
key length	The number of bits representing the key size; the longer the key, the stronger it is.
key management	The process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic key to authorized recipients in a secure manner.
keypair	A public key and its complimentary private key. In public-key cryptosystems, like the PGP program, each user has at least one keypair.
keyring	A set of keys. Each user has two types of keyrings: a private keyring and a public keyring.
key splitting or "secret sharing"	The process of dividing up a private key into multiple pieces, and share those pieces among a group of people. A designated number of those people must bring their shares of the key together to use the key.
LDAP (Lightweight Directory Access Protocol)	A simple protocol that supports access and search operations on directories containing information such as names, phone numbers, and addresses across otherwise incompatible systems over the Internet.
MD5 (128 bits)	A legacy hash algorithm provided only for backwards compatibility. Deprecated.

message digest	A compact “distillate” of your message or file checksum. It represents your message, such that if the message were altered in any way, a different message digest would be computed from it.
meta-introducer	A trusted introducer of trusted introducers.
MIME (Multipurpose Internet Mail Extensions)	A freely available set of specifications that offers a way to interchange text in languages with different character sets, and multimedia email among many different computer systems that use Internet mail standards.
non-repudiation	Preventing the denial of previous commitments or actions.
one-way hash	A function of a variable string to create a fixed length value representing the original pre-image, also called message digest, fingerprint, message integrity check (MIC).
passphrase	An easy-to-remember phrase used for better security than a single password. A passphrase can generally use non-alphanumeric characters such as *, +, or ~. Because passphrases are generally longer than passwords and use a wider variety of characters, they are more secure than passwords.
password	A sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification. Passwords are generally restricted to letters and numbers.
PGP/MIME	An IETF standard (RFC 2015) that provides privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC1847, currently deployed in PGP 5.0 and later versions.
PKCS (Public Key Cryptography Standards)	A set of de facto standards for public key cryptography developed in cooperation with an informal consortium (Apple, DEC, Lotus, Microsoft, MIT, RSA, and Sun) that includes algorithm-specific and algorithm-independent implementation standards. Specifications defining message syntax and other protocols controlled by RSA Data Security, Inc.
PKI (Public Key Infrastructure)	A widely available and accessible certificate system for obtaining an entity's public key with some degree of certainty that you have the “right” key and that it has not been revoked.
plaintext	Normal, legible, un-encrypted, unsigned text.
private key	The secret portion of a keypair; used to sign and decrypt information. A user's private key should be kept secret, known only to the user.
private keyring	A set of one or more private keys, all of which belong to the owner of the private keyring.
public key	One of two keys in a keypair-used to encrypt information and verify signatures. A user's public key can be widely disseminated to colleagues or strangers. Knowing a person's public key does not help anyone discover the corresponding private key.
public keyring	A set of public keys. Your public keyring includes your own public key(s).

public-key cryptography	Cryptography in which a public and private keypair is used, and no security is needed in the channel itself.
random number	An important aspect to many cryptosystems, and a necessary element in generating a unique key(s) that are unpredictable to an adversary. True random numbers are usually derived from analog sources, and usually involve the use of special hardware.
revocation	Retraction of certification or authorization.
RFC (Request for Comment)	An IETF document, either FYI (For Your Information) RFC sub-series that are overviews and introductory or STD RFC sub-series that identify and specify Internet standards. Each RFC has an RFC number by which it is indexed and by which it can be retrieved (www.ietf.org).
Rijndael	A block cipher designed by Joan Daemen and Vincent Rijmen, chosen as the new Advanced Encryption Standard (AES). It is considered to be both faster and smaller than its competitors. The key size and block size can be 128-bit, 192-bit, or 256-bit in size and either can be increased by increments of 32 bits.
RIPMD-160 (160 bits)	An independent hash algorithm; it provides up to 80 bits of brute force resistance.
RSA	Short for RSA Data Security, Inc.; or referring to the principals: Ron Rivest, Adi Shamir, and Len Adleman; or referring to the algorithm they invented. The RSA algorithm is used in public-key cryptography and is based on the fact that it is easy to multiply two large prime numbers together, but hard to factor them out of the product.
secure channel	A means of conveying information from one entity to another such that an adversary does not have the ability to reorder, delete, insert, or read (SSL, IPSec, whispering in someone's ear).
self-signed key	A public key that has been signed by the corresponding private key for proof of ownership.
session key	The secret (symmetric) key used to encrypt each set of data on a transaction basis. A different session key is used for each communication session.
SHA-1	A second-generation hash algorithm; it provides up to 80 bits of brute force resistance. Partially deprecated.
SHA-2 (256 bits)	A third-generation hash algorithm; it provides up to 128 bits of brute force resistance.
SHA-2 (384 bits)	A third-generation hash algorithm; it provides up to 192 bits of brute force resistance.
SHA-2 (512 bits)	A third-generation hash algorithm; it provides up to 256 bits of brute force resistance.
sign	To apply a signature.

signature	A digital code created with a private key. Signatures allow authentication of information by the process of signature verification. When you sign a message or file, the PGP program uses your private key to create a digital code that is unique to both the contents of the message and your private key. Anyone can use your public key to verify your signature.
S/MIME (Secure Multipurpose Mail Extension)	A proposed standard developed by Deming software and RSA Data Security for encrypting and/or authenticating MIME data. S/MIME defines a format for the MIME data, the algorithms that must be used for interoperability (RSA, RC2, SHA-1), and the additional operational concerns such as ANSI X.509 certificates and transport over the Internet.
SSL (Secure Socket Layer)	Developed by Netscape to provide security and privacy over the Internet. Supports server and client authentication and maintains the security and integrity of the transmission channel. Operates at the transport layer and mimics the "sockets library," allowing it to be application independent. Encrypts the entire communication channel and does not support digital signatures at the message level.
symmetric algorithm	Also known as conventional, secret key, and single key algorithms; the encryption and decryption key are either the same or can be calculated from one another. Two sub-categories exist: Block and Stream.
subkey	A subkey is a Diffie-Hellman encryption key that is added as a subset to your master key. Once a subkey is created, you can expire or revoke it without affecting your master key or the signatures collected on it.
text	Standard, printable, 7-bit ASCII text.
timestamping	Recording the time of creation or existence of information.
TLS (Transport Layer Security)	An IETF draft, version 1 is based on the Secure Sockets Layer (SSL) version 3.0 protocol, and provides communications privacy over the Internet.
TLSP (Transport Layer Security Protocol)	ISO 10736, draft international standard.
Triple DES	An encryption configuration in which the DES algorithm is used three times with three different keys.
trusted	A public key is said to be trusted by you if it has been validated by you or by someone you have designated as an introducer.
trusted introducer	Someone whom you trust to provide you with keys that are valid. When a trusted introducer signs another person's key, you trust that the person's key is valid, and you do not need to verify the key before using it.
Twofish	A 256-bit block cipher, symmetric algorithm. Twofish was one of five algorithms that the U.S. National Institute of Standards and Technology (NIST) considered for the Advanced Encryption Standard (AES).

user ID	A text phrase that identifies a keypair. For example, one common format for a user ID is the owner's name and email address. The user ID helps users (both the owner and colleagues) identify the owner of the keypair.
validity	Indicates the level of confidence that the key actually belongs to the alleged owner.
verification	The act of comparing a signature created with a private key to its public key. Verification proves that the information was actually sent by the signer, and that the message has not been subsequently altered by anyone else.
web of trust	A distributed trust model used by PGP technology to validate the ownership of a public key where the level of trust is cumulative, based on the individuals' knowledge of the introducers.
X.509	An ITU-T digital certificate that is an internationally recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, the user's identifying information, and the issuer's digital signature, as well as other possible extensions.

Index

A

- access lists, importing in PGP NetShare **135**
- Active Directory groups in PGP NetShare **136**
- Aladdin eToken Pro USB token **72, 224**
- alternate passphrases
 - adding to PGP Virtual Disk **91**
 - adding to PGPdisk **105**
- archives
 - advanced options in PGP Zip **150**
 - creating with PGP Zip **148**
 - editing in PGP Zip **169**
 - opening in PGP Zip **169**
 - self-decrypting in PGP Zip **161**
 - self-decrypting, opening **167**
 - signing only in PGP Zip **165**
 - verifying signed **168**
- Athena ASEKey USB token **225**
- authentication
 - bypassing in PGP WDE **87**
 - PGP Whole Disk Encryption **70**
- authorized users, in PGP NetShare **116**
- automatic
 - mounting of PGP Virtual Disk volumes **101**
- automatic backup software, using on PGP WDE disks **91**

B

- biometric word list
 - explained **187**

C

- CACs **216**
- changing your passphrase **191**
- Common Access Cards (CACs) **216**
- coordinator for PGP NetShare **119**

- creating

- a keypair **174**
- a keypair on a smartcard **218**
- a keypair on a token **218**
- a messaging policy **39**
- a messaging service **29**
- a new PGP Virtual Disk volume **100**
- a PGP Zip archive **148**
- strong passphrases **251**

- cryptography

- conventional **3**
- public-key **3**

D

- decrypting **3**

- deleting

- a subkey **199**
- digital signatures **192**
- keys
 - from a smartcard **220**
 - from your keyring **192**
- user IDs **192**

- Department of Defense **216**

- designated revoker

- properties **201**

- digital signature

- deleting **192**

- disk read/write error **78**

- disks

- adding users to encrypted **91**
- encrypting **74**
- encrypting in PGP WDE **75**
- errors during encryption, PGP WDE **79**
- scheduled wiping **212**
- supported in PGP WDE **65**
- using PGP WDE-encrypted **80**

- distributing

- PGP Virtual Disk volumes **111**

- drives, removable in PGP WDE **90**

E

- email
 - copying public keys from **181**
 - including your public key in **179**
- email accounts
 - multiple services **37**
- email options **237**
- encrypt **3**
- encrypting IM sessions **60**
- encryption **3**
 - adding users to **91**
 - algorithm used in PGP Whole Disk Encryption **66**
 - calculate duration of in PGP WDE **68**
 - deleting users from PGP WDE **87**
 - disk errors during **79**
 - disk read/write error **78**
 - disks or partitions **74**
 - disks or partitions in PGP WDE **75**
 - Maximum CPU Usage option **68, 73**
 - partitions in PGP Whole Disk options **71**
 - passphrase in PGP Zip **156**
 - PGP Whole Disk options **71**
 - pilot test **69**
 - Power Failure Safety **73**
 - Power Failure Safety in PGP WDE **69**
 - recipient keys in PGP Zip **151**
 - reducing time of initial **68, 73**
 - re-encrypting disk or partition **90**
 - using PGP WDE-encrypted disk **80**
- examining
 - smartcard properties **218**
- exchanging
 - PGP Virtual Disk volumes **111**
- exporting
 - keys
 - to files **180**
 - your key from a smartcard **220**

F

- files
 - blacklisted in PGP NetShare **120**
 - exporting public keys to **180**
 - properties of, PGP NetShare **142**
 - protecting outside of Protected Folder in PGP NetShare **140**
 - using in Protected Folders **127, 128**
 - viewing in Protected Folders **129**
- folder wiping
 - scheduling **212**
- folders, protected in PGP NetShare **116**
- forgotten passphrases **205**
- Free Space Wipe
 - scheduling tasks **212**

G

- generating
 - a key pair **174**
 - a key pair on a smartcard **218**
- granting
 - trust for key validations **195**

I

- importing
 - PKCS-12 X.509 private keys **190**
 - private keys **190**
- instant messaging
 - options **238**
 - securing **59**
 - sessions encrypting **60**

J

- JavaCards **216**

K

- key ID **196**
 - properties **196**
- key reconstruction server
 - send your key to **206**
- keyboard layouts for WDE **82**

- keypair
 - copying to a smartcard 221
 - See also "Keys" 4
- keys
 - copying keypair to a smartcard 221
 - creating 174
 - creating on a smartcard 218
 - deleting from your keyring 192
 - disabling 192
 - enabling 192
 - exporting from a smartcard 220
 - granting trust for validations 195
 - importing a PGP key 190
 - lost 205
 - on a smartcard 218
 - protecting 207
 - reconstructing 205
 - rejoining 203
 - rejoining a split key 204
 - replacing a photo ID 189
 - revoking 202
 - signing 194
 - splitting 203
 - subkeys 196
- keyserver 4
 - getting someone's public key from 181
 - searching 181
 - sending your public key to 178
 - using to circulate revoke keys 202
- Keyservers List 231

L

- licensing
 - PGP NetShare 117
 - PGP Whole Disk Encryption 63
- log
 - messaging 56
- logging in, PGP Bootguard screen 80
- Lotus Notes email client
 - full Notes name 258

M

- mac.com 37

- mail servers
 - multiple messaging services 37
- messaging log 56
- messaging services
 - multiple for single account 37
 - troubleshooting 37
- mounting PGP Virtual Disk volumes 104
 - automatically 101
- multiple messaging services 37

N

- Notes ID 258
- Notes name in email client 258

O

- options
 - PGP NetShare 140
- overview
 - of PGP Virtual Disk volumes 111

P

- partitions
 - encrypting 74
 - encrypting in PGP WDE 75
- Passphrase Quality bar 250
- passphrases 249
 - adding alternate ones for PGP Virtual Disk 91
 - adding alternate ones for PGPdisk 105
 - changing 191
 - changing in PGP WDE 88, 91
 - changing on smartcard 222
 - clearing in PGP NetShare 139
 - creating strong 251
 - encrypting with in PGP Zip 156
 - forgotten 205
 - PGP Whole Disk Encryption 70
 - setting 175
 - supported characters in PGP WDE 75
- password 249
- personalization 216
- PGP Whole Disk Encryption feature
 - re-encrypting a disk or partition 90
- PGP administrator 254

- PGP Bootguard screen
 - read-only disk information **86**
- PGP Bootguard screen, logging in at **80**
- PGP Desktop
 - described **1**
 - in PGP Universal-managed environment **253**
 - installing **8**
 - main screen **13, 14**
 - PGP tray icon **15**
 - Setup Assistant **9**
 - SSL/TLS support **35**
 - system requirements **7**
 - uninstalling **10**
 - upgrading **8**
- PGP Desktop options
 - email **237**
 - General **228**
 - instant messaging **238**
 - Keys **229**
 - Messaging **234**
 - overview **227**
- PGP Global Directory **1**
- PGP Keys **1**
- PGP Keyservers List **231**
- PGP Messaging **1**
 - creating
 - a policy **39**
 - creating a service **29**
 - described **25**
 - log **56**
 - policy examples **44**
 - services and policies **27**
 - troubleshooting services **37**
- PGP NetShare **2**
 - Active Directory groups, refreshing **136**
 - Active Directory groups, working with **136**
 - adding authorized users **131**
 - adding subfolders in Protected Folder **129**
 - authorized users in **116**
 - authorized users of **131**
 - blacklisted files **120**
 - clearing passphrases **139**
 - context menus, using **141**
 - coordinator, establishing **119**
 - copying Protected Folders to another location **131**
 - corrupted, deleted, or overwritten file usage of Protected Folders **120**
 - creating Protected Folders **121**
 - deleting users from **133**
 - direct access to ciphertext usage of Protected Folders **120**
 - Edit menu options **144**
 - file access usage of Protected Folders **120**
 - File menu options **144**
 - folder status, checking **130**
 - importing access lists from another folder **135**
 - in PGP Universal-managed environment **142**
 - licensing **117**
 - Netshare menu options **144**
 - normal usage of Protected Folders **119**
 - options **140**
 - overview of **115**
 - passphrase, clearing **139**
 - properties of file or folder **142**
 - Protected Folder Properties tab **143**
 - Protected Folder, choosing location of **119**
 - Protected Folder, creating **121**
 - Protected Folder, definition of **116**
 - protecting files outside Protected Folders **140**
 - re-encrypting a folder **138**
 - removing a Protected Folder **137**
 - shortcut menus, using **141**
 - unlocking Protected Folders **128**
 - using files in Protected Folder **127**
 - using with PGP Virtual Disk or PGP WDE **116**
 - viewing files in Protected Folder **129**
- PGP Shred **2**
 - using **209**

- PGP Shredder
 - using with PGP Zip 149
- PGP Universal 2, 253
 - PGP NetShare, using with 142
 - PGP WDE, using with 92
- PGP Virtual Disk
 - AES 112
 - CAST 112
 - creating a new volume 100
 - encryption algorithms 112
 - security precautions
 - memory static ion migration 113
 - passphrase erasure 112
 - tips for the user 113
 - virtual memory protection 113
 - Twofish 112
- PGP Virtual Disk volumes 2
 - alternate users 105
 - backing up 110
 - creating 100
 - described 99
 - encryption algorithms 112
 - exchanging 111
 - finding 103
 - maintaining 110
 - mounting 100, 104
 - overview 111
 - re-encrypting 108
 - security precautions 112
 - unmounting 104
 - using 104
- PGP Whole Disk Encryption
 - PGP Universal-managed 92
 - PGP Whole Disk Encryption feature 2
 - adding users 91
 - administration 92
 - authentication options 70
 - automatic backup software, using 91
 - bypassing authentication 87
 - calculate encryption duration 68
 - changing passphrase with Single Sign-On 85
 - deleting users from 87
 - disk errors during encryption 79
 - disk read/write error 78
 - encrypted disk, using 80
 - encrypting a disk 75
 - encryption algorithm used 66
 - encryption options 71, 73
 - keyboard layouts 82
 - licensing 63
 - logging in with Single Sign-On 85
 - overview of 63
 - partitions 71
 - passphrase and Single Sign-On 70
 - passphrase, changing 88, 91
 - passphrase, supported characters in 75
 - PGP Bootguard screen 80
 - Power Failure Safety 69
 - public key authentication 70
 - recovery disks, creating 66
 - recovery tokens 93
 - removable drives 90
 - security precautions 96
 - Single Sign-On 83
 - Single Sign-On and multiple users 85
 - Single Sign-On, encrypting disk to use with 84
 - software compatibility 69
 - supported disk types 65
 - token-based authentication 70, 72
 - uninstalling 90

PGP Zip

- advanced options, creating archive 150
- archive, creating 148
- editing an archive 169
- editing archive settings 170
- encrypting to recipient keys 151
- encrypting with a passphrase 156
- opening an archive 169
- overview of 147
- self-decrypting archives, creating 161
- self-decrypting archives, opening 167
- shredding files after archiving 149
- signing only 165
- verifying signed archives 168

PGP Zip archive 2

- adding a file 170
- adding a folder 171
- deleting a file or folder 171
- extracting a file 171
- opening 170
- saving changes 171

PGP Zip archives 2

photo ID

- adding 188
- removing 188
- removing from a key 189

PKCS-11 216

PKCS-12 keys

- obtaining 190

policies

- creating messaging 39
- examples of messaging 44

private keys 4

- creating 174
- importing PKCS-12 X.509 190

Properties tab, in Protected Folder properties 143

Protected Folder

- adding authorized users 131
- adding subfolders in 129
- authorized users 131
- blacklisted files 120
- checking folder status 130
- choosing location of 119
- clearing passphrases from 139
- copying to another location 131
- corrupted, deleted, or overwritten file usage 120
- creating in PGP NetShare 121
- definition of in PGP NetShare 116
- deleting users from 133
- direct access to ciphertext usage 120
- file access usage 120
- importing access lists from one to another 135
- normal usage 119
- properties of 142
- Properties tab 143
- protecting files outside of 140
- re-encrypting 138
- removing 137
- unlocking 128
- using files in 127
- viewing files in 129

protecting keys 207

public keys 4

- add or remove for a PGPDisk file 104
- advantages of sending to key server 178
- copying from a smartcard 220
- copying from email messages 181
- exporting to files 180
- getting from a keyserver 181
- including in an email message 179
- PGP Whole Disk Encryption 70
- searching keyserver 181
- sending to keyserver 178
- signing 194

R

- read/write error 78
- read-only disk or partition information 86
- reconstructing your key 205

- recovery disks
 - creating in PGP Whole Disk Encryption **66**
- recovery tokens **93**
- re-encrypting
 - disk or partition in PGP WDE **90**
 - Protected Folder in PGP NetShare **138**
- rejoining split keys **203, 204**
- removable drives in PGP WDE **90**
- removing
 - a photo ID from a key **189**
 - a subkey **199**
 - keys from a smartcard **220**
- revoker
 - viewing key properties **201**
- revoking
 - a subkey **199**
 - keys **202**

S

- scheduling
 - folder wiping **212**
 - free space wiping **212**
 - the Free Space Wiper **212**
- searching keyserver **181**
- secure instant messaging (IM) **59**
- self-decrypting archives
 - creating in PGP Zip **161**
 - opening **167**
- Separate Signing Subkey **2**
- separate subkeys **196**
- services
 - creating **29**
 - multiple for single account **37**
- setting
 - passphrase for a key **175**
- shortcut menus, in PGP Netshare **141**
- shredding **2**
 - described **209**
 - using **209**
- signing **3, 192**
 - archives in PGP Zip **165**
 - keys **194**
 - public keys **194**
 - verifying in PGP Zip **168**
- Single Sign-On
 - passphrase, changing **91**
 - PGP Whole Disk Encryption **70**
- Single Sign-On, changing passphrase with PGP WDE **85**
- Single Sign-On, logging in with PGP WDE **85**
- Single Sign-On, using with PGP WDE **83, 84, 85**
- smartcard
 - changing passphrase **222**
 - copying keypair to **221**
 - copying to keyring **220**
 - copying your public key from **220**
 - creating a new keypair on **218**
- JavaCards **216**
- overview **215**
- personalization **216**
- PKCS-11 **216**
- properties **218**
- viewing properties of **218**
- wiping **220**
- wiping keys from **220**

- splitting keys **203**
- SSL/TLS support **35**
- Start Menu **18**
- strong passphrases **251**
- subkey expiration
 - setting during creation **198**
- subkey size
 - setting during creation **198**
- subkeys **196**
 - creating
 - encryption **198**
 - encryption and signing **198**

- signing 198
- creating new 198
- expiration 196, 198
- icons 196
- looking at 198
- properties 196
- removing 199
- revoking 199
- separate 196
- setting size of 198
- size 196
- symbols 196
- validity 196
- viewing 196
- working with 196

T

- tasks
 - scheduled freespace wiping 212
- token
 - copying keypair to 221
 - copying to keyring 220
 - creating a new keypair on 218
 - overview 215
 - PGP Whole Disk Encryption 70, 72
 - properties 218
 - wiping keys from 220
- troubleshooting
 - messaging services 37
- trust
 - granting for key validations 195

U

- uninstalling PGP Whole Disk Encryption 90
- unlocking Protected Folders 128
- unmounting
 - PGP Virtual Disk volumes 104

- users
 - adding authorized to Protected Folders 131
 - adding to an encrypted disk or partition 91
 - authorized in Protected Folders 131
 - authorized, in PGP NetShare 116
 - deleting from PGP WDE access 87
 - deleting from Protected Folders 133
 - importing access lists in PGP NetShare 135
- using
 - Free Space Wipe 212

V

- validating keys 195
- verifying 3
 - PGP Zip signed archives 168
- viewing subkeys 196

W

- Windows Explorer 17
- WINS host 258
- wiping
 - disks 212
 - your smartcard 220
- word list
 - biometric 187

X

- X.509 certificates
 - adding to keypair 191
 - importing 190

Y

- yahoo.com 37