PGP® Desktop for Mac OS X

User's Guide

Version Information

PGP Desktop for Macintosh OS X User's Guide. PGP Desktop Version 10.0.0. Released December 2009.

Copyright Information

Trademark Information

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-128 encryption algorithm, implemented from RFC 2144, is available worldwide on a royalty-free basis for commercial and non-commercial uses. 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. Some third-party software included in PGP Universal Server is licensed under the GNU General Public License (GPL). PGP Universal Server as a whole is not licensed under the GPL. If you would like a copy of the source code for the GPL software included in PGP Universal Server, contact *PGP Support* (https://support.pgp.com). 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

This product includes or may include:

● The Zip and ZLib compression code, created by Mark Adler and Jean-Loup Gailly, is used with permission from the free Info-ZIP implementation, developed by zlib (http://www.zlib.net). ● Libxml2, the XML C parser and toolkit developed for the Gnome project and distributed and copyrighted under the MIT License found at http://www.opensource.org/licenses/mit-license.html. Copyright © 2007 by the Open Source Initiative. ● bzip2 1.0, a freely available high-quality data compressor, is copyrighted by Julian Seward, © 1996-2005. ● Application server (http://jakarta.apache.org/), web server (http://www.apache.org/), Jakarta Commons (http://jakarta.apache.org/commons/license.html) and log4j, a Java-based library used to parse HTML, developed by the Apache Software Foundation. The license is at www.apache.org/licenses/LICENSE-2.0.txt. ● Castor, an open-source, data-binding framework for moving data from XML to Java programming language objects and from Java to databases, is released by the ExoLab Group under an Apache 2.0-style license, available at http://www.castor.org/license.html. ● Xalan, an open-source software library from the Apache Software Foundation that implements the XSLT XML transformation language and the XPath XML query language, is released under the Apache Software License, version 1.1, available at http://xml.apache.org/xalan-j/#license1.1. ● Apache Axis is an implementation of the SOAP ("Simple Object Access Protocol") used for communications between various PGP products is provided under the Apache license found at http://www.apache.org/licenses/LICENSE-2.0.txt. ● mx4j, an open-source implementation of the Java Management Extensions (JMX), is released under an Apache-style license, available at http://mx4j.sourceforge.net/docs/ch01s06.html. ● jpeglib version 6a is based in part on the work of the Independent JPEG Group. (http://www.ijg.org/) ● libxslt the XSLT C library developed for the GNOME project and used for XML transformations is distributed under the MIT License http://www.opensource.org/licenses/mit-license.html. ● PCRE version 4.5 Perl regular expression compiler, copyrighted and distributed by University of Cambridge. ©1997-2006. The license agreement is at http://www.pcre.org/license.txt. ● BIND Balanced Binary Tree Library and Domain Name System (DNS) protocols developed and copyrighted by Internet Systems Consortium, Inc. (http://www.isc.org) ● Free BSD implementation of daemon developed by The FreeBSD Project, © 1994-2006. ● Simple Network Management Protocol Library developed and copyrighted by Carnegie Mellon University © 1989, 1991, 1992, Networks Associates Technology, Inc, © 2001- 2003, Cambridge Broadband Ltd. © 2001- 2003, Sun Microsystems, Inc., © 2003, Sparta, Inc, © 2003-2006, Cisco, Inc and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. The license agreement for these is at http://net-snmp.sourceforge.net/about/license.html. ● NTP version 4.2 developed by Network Time Protocol and copyrighted to various contributors. ● Lightweight Directory Access Protocol developed and copyrighted by OpenLDAP Foundation. OpenLDAP is an open-source implementation of the Lightweight Directory Access Protocol (LDAP). Copyright © 1999-2003, The OpenLDAP Foundation. The license agreement is at http://www.openldap.org/software/release/license.html. Secure shell OpenSSH version 4.2.1 developed by OpenBSD project is released by the OpenBSD Project under a BSD-style license, available at http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/LICENCE?rev=HEAD. ● PC/SC Lite is a free implementation of PC/SC, a specification for SmartCard integration is released under the BSD license. ● Postfix, an open source mail transfer agent (MTA), is released under the IBM Public License 1.0, available at http://www.opensource.org/licenses/ibmpl.php. ● PostgreSQL, a free software object-relational database management system, is released under a BSD-style license, available at http://www.postgresql.org/about/licence. ● PostgreSQL JDBC driver, a free Java program used to connect to a PostgreSQL database using standard, database independent Java code, (c) 1997-2005, PostgreSQL Global Development Group, is released under a BSD-style license, available at http://jdbc.postgresql.org/license.html. ● PostgreSQL Regular Expression Library, a free software object-relational database management system, is released under a BSD-style license, available at http://www.postgresql.org/about/licence. ● 21.vixie-cron is the Vixie version of cron, a standard UNIX daemon that runs specified programs at scheduled times. Copyright © 1993, 1994 by Paul Vixie; used by permission. ● JacORB, a Java object used to facilitate communication between processes written in Java and the data layer, is open source licensed under the GNU Library General Public License (LGPL) available at http://www.jacorb.org/lgpl.html. Copyright © 2006 The JacORB Project. ● TAO (The ACE ORB) is an open-source implementation of a CORBA Object Request Broker (ORB), and is used for communication between processes written in C/C++ and the data layer. Copyright (c) 1993-2006 by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University. The open source software license is available at http://www.cs.wustl.edu/~schmidt/ACE-copying.html. ● libcURL, a library for downloading files via common network services, is open source software provided under a MIT/X derivate license available at http://curl.haxx.se/docs/copyright.html. Copyright (c) 1996 - 2007, Daniel Stenberg. ● libuuid, a library used to generate unique identifiers, is released under a BSD-style license, available at http://thunk.org/hg/e2fsprogs/?file/fe55db3e508c/lib/uuid/COPYING. Copyright (C) 1996, 1997 Theodore Ts'o. ● libpopt, a library that parses command line options, is released under the terms of the GNU Free Documentation License available at http://directory.fsf.org/libs/COPYING.DOC. Copyright © 2000-2003 Free Software Foundation, Inc. ● gSOAP, a development tool for Windows clients to communicate with the Intel Corporation AMT chipset

on a motherboard, is distributed under the GNU Public License, available at http://www.cs.fsu.edu/~engelen/soaplicense.html. ● Windows Template Library (WTL) is used for developing user interface components and is distributed under the Common Public License v1.0 found at http://opensource.org/licenses/cpl1.0.php. ● The Perl Kit provides several independent utilities used to automate a variety of maintenance functions and is provided under the Perl Artistic License, found at http://www.perl.com/pub/a/language/misc/Artistic.html. ● rEFIt - libeg, provides a graphical interface library for EFI, including image rendering, text rendering, and alpha blending, and is distributed under the license found at http://refit.svn.sourceforge.net/viewvc/*checkout*/refit/trunk/refit/LICENSE.txt?revision=288. Copyright (c) 2006 Christoph Pfisterer. All rights reserved. ● Java Radius Client, used to authenticate PGP Universal Web Messenger users via Radius, is distributed under the Lesser General Public License (LGPL) found at http://www.gnu.org/licenses/lgpl.html. ● Yahoo! User Interface (YUI) library version 2.5.2, a Web UI interface library for AJAX. Copyright (c) 2009, Yahoo! Inc. All rights reserved. Released under a BSD-style license, available at http://developer.yahoo.com/yui/license.html. ● JSON-lib version 2.2.1, a Java library used to convert Java objects to JSON (JavaScript Object Notation) objects for AJAX. Distributed under the Apache 2.0 license, available at http://json-lib.sourceforge.net/license.html. ● EZMorph, used by JSON-lib, is distributed under the Apache 2.0 license, available at http://ezmorph.sourceforge.net/license.html. ● Apache Commons Lang, used by JSON-lib, is distributed under the Apache 2.0 license, available at http://commons.apache.org/license.html. ● Apache Commons BeanUtils, used by JSON-lib, is distributed under the Apache 2.0 license, available at http://commons.apache.org/license.html.

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.

Contents

1 About PGP Desktop 10.0 for Mac OS X

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 (on Windows systems)—so everything is protected all the time—or just a portion of your hard drive, via a virtual disk on which you can securely store your most sensitive data. You can use it to share your files and folders securely with others over a network. It lets you put any combination of files and folders into an encrypted, compressed package for easy distribution or backup. Finally, use PGP Desktop to shred (securely delete) sensitive files—so that no one can retrieve them—and shred free space on your hard drive, so there are no unsecured remains of any files.

Use PGP Desktop to create PGP keypairs and manage both your personal keypairs and the public keys of others.

To make the most of PGP Desktop, you should be familiar with *PGP Desktop Terminology* (on page 11). You should also understand conventional and public-key cryptography, as described in *Conventional and Public Key Cryptography* (on page 14).

In This Chapter

What's New in PGP Desktop for Mac OS X Version 10.0

Building on PGP Corporation's proven technology, PGP Desktop 10.0 for Mac OS X includes numerous improvements and the following new and resolved features.

General

- **New localized versions**. PGP Desktop has been localized and can now be installed in French (France) and Spanish (Latin America).
- **PGP Universal Server connectivity**. Increased resiliency of PGP Desktop when connectivity to the PGP Universal Server is dependent on a VPN connection or is otherwise intermittent.
- **Enrollment after installation**. Following installation of PGP Desktop for Mac OS X, enrollment to the PGP Universal Server is initiated immediately after the user logs on to the Mac OS X system.

PGP Keys

- **Enhanced Server Key Mode (SKM) keys**. SKM keys now include the entire key on your keyring. In addition, SKM keys can now be used for encryption functions such as disk and file encryption and decryption, as well as decrypting MAPI email messages when you are offline.
- **Flexible key types**. Adds the capability to handle asymmetric keys and certificates (such as X.509 and OpenPGP) as well as symmetric keys.
- **Key usage flags**. Each subkey can now have its own key usage properties, so that one subkey could be used for PGP WDE only, and another could be used for all other PGP Desktop functions. Set the key usage of a key when you want to use a key for disk encryption only but you do not want to receive encrypted email using that key.
- **Universal Server Protocol (USP) key searches**. The PGP Universal Services Protocol (USP) is a SOAP protocol operating over standard HTTP/HTTPS ports. This is now the default key lookup mechanism. If you are in a PGP Universal Server-managed environment, all key search requests as well as all other communications between the PGP Universal Server and PGP Desktop use PGP USP.

PGP Messaging

- **PGP Viewer**. Use PGP Viewer to decrypt and view legacy IMAP/POP/SMTP email messages.
- **Offline policy enhancements**. In a managed environment, mail policy is now enforced even if you are offline and not connected to the PGP Universal Server or if the server itself is offline.

PGP Whole Disk Encryption

- **Additional keyboard compatibility**. Four new language keyboards have been added for support at PGP BootGuard. These are: English (US-International), Japanese (Japan), German (Germany), French (France), Spanish (Latin America), Spanish (Spain, ISO).

- **Full disk encryption support on Linux**. PGP WDE for Linux provides full disk encryption with pre-boot authentication on Ubuntu and Red Hat. For more information, see the PGP Whole Disk Encryption for Linux Command Line Guide.
- **Force encryption enhancements**. When your PGP Universal Server administrator changes policy to require that all disks be encrypted, the next time policy is downloaded to your system, the PGP WDE assistant is displayed so you can begin to encrypt your disk.
- **Extended ASCII character support**. Extended ASCII characters can now be used when creating PGP WDE users.
- **Support added for Boot Camp**. PGP Desktop for Mac OS X can now be used on systems where Boot Camp has been installed. For information on how to use Boot Camp with PGP Desktop, see the installation instructions.

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 document describes 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. For more information, see *Using PGP Desktop with PGP Universal Server* (on page 207).

Note: References to PGP Universal Server-managed environments do not apply to the PGP Virtual Disk or PGP Virtual Disk Professional products.

Features Customized by Your PGP Universal Server Administrator

If you are using PGP Desktop as a "managed" user in a PGP Universal Server-managed environment, there are some settings that can be specified by your administrator. These settings may change the way features are displayed in PGP Desktop.

- **Disabled features**. Your PGP Universal Server administrator can enable or disable specific functionality. For example, your administrator may disable the ability to create PGP Zip archives, or to create PGP NetShare protected folders (on Windows systems).

  When a feature is disabled, the control item in the left side is not displayed and the menu for that feature is not available. The graphics included in this guide depict the default installation with all features enabled. The PGP Desktop interface may look different if your administrator has customized the features available.

Conventions Used in This Guide

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

Notes: 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: 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: 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.

Who Should Read This Document

This document is for anyone who is going to be using the PGP Desktop for Mac OS X software to protect their data.

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

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.

There are three types of licenses:

- **Evaluation**: This type of license is typically time-delimited and may not include all PGP Desktop functionality.
- **Subscription**: This type of license is typically valid for a subscription period of one year. During the subscription period, you receive the current version of PGP software and all upgrades and updates released during this period.
- **Perpetual**: This type of license allows you to use PGP Desktop indefinitely. With the addition of the annual Software Insurance policy, which must be renewed annually, you also receive all upgrades and updates released during the policy term.

About PGP Desktop Licensing

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 5). 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* (on page 5). If you need to authorize your copy of PGP Desktop, do so as described in *Authorizing PGP Desktop for Mac OS X* (see "Authorizing PGP Desktop or Mac OS X" on page 6).

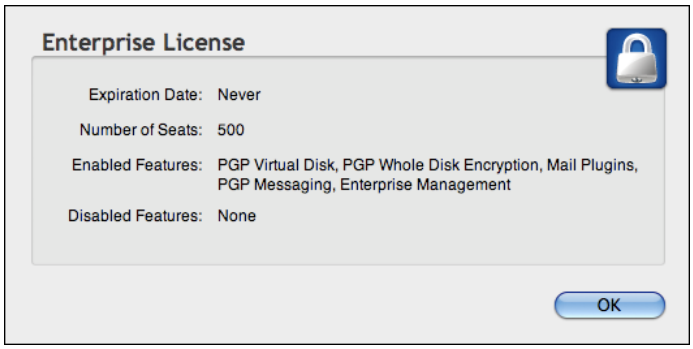
Checking License Details

To see the details of your PGP Desktop license:

1. Open PGP Desktop.
2. From the **PGP** menu, select **License**. The License Information dialog box is displayed. This dialog box displays:
   - **Name**: The name your license is registered to.

- **Organization**: The organization your license is registered to.
- **Email**: The email address associated with your license.
- **Type**: The type of license you have, Enterprise or Home.

3 Click **Details**. The details of your license are displayed.



- **Expiration Date**: The date your license expires.
- **Number of Seats**: The number of seats available for this license.
- **Enabled Features**: The components that are active in your license.
- **Disabled Features**: The components that are *not* active in your license.

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

Authorizing PGP Desktop or Mac OS X

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.

Note: 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.

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

2 OpenPGP Desktop.

3 From the **PGP** menu, select **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 want to assign to the licensing of the product.

Note: 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.

7 Do one of the following:

- Type your 28-character license number in the **License Number** fields (for example, DEMO1-DEMO2-DEMO3-DEMO4-DEMO5-ABC).

Note: 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 **Try for 30 Days**. 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 Now.** A Web browser opens so you can access the online PGP Store.

8 Click **Authorize**.

9 When your license is authorized, click **OK** 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* (https://support.pgp.com) for suggestions.

If Your License Has Expired

If your PGP Desktop license has expired, you will receive a PGP License Expiration message when you launch PGP Desktop. See the following sections for information on how an expired license affects the functionality of PGP Desktop.

PGP Desktop Email

- Outgoing email messages are no longer sent encrypted.

PGP Virtual Disk

- PGP Virtual Disks are still accessible in Read-Only mode. Read-Only allows data to be copied from a PGP Virtual Disk, however no data can be copied to a PGP Virtual Disk.

PGP Whole Disk Encryption

Any fixed disks that have been encrypted with PGP Desktop are automatically decrypted 90 days after the license expiration date.

Getting Assistance

For additional resources, see these sections.

Getting product information

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

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

Contact Information

Contacting Technical Support

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

Contacting Customer Service

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

Contacting Other Departments

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

2 PGP Desktop Basics

This section describes the PGP Desktop terminology and provides some high-level conceptual information on cryptography.

In This Chapter

PGP Desktop Terminology

To make the most of PGP Desktop, you should be familiar with the terms in the following sections.

PGP Product Components

PGP Desktop and its components are described in the following list. Depending on your license, you may not have all functionality available. For more information, see *About PGP Desktop Licensing* (on page 5).

- **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 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 plug-in technology is also available. PGP Messaging also protects many IM clients, such as AIM and iChat (both users must have PGP Messaging enabled).
  - **PGP Whole Disk Encryption**: Whole Disk Encryption is a feature of PGP Desktop that encrypts your entire hard drive or partition (on Windows systems), including your boot record, thus protecting all your files when you are not using them. You can use PGP Whole Disk Encryption and PGP Virtual Disk volumes on the same system. On Windows systems, you can protect whole disk encrypted drives with a passphrase or with a keypair on a USB token for added security.

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

- **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 Server-managed environment, your messaging policies and other settings may be controlled by your organization's PGP administrator.
  - **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 queries the email address on a key (to verify that the owner of the email address wants their key posted) 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.

Terms Used in PGP Desktop

Before you use PGP Desktop, you should be familiar with the following terms:

- **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.
- **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.
- **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.
- **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.

  Caution: 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.
- **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.

- **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. Smart cards and tokens are not available for key storage when used with PGP Desktop for Mac OS X.

Conventional and Public Key Cryptography

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.

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 keyservers.)

Once the public keys are on the keyserver, you can go back to the keyserver 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; for more information, see *Working with PGP Keys* (on page 45)). 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.**

Your public and private keys are mathematically related, but there's no feasible way to figure out someone's private key if you just have a public key.

Learning More About Cryptography

For more information about cryptography, see *An Introduction to Cryptography*, which was installed on your system when PGP Desktop was installed. It is available through the Start menu.

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 or may have configured your PGP installer with certain settings. Either way, this is the first step.

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 is displayed. 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 (once you have exchanged public keys with them). 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 to compare the unique fingerprint on your copy of someone's public key to the fingerprint on that person's key (a good way to do that is by telephoning the key's owner and having them read you the fingerprint information so that you can compare it). 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. The secure IM chat session feature generates its own keys automatically, so you can use this feature even before you generate your keypair. The only requirement is that you must be chatting with another PGP Desktop user for the chat session to be secured.

6 **Watch for information boxes from the PGP Desktop Notifier feature to appear**.

As you send or receive messages, or perform other PGP Desktop functions, the PGP Desktop Notifier feature displays information boxes that appear in whichever corner of the screen you specify. These PGP Notifier boxes tell you the action that PGP Desktop took, or will take. After you grow familiar with the process of sending and receiving messages, you can change options for the PGP Notifier feature—or turn it off.

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

If you want more information than the Notifier feature displays, the PGP Log provides detailed information about all messaging operations.

8 **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's **verified** 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.

9 **Start using the other features in PGP Desktop.**

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

- Use **PGP Whole Disk Encryption** to encrypt a boot disk, disk partition (on Windows systems), external disk, or USB thumb drive. All files on the disk or partition are secured — encrypted and decrypted on the fly as you use them. The process is completely transparent to you.
- Use **PGP Virtual Disk** 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 or the Mac OS X finder to unmount and lock the virtual disk, and your files are secure, even if the rest of your computer is unlocked.
- Use **PGP Zip** to create compressed and encrypted PGP Zip archives. These archives offer an efficient way to transport or store files securely.
- Use **PGP Shredder** to delete sensitive files that you no longer need. PGP Shredder removes them completely, eliminating any possibility of recovery.

3 Installing PGP Desktop

This section describes how to install PGP Desktop onto your computer and how to get started after installation.

In This Chapter

System Requirements

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

- Apple Mac OS X10.5.x or 10.6.x (Intel)
- 512 MB of RAM
- 64 MB hard disk space

Installing and Configuring PGP Desktop

This section includes information on installing or upgrading PGP Desktop, as well as information on the Setup Assistant.

Installing the Software

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

The PGP Desktop installer walks you through the installation process.

To install PGP Desktop on your Mac OS X system

1. Quit all other applications.
2. Mount the PGP DiskCopy image.
3. Double-click `PGP.pkg`.
4. Follow the on-screen instructions.
5. If prompted to do so, restart your system.

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

Using PGP Desktop with Apple Boot Camp

Apple Boot Camp is compatible with PGP Desktop ver 10.0 or later. To use PGP Desktop with Boot Camp, you must install the software and encrypt the disk in a specific order.

Note: Be sure that your disk is not encrypted (if it is, decrypt the disk before installing Boot Camp) and then uninstall PGP Desktop.

To use Apple Boot Camp

1. Install Apple Boot Camp.
2. Install PGP Desktop on the Mac OS X partition and complete enrollment with the setup assistant.
3. Boot into the Windows partition and install PGP Desktop on the Windows and complete enrollment with the setup assistant.
4. Boot into the Mac OS X partition and encrypt your disk. At this point, if you pause the encryption process while running Mac OS X, you can resume encryption while running Windows.

If you need to decrypt your disk, PGP Corporation recommends that you do so from the Mac OS X partition.

For more information on using PGP Desktop with Apple Boot Camp, see *PGP KB Article 1697* (https://support.pgp.com/?faq=1697).

Upgrading the Software

Note: PGP Desktop for Mac OS X, and PGP Universal Satellite for Mac OS X cannot both be installed in the same system. The installers for both products will detect the presence of the other program and end the install.

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

- PGP Desktop for Mac OS X
- PGP Universal Satellite for Mac OS X

Important Note: If you are upgrading your computer to a new version of the operating system and want to use this version of PGP Desktop, be sure to uninstall any previous versions of PGP Desktop before upgrading the OS and installing this release. Be sure to back up your keys and keyrings before uninstalling. Note that if you have used PGP Whole Disk Encryption, you will need to unencrypt your disk before you can uninstall PGP Desktop.

Upgrading PGP Desktop

Do one of the following:

- **From PGP Desktop 8.x or 9.x for Mac OS X**, begin the installation process for PGP Desktop 10.0 for Mac OS X.

  The existing version of PGP Desktop for Mac OS X is automatically uninstalled, then PGP Desktop 10.0 for Mac OS X is installed. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version.

- **From a version of PGP Desktop for Mac OS X prior to Version 8.0**, you must manually uninstall the existing software before beginning the installation of PGP Desktop 10.0 for Mac OS X. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version.

Upgrading from PGP Universal Satellite

Do one of the following:

- **From PGP Universal Satellite version 1.2 or previous for Mac OS X**, begin the installation process for PGP Desktop 10.0 for Mac OS X.

  Existing versions of PGP Universal Satellite for Mac OS X are automatically uninstalled, then PGP Desktop 10.0 for Mac OS X is installed. Existing settings are retained.

  Caution: Installing any version of PGP Universal Satellite on top of PGP Desktop 10.0 for Mac OS X is an unsupported configuration. Neither program will work correctly. Uninstall both programs and then reinstall only PGP Desktop.

- **From PGP Desktop for Mac OS X (version 8.x) and PGP Universal Satellite:** Follow the installation process for PGP Desktop 10.0 for Mac OS X.

  PGP Desktop for Mac OS X and PGP Universal Satellite for Mac OS X are both automatically uninstalled, then PGP Desktop 10.0 for Mac OS X is installed. Existing keyrings and PGP Virtual Disk files are usable in the upgraded version, as are existing PGP Universal Satellite for Mac OS X settings.

Checking for Updates

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 is displayed that lets you download the new version. When disabled, PGP Desktop does not automatically check for software updates. For more information, see *General Options* (see "General Preferences" on page 188).

Once you have downloaded the update, install the update by following the prompts.

This option requires an active Internet connection.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, this option may be required. PGP Desktop then searches for updates on its associated PGP Universal Server.

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

Upgrading From Standalone to Managed PGP Desktop Installations

If you have been using PGP Desktop in standalone mode and now will be managed by a PGP Universal Server, you must install a bound and stamped version of PGP Desktop over your existing, standalone installation. You must also complete the enrollment process. Your PGP Administrator will provide an installation file so you can install a bound and stamped version.

Upgrading the Operating System Software

If you are upgrading your computer to a new major release of the operating system (for example, on a Windows system to Windows Vista or on a Mac OS X system from 10.4.x to 10.5.x), be sure to do the following:

1. Back up your keys and keyrings before uninstalling.
2. If you have used PGP Whole Disk Encryption, dencrypt your disk before you uninstall PGP Desktop.

3 Uninstall any previous versions of PGP Desktop *before* upgrading to the new version of the operating system.

4 Once you have upgraded your version of the operating system, reinstall PGP Desktop. Import your keys/keyring and, if necessary, you can then encrypt your disk.

Licensing PGP Desktop

For license information for this release, see the *PGP Desktop Release Notes*.

Running the Setup Assistant

The Setup Assistant displays a series of screens that ask you questions—then uses your answers to configure PGP Desktop for you.

If you have questions about any of the content on the Setup Assistant screens, click **Help** on the screen.

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.

Integrating with Entourage 2008

The PGP Desktop for Mac OS X installation package includes scripts so you can integrate PGP Desktop with Entourage. Once the scripts are copied to the required folders, the Scripts menu in Entourage includes a PGP menu option. Use the Entourage scripts to encrypt email text without having to use an email proxy.

To integrate PGP scripts with Entourage

1 If it is running, quit Entourage.

2 Open the PGP Desktop for Mac OS X download.

3 In the PGP Desktop download folder, open the Extras folder.

4 In the Extras folder, open the Entourage folder.

5 Double-click the file `EntourageScripts.zip` to extract the following scripts from the zip file:

- Decrypt & Verify\mod
- Encrypt & Sign\moc
- Encript\moe
- Sign\mos

6 Copy and paste the scripts to the following folder:

- User Profile\Documents\Microsoft User Data\Entourage Script Menu items\PGP

7 Start Entourage. The Scripts menu now includes a PGP menu option.

See *Using PGP Scripts with Entourage 2008* (on page 119) for information on how to encrypt and decrypt messages.

Uninstalling PGP Desktop

To uninstall PGP Desktop

1 In PGP Desktop, from the **PGP** menu, select **Uninstall**. A confirmation dialog box is displayed.

2 Click **Yes** to continue with the uninstall process.

3 You are prompted to authenticate as the administrative user of the Mac OS X system from which you are uninstalling PGP Desktop. Enter the appropriate password, then click **OK**. The PGP Desktop software is removed from your system.

Your keyring and PGP Virtual Disk files are not removed from your system, in case you decide to reinstall PGP Desktop in the future.

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:

To transfer your PGP Desktop installation to another computer

1 Uninstall PGP Desktop. To do this, in PGP Desktop from the **PGP** menu, select **Uninstall**.

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 removable media such as a flash drive, and then copy them to the new computer. The default location for the keyring files is in the PGP folder.

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.

4 The PGP Desktop User Interface

This section describes the PGP Desktop user interface.

In This Chapter

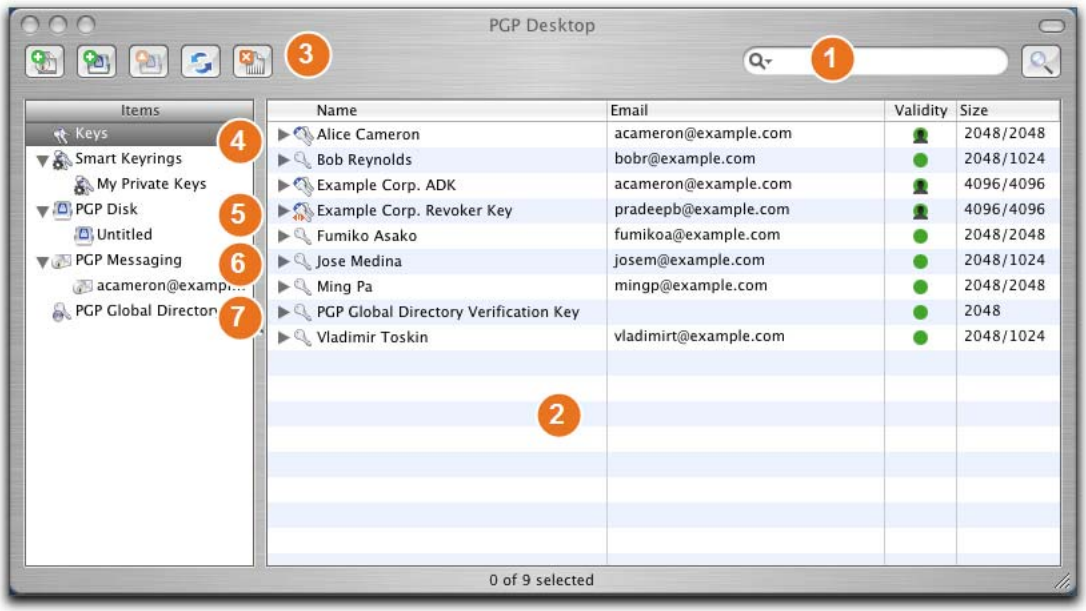
Accessing PGP Desktop Features

There are four main ways to access PGP Desktop:

- *PGP Desktop Main Screen* (on page 28)
- *Using the PGP Desktop Icon in the Menu Bar* (on page 29)
- *Using the PGP Dock Icon* (on page 30)
- *Using the Mac OS X Finder* (on page 31)

PGP Desktop Main Screen

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



The PGP Desktop main screen includes:

1	**The search field**. Lets you search for keys on the local keyring. Simply enter characters and the names and email addresses on the local keyring that include those characters will display. Click **Advanced Search** for more search criteria.
2	**The PGP Desktop Work area**. Displays information about and actions you can take for the selected item.
3	**The Toolbar**. Provides access to frequently used features. You can: Create a new PGP Zip archive. Create a new PGP Virtual Disk. Mount an existing PGP Virtual Disk. Synchronize keys. Shred files.
4	**The Keys item**. Gives you control over the PGP keys that PGP Desktop is managing for you.
5	**The PGP Disk item**. Use this item to view and manage PGP Virtual Disk volumes. Also, you can use this item to create new PGP Virtual Disk volumes, as well as encrypting an entire non-boot disk using the

	PGP Whole Disk Encryption feature.
6	**The PGP Messaging item**. Use this item to manage PGP Messaging services. You can also use this item to create new services and policies, and manage existing services and policies.
7	**The Keyservers item**. Use this item to view and manage keyservers.
	(not shown) **The PGP Zip item.** Use this item to view and manage PGP Zip archives.

Using the PGP Desktop Icon in the Menu Bar

One way to access many PGP Desktop features is from the PGP Desktop icon in the Menu Bar.

When you click the PGP Desktop icon in the Menu Bar, the PGP menu is displayed. Note that not all options may be available, depending on if you are a standalone or managed installation.

- **About PGP Desktop**. Displays a window with information about the version of PGP Desktop you are using, licensing information, and a list of the people who helped create PGP Desktop. This window also has a button that you can use to uninstall PGP Desktop.
- **Help**. Opens the PGP Desktop integrated online help.
- **Open PGP Desktop.** Opens the PGP Desktop main screen.
- **Open PGP Viewer**. Opens PGP Viewer so you can decrypt email out of the mail stream.
- **View Notifier.** Displays the PGP Desktop Notifier box, so you can review the Notifier messages that have appeared.
- **Show Log.** Displays the PGP Desktop Log. Use the PGP Desktop Log to see what actions PGP Desktop is taking to secure your data.
- **Clear Log.** Clears the PGP Log.
- **Update Policy**. Manually downloads policy from the PGP Universal Server. This option is available only for managed installations.
- **Change Passphrase**. Provides a shortcut so you can change your passphrase on your key. This option is available only for managed installations.

- **Purge Caches.** Clears from memory any cached information, such as passphrases and cached public keys.
- **Hide.** Removes the PGP icon from the menu bar, but leaves the background parts of the application running.

  The **Hide** command becomes the **Quit** command if you hold down the **Option** key before clicking the PGP Desktop icon. This removes the PGP Desktop icon from the menu bar and *causes the background parts of PGP Desktop to quit*. Shortcut menu functionality continues to work.

Caution: If you use the Option key and the PGP Menu Bar icon to quit the background parts of PGP Desktop, email messages are no longer encrypted, decrypted, signed, or verified. You may also not be able to decrypt messages received while the background parts of PGP Desktop were not running, even after they are started again. Finally, no key management is done while the background parts of the software is not running. For these reasons, it is recommended that you keep the PGP Desktop background processes running at all times.

To restart the background processes of PGP Desktop if the application is not running

1. Locate the PGP Desktop application on your system. The default location is in the Applications folder.
2. Double-click the PGP Desktop application icon. PGP Desktop starts and its icon is displayed in the Menu Bar.

Using the PGP Dock Icon

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

Use the PGP Desktop icon in the Mac OS X Dock in any of these ways, then select an option from the menu displayed:

- Click the PGP Desktop Dock icon and hold the mouse button down.
- Ctrl+click the Dock icon.
- Right-click the Dock icon, if you are using a two-button mouse.

The PGP Desktop icon is displayed in the Dock when the application is open, or when you have put the PGP Desktop icon into the Dock manually.

When you click *and hold* the PGP Desktop icon in the Dock when the application is already open (or Ctrl+click it, or use the right mouse button if you are using a two-button mouse), a menu is displayed giving you access to the following commands:

- Any currently-open PGP Desktop windows. If PGP Desktop is currently running, any of its windows that you have open appear at the top of this menu.
- **About PGP Desktop**. Displays the PGP Desktop About dialog box. The About dialog box displays the PGP Desktop credits, what version you are currently using, and has a button that you can use to uninstall the PGP Desktop software.
- **Preferences**. Opens the PGP Desktop Preferences.
- **Clipboard**. Lets you Encrypt, Sign, Encrypt & Sign, or Decrypt/Verify the contents of the Clipboard.
- **Check For Updates**. Checks for newer versions of PGP Desktop. If a newer version is found, you have the option of downloading it.
- **Purge Caches**. Clears from memory any cached information, such as passphrases and cached public keys.

The remaining menu items, in the lowest section of the menu, are standard Mac OS X Dock items:

- **Remove from Dock/Keep in Dock.** Removes or adds the PGP Desktop icon in the Dock.
- **Open at Login.** Sets your Mac OS X Account System Preference so that PGP Desktop starts when you log on to your computer.
- **Show In Finder**. Shows the location of the PGP Desktop application in a Finder window.
- **Hide**. Hides any PGP Desktop application screens.
- **Quit**. Quits the PGP Desktop application.

If you click and hold the PGP Desktop icon in the Dock when the application is not open, you see the standard Mac OS X Dock items.

Using the Mac OS X Finder

From the Desktop or a Finder window, Ctrl+click a file or folder (or right-click it if you have two-button mouse) then select **PGP** from the shortcut menu displayed.

You can also access PGP Desktop functions from the Mac OS X Finder.

To use the Mac OS X Finder

1. Open a Finder window.
2. Ctrl+click (or right-click, if you are using a two-button mouse) the desired file or folder.
3. Select the appropriate option from the PGP shortcut menu. Choose **Encrypt**, **Sign**, **Encrypt & Sign**, **Decrypt/Verify**, **Shred**, or **Mount** (if you have PGP Virtual Disks).

Tip: You can also right-click a file or folder from the 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, as well as instant messaging sessions.

PGP Desktop Notifier for Messaging

Use the PGP Desktop Notifier for Messaging feature to:

- See if an incoming email is properly decrypted and/or signed.
- See if an 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.
- See that a chat session with another PGP Desktop user is being secured.

Use the PGP Desktop Notifier feature to monitor all or some of your incoming email, as well as maintain precise control over all or some of your outgoing messages. 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, use the 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 cursor away from them.
- Unless the cursor is over them, Notifier messages display for four seconds (this default setting can be changed in the Notifier options). If you want more time to read a Notifier, move your cursor over the Notifier and it remains on your display.
- If you completely miss reading a Notifier, or you would like to review previous ones, do the following:
    - On Windows systems, choose **View Notifier** from the PGP Tray icon.

- On Mac OS X systems, choose **View Notifier** from the PGP Desktop icon in the Mac OS X Menu Bar.

- Close a Notifier message by clicking the **X** (in the upper right corner of the message on Windows systems, in the upper left corner on Mac OS X systems).

For more information about setting PGP Desktop Notifier options, see *Notifier Options* (see "Notifications Preferences" on page 198).

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.

Outgoing PGP Desktop Notifier messages

For simple notification, choose to have a PGP Desktop Notifier appear momentarily when email is sent (all email, or email meeting certain criteria). The notifier message displays information that PGP Desktop is searching for the public keys of the person in the To line. When the appropriate keys are found, the Status line changes to indicate the message will be sent encrypted. If the appropriate keys cannot be found, PGP Desktop follows policy and may send the message unencrypted or block the message.

After a message has been sent encrypted, click **More** to see the details of how PGP Desktop handled the message. It is not necessary for you to view this additional information unless you want to see it. To hide the additional information again, click **Less**.

You can delay a message from being sent by moving your cursor over the Notifier box. If you do not do this within 4 seconds (you can set this interval in preferences for the Notifier feature) the message is sent unencrypted, and the Status field reflects that.

If you do move your cursor over the message, **Block** and **Send** buttons appear in the Notifier box. Click **Block** to stop the message from being transmitted, or **Send** to send the message.

If you send an email to more than one recipient, and PGP Desktop is able to find keys for some recipients but not others, the Notifier informs you of the status, and gives you two options:

- Send the email encrypted to those with keys, and unencrypted to those without them.
- Block the message so it is sent to no one.

Outgoing PGP Desktop Notifier Messages for Offline Policy

If you are using PGP Desktop in a PGP Universal Server-managed environment, your administrator may have specified what actions to take on outgoing messages if the PGP Universal Server is not available. The outgoing notifier message indicates one of the following:

- Your PGP Universal Server is not available and policy has been set to block all messages. Email messages remain in your outbox and are sent when the PGP Universal Server can be contacted.
- Your PGP Universal Server is not available and policy has been set to send all messages in the clear.
- Your PGP Universal Server is not available and policy has been set to allow your local policy to take precedence.

In the latter two cases, you can choose to send or block the outgoing message as you would any other outgoing message.

PGP Notifier for Instant Messaging

If you have PGP Desktop installed on your computer, and if you have specified to receive Notifiers for Instant Messaging (under the **Notifications** tab in PGP Desktop Preferences), then PGP Desktop Notifiers alert you when the AOL Instant Messenger (AIM) sessions that you have with other PGP Desktop users are protected.

When you use the secure instant messaging feature, a Notifier displays when you log on to the instant messaging program to inform you that your chat is secure, and a padlock icon displays next to your "buddy name" with most AIM-compliant instant messaging clients.

When you log off of your instant messaging program, a final Notifier message informs you that the secure session has ended.

For more information on proper configuration, as well as the use of the secure instant message chat feature, see Securing Instant Messages.

Enabling or Disabling Notifers

To enable or disable Notifiers

1. Open PGP Desktop and select **PGP > Preferences**.
2. Click the Notifier icon.

3 Under **Usage**, specify if you want to **Use PGP Notifer** and, if so, the location. PGP Desktop Notifications can appear at any of the four corners of your screen (**Lower Right**, **Lower Left**, **Upper Right**, or **Upper Left**). Select the corner that you want PGP Desktop Notifications to appear. The default position is **Upper Left**.

4 If you are using PGP Desktop Messaging and you want PGP Desktop Notifiers to appear, informing you of encryption and/or signing status when you send email, select the checkbox to **Notify when processing outbound email**. Deselect this checkbox to stop PGP Desktop Notifiers from appearing when you send mail.

5 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). Select **Ask me before sending email when the recipient's key is not found** if you want to be notified when a key is not found and be given a chance to block the email so that it is not sent. Then specify the following options:

- **Always ask me before sending email:** 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; the default is 4 seconds). 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.

(For more information on the PGP Desktop default policy settings, see *Services and Policies* (on page 91).)

6 For incoming email, specify how you are notified of its status upon arrival. Select one of the following for **Display notifications for incoming mail:**

- **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.

7 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, select the checkbox to **Notify for status of PGP Encrypted IM sessions**.

5

PGP Desktop and the Finder

This section describes how you can access certain PGP Desktop functions using shortcut menus in the Finder.

In This Chapter

Overview

Access PGP Desktop functions using shortcut menus in the Finder to get the same PGP Desktop functionality from the Mac OS X Services menu.

Depending on what you select, you can:

- Encrypt, Sign, or Encrypt and Sign
- Shred
- Decrypt/verify
- Mount, edit, or unmount a PGP Virtual Disk volume
- Import a PGP key
- Add PGP keys to your keyring

View the contents of a PGP Zip archive Access shortcut menus in the Finder by:

- Ctrl+clicking: With a one-button mouse, hold down the Control (ctrl) key on the keyboard and click the item.

- Right-clicking: On a two-button mouse, click the item with the right mouse button held down.

In this document, the Ctrl+click method is used. If you right-click or use a different method for accessing shortcut menus in the Finder, substitute that method where it says to Ctrl+click.

Note: Files "in the Finder" also include files on the Mac OS X Desktop.

Encrypt, Sign, or Encrypt and Sign

PGP Desktop lets you encrypt, sign, or encrypt and sign unencrypted files, folders, and even entire drives from the Finder.

Encrypting and/or signing files and folders is a good way to protect just a few important files and/or folders in a situation where a PGP Virtual Disk volume is not justified.

If you are considering encrypting and/or signing a drive in the Finder, a PGP Virtual Disk volume might be a better solution. For more information, see Using PGP Virtual Disks.

To encrypt and/or sign files and/or folders in the Finder

1. In the Finder, select the files and/or folders you want to encrypt and/or sign. Use the Shift or Command keys to select any combination of files and folders.
2. Ctrl+click the selected files and/or folders, or right-click if you have a two-button mouse. From the shortcut menu, choose **Encrypt & Sign** from the **PGP** menu. (If you select just **Encrypt**, you will *not* be prompted for a signing key; if you select just **Sign**, you will *not* be prompted to select a public key to encrypt to.) The PGP Recipients dialog box is displayed.
3. Drag the public keys of the persons you want to be able to decrypt the items you are encrypting into the **Recipients** field at the bottom of the dialog box.
4. Click the down arrow icon above the **OK** button to specify the appropriate options:

   - **Conventional Encrypt**. Select this checkbox to rely on a common passphrase rather than on public-key cryptography. The file is encrypted using a session key, which encrypts (and decrypts) using a passphrase you specify.

     If you are using PGP Desktop in a PGP Universal Server-managed environment, conventional encryption may be disabled.

   - **Text Output**. When sending files as attachments with some email applications, you may need to select the **Text Output** checkbox to save the file as ASCII text. This is sometimes necessary in order to send a binary file using older email applications. Selecting this option increases the size of the encrypted file by about 30 percent.

- **Shred Original**. Select this checkbox to overwrite the original document that you are encrypting, so that your sensitive information is not readable by anyone who can access your system.
- **MacBinary**. MacBinary is the standard method by which a Mac OS X file is converted into a single file so that it can be transferred to another Macintosh or PC without losing either its Data or Resource segment. Options are Yes, No, or Smart.

  Yes means the whole file is included, including the Mac OS X specific information. **No** means only the data segment is included. **Smart** means the file type determines if the Mac OS X specific information is included.

5 Click **OK**. If you selected the Conventional Encryption option, you are prompted for a passphrase to protect the encrypted items.

6 Enter a passphrase, enter it again, then click **OK**. The Enter PGP Passphrase dialog box is displayed.

7 Using the Signing Key list, specify a private key to be used to sign the items you are encrypting and signing, then enter the passphrase of the signing key. If the passphrase is cached, you do not have to enter it.

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 (either physically or over the network) and you would like to see the characters of your passphrase as you type, select the **Show Keystrokes** checkbox.

8 To save your passphrase in the Mac OS X Keychain, select the box. You will not need to enter the passphrase the next time you access this feature.

9 Click **OK**. A PGP Zip archive (<file name>.pgp) file is created at the same location as the encrypted and signed items.

Shred

For those situations where you want to be absolutely certain that specific files and/or folders are securely deleted from your system, you can Shred them from the Finder.

Putting a file or folder into the Mac OS X Trash just allows new files to overwrite the file or folder you think you are "deleting." In fact, there could be days, weeks, or even months when just about anyone with physical access your system could retrieve these files.

The PGP Desktop Shred feature, in comparison, overwrites your files multiple times as soon as you ask them to be shredded. For more information about how thoroughly the Shred feature erases your files, see Shredding Files.

To Shred files and/or folders in the Finder

1. In the Finder, select the files and/or folders you want to Shred. Use the Shift or Command keys to select any combination of files and folders.
2. Ctrl+click the selected files and/or folders, or right-click if you are using a two-button mouse.
3. Choose **PGP**, then **Shred** from the shortcut menu. A PGP screen is displayed, asking if you are sure you want to Shred the listed files.
4. Click **OK.** The file(s) are Shredded (secure deleted) from your system; they do not appear in the Trash.

Decrypt/Verify

If you have a PGP Zip (.pgp) file on your system, you can decrypt and verify it in the Finder. Decrypt/verify will always decrypt an encrypted (.pgp) file. However, if the encrypted file was not signed, then the file will not be verified (as there's no signature to verify).

You can also decrypt/verify a PGP key (`.asc`) file, but this is just for importing the keys, not for decrypting or verifying the file. For more information about importing PGP keys from a `.asc` file in the Finder, see *Import a PGP Key* (on page 41).

To decrypt/verify a PGP Zip file in the Finder

1. In the Finder, select the PGP Zip (`.pgp`) file you want to decrypt/verify.
2. Ctrl+click the selected files and/or folders, or right-click if you are using a two-button mouse. Choose **PGP**, then **Decrypt & Verify** from the shortcut menu. The Enter PGP Passphrase dialog box is displayed.
3. Enter the appropriate passphrase for the private key. If the passphrase is cached, you aren't prompted for it.

   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 (either physically or over the network) and you would like to see the characters of your passphrase as you type, select the **Show Keystrokes** checkbox.
4. To save your passphrase in the Mac OS X Keychain, select the box. You will not need to enter the passphrase the next time you access this feature.
5. Click **OK**. The file is decrypted at the location of the `.pgp` file. If the file was signed, PGP Desktop opens the Verification Info window and displays the results of the verification of the file.

Mount or Unmount a PGP Virtual Disk Volume

If you have an unmounted PGP Virtual Disk (.pgd) file, you can mount the corresponding PGP Virtual Disk volume from the Finder. For more information about PGP Virtual Disk volumes, see Using PGP Virtual Disks.

To mount a PGP Virtual Disk volume from the Finder

1. In the Finder select the PGP Disk (`.pgd`) file for the volume you want to mount. Ctrl+click the selected `.pgd` file, or right-click if you are using a two button mouse. From the **PGP** menu, select **Mount**. The Enter PGP Passphrase dialog box is displayed.
2. Enter the passphrase that protects the PGP Disk volume you want to mount.

   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 (either physically or over the network) and you would like to see the characters of your passphrase as you type, click **Typing Hidden**.
3. Click **OK**. The PGP Disk volume is mounted.

To unmount a PGP Virtual Disk volume in the Finder

1. Select the *mounted* PGP Disk (`.pgd`) file for the volume you want to unmount.
2. Ctrl+click the `.pgd` file, or right-click if you are using a two-button mouse. From the shortcut menu, choose **Unmount** from the **PGP** menu. The selected PGP Disk volume is unmounted.

Tip: If the menu says **Mount**, then the volume is already unmounted.

Import a PGP Key

PGP keys can be exported from PGP Desktop as `.asc` files. This is a good way to back up your keys or exchange your public keys with others. If you have an `.asc` file on your system that includes a PGP key that you want on your keyring, you can import it from the Finder.

To import keys from an .asc file in the Finder

1. In the Finder, locate the PGP key (`.asc`) file with the PGP keys you want to import.
2. Double-click the selected `.asc` file. PGP Desktop opens and the Select Keys dialog box is displayed.

3 Select the PGP key(s) you want to import, then click **OK**. The selected key(s) are added to your keyring.

Tip: You can also import a key by selecting File > Open and browsing to the desired `.asc` file.

Add PGP Public Keys to Your Keyring

PGP Desktop stores your PGP keys on keyrings; you always have one private keyring (`.skr`) file that holds private keys and one public keyring (`.pkr`) file that holds public keys.

If you have a public keyring file (not your active public keyring file) on your system that holds keys you would like to add to your active keyring, you can add them from the Finder.

To add PGP public keys from a keyring file in the Finder

1 In the Finder, drag the PGP public keyring (`.pkr`) or PGP private keyring (`.skr`) file and drop it onto your active keyring in the PGP DT window. The Select Keys dialog box opens and displays the public keys on the selected public keyring file.

2 Select the keys you want to add to your active keyring, then click **OK**. You can use **Select All** or **Select None** and the Shift and Command keys to select the desired keys. The Select Keys dialog disappears and the selected keys are added to your active keyring.

Tip: In the Finder, double-click the PGP public keyring (`.pkr`) or PGP private keyring (`.skr`) file. The new keyring will appear in PGP Desktop, below your existing keyrings, as "PGP Public Keyring."

Extract the Contents of a PGP Zip Archive

If you have a PGP Zip archive on your system whose contents you want to extract, you can do that in the Finder.

To extract the contents of a PGP Zip archive in the Finder

1 In the Finder, select the PGP Zip archive (.pgp) file whose contents you want to extract.

2 Ctrl+click the `.pgp` file, or right-click if you are using a two-button mouse. From the shortcut menu, choose **Decrypt & Verify** from the `PGP` menu. The Enter PGP Passphrase dialog box is displayed.

3 Enter the passphrase that protects the PGP Zip archive from which you are extracting files, then click **OK**. The file(s) are extracted from the archive to the same location in the Finder as the archive.

4 If the archive was signed, the Verification Info dialog is displayed.

Viewing the PGP Log

Use the PGP Log to see what actions PGP Desktop is taking to secure your data. For more information, see *Viewing the PGP Log* (on page 118).

6 Working with 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.

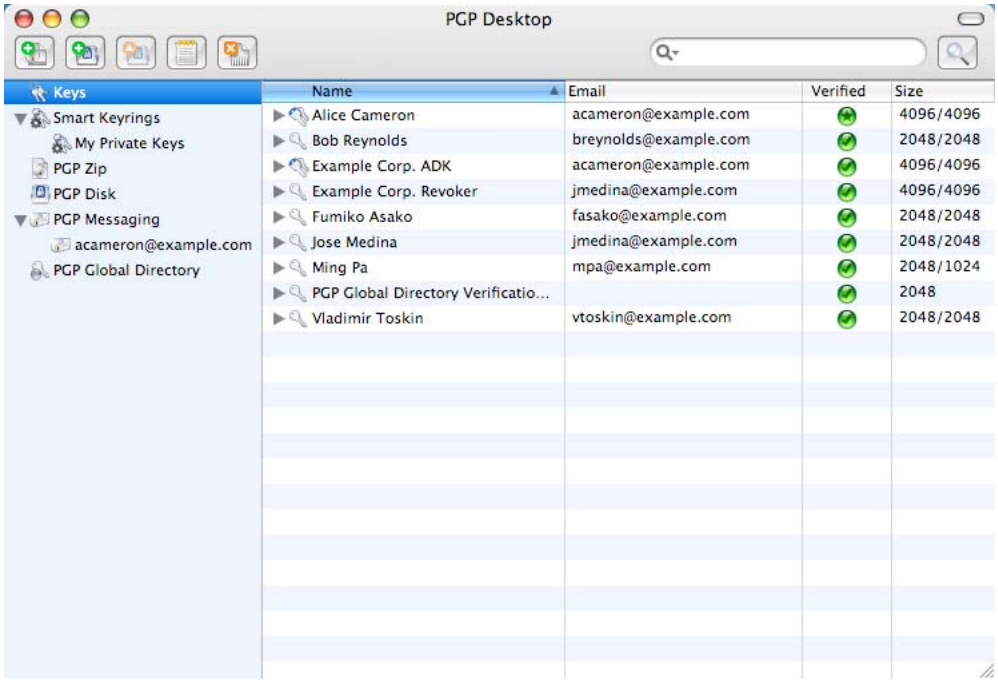
This section describes viewing keys, creating a keypair, distributing your public key, getting the public keys of others, and working with keyservers.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

Viewing Keys

To view all of the keys on the local keyring, open PGP Desktop and click the **Keys** item.



You can also use the *Smart Keyrings* feature. A Smart Keyring is a set of keys that fits the criteria you establish. For example, if you frequently send messages to PGP Desktop users from a particular email domain, you could create a Smart Keying that shows just the users from that email domain. The default Smart Keyring is *My Private Keys*.

Some of the more common tasks you may want to perform are available from the PGP Keys work area. These are:

- Send an email to the owner of a public key. To do this, Ctrl+click (or right-click) a public key in any view of the PGP Keys on your keyrings and select **Send Email**.
- If you perform a search, and you select a public key found in the search that is not on your local keyrings, add the key to your keyring. To do this, Ctrl+click (or right-click) the key and select **Add to Default Keyring**.
- To see the properties of any key displayed in the work area, double-click any part of the key listing to display the Key Info dialog box for that key.

Creating a Smart Keyring

To create a Smart Keyring

1. Open PGP Desktop.
2. Click the **Keys** item.
3. Select **File > New > Smart Keyring**. The New Smart Keyring dialog box is displayed.
4. In the **Smart Keyring name** field, enter a descriptive name for the Smart Keyring you are creating.
5. In the **Include keys which match the following conditions** menu, select either:
   - **Any**. Displays keys that match any of the specified criteria (logical "OR").
   - **All**. Only displays keys that match all of the specified criteria (logical "AND").
6. In the first matching column, select one of the following:
   - **Key is**. Displays keys that meet the criteria.
   - **Key is not**. Displays keys that do not meet the criteria.
   - **Name**. Displays keys with the specified criteria in the Name.
   - **Email**. Displays keys with the specified criteria in the Email address.
   - **Key ID**. Displays keys with the specified criteria in the Key ID.
   - **Key Size**. Displays keys of the specified Key Size.
   - **Creation Date**. Displays keys created on the specified Creation Date.
   - **Expiration Date**. Displays keys that expire on the specified Expiration Date.
7. The options in the second matching column change based on what you selected in the first matching column; select between:
   - **Public**. Matches on public keys only.
   - **Private**. Matches on private keys only.
   - **Revoked**. Matches on revoked keys only.
   - **Enabled**. Matches on enabled keys only.
   - **Expired**. Matches on expired keys only.
   - **Signed by**. Matches on keys signed by the specified person.
   - **Contains**. Matches when key contains specified criteria.

- **Does not contain**. Matches when key does not contain specified criteria.
- **Is**. Matches when specified criteria (name or date) is met.
- **Is not**. Matches when specified criteria is not met.
- **Is at least**. Matches when specified criteria is at least the key size entered.
- **Is at most**. Matches when specified criteria is no great than the key size entered.
- **Is on or before**. Matches when specified date is on or before the listed date.
- **Is on or after**. Matches when specified data is on or after the listed date.

8 In the text box that is available for some matching items, you can enter text (such as an email address or a domain; wildcards are allowed), numbers, or dates.

9 To add extra rows for matching or excluding, click the plus sign icon. Click the minus sign icon to remove rows.

10 Click **Save**. The Smart Keyring is displayed in the Items list.

When you select this Smart Keyring, only those keys that match these criteria are listed. The following Smart Keyring, for example, matches the public keys of PGP Desktop users at your company's law firm.

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 have not, you need to now. Most of the things you do with PGP Desktop require a keypair.

Caution: It is bad practice to keep creating new keys for yourself. A PGP keypair is like a digital driver's license or passport; if you create lots of them, you're going to end up confusing yourself and those people who want to send you encrypted messages. It is best to have only one key that contains all the email addresses that you use. The PGP Global Directory will publish only one key per email address.

If you are using PGP Desktop in a PGP Universal Server-managed environment, keypair creation may be disabled.

To create a PGP keypair

1 Open PGP Desktop.

2 From the **File** menu, select **New > PGP Key**. The Create a key to secure your communications dialog box is displayed. Information on this dialog box explains what a key pair is and how it is used.

3 To specify advanced properties for your new key, select the Expert Mode checkbox if you want to specify advanced properties for your new key. For more information on these settings, see *Expert Mode Key Settings* (on page 50). Skip this step if you do not want to use Expert Mode.

4 Click **Continue**. The Set your key's contact information dialog box is displayed.

5 Enter your real name in the **Full Name** field and your correct email address in the **Email Address** field.

Note: It is not absolutely necessary to enter 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.

6 Click **Continue**. The Set your key's passphrase dialog box is displayed.

7 Enter a passphrase for the key you are creating, then enter it again to confirm it.

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, click **Show Keystrokes**.

Caution: Make sure that your passphrase is one that you can easily remember (without writing it down). Unless your PGP administrator has implemented a PGP key reconstruction policy for your company, no one, including PGP Corporation, can salvage a key with a forgotten passphrase.

The Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating by comparing the amount of entropy in the passphrase you type against a true 128-bit random string (the same amount of entropy in an AES128 key). For more information, see *The Passphrase Quality Bar* (on page 202).

8 To save this passphrase in the Mac OS X Keychain, select the check box.

9 Click **Continue**. The PGP Key creation summary dialog box is displayed.

10 If desired, do the following:

- To show details about the key, select **Show Details**.
- To make any changes to your key, click **Go Back**.

11 Click **Create Key**. PGP Desktop generates your new keypair. This process can take several minutes.

12 When the key generation process indicates that it is complete, click **Finish**.

Expert Mode Key Settings

1 When you select **Expert Mode** on the New PGP Key dialog box, in addition to specifying your name and email address, you also specify:

- **Key Type**. Choose between **Diffie-Hellman/DSS** and **RSA**.

Note: Beginning with PGP Desktop 9.0, the older RSA Legacy key format from the early 1990s is no longer fully supported. You cannot create **new** PGP keypairs using the RSA Legacy key format; however, **existing** RSA Legacy keypairs continue to be supported in PGP Desktop.

- **Keyserver**. Specify a trusted keyserver or **<None>**.
- **Allowed Compression**. Deselect any compression type you do not want the key you are creating to support.
- **Allowed Ciphers**. Deselect any cipher you do not want the key you are creating to support.
- **Allowed Hashes**. Deselect any hash 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 cipher is specified. Only a cipher that is allowed can be selected as preferred.
- **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.
- **Key size**. Enter from 1024 bits to 4096 bits. The larger the key, the more secure it is, but the longer it will take to generate.
- **Key Expires.** Select **Never** or specify a date on which the key you are creating will expire.

2 Click **Continue**. The Set Your Key's Passphrase dialog box is displayed.

3 Enter the passphrase that you would like to use with this key, then type it again in the **Confirm your passphrase** field. It is critical that you keep this passphrase secret.

4 Click **Continue.**

5 Review the summary information, then click **Create Key** to begin the key generation process. PGP Desktop generates your new keypair.

This process can take several minutes.

6 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.

7 Read the text on the screen and click **Next**.

8 Click **Skip** to prevent the public key from being posted to the PGP Global Directory. The Completing the PGP Global Directory Assistant screen is displayed.

9 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 item.

Protecting Your Private Key

PGP Corporation recommends that you take these actions immediately after you create your keypair:

Caution: 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* (on page 52).
- 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 64, on page 65).

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.

Protecting Keys and Keyrings

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 diskette, 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. Use the Keys tab of the Options dialog box to specify a name and location for your private and public keyring files.

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 diskette. 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.

Keys generated on a smart card cannot be backed up because the private portion of your keypair is non-exportable. (Keys can be generated on a smart card on Windows systems only.)

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 dialog box (for Windows) and in the Keys section of the Preferences dialog box (for Mac OS X).

Backing up Your Private Key

To back up your private key

1. In the Smart Keyrings item, 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 in the **Save As** field and specify a location in the **Where** field.
5. Select the **Include Private Key(s)** check box. This is important, because if you do not do this, only your *public* key will be exported.
6. Click **Save**.
7. Copy the file 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.

Note: If you are in a PGP Universal Server-managed environment and your key mode is SKM, you cannot export your key using this method. To export your keypair, ask your PGP Universal Server administrator to export it from the management console. To determine what your key mode is, see *Key Modes* (on page 115).

What if You Lose Your Key?

If you lose your key 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 key restoration policy for your company. For more information, see *PGP Key Reconstruction* (see "Reconstructing Keys with PGP Universal Server" on page 82, "If You Lost Your Key or Passphrase" on page 82) and contact your PGP administrator.

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; and 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* (see "Placing Your Public Key on a Keyserver" on page 54).

  Generally none of the other methods are necessary once your key is published to this directory.
- *Include your public key in an email message* (see "Including Your Public Key in an Email Message" on page 55).
- *Export your public key or copy it to a text file* (see "Exporting Your Public Key to a File" on page 55).

On Windows systems, you can also:

- Copy from a Smart Card directly to someone's keyring.

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. Ctrl+click the keypair whose public key you want to send to the keyserver.
3. Select **Send Key To Server**, then select the keyserver you want to send the public key to from the list. If the keyserver you want to send your public key to is not on the list, see *Working with Keyservers* (on page 58).

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. Open PGP Desktop.
2. Open your email client, create a new message, and address it to the person to whom you are sending your public key.
3. From PGP Desktop, drag and drop your keypair onto the body of the email message.
4. Send the message.

If this method does not work for you, you can open PGP Desktop, select your keypair, then select **Edit > Copy**. Open an email message, then paste the public key into the body of the message. With some email applications you can simply drag your key from PGP Desktop into the text of your email message to transfer the public key information.

Exporting Your Public Key to a File

Another method of distributing your public key is to export 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 your keypair, then select **File > Export**. Enter a name and a location for the file, then click **Save**. Be sure *not* to include your private key along with your public key if you plan on giving this file to others.
- Ctrl+click the key you want to save to a file, select **Export** from the list, enter a name and a location for the file, then click **Save**. Be sure *not* to include your private key along with your public key if you plan on giving this file to others.

- Select your keypair, then select **Edit > Copy**. Open a text editor and select **Paste** to insert the key information into the text file, and save the file. You can then email or give the file to anyone you like. The recipient needs to use PGP Desktop on his or her system to retrieve the public key portion.

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 in PGP Desktop.

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.

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.

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.

To get someone's public key from a keyserver

1. Open PGP Desktop.
2. Click the PGP Global Directory item or the item of another keyserver you want to search. The Search for Keys screen is displayed in the Work area.
3. Specify your search criteria, then click **Search**.
   - If the keyserver you want to search is not shown, from the **Keys** menu, select **Add Keyserver**, and configure it.
   - You can search for keys on a keyserver by specifying values for multiple key characteristics. You can also search for exclusions, such a 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, Ctrl+click it and select **Add To Default Keying**. The selected key is added to your keyring.

Tip: If you set the search criteria to look for a very common name (for example, 'Name', 'contains', "John"), only the first match found is returned. This is by design, to prevent phishing (or harvesting keys from a keyserver). For common names or domains, you may have to enter the entire name or email address in order to find the correct key.

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 opens the Select key(s) dialog box.
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 Keyservers

PGP Desktop understands the following kinds of keyservers:

- **PGP Universal keyservers**. If you are using PGP Desktop in a domain protected by a PGP Universal Server, PGP Desktop is pre-configured 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 pre-configured 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 keyservers) 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.
- **PGP Universal Services Protocol**. The PGP Universal Services Protocol (USP) is a SOAP protocol operating over standard HTTP/HTTPS ports. This is the default key lookup mechanism. If you are in a PGP Universal Server-managed environment, all key search requests as well as all other communications between the the PGP Universal Server and PGP Desktop use PGP USP.
- **Other keyservers**. In most cases, other keyservers are other public keyservers. However, you may have access, through your company or some other means, to a private keyserver.

For more information about working with keyservers, see *Keys Preferences* (on page 190).

Using Master Keys

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, and PGP Zip. This saves you the step of dragging the keys that you regularly use into the **Recipients** field.

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.

Note: If you generated your key using the Setup Assistant, your key is automatically added to the Master Key list. If you skipped key generation and imported your key into PGP Desktop, your key is not automatically added to the list.

Adding Keys to the Master Key List

To add keys to the Master Key List

1. Open PGP Desktop.
2. Select **PGP > Preferences**.
3. Select the **Master Keys** icon.
4. Click the plus sign icon beneath the key list. The Select Master Keys dialog box is displayed.
5. From the **Name** list on the left, select the key(s) that you want to use. Use Shift+click or Cmd+click to select multiple keys.

6 After selecting the keys you want, click **OK.** The keys you have selected appear in the Master Key List.

Deleting Keys from the Master Key List

To remove keys from the Master Key List

1 Open PGP Desktop.

2 Select **PGP > Preferences**.

3 Select the **Master Keys** icon.

4 Select the key(s) that you want to remove. You can Shift+click or Cmd+click to select multiple keys.

5 Click the minus sign icon beneath the key list. The key(s) are removed.

7 Managing PGP Keys

This section describes how to manage keys with the PGP Desktop application.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

Examining and Setting Key Properties

The Key Info dialog box displays everything there is to know about a key. 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
- Key usage

Note: If you are in a PGP Universal Server-managed environment and your key mode is SKM, you cannot make changes to your key. In addition, SKM keys are set to never expire. To determine what your key mode is, see *Key Modes* (on page 115).

To view a key's properties

1. Open PGP Desktop, then click the Keys item. All keys on your keyring appear.
2. Double-click the key with the properties you want to view. The Key Properties dialog box for the key you selected is displayed.

Adding and Removing Photographs

You can include a photograph to your Diffie-Hellman/DSS and RSA keys.

Note: When you add or change key information, be sure to update it on the keyserver so that your most current key is always available.

Caution: Although you can view for verification the photograph accompanied with someone's key, the digital fingerprint is the final word. Always check and compare it.

To add your photograph to your key

1. Open PGP Desktop, then click **My Private Keys**.
2. Double-click the private key to which you are adding the photo. The Key Info dialog box for the selected key is displayed.
3. Click the plus sign icon under the current photo for the key. The Add Photo dialog box is displayed.

4 Drag and drop, or paste, your photograph into the blank area of the Add Photo dialog box.

Note: The photograph can be from the Clipboard, a JPG, or BMP file. For maximum picture quality, crop the picture to 120 x 144 pixels before adding it. If you do not do this, PGP Desktop scales it for you.

5 Click **OK**. The Enter PGP Passphrase dialog box is displayed, unless the passphrase for the key you are modifying is cached.

6 Enter your passphrase for the key you are modifying, then click **OK**. Your photo ID is added to your private key.

To view an enlargement of the photo

- Click the magnifying glass icon under the existing photo. A window displaying an enlarged version of the photo ID appears. To remove the enlargement, click inside the window.

To delete a photo ID

1 Click the minus sign icon under the existing photo. A confirmation dialog box is displayed.

2 Confirm that this is your choice. The photo is removed from the key.

To copy a photo ID

- Right-click the existing photo on the Key Properties dialog box and select **Copy Photo ID**. You can then paste the photo into another key or into a graphics program.

Managing User Names and Email Addresses on 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/address to your keypair

1 Open PGP Desktop, then double-click the appropriate key. The Key Info dialog box for the key you double-clicked is displayed.

2 Click **Add Email Address**. The Add Name dialog box is displayed.

3 Enter the new **Full Name** and **Email Address** in the appropriate fields, then click **OK**. The Enter PGP Passphrase dialog box is displayed, unless the passphrase for the key you are modifying is cached.

4 Enter 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.

Note: When you add or change information in your keypair, always synchronize it with your keyserver so that your most current key is always available.

To delete a name/email address from your keypair

1 From the list of keys, click the plus sign to the left of the key name to expand the key.

2 Select the user ID you want to delete.

3 Press the Delete key on your keyboard. A confirmation dialog box is displayed.

Tip: You can also select **Edit > Delete** (on Windows systems) or **Edit > Clear** (on Mac OS X systems).

4 Click **Delete**. The user ID is deleted.

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.

Tip: Changing your passphrase on your key does not change the passphrase on any copies of the key (such as backups you may have made). If you think your key has been compromised, PGP Corporation recommends that you shred any previous backup copies and then make new backups of your key.

If you are in a PGP Universal Server-managed environment and your key mode is SKM, you cannot change the passphrase for your key. SKM keys are protected by a randomly generated passphrase (that is itself protected) and you are never prompted to enter a passphrase for an SKM key. To determine what your key mode is, see *Key Modes* (on page 115).

To change your private key passphrase

1. Open PGP Desktop, then double-click the appropriate key. The Key Info dialog box for the key you double clicked is displayed.
2. Click **Change Passphrase**, then select **Change Passphrase** from the list of commands displayed. The Enter PGP Passphrase dialog is displayed.
3. Enter the *current* passphrase for the private key, then click **OK**. The Confirm PGP Passphrase dialog box is displayed.
4. Enter your new passphrase in the first text field.
5. Re-enter your passphrase in the **Confirmation** field.

   The Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating by comparing the amount of entropy in the passphrase you type against a true 128-bit random string (the same amount of entropy in an AES128 key). For more information, see *The Passphrase Quality Bar* (on page 202).
6. Click **OK**. An information dialog box is displayed, informing you the passphrase has been changed.
7. Click **OK**. The passphrase is changed.

Caution: If you are changing your passphrase because you feel that it has been compromised, it is recommended that you shred all backup keyrings, then make a backup copy of the key with the new passphrase.

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 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, as well as delete user IDs from a keypair as long as that is not the only user ID on the keypair.

Note, however, that you cannot delete a user ID on a key if it is the only user ID, and you cannot delete self-signatures from keys.

To delete a key from your PGP keyring

1. Open PGP Desktop, then click the **Keys** item. All keys on your keyring appear.
2. Do one of the following:

- To delete a key, select the key, select **Edit > Clear**, then click **OK** on the Confirmation dialog box. The key is deleted from your keyring.
- To delete a user ID (from a public key) or signature, click the triangle to the left of the key with the User ID or Signature that you want to delete to display the user IDs and signatures. When you see the user ID or signature you want to delete, click the User ID, select **Edit > Clear**, then click **OK** on the Confirmation dialog box. The user ID or signature is deleted.

Remember that you cannot delete a user ID from a keypair.

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, then click the Keys item. All keys on your keyring appear.
2. Double-click the public key you want to disable. The Key Info dialog box for the key you selected is displayed.
3. Locate the **Enabled** field in the Key Properties.
   - If the current **Enabled** setting is **Yes**, the key is enabled. To disable the key, click **Yes** once. The **Enabled** field changes to **No;** the key is disabled.
   - If the current **Enabled** setting is **No,** the key is disabled. To enable the key, click **No** once. The **Enabled** field changes to **Yes** and the key is enabled.

A disabled key cannot be used to encrypt, sign, decrypt, or verify.

Tip: You can also synchronize keys on your keyring with the PGP Universal Server. This option is used primarily to enable/disable public keys on your keyring. To do this, right-click (or Ctrl+click) a key and choose **Synchronize**.

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 the digital fingerprint of a public key

1. Open PGP Desktop, then click the Keys item. All keys on your keyring appear.
2. Double-click the public key with the fingerprint that you want to check. The Key Info dialog box is displayed.
3. Locate the **Digital Fingerprint** in the second section of the Key Info dialog box.

   If necessary, click the triangle to face downward and display the fingerprint, which is shown either in hexadecimal format (10 sets of four characters per set) or word list format (four columns with five unique words per column).
4. Compare the fingerprint on the key with the original fingerprint. If the two are the same, then you have the real key—otherwise, you likely do not.

   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.
5. If you have a forged key, delete it.
6. Open your Web browser, navigate to the *PGP Global Directory* (https://keyserver.pgp.com), and search 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 the correct person, you can sign that person's public key, indicating that you have verified the key. When you sign someone's public key, a signature icon along with your user name is shown attached to that key.

If you import a keypair from a backup or from a different computer, that keypair needs to be signed.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, key signing may be disabled.

To sign a key

1. Open PGP Desktop, then click the **Keys item**. All keys on your keyring appear.
2. Select the key you want to sign, then from the **Keys** menu, select **Sign.** The Sign Key dialog box is displayed with the user name/email address and hexadecimal fingerprint displayed in the text box.

   Tip: You can also Ctrl+click the key (or right-click it if you have a two-button mouse). When the shortcut menu is displayed, select **Sign.**
3. Under **Sign With Key**, click to display and select which of your keys you want to sign with.
4. To allow your signature to be exported with this key, select **Allow signature to be exported**.

   An exportable signature is one that is allowed to be sent to servers and travels with the key whenever it is exported. The checkbox indicates your approval that your signature be exported.
5. In the **Select Items to Sign** box, verify that you are signing the right key.
6. If you want to configure additional options, such as such as signature type and signature expiration, click **Options**.
7. 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 keyserver or exported in any way.

- **Exportable**. Use exportable signatures in situations where your signature is sent with the key to the keyserver, so that others can rely on your signature and trust your keys as a result. This is equivalent to checking 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.

8 In the **Expires** field, select **Never** if you do not want this signature to expire. Otherwise, select a date for it to expire.

9 In the **Advanced** field, specify a maximum depth for trust and a domain restriction:

- The **Maximum 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, enter the domain name in the **Domain Restriction** text box.

10 Click **Sign**. The Enter PGP Passphrase dialog box is displayed (if your passphrase was not saved in the Keychain).

11 Type the passphrase of the signing key, if required. PGP Desktop does not ask you to type your passphrase if it is cached.

12 Click **OK**. The key is signed.

Revoking Your Signature from a Public Key

You may, on occasion, want or need to revoke your signature from a key on your keyring.

To revoke your signature

1 Open PGP Desktop, then click the **Keys** item. All keys on your keyring appear.

2 Click the triangle to the left of the key from which you want to revoke your signature. The signatures appear.

3 Click your signing key.

4 Select **Edit > Revoke**. A confirmation dialog box is displayed.

5 Verify that the Key ID and Name are the correct key (from which you want to revoke your signature) and click **OK**. The PGP Enter PGP Passphrase for Key dialog box is displayed.

6 Enter your passphrase and click **OK**. Your signature is revoked from the key.

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.

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 is your own key and thus you trust it completely). You shouldn't have anyone else's keypairs.

For more information about trusting keys, see *An Introduction to Cryptography*.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, the ability to grant trust to keys may be disabled.

To grant trust to a key

▸ **To grant trust to a key**

1 Open PGP Desktop, then click the Keys item. All keys on your keyring appear.

2 Double-click the key for which you are granting trust. The Key Info dialog box is displayed.

3 In the **General Information** section, click the current **Trust** field setting. A menu of trust settings is displayed.

4 Select the desired setting.

Note: Selecting a Trust setting of **None** or **Marginal** is not intended to indicate that an owner of a key is untrustworthy or dishonest. It means that *you do not have enough information* to be sure that a key's owner or source is genuine.

Working with Subkeys

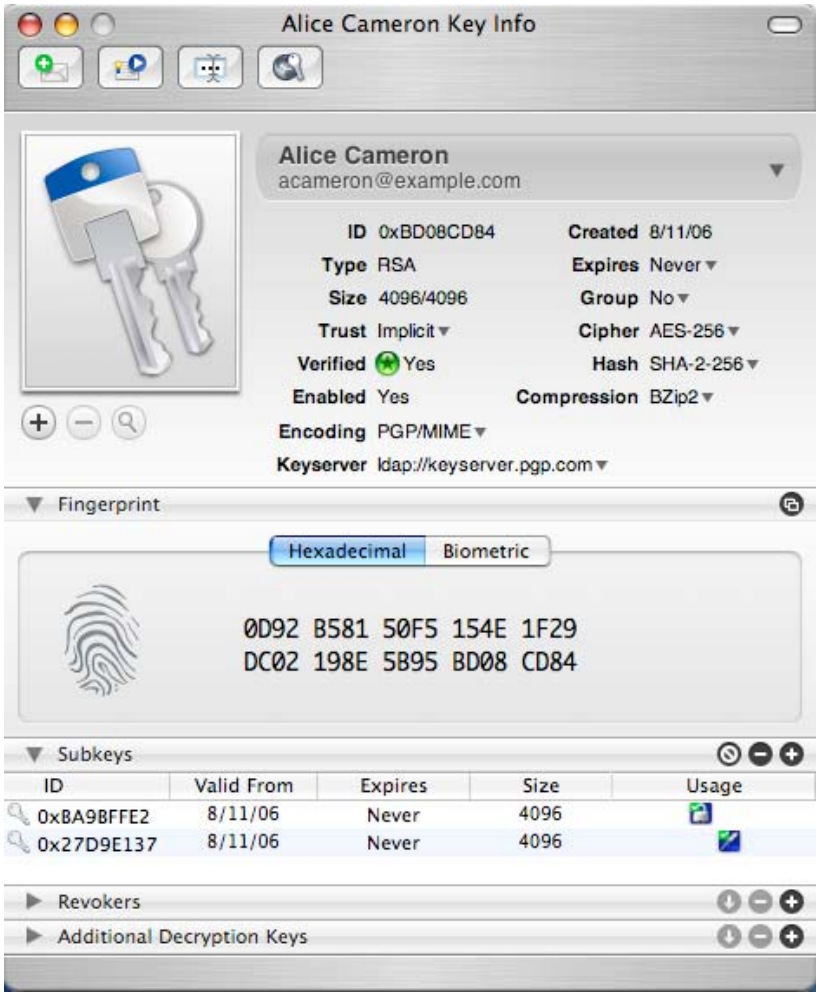
A PGP Desktop keypair consists of these elements:

- 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 box. The Usage column indicates the function that a subkey performs:



Key	Description
	Encryption subkeys display a blue padlock symbol.
	Signing subkeys display a blue pen symbol.
	Subkeys used for both encryption and signing display both symbols.
	The default encryption subkey displays a small green checkmark in the upper left corner.
	The default signing subkey displays a small green check mark in the upper left corner.

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 keypairs. However, you can only view subkey information on the public keys on your keyring.

To see what subkeys are on a key

1. Open PGP Desktop, then click the Keys item. All keys on your keyring appear.
2. Double-click the key with the properties you want to view. The Key Properties dialog box for the key you selected is displayed.
3. Click the triangle to the left of **Subkeys**. The Subkeys information for this key is displayed.

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 15).

To create new subkeys for a keypair

1. In the **Subkeys** section of the Key Properties dialog box, click the plus sign icon. The New Subkey dialog box is displayed.
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, type a key size from 1024 to 4096 bits.
4. In the **Start Date** field, enter a date on which the subkey you are creating becomes effective.
5. In the **Expiration Date** field, select **Never**, or specify a date. This information controls when the subkey expires.

   Note: To avoid confusion when maintaining more than one subkey on your keypair, try not to overlap the start and expiration dates of your subkeys.
6. Click **Create**. The Passphrase dialog box is displayed.
7. Enter your passphrase and then click **OK**. The subkey is created.

Note: When you add or change information in your keypair, update it on the keyserver so that your most current key is always available. With the key selected in the Keys list, from the **Keys** menu, select **Update Selection**.

Specifying Key Usage for Subkeys

Each subkey can have its own key usage properties. For example, one subkey could be used for PGP WDE only, and another could be used for all other PGP Desktop functions.

An example of why you would want to set the key usage of a key is when you want to use a key for disk encryption only but you do not want to receive encrypted email. If you distribute your public key that does not allow for PGP Messaging, then email sent by another user would not be encrypted to your public key.

Note: If you are in a PGP Universal Server-managed environment and your key mode is SKM, you cannot make changes to the key usage flags. To determine what your key mode is, see *Key Modes* (on page 115).

▸ **To specify key usage**

1. Open PGP Desktop, then click the Keys item. All keys on your keyring appear.

   Double-click the key with the properties you want to view. The Key Properties dialog box for the key you selected is displayed.
2. Click the **Subkeys** heading in the Key Properties dialog box. The Subkeys for this key are displayed.
3. Double-click the subkey you want to change.
4. Click the arrow next to **Subkey Usage Edit**. The usage properties for the key are displayed.
5. In the list displayed, select the PGP Desktop functions for which this key can be used. A check next to the item indicates the key can be used for that function.
6. Click **Close** to save the subkey properties.
7. Click **Close** again to save the key properties.

Revoking Subkeys

▸ **To revoke a subkey**

1. In the **Subkeys** section of the Key Properties dialog box, select the subkey you want to revoke.
2. Click **Revoke** (backslash-circle icon above the subkey list). A confirmation dialog box is displayed.
3. Click **OK** to revoke the subkey. The Passphrase dialog box is displayed.
4. Type your passphrase, then click **OK**. The subkey is revoked and the icon changes to a key with a red circle/slash.

Removing Subkeys

▸ **To remove a subkey**

1. In the **Subkeys** section of the Key Properties dialog box, select the subkey you want to remove.
2. Click **Remove** (a minus sign icon above the subkey list). A confirmation dialog box is displayed.
3. Click **OK** to remove the subkey. 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.

ADKs are rarely used or needed outside of a PGP Universal Server-managed environment. Although your PGP administrator should not ordinarily need to use the additional decryption keys, there may be circumstances when it is necessary to recover someone's email. For example, if someone is injured and out of work for some time, or if email records are subpoenaed by a law enforcement agency and the corporation must decrypt mail as evidence for a court case.

You can only modify ADKs on your keypairs.

Adding an ADK to a Keypair

To add an ADK to a keypair

1. Open PGP Desktop, then click the Keys item. All keys on your keyring appear.
2. Double-click the keypair to which you are adding the ADK. The Key Info dialog box for the key you double-clicked is displayed.
3. If necessary, click the triangle icon, on the left side of the **Additional Decryption Keys** section, so that it is pointing downward. The ADK information for this key is displayed, if it has been configured.
4. Click the plus sign icon on the right side of the **Additional Decryption Keys** section.
5. From the list displayed, select the key you want to use as the ADK.
6. Click **OK**. The PGP Enter PGP Passphrase for Key dialog box is displayed.
7. Enter the passphrase for the key to which you are adding the ADK, then click **OK**. The ADK is added.

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 arrow icon. The ADK is updated.

Removing an ADK

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 box is displayed, asking if you are sure you want to remove the ADK.
3. Click **OK** 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, then select **My Private Keys**, under the Keys item. All of the keys on your keyring appear.

2 Double-click the key to which you are adding a revoker. The Key Info dialog box for the key you selected is displayed.

3 Click the plus sign icon on the right side of the **Revokers** section. The Select key(s) dialog box is displayed.

4 Select the key you want to use as the revoker key, then click **OK**. A PGP Warning dialog box is displayed, asking if you are certain that you want to grant revoker privileges to the selected key(s).

5 Click **Yes** to continue or **No** to cancel. The Enter PGP Passphrase for Key dialog box is displayed.

6 Enter the passphrase for the keypair to which you are adding the revoker, then click **OK**. A PGP Information dialog box is displayed.

7 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, then select **My Private Keys** under the Keys item. All of the keys on your keyring appear.

2 Ctrl+click the key you want to revoke (or right-click if you are using a two-button mouse).

3 In the shortcut menu, select **Revoke**. A Confirm Revocation dialog box is displayed, asking if you are sure you want to revoke this key.

4 Click **OK** to confirm your intent to revoke the selected key or **Cancel** to cancel.

5 Enter 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.

6 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, any attempts to sign or decrypt with it will automatically attempt to rejoin the key.

To create a split key

1. Open PGP Desktop, then click the PGP Keys item. All of the keys on your keyring appear.
2. Select the keypair you want to split. The selected keypair highlights.
3. Select **Keys > Share Key > Make Shared.** The Split Key dialog box is displayed.
4. Add shareholders for the split key by dragging and dropping their keys in the **Key/User Name** list.
5. To add a shareholder who does not have a public key, *that person must be physically present to enter their own passphrase***.** Click **Add**.
   - Allow the shareholder to type in their passphrase twice, then click **OK**. Unnamed User is displayed in the list.
   - Double-click Unnamed User and enter a descriptive name for the person or organization holding the shares.
6. To specify a location for the split shares, click **Browse** in the Share File Destination Folder, then select the desired location.
7. 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 possesses, double-click the number in the Shares column and enter the number of shares they control.
8. Click **Split Key**. The Confirm Key Split dialog box is displayed.
9. Click **OK** to continue splitting the key. The Passphrase screen is displayed.

10 Enter the passphrase for the key being split, then click **OK**. A minimum of six characters is required for this passphrase. A confirmation dialog box opens.

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 a `.shf` extension.

11 Distribute the key shares to the owners, then delete the local copies of the shares.

Be sure you keep the original key that was split. You will need to have this key before you can rejoin the split key for any decryption functions.

Rejoining Split Keys

Once a key is split among multiple shareholders, attempting to sign or decrypt with it causes PGP Desktop to attempt to rejoin the key automatically. 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 enter 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. The PGP Desktop Transport Layer Security (TLS) feature provides a secure link to transmit key shares, allowing multiple individuals in distant locations to securely sign or decrypt with their key share.

Caution: Before receiving key shares over the network, you should verify each shareholder's fingerprint and sign their public key to ensure that their authenticating key is legitimate.

Before you begin, be sure you have the original key that was split on the rejoining computer.

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 the Finder to select the file(s) that you want to sign or decrypt with the split key.

3 Ctrl+click the file(s) and select **Sign or Decrypt** from the PGP shortcut menu. The Enter PGP Passphrase for Selected Key screen is displayed with the split key selected.

4 Click **OK** to reconstitute the selected key. The Key Share Collection screen is displayed.

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 removable drive, or a mounted drive. Continue with the next step.
- If you are collecting key shares over the network, click **Start Network**.

  The Passphrase dialog box opens. In the **Signing Key** field, select the keypair that you want to use for authentication to the remote system and enter 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 is displayed. 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.

If You Lost Your Key or Passphrase

If you lost your key, you can reconstruct your key so you can continue to encrypt and decrypt data. How you do this depends on if you are using PGP Desktop in a standalone environment or in a PGP Universal Server-managed environment.

If you forgot your passphrase, you can reset your passphrase. To do this, you answer correctly three of the five security questions you answered when you set up your key or created your security questions.

Reconstructing Keys with PGP Universal Server

This section applies only to PGP Desktop users in a PGP Universal Server-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 or when you create your security questions.

Once your key is on the server, you can restore it at anytime by selecting **Keys > I Lost My Key** or **Keys > I Forgot My Passphrase** in PGP Desktop for Windows, or **Keys > Reconstruct** in PGP Desktop for Mac OS X.

Tip: If you were not prompted to create your PGP questions during installation of PGP Desktop, and your PGP Universal Server administrator allows local key reconstruction, you can manually create your questions. For more information, see *Creating Your Security Questions* (on page 83).

Creating Key Reconstruction Data

When you answer the PGP security questions, you are creating the key reconstruction data. In a standalone environment, this information is stored on your local disk in a .krb file. In a managed environment, you send the key reconstruction data to your company's PGP Universal Server whenever you install PGP Desktop or when you reset your key.

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?"

When you have created and answered all five PGP questions, 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.

Creating Your Security Questions

Before you can reconstruct your key or create a new passphrase when you've forgotten it, you must create your security questions. You can customize the five security questions so that the answers are something that only you would know.

To create your security questions

1. In PGP Desktop, click the Keys item and then select your key.
2. Select **Keys > Create My PGP Questions**. The PGP Security Question Assistant is displayed.
3. When the Key Reconstruction screen dialog box is displayed, type five questions that only you can answer in the Question fields (the default questions are examples only).

4. In the first Create Security Question screen, click the arrow for the first field to select the question you want to use. Note that you can customize parts of the question in the next step.

If you want to completely customize the question to create your own question, select **Enter my own question**.

5 For **Personalize Your Question**, click the arrows next to any of the text that you can customize. For example, if you selected the first question, you can customize that question by changing "friend" to "boy" and "had a crush on" to "held hands with."

If you chose to create your own question, enter the question in this field. Be sure to enter a question that only you can know the answer to.

6 For **Answer Your Question**, enter the answer to this security question. You can enter the answer using mixed upper- and lowercase letters, or use all one case (when you answer the question, the case will not matter).

A hint is displayed in this field that disappears once you start entering the answer. For example, to answer the question "Who was the first boy that I ever held hands with?", the hint is "Enter first and last name".

7 When you have defined your question and entered the answer, click **Next** to continue. The Create Security Question 2 of 5 dialog box is displayed.

8 You are prompted to create and answer a total of five security questions. Continue to follow the steps above to select the question, customize the question, and answer the question.

9 When you have entered all five questions and answers, the Enter PGP Passphrase dialog box is displayed.

10 Enter the passphrase for your key and click **OK**.

11 You are then prompted to save the key reconstruction file. Enter the name and location where you want to save the file and click **Save**.

12 Click **Finish** to exit the assistant.

You have now defined the five security questions. If you lost your key or forget your passphrase, you can reconstruct your key or reset your passphrase by answering three of these five questions.

Reconstructing Your Key if You Lost Your Key or Passphrase

If you have lost your key or have forgotten your passphrase, you can recover by reconstructing your key. You must first have created a set of security questions that only you can answer. For more information, see *Creating Your Security Questions* (on page 83).

To reconstruct your key

1 In PGP Desktop, click the Keys item and then select your key.

2 Select **Keys > Reconstruct**.

- If you are managed by a PGP Universal Server, the PGP Passphrase Assistant: Answer Security Questions dialog box is displayed.

- If you are in a standalone environment, the Select Key Reconstruction File dialog box is displayed. Select the .krb file that you saved when you created your security questions and click **Open**.

The Key Reconstruction dialog box is displayed.

3 Answer three of the five security questions correctly and click **Continue**. The Confirm PGP Passphrase dialog box is displayed.

4 Enter and re-enter your new passphrase.

Select **Show Keystrokes** if you want to see the characters you type for your passphrase. Be sure no one can see what you type.

The Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating by comparing the amount of entropy in the passphrase you type against a true 128-bit random string (the same amount of entropy in an AES128 key). For more information, see *The Passphrase Quality Bar* (on page 202).

5 Click **OK**. Your key has been 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 diskette. 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 dialog box (for Windows systems) or the Preferences dialog box (for Mac OS X systems).

Tip: If you have changed your passphrase on your key, remember that it does not change the passphrase on any copies of the key (such as backups you may have made). If you think your key has been compromised, PGP Corporation recommends that you shred any previous backup copies and then make new backups of your key.

8 Securing Email Messages

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

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

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 (such as "In this circumstance, to this") that tells PGP Desktop what to do in specific situations. By combining these instructions, policies can be tailored to meet all of your email security requirements. 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 if you want to change them.

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 (called "All Keys" on Windows systems) or the local keyring (called "Keys" on Mac OS X systems) for the public key of the recipient. 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, which is unencrypted. This default behavior, called *Opportunistic Encryption,* strikes a balance between protecting outgoing messages and making sure they get sent.

Creating new policies is covered in detail in *Creating a New Security Policy* (on page 98).

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 Server 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 Server administrator can apply):

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

If the PGP Desktop messaging proxy is turned off, PGP Desktop will not be able to decrypt incoming encrypted messages; it will pass them along to your email client still encrypted. It is recommended that you leave your messaging proxy on all the time if you expect to be sending and receiving encrypted messages. On is the default setting.

- **Message signed, but not encrypted.** PGP Desktop will search the local keyring for a public key that can be used to verify the signature. If PGP Desktop cannot find the appropriate public key on the local keyring, it will try to search for a keyserver at keys.domain (where **domain** is the domain of the sender of the message), then the *PGP Global Directory* (https://keyserver.pgp.com), and finally any other configured keyservers. If PGP Desktop finds the right public key at any of these locations, it verifies the signature (or not, if the signature is bad) and passes the message to your email client annotated with information about the signature—information is also put into the PGP Log. If PGP Desktop cannot find the appropriate public key, it passes the message to your email client unverified.
- **Message encrypted and signed.** PGP Desktop goes through both of the processes described above: first finding the private key to decrypt the message and then finding the public key to verify the signature. However, if a message cannot be decrypted, then it cannot be verified.

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

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

Outgoing Messages

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

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

Using Offline Policy

If you are using PGP Desktop in a PGP Universal Server-managed environment, the offline mail policy is defined by your PGP Universal Server administrator. This policy defines what happens to email messages when the PGP Universal Server is offline or cannot be reached by PGP Desktop.

- **Block outbound messages**. Your outbound messages are not sent. If the messages can be queued by your mail client, they stay in the queue until the PGP Universal Server is available. If the messages cannot be queued, the email messages are blocked.
- **Send outbound messages in the clear**. You are prompted to choose if you want to allow the email message to be sent unsecured. If you choose to send, the message is sent in the clear. If you choose not to send, the message is blocked.
- **Follow standalone policy**. PGP Desktop follows the standalone policy to process your outbound messages. For more information, see *Viewing Services and Policies* (on page 92).

For information on the notifiers you receive when any of the above occurs, see *Outgoing PGP Desktop Notifier Messages for Offline Policy* (on page 34).

Your PGP Universal Server administrator can specify how often your mail policies get downloaded to PGP Desktop. When you are in offline mode, the last downloaded offline mail policy remains in effect for processing your outbound email messages. If you have been in offline mode for a period of time that is longer than the grace period allowed for the offline standalone mail policy to be in effect, your administrator could have also specified how outgoing email should be processed. In this case, PGP Desktop can start blocking your outbound messages or the same offline standalone mail policy can be used for processing your outbound messages, depending on how policy is defined by your administrator.

When you have been offline for some time, you can manually request a download of policy from the PGP Universal Server once you are back online. To do this when you are back online, select the PGP Desktop icon in the tray and then select **Update Policy**. The latest policies are downloaded from the PGP Universal Server and any client logs are uploaded to the server. The option to manually update a policy is available for managed users only.

If your PGP Universal Server administrator allows you to use standalone policies, see *Creating a New Security Policy* (on page 98).

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:

- **Encrypt and Sign Buttons**. Specifies that email is both signed and encrypted when both the **Encrypt** and **Sign** buttons are enabled in Microsoft Outlook 2002, 2003, or 2007. This policy is available only on PGP Desktop for Windows.
- **Sign Button**. Specifies that email is signed when the **Sign** button is enabled in Microsoft Outlook 2002, 2003, or 2007. This policy is available only on PGP Desktop for Windows.
- **Encrypt Button**. Specifies that email is encrypted when the **Encrypt** button is enabled in Microsoft Outlook 2002, 2003, or 2007. This policy is available only on PGP Desktop for Windows.
- **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.

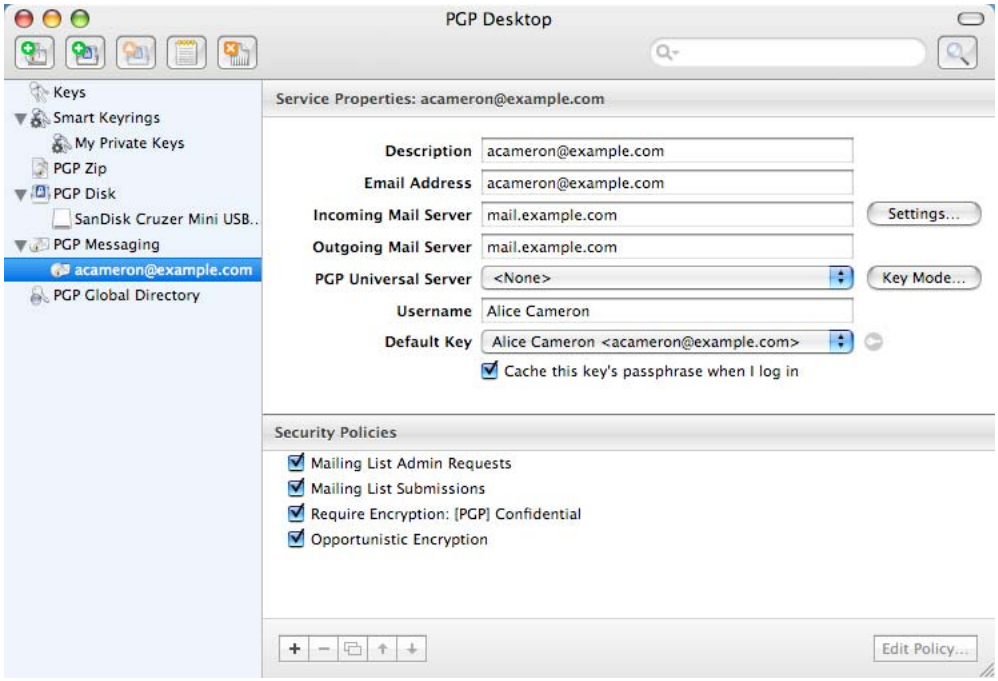
Do not put Opportunistic Encryption first in the list of policies (or anywhere but last, for that matter) because when PGP Desktop finds a policy that matches, and Opportunistic Encryption matches everything, it stops searching and implements the matching policy. So if a policy is lower on the list than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

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

Viewing Services and Policies

To view services and policies

1. Open PGP Desktop and click the PGP Messaging item.
2. Click the name of the service whose account properties you want to view. The settings for the selected service appear in the PGP Messaging Work area.
3. To view the details of a policy, under **Security Policies**, click the name of the policy you want to view and click **View Policy**. The settings for the policy are displayed. This section provides information on what security policy is being enforced. If you are managed by a PGP Universal Server, the security policies are set by your administrator.



If you are using PGP Desktop in a PGP Universal Server-managed environment, you may have the option to override server policies with local policies. If specified by policy, your local policies may be enforced if your PGP Universal Server becomes unavailable for any reason.

Creating a New Messaging Service

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.

Important: 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 item. The PGP Messaging screen is displayed.
2. Click **Create New Service**. Or, from the **Messaging** menu, select **New Service**. The New Service screen is displayed. The **Service Properties** section shows default settings and the Security Policies section displays default security policies.
3. In the **Description** field, enter a descriptive name for this service. (This step is optional, but helpful when you work with multiple services).
4. In the **Email Address** field, enter the email address associated with this service (for example, acameron@example.com).
5. Type the name of your incoming and outgoing email servers, or click **Server Settings** if you want to set advanced options.
6. If you chose to set advanced options, the Server Settings dialog box is displayed.

   Enter the appropriate settings:

   - **Server Type:** Select the type of server that the new service will be using:

     PGP Universal Server—for PGP Desktop users who are in a PGP Universal Server-managed environment. Contact your PGP administrator for more details on correct settings. If you are using PGP Desktop in a PGP Universal Server-managed environment, the correct settings for the Server Settings dialog box were automatically downloaded.

     Internet Mail—for standalone PGP Desktop users who have a POP or IMAP mail connections.

   - **Name**: Enter 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 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:
- **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.
- **Require STARTTLS:** PGP Desktop requires the server honor the STARTTLS command.
- **Require SSL:** PGP Desktop requires that the server honor SSL-protected connections on the specified alternate port.
- **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.)

Caution: This option should be enabled only 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.**

- **Name**: Enter 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 available only 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:

  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.

  Require STARTTLS: PGP Desktop requires that the server honor the STARTTLS command.

  Require SSL: PGP Desktop requires that the server honor SSL-protected connections on the specified alternate port.

  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.)

Note: If you are manually connecting to a PGP Universal Server, see *Manually binding to a PGP Universal Server* (on page 209).

Editing Message Service Properties

Caution: Before making any changes to an existing messaging service, be sure to exit your email client.

To make changes to the account properties of an existing service

1. Open PGP Desktop and click the **PGP Messaging** item.

   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.

2. Make the desired changes to the account properties of the service. For more information, see *Creating a New Messaging Service* (on page 93).

Disabling or Enabling 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, you can *delete the service* (see "Deleting a Service" on page 96).

To enable or disable an existing service

1. Under the PGP Messaging item, select the name of the service you want to disable. The settings for the service appear. Confirm that you have selected the correct service.

2. Do one of the following:

   - To disable the service, select **Messaging > Disable Service**. The service is disabled.
   - To enable the service select **Messaging > Enable Service**. The service is enabled.

Tip: You can also Ctrl+click the name of the service (or right-click it if you are using a two-button mouse) and select the option to enable or disable the service from the shortcut menu.

Deleting a Service

If you are certain that you will not need a messaging service any longer, you can delete the service from PGP Desktop.

To delete a service

1. Under the PGP Messaging item, select the name of the service you want to enable. The settings for the service appear. Confirm that you have selected the correct service.
2. Ctrl+click the name of the service (or right-click it if you are using a two-button mouse) and select **Remove Item** from the shortcut menu. The service is deleted.

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 *.me.com (or *.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 dialog box for one of the services to `mail*.example.com`, and 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 PGP Messaging 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 is not 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. To do this:
  - On Windows systems, right-click the PGP Desktop tray icon and select **Stop PGP Services** from the list of commands.
  - On Mac OS X systems, hold down the Option key and select **Quit** from the PGP Desktop icon in the Menu bar.

  Note: 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 Server-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 PGP 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; by default PGP Desktop 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** is selected (in the SSL/TLS settings of the Server Settings dialog box) your mail server *must* support SSL/TLS or PGP Desktop will not 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, use a wild card for your mail server name. For more information, see *Multiple Services* (on page 96).
- Delete the PGP Messaging service that is not working correctly and send/receive email. PGP Desktop regenerates the messaging service.

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

1. Delete the PGP Messaging service that is not working correctly.
2. Stop all PGP Desktop services and then exit PGP Desktop if it was open. To stop the services:
   - On Windows systems, right-click the PGP Desktop tray icon and select **Exit PGP Services** from the list of commands.
   - On Mac OS X systems, hold down the Option key and elect **Quit** from the PGP Desktop icon in the Menu bar.
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 user name, 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:
   - On Windows systems, either restart your computer or open PGP Desktop from the Windows Start menu.
   - On Mac OS X systems, either restart your computer or open PGP Desktop.
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.
8. If you continue to have problems with a PGP Messaging service, access any of the following for assistance:
   - *PGP Corporation website* (http://www.pgp.com)
   - *PGP Support website* (https://support.pgp.com)
   - *PGP Support forums* (http://forum.pgp.com)

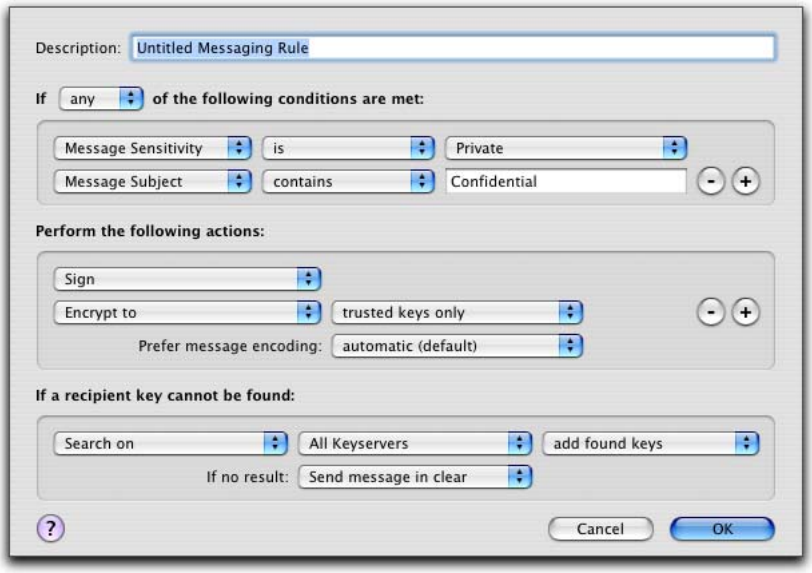
Creating a New Security Policy

Security policies control how PGP Desktop handles outgoing email messages.

Note: 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 item, click the name of the service for which you want to create a new security policy. The settings for the service appear, including the list of existing security policies.
2. Click the plus sign icon at the bottom of the screen. The Untitled Messaging Rule dialog box is displayed.



   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), 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.
5. 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 is displayed when you select **Message Header**.

Note: 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.

6 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.

7 In the third condition field, select:

- **text entry box**. Type text for the matching criteria. For example, if you selected **Message Size** i**s greater than**, then type a number representing the size of the message.
- **normal**. Matching criteria for Message Sensitivity is *normal*.
- **none** or **normal**. Matching criteria for Message Sensitivity is *none* (for Mac OS X systems) or *normal* (for Windows systems).
- **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*.

Create more condition lines by clicking the plus sign icon.

8 In the **Perform the following actions on the message** section, 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.

9 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. Will also encrypt to a verified key, if available.
- **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 Server-managed environment, this is a Client Key Mode key which is different from 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 in the **Group** field on the Key Properties dialog box on Windows systems or the Key Info dialog box on Mac OS X systems. **No** means that the key *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. Will also encrypt to a verified key, if available.
- **a list of keys**. Specifies that the message can only be encrypted to keys on the list.

Create more action lines by clicking the plus sign icon.

10 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.

11 In the **Recipient's key is not available** section (or in the **If a Recipient key cannot be found** section on Mac OS X systems), 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.

12 In the second Key Not Found field, select:

- **All keyservers**. Allows all keyservers, including the PGP Global Directory, to be searched for an appropriate key.
- **PGP Global Directory or keyserver.pgp.com**. Specifies that only the PGP Global Directory is searched.

- **[configured keyservers]**. Specifies that only the keyserver you choose from the list of currently configured keyservers is searched. Note that keyservers 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. This option is available only on Windows systems.
- **Edit Keyserver List**. Lets you add keyservers to the list of currently configured keyservers. This option is available only on Windows systems.

13 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.

14 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.

15 Click **OK** when the policy settings are configured. The new policy is displayed in the list of security policies.

Regular Expressions in Policies

PGP Desktop supports the use of regular expressions in security policies in text entry boxes. Using regular expressions lets you match multiple text strings using a single text string.

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

Some mail policy rule conditions require that some part of an email must match a pattern. The patterns in the condition take the form of a regular expression. A regular expression is a string of characters that represents the format for a term to match. Any term that fits the format of the regular expression is a match.

Some common elements of regular expressions:

?	indicates that there should be one or none of the previous expression
+	indicates that there is at least one of the previous expression
.	matches any single character
*	indicates that there should be none, one, or any number of the previous expression
[ ]	matches any single character contained within the brackets
[a-z]	matches any lowercase letter within the set from a to z
[1-9]	matches any digit within the set from 1 to 9
{n}	a sequence of exactly n matches of the expression

The following are examples of regular expressions to match common items that may appear in a sensitive email message.

Data	Example	Regular Expression
Phone number	(555)555-4567	\(?[2-9][0-9]{2}[\]-.)[2-9][0-9]{2}[-.][0-9]{4}
Email address	joe@example.com	[a-zA-Z0-9._%-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,6}
Credit card number	1234 1234 1234 1234	[1-9][0-9]{3} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
Social Security Number	123-45-6789	[0-9]{3}-[0-9]{2}-[0-9]{4}
City, state abbreviation	Palo Alto, CA	.*, [A-Z][A-Z]
2-character state abbreviation	CA	[A-Z][A-Z]
Zip code	12345	[0-9]{5}(-[0-9]{4})?
Dollar amounts, with leading $ symbol	$3.95	\$[0-9]+.[0-9][0-9]
Date, numeric	2003-08-06	[0-9]{4}-[0-9]{2}-[0-9]{2}
Date, alpha-numeric	Jan 3, 2003	(Jan|Feb|Mar|Apr|May|Jun|Jul|Aug|Sep|Oct|Nov|Dec)\.?(3[0-1]|[1-2][0-9]|0?[0-9]), [0-9]{4}
HTTP URL	http://www.example.com	https?://(([012][0-9]{0,2}\.){3}[012][0-9]{0,2}|([a-zA-Z0-9]+\.)+[a-zA-Z0-9

Data	Example	Regular Expression
		]{2,6})(/.*)?
IP address	123.123.123.123	([012][0-9]{0,2}\.){3}[012][0-9]{0,2}
A blank line		^$

Security Policy Information and Examples

When you create a service, several default security policies are automatically created:

- Require Encryption: [PGP] Confidential
- Sign + Encrypt Button*
- Sign Button*
- Encrypt Button*
- Mailing List Admin Requests
- Mailing List Submissions
- Opportunistic Encryption.

* *These policies are available only on PGP Desktop for Windows.*

The order of the default policy rules is important. Be sure the order appears exactly as described above.

This section describes how the default security policies work. It also describes two example situations for which you might want to create a security policy and explains how to configure them.

Note: If you make any changes to the default policies and want to restore the default settings, click **Revert to Default** (for Windows systems) or **Revert** (for Mac OS X systems) in the Message Policy dialog box.

Opportunistic Encryption Default Policy

Opportunistic Encryption is one of the default security policies that PGP Desktop automatically creates for a service. The settings for this default policy 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 This rule should appear seventh (last) in the list of default policies. 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.

This policy 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: [PGP] Confidential is one of the default security policies that PGP Desktop automatically creates for a service. The settings for this default policy 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 Keyservers / temporarily cache found keys
- If no result: Block message

This rule should appear first in the list of policies.

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 default security policies that PGP Desktop automatically creates for a service.

The settings for this default policy are:

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

Prefer Encoding: PGP Partitioned This rule should appear sixth in the list of default policies.

Mailing List Admin Requests Default Policy

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

The settings for this default policy are:

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

This rule should appear fifth in the list of default policies.

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 98)), 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 item. The PGP Messaging screen is displayed.
2. Click the name of the service with the security policy you want to edit. The properties for the service you selected appear.
3. Select the security policy you want to edit, then click **View Policy.** The Message Policy dialog box is displayed, displaying the settings for the specified policy.s

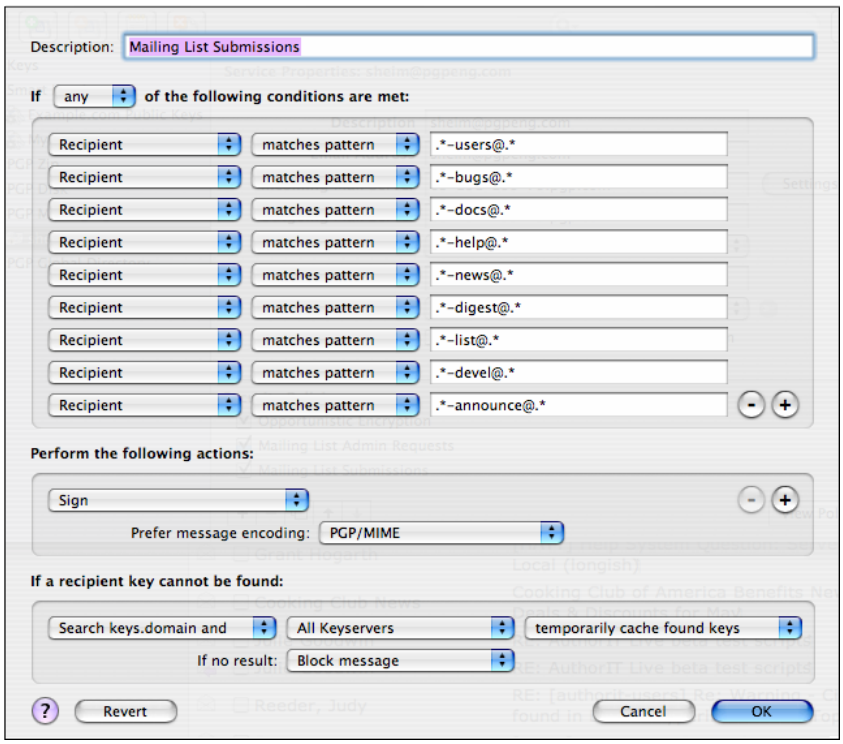
   The default policies can be viewed, modified, and disabled, but not deleted.
4. Make the desired changes to the policy. For information about the fields on the Message Policy dialog box, see *Creating a New Security Policy* (on page 98).
5. When you have made the desired changes, click **OK** to close the Message Policy dialog box. The specified security policy is changed.

Editing a Mailing List Policy

To edit a default Mailing List policy

1. Open PGP Desktop and click the PGP Messaging item. The PGP Messaging screen is displayed.
2. Click the name of the service with the security policy you want to edit. The properties for the service you selected appear.

3 Select the mailing list policy you want to edit, then click **View Policy.** The Message Policy dialog box is displayed, displaying the settings for the specified policy.



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

4 Make the desired changes to the policy. 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.

5 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 is displayed when you select **Message Header**.

Note: 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.

6 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.

7 In the third condition field, in the text entry box, type the text for the matching criteria.

8 In the Perform the following actions on the message section, 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.

9 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 which is different from 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 in the **Group** field on the Key Properties dialog box on Windows systems or the Key Info dialog box on Mac OS X systems. **No** means that the key *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.

10 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.

11 In the **Recipient's key is not available** section, 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.

12 In the second Key Not Found field, select:

- **All keyservers**. Allows all keyservers, including the PGP Global Directory, to be searched for an appropriate key.
- **PGP Global Directory or keyserver.pgp.com**. Specifies that only the PGP Global Directory is searched.
- **[configured keyservers]**. Specifies that only the keyserver you choose from the list of currently configured keyservers is searched. Note that keyservers 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. This option is available only on Windows systems.
- **Edit Keyserver List**. Lets you add keyservers to the list of currently configured keyservers. This option is available only on Windows systems.

13 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.

14 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.

15 When you have made the desired changes, click **OK** to close the Message Policy dialog box. The specified security policy is changed.

Deleting a Security Policy

To delete an existing security policy

1. Click the name of the service with the security policy you want to delete. The properties for the service you selected appear.
2. Deselect the check box next to the policy you want to delete.
3. Be sure the policy is still selected and click **[-]** at the bottom of the **Security Policies** area. A confirmation dialog box is displayed.
4. Click **Remove** to delete the policy. The specified security policy is deleted from the list.

Changing the Order of Policies in the List

To change the order of policies in the Security Policy list

1. In the PGP Messaging item, select the name of the service that has the security policy whose order you want to change. The properties for the service you selected appear.
2. From the **Security Policies** list, click on the name of the policy whose order in the list you want to change. The specified policy highlights.
3. Click the Up arrow or Down arrow at the bottom of the Security Policies window until the policy is in the desired location in the list.

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

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.

Tip: 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 or 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.

  Note: 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 cannot 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 box (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 list *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.

Note: This option should be enabled only 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.** To use PGP Desktop with SSL enabled in your email client, you must deselect the option to **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 ignores incoming and outgoing traffic over that connection when the connection is protected by SSL.

  PGP Desktop monitors 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 handles the traffic like any other unprotected connection and attempts to upgrade the connection to SSL (if in Automatic mode) and apply applicable policies to messages.

Key Modes

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

Note: 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 (smart cards can be used on Windows systems only).

  Starting with PGP Desktop version 10.0, SKM keys that previously could be used only for messaging can be used for all other PGP Desktop encryption actions. This includes encrypting disks and files, and decrypting MAPI email messages when offline.

If you are using an SKM key, you will never need to enter a passphrase for authentication. SKM key passphrases are randomly generated by PGP Desktop and are stored encrypted. When PGP Desktop requires a passphrase, PGP Desktop retrieves the encrypted passphrase from your system without requiring interaction from you.

- **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. On Windows systems, 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 (on Windows systems only) 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 (on Windows systems only) 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 later or added to an older PGP key using PGP Desktop 9.5 or later.

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.

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

- 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.

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 indicates that the key mode for the selected service, in this example, 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 for the key mode you want to change. The account properties and security policies for the selected service appear.
2. Click **Key Mode**. The PGP Universal Key Mode screen is displayed, describing your current key management mode.
3. Click **Reset Key** and then click **Yes** in the confirmation message displayed. The PGP Key Setup Assistant is displayed.
4. Read the text, then click **Next**. The Key Management Selection screen is displayed.
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 is displayed.
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**, do the following:
   - Enter a passphrase for the key, then click **Next**.
   - When the key is generated, click **Next**.
   - Click **Finish**.
10. If you selected **PGP Desktop Key**, do the following:
    - Select the key from the local keyring that you want to use, then click **Next**.

- Click **Finish**.

11 If you selected **Import Key**, do the following:

- Browse to file that holds the PGP key you want to import (it must contain a private key), then click **Next**.
- Click **Finish**.

Viewing the PGP Log

Use the PGP Log to see what actions PGP Desktop is taking to secure your messages.

To view the PGP Log

1 Do one of the following:

- Click the PGP Desktop icon in the Menu Bar and select **Show Log** from the menu. The PGP Log is displayed.
- Open PGP Desktop and select **Window > PGP Log**. The PGP Log is displayed.

2 Do the following:

- Click **Clear** to clear all of the entries in the PGP Log. You are prompted to confirm you want to clear all entries in the log; click **Yes**.
- Click **Find** to search the entries in the PGP Log. Enter the search terms and click **Next**.
- Click the arrow for **Logging level** to select the minimum information level of log entries you want to view: **Info** or **Verbose**. Note that **Verbose** can result in large log files.

  To view **Verbose** logs, the PGP Log view window must remain open. When you close the window, the level of logging reverts back to the default level, **Info**. Note that **Verbose** can result in some large log files.
- Click **Save** to save a copy of the entries in the log. Specify a file name, location, and format (the default is a plain text file) for the log file, then click **Save**.

3 Click the red circle in the upper left corner of the screen to close the PGP Log window.

Using PGP Scripts with Entourage 2008

To use the PGP scripts in Entourage to encrypt email

1. Create your email message.
2. Click the **Scripts** icon listed in the Entourage toolbar, and select **PGP**.
3. Select the option to **Encrypt** or **Encrypt & Sign**, and select the key to sign to.
4. The email text is encrypted and a block of cipher text is displayed in its place.
5. You can now send your email securely.

To use the PGP scripts in Entourage to decrypt email

1. Open the encrypted email.
2. Click on the **Scripts** menu item and select **PGP**.
3. Select **Decrypt & Verify** and enter the passphrase when prompted. The email is decrypted.

9 Securing Instant Messaging

This section provides information on how to use PGP Desktop to secure your instant messaging (IM) sessions. For information about the PGP Options that affect IM sessions, see *Messaging Options* (see "Messaging Preferences" on page 193).

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

About PGP Desktop's Instant Messaging Compatibility

PGP Desktop automatically encrypts AOL and iChat standard 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 installed and running on the system on which they are using IM. To confirm that you are using PGP Desktop 9.0 or later, click the PGP Tray icon and select **About PGP** from the shortcut menu (from within the PGP Desktop window, select **Help > About PGP**).
- Both users have the **Encrypt instant messages** setting enabled. To do this:
  - On Windows systems, select **Tools > Options**, click the Messaging tab, and select the checkbox to **Encrypt AOL Instant Messages (AIM)**.

- On Mac OS X systems, select **PGP > Preferences**, click the Messaging icon, and select the checkbox to **Encrypt AOL Instant Messages (AIM)**.

Tip: On Windows systems, quickly verify that instant messaging encryption is enabled by clicking the PGP Tray icon. There should be a check mark next to **Use PGP AIM Proxy** in the shortcut menu.

- Both users are using compatible IM clients. For information on the compatible IM clients, see the following section.
- The AIM address of the initiator of the IM session is 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.

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

Notes:

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.

Instant Messaging Client Compatibility

PGP Desktop is compatible with the following instant messaging clients when encrypting AIM instant messages, file transfers, and direct connections:

- iChat 3.1.x, 4.0

  Encryption of file transfers and direct connections requires AIM 5.9.3702 on Windows or iChat 3.1 on Mac OS X. Audio and video connections are not encrypted by PGP Desktop.

Other instant messaging clients may work for basic instant messaging, but have not been certified for use.

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.

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

Encrypting your IM Sessions

Once you have met the conditions described in *About PGP Desktop's Instant Messaging Compatibility* (on page 121), start your IM session as you normally would. Your IM sessions with any other PGP Desktop user using a compatible IM client are 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 is displayed, informing 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."
- If you open the PGP Log after you have started your IM session, you see entries noting that the IM session is being proxied, that the session is being encrypted, and so on, as in the following example:

  ```
  2006-09-15 11:39:49 Proxying AIM connection from AliceIM
  using Apple iChat.

  Initiating PGP Desktop encrypted AIM session with JMedinaX
  using your key with id 0x0910D29E.

  Encrypted AIM session with JMedinaX established.
  ```

10 Viewing Email with PGP Viewer

This section provides information on how to use PGP Desktop to decrypt, verify, and display encrypted messages using PGP Viewer.

Note: PGP Viewer only runs on systems with PGP Desktop installed. You cannot use PGP Viewer standalone.

In This Chapter

Overview of PGP Viewer

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

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

There are multiple ways you could have ended up with encrypted messages outside the mail stream:

- **Encrypted messages saved securely.** Many organizations store messages encrypted for security purposes. Storing them puts them outside the mail stream, but PGP Viewer can decrypt, verify, and display them while maintaining the original encrypted message.
- **Encrypted text in a webmail message.** Encrypted messages sent to a webmail account cannot be decrypted by PGP Desktop. However, PGP Viewer can decrypt those messages. Open the message.pgp file attachment using PGP Viewer or copy/paste the encrypted text into PGP Viewer.

- **Encrypted text not decrypted by PGP Desktop.** If a message was automatically downloaded by your email client when PGP Desktop was not running or when your passphrase was not cached, you could end up with encrypted message text that is now outside the mail stream.

PGP Viewer decrypts, verifies, and displays multiple types of messaging content:

- Modern PGP-encrypted content (PGP/MIME and PGP Partitioned)
- Legacy PGP-encrypted content (PGP/MIME and PGP Partitioned)

RFC-2822 compliant encrypted content PGP Viewer uses PGP Desktop keyrings for operations that require keys. PGP Viewer honors applicable PGP Desktop preferences; passphrase caching options, for example.

In a PGP Universal Server-managed environment, PGP Viewer searches for verification keys per the applicable policy.

PGP Viewer displays signature information for messages it decrypts in the message window, not in the message itself. This provides access to full signature information and prevents spoofing of inline signature annotations.

Supported Email Clients

Use PGP Viewer to copy the text of a decrypted/verified message to the following email clients:

- Windows Mail (Windows)
- Microsoft Outlook (Windows)
- Thunderbird (Windows and Mac OS X)
- Outlook Express (Windows)
- Lotus Notes (Windows)
- Mail.app (Mac OS X)

Due to the design of Lotus Notes architecture, an encrypted message cannot be dragged from Lotus Notes email client and dropped into PGP Viewer to be decrypted.

Opening an Encrypted Email Message or File

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

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

- **.msg:** Created by Microsoft Outlook.

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

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

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

   Note: You can drag and drop the file you want to decrypt onto the portion of the PGP Viewer screen that displays: **Drag Email or Files Here**. PGP Viewer opens the file, decrypts and verifies it, and displays the message.
4. To open another message, click **Open Message** in the toolbar, navigate to the desired file, select it, then click **Open**. PGP Viewer decrypts, verifies, and displays the message.
5. Click **Smaller** to make text smaller or **Bigger** to make text larger.
6. Click **Rich Text** to display the message or file in RTF (rich text format) or **Plain Text** for plaintext.
7. Click **Print** to print the message or file.

Copying Email Messages to Your Inbox

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

To copy a message to the inbox of your email client

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

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

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

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

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

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

Exporting Email Messages

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

To export a message from PGP Viewer to a file

1 With the message displayed in the PGP Viewer window, click **Export**.

2 In the **Export Message** dialog box, specify the desired filename, location, and format for the file, then click **Export**.

PGP Viewer saves the file to the specified location.

PGP Viewer Preferences

PGP Viewer includes preferences that provide control of certain functionality.

To access PGP Viewer preferences

1 Open PGP Viewer or use PGP Viewer to decrypt, verify, and display a message.

2 Pull down the **PGP Viewer** menu and select **Preferences**.

The **Preferences** dialog box appears.

3 Select the **General** tab and specify the following preferences:

- **Ask for confirmation when using Copy to Inbox**: Controls whether or not a confirmation prompt is displayed when you copy text from PGP Viewer to the inbox of your email client. The default is enabled.
- **Automatically load remote images in HTML messages**: Controls whether external resources like images, CSS style sheets, or iframe content, for example, are automatically loaded by PGP Viewer. The default is disabled, as this may be a security risk.
- **Email Client**: Lets you specify the email client to which PGP Viewer will copy content. The default is the system default email client (PGP Viewer determines your default system email client and uses that as its default). You can select **Mail.app** or **Thunderbird**.

4 Select the **Fonts and Colors** tab specify the following preferences:

- **Font**: Controls the font PGP Viewer uses to display text. Click **Select**, then specify the desired **Collection**, **Family**, **Typeface**, and **Size**.
- **Text Color**: Controls the color of text that PGP Viewer displays. Click the color block and select the desired color.
- **Background Color**: Controls the background color of text that PGP Viewer displays. Click the color block and select the desired color.

Security Features in PGP Viewer

PGP Viewer proactively protects your security:

- The Web browser embedded in PGP Viewer, which displays messaging content, has JavaScript, Java Applets, and plugins disabled. This prevents an attacker from delivering a malicious payload that PGP Viewer might otherwise load.
- External resources — images, CSS style sheets, iframe content (an inline frame that contains another document), and so on — are loaded automatically based on the **Automatically load remote images** preference. For security purposes, this preference is disabled by default. When this preference is disabled, PGP Viewer does not generate any network traffic to external sites.

11 Protecting Disks with PGP Whole Disk Encryption

PGP Whole Disk Encryption (PGP 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.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP administrator may have specified, by policy, that all system disks must be encrypted. If this is the case, PGP Desktop periodically verifies that disks are encrypted and will enforce policy by automatically encrypting unencrypted system disks.

In This Chapter

About PGP Whole Disk Encryption

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

Important: PGP Desktop 9.9 and later use a different partitioning method than did versions of PGP Desktop prior to Version 9.9. If you used the PGP WDE feature of versions of PGP Desktop prior to Version 9.9, you must decrypt those disks *before* installing Version 10.0 or you will no longer be able to access the data on them.

When you encrypt an entire disk using the PGP WDE feature, every sector is encrypted using a symmetric key. This includes all files including 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 authenticated to your PGP WDE-encrypted disk (after you have entered the correct passphrase at the PGP BootGuard screen), the files are available. When you shut down your system, 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* (on page 134).
2. Perform the tasks to *Prepare Your Disk for Encryption* (on page 135).
3. Choose how you want to authenticate yourself to encrypt the disk in *Determine the Authentication Method for the Disk* (on page 138).
4. Start the encryption process in *Encrypting a Disk* (on page 139).
5. Learn how to use an encrypted disk in Using a *PGP WDE-Encrypted Disk* (see "Using a PGP-WDE Encrypted Disk" on page 142).
6. Learn how to maintain your encrypted disk in *Maintaining the Security of Your Disk* (on page 144).
7. Learn how to decrypt the disk, if needed, in *Decrypting a PGP WDE-Encrypted Disk* (on page 152).
8. Understand the features that help avoid security problems in *Special Security Precautions Taken by PGP Desktop* (on page 153).

If you are a PGP Universal Server Administrator, or are using PGP WDE in a PGP Universal Server-managed environment, see *Using PGP WDE in a PGP Universal Server-Managed Environment* (on page 148) for additional information.

Warning: Once you unlock a disk, 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. Use a PGP Virtual Disk volume for files that need to be secured even while your computer is in use. For more information, see *Using PGP Virtual Disks* (on page 157).

Encrypting Boot Disks

Starting with PGP Desktop for Mac OS X version 10.0, you can fully encrypt the boot disk on an Intel-based Macintosh. You can, of course, continue to encrypt removable disks, and USB flash disks as you could with versions of PGP Desktop prior to Version 10.0.

Important: Apple's Boot Camp product works only when there are two partitions on the disk: one for Mac OS X and one for Boot Camp. Because PGP Desktop adds another partition, Boot Camp does not work on a Mac OS X system with PGP Desktop 10.0 or later. Other virtualization software (Parallels, for example) work normally on a Mac OS X system with PGP Desktop 10.0 or later. PGP Corporation strongly recommends uninstalling Apple Boot Camp before installing PGP Desktop. For more information on using PGP Desktop with Apple Boot Camp, see *PGP KB Article 1697* (https://support.pgp.com/?faq=1697).

The PGP WDE feature supports both 32- and 64-bit Intel-based Mac OS X systems.

Note: The Mac OS X Safe Boot feature does not work on a boot disk that has been whole disk encrypted; Safe Boot disables kernel extensions required by PGP WDE. If you hold down the Shift key after authenticating at the PGP BootGuard screen, the system will *not* boot; however, it does restart after a few minutes.

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.

Both products work independently of each other, so you can use them at the same time. For more information, see *Using PGP Virtual Disks* (on page 157).

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.

To verify your license supports PGP Whole Disk Encryption

1. Open PGP Desktop.
2. From the **PGP** menu, select **License**. The License Information dialog box is displayed.
3. Click **Details**. The details of your license are displayed. In the Enabled Features section, verify that **PGP Whole Disk Encryption** is listed.

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 Server-managed environment, contact your PGP administrator for more information about support for the PGP WDE feature in your license. For more information, see *Using PGP Desktop with PGP Universal Server* (on page 207).
- If you are using PGP Desktop outside of a PGP Universal Server-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. Ninety days after the subscription license expires, the PGP WDE feature decrypts your data (after notifying you) so you can retrieve your files.

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 136).
- **Make sure you use supported characters in your passphrase.** See *Supported Characters* (on page 139).
- **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 137).
- **Back up the disk before you encrypt it**. Before you encrypt your disk, be sure to back it up so that you will not lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk. Also be sure to make regular backups of your disk.
- **Consider the time it will take to encrypt the disk** and prepare accordingly. See *Calculate the Encryption Duration* (on page 137).
- **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. See *Run a Pilot Test to Ensure Software Compatibility* (on page 138) for known interoperability issues, and review the *PGP Desktop Release Notes* for the latest updates to this list.
- **Ensure that Sleep mode has been disabled**. PGP Desktop is not compatible with hibernation mode on Mac OS X systems.

Supported Disk Types

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

- Desktop or laptop disks, including solid-state drives.

  Note: Do not use PGP WDE to encrypt server hardware. PGP WDE is not supported on Mac OS X server hardware.

- External disks, *excluding* music devices and digital cameras.
- USB flash disks, sometimes called thumb drives.

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

If you want to partition a drive that has been encrypted with PGP WDE, you must first decrypt the drive. After you have decrypted the drive, you may partition it.

PGP WDE supports all Mac OS X power management modes.

Unsupported Disk Types

The following disk types are *not* supported:

- Disks formatted using the APM partition scheme.
- Any type of server hardware, including RAID disk drives.
- Diskettes and CD-RW/DVD-RWs.

Supported Keyboards

The PGP Whole Disk Encryption log-in screen supports the following keyboard layouts:

- English (US-International)
- Japanese (Japan)
- German (Germany)
- French (France)
- Spanish (Latin America)
- Spanish (Spain; ISO)

Different keyboard layouts can have different mappings between characters, potentially causing problems when you enter your passphrase to authenticate. Be sure to specify the supported keyboard layout (in System Preferences > Personal > International), and then make sure to use that same layout each time you authenticate.

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 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.

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

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. These software applications can correct errors that would otherwise disrupt encryption.

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

Caution: As a best practice, highly fragmented disks should be defragmented before you attempt to encrypt them.

Calculate the Encryption Duration

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

Factors that may affect encryption speed include:

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

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

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

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

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

Run a Pilot Test to Ensure Software Compatibility

As a good security practice, 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.

Determine the Authentication Method for the Disk

When you encrypt a disk using PGP WDE, you choose a method that determines how you will authenticate yourself to decrypt the disk.

You have the following options:

- **Passphrase.** With passphrase authentication, you specify a passphrase when encrypting a disk. When attempting to access the encrypted disk, you must enter the passphrase.
- **Public key.** With public-key authentication, you specify a public key when encrypting a disk. Only the holder of the corresponding private key can access the contents of the disk. 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 or disks in USB enclosures, must be encrypted using a passphrase user.

During initial encryption of a *boot disk*, you can only select passphrase authentication as the authentication method. After initial encryption, you can add additional passphrase users to the disk.

During initial encryption of a *non-boot disk* (such as an external disk), you can select between passphrase or public-key authentication.

Encrypting a Disk

Once you have prepared the disk, you can encrypt it. Note the following before you begin:

- 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, click **Stop**, then click **Pause** on 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 at a time. Once you begin an operation on a disk, 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

The PGP Whole Disk Encryption feature supports alphanumeric characters, punctuation characters, and standard meta-characters when creating passphrases. Tab and control characters are not supported. As you choose a passphrase, please note the following.

The following characters are supported: `abcdefghijklmnopqrstuvwxyz ABCDEFGHIJKLMNOPQRSTUVWXYZ`

`0123456789`

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

Most extended ASII characters (such as ç é è ê ë î ï ô û ù ü ÿ) or symbols (such as ¢ ® œ), are supported.

- For Japanese versions of PGP Desktop, additional *invalid characters* are:

  ` and ~

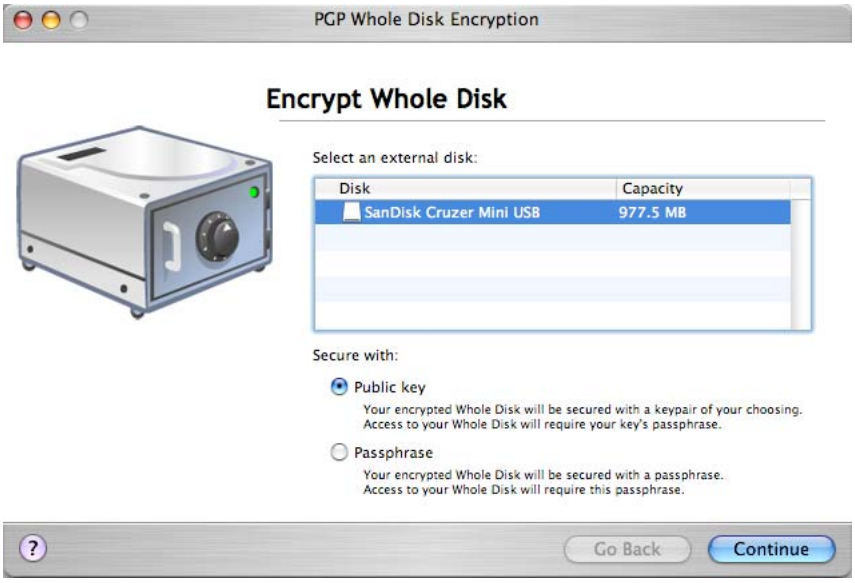
Encrypting the Disk

Before you encrypt your disk, be sure to back it up so that you will not lose any data if your laptop or computer is lost, stolen, or you are unable to decrypt the disk.

To protect a disk using the PGP Whole Disk Encryption feature

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

2 Click **Encrypt Whole Disk**. The Encrypt Whole Disk screen is displayed, showing a listing of disks on your system that can be protected.



3 From the **Select a disk** list, click on the disk you want to protect.

4 In the **Secure with** section, specify how you want to access your protected disk: **Public Key User** or **Passphrase User**.

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

- If you want to protect your disk with a public key, select **Public Key**, then click **Continue**. The Add PGP Whole Disk User screen is displayed. This option is not available if you have already encrypted your disk.

  Select a key from the list, then click **Continue**. The Enter PGP Passphrase dialog box is displayed.

Type the passphrase for the key you selected, then click **OK**. The PGP Whole Disk Encryption Summary screen displays, showing you a summary of how your disk is going to be encrypted, what key is used, and so on.

- If you want to protect your disk with a passphrase, select **Passphrase,** then click **Continue.** The Add PGP Whole Disk User screen is displayed.

  Type a **Name** (or accept the default name), then type the desired passphrase in the **Enter your passphrase** field, and then type it again in the **Confirm your passphrase** field. To see your passphrase as you type, select **Show Keystrokes**.

  The Passphrase Quality bar provides a basic guideline for the strength of the passphrase you are creating by comparing the amount of entropy in the passphrase you type against a true 128-bit random string (the same amount of entropy in an AES128 key). For more information, see *The Passphrase Quality Bar* (on page 202).

  Click **Continue**. The PGP Whole Disk Encryption Summary screen is displayed, showing you a summary of how your disk is going to be encrypted, what key is used, and so on.

5 Review the information, then click **Encrypt.** The encryption process begins and the Encryption Progress screen is displayed.

6 Click **Close**. The PGP Desktop screen is displayed; the encryption process continues in the background. A progress bar shows how the encryption process is progressing.

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

7 During the encryption process, you can do the following:

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

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

When the encryption process completes, the disk properties for the encrypted disk is displayed and include the description, type of disk, size, encrypted status, and the user access information.

Encountering Disk Errors During Encryption

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

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 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. When you successfully enter a valid passphrase, PGP WDE then decrypts the disk.

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, 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.

Warning: 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 *Using PGP Virtual Disks* (on page 157).

When you shut down a system with an encrypted boot disk, or if you remove an encrypted removable disk from the system, all files on the disk remain encrypted and fully protected—data is never written to the disk in an unencrypted form. Proper authentication (passphrase 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 a protected disk for one of two reasons:

- If your boot disk 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.
- If a secondary fixed disk is protected using PGP Whole Disk Encryption, you can authenticate at startup so that you do not have to authenticate later when you need to use files on the secondary disk. Because the files on the secondary (non-boot) disk 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.

Note: The PGP BootGuard log-in screen accepts the authentication information from any user configured for an encrypted disk. For example, if you have two users configured for a boot disk nd two different users configured for a secondary fixed disk 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.

On the PGP BootGuard log-in screen you can authenticate an encrypted boot or secondary disk on the system.

To authenticate using the PGP BootGuard log-in screen

1 Start or restart the system that has a disk protected by PGP Whole Disk Encryption. On startup, the PGP BootGuard log-in screen is displayed.

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

Note: Some characters cannot be entered at the PGP BootGuard screen. See *Supported Characters* (on page 139).

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.

If you typed an invalid passphrase, an error message is displayed. Try typing the passphrase again.

Maintaining the Security of Your Disk

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

Viewing Key Information on an Encrypted Disk

To view key information of a public key user on an encrypted disk

1 Select the encrypted disk with the public key user whose key information you want to view.

2 In the **User Access** list, either Ctrl+click the user's name or right-click it if you are have a two-button mouse.

3 In the shortcut menu, select **Show Key Info.** The **Key Info** screen for the specified key is displayed.

Modifying the System Partition

Do not make any changes to the system partition on a boot disk that has been encrypted by PGP WDE; it will fail to boot properly on the next startup. If you must make changes to the partitioning of an encrypted disk, decrypt the disk first and then make the partition changes.

Adding Other Users to an Encrypted Disk

The user who creates an encrypted disk can make it available to others. These additional users can access the encrypted disk using their own unique passphrase or private key. You can have up to 120 users per encrypted disk

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

▸ **To add additional users to a disk protected by PGP Whole Disk Encryption**

1 Select the encrypted disk to which you want to add another user.

2 Click the plus sign icon (**+**) below the **User Access** list.

3 Select **Add Public Key User** or **Add Passphrase User**, from the list displayed.

- If you select **Add Public Key User**, you are prompted to select the public key of the user(s) you want to add. Drag the users you want to add from the **Key Source** column into the **Keys to Add** column, then click **OK**.
- If you select **Add Passphrase User**, you are prompted for a user name and a passphrase for the user you want to add. In the **Username** field, enter a user name for the user you are adding.

  In the **Enter a passphrase for this user** field, enter a passphrase. In the **Confirm user's passphrase** field, enter the same passphrase again. To see your passphrase as you type, select **Show Keystrokes**.

  Click **OK**.

You are prompted for the passphrase of the encrypted disk.

4 Enter the passphrase of the encrypted disk, then click **OK**. The specified public key user(s) or passphrase user is added.

Note: Public-key encryption is the most secure protection method when adding other users to disks 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.

Deleting Users From an Encrypted Disk

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

To remove a user from an encrypted disk

1 Select the encrypted disk from which you want to remove a user.

2 From the **User Access** list, select the name of the user you want to remove.

3 Click the minus sign icon (**–**) below the **User Access** list. You are prompted for the passphrase of the encrypted disk.

4 Enter the passphrase of the encrypted disk, then click **OK**. The alternate user is removed.

Note: You cannot remove all users from an encrypted disk; when only one user is listed in the User Access list, you cannot remove that user.

Changing User Passphrases

To change the passphrase of a passphrase user on an encrypted disk

1 Select the encrypted disk with the user whose passphrase you want to change.

2 In the **User Access** list, either Ctrl+click the user's name or right-click it if you have a two-button mouse.

3 From the shortcut menu, select **Change User Passphrase.** You are prompted for the passphrase of the encrypted disk.

4 Enter the passphrase of the encrypted disk, then click **OK**. The **Confirm PGP Passphrase** screen is displayed.

5 Type a new passphrase in the **Enter your new passphrase** box, move to the **Confirmation** field and type the new passphrase again, then click **OK**.

6 Click **OK** on the Passphrase Changed box. The passphrase is changed.

Re-Encrypting an Encrypted Disk

Consider re-encrypting a protected disk that you suspect of having a passphrase that has been compromised.

To re-encrypt a disk, the PGP Whole Disk Encryption feature uses the same encryption algorithm (AES 256)—but a different underlying encryption key—to encrypt the disk again. The result is as if you decrypted the disk and encrypted it again, but much faster.

To re-encrypt an encrypted disk

1. Select the encrypted disk you would like to re-encrypt.
2. From the **Disk** menu, select **Re-Encrypt Disk**. You are prompted for the passphrase of the encrypted disk.
3. Enter the passphrase of the encrypted disk, then click **OK**. The re-encryption process begins.

Backing Up and Restoring

While most modern backup programs have no problem backing up the data on a PGP WDE-encrypted disk, some other backup programs do have problems with it. These other backup programs fail when they encounter the file PGPWDE01, a file used by PGP WDE. The solution is to have these programs exclude PGPWDE01 from the backup (most backup programs let you exclude individual files). Once you get your backups working again with these programs, it is a good idea to test the backup to make sure it works.

Using Automatic Backup Software on a PGP WDE-Encrypted Disk

You can automatically back up any disk this is protected with PGP WDE. Files the software backs up will be decrypted before being backed up.

For example, backups made using Time Machine, the automatic backup software built into Mac OS X 10.5 (Leopard), are made normally, and the files in the backup are not encrypted.

Note: Data recovery software (such as the Mac OS X version of Boomerang Data Recovery) attempts to recover data from a hard drive that is not currently accessible. If data recovery software is used on a disk that is protected with PGP WDE, it will find encrypted data that is *not* in a usable form.

Uninstalling PGP Desktop from Encrypted Disks

If you have any disks on your system that are protected by PGP Whole Disk Encryption, these disks 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 protected by PGP Whole Disk Encryption. In this instance you see an error message explaining that the uninstall process is being terminated to protect the encrypted disk.

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

Using PGP WDE in a PGP Universal Server-Managed Environment

The PGP Whole Disk Encryption feature can be administered for PGP Desktop users in a PGP Universal Server-managed environment. Administrators can 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 that are protected with PGP Whole Disk Encryption**. If you forget the passphrase to a disk encrypted with PGP Whole Disk Encryption, the disk is not accessible. However, if you are using the PGP Whole Disk Encryption feature in a PGP Universal Server-managed environment, check with your PGP administrator to see if disk 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 Server-managed environment, contact your PGP administrator 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.

Creating a Recovery Token

If you are working within a PGP Universal Server-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, partition (on Windows systems), or removable disk with PGP Whole Disk Encryption. This recovery token can be used to access the disk or partition (on Windows systems) in case the passphrase or authentication token (on Windows systems) is lost.

If the policy that applies to you does not support it, or if you are not in a PGP Universal Server-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 (on Windows systems) protected by PGP Whole Disk Encryption.

If you are in a PGP Universal Server-managed environment, and you lose the passphrase or authentication token used to protect a disk or partition (on Windows systems) 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 gain access to a disk or partition (on Windows systems) 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.

Note that the recovery token is used only to gain access to an encrypted disk or partition (on Windows systems). You cannot use the recovery token to encrypt or decrypt data.

Caution: Consider re-encrypting disks or partitions (on Windows systems) protected by PGP Whole Disk Encryption if security is compromised, by passphrase exposure for example, or loss of the authentication token (on Windows systems). 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.

Using a Recovery Token

Once you have received the recovery token from your PGP Universal Administrator, follow the steps below to unlock your disk.

When you enter a recovery token, you do not need to match the case (all uppercase) or dashes that you received from your PGP Universal Administrator. You can enter all lowercase characters without the dashes if you want.

To use a recovery token on a boot disk

- At the PGP BootGuard screen, enter the recovery token in the passphrase field.

To use a recovery token on a removable drive

- Insert the disk and enter the recovery token when prompted to enter the passphrase.

Recovering Data From an Encrypted Drive

Although rare, you may find it necessary to recover data from an encrypted drive that has been damaged or corrupted. Or, you may find that you do not have the login information in order to access a drive (such as a former employee's encrypted drive).

In these cases, there are several things you can do:

1. Use a recovery disk. If a recovery disk was created before the disk or partition was encrypted, you can use it to decrypt the disk. For more information, see *Creating and Using Recovery Disks* (on page 151).
2. Use another system to decrypt the drive. For more information about creating a new policy or editing existing ones, see *Decrypting a PGP WDE-Encrypted Disk* (on page 152).
3. Use the Whole Disk Recovery Token. If you are using PGP Desktop in a PGP Universal Server-managed environment, the recovery token is created automatically when the disk is encrypted. For more information, see *Using a Recovery Token* (on page 150).

For more information on how to recover data, see the *PGP Support KB Article 1018* https://support.pgp.com/?faq=1018.

For information on how to recover data using target disk mode, see the *PGP Support KB Article 1583* (http://support.pgp.com/?faq=1583).

Creating and Using Recovery Disks

While the chances are extremely low that a boot.efi file could become corrupt on a boot disk or partition protected by PGP Whole Disk Encryption, it is possible. If this occurs, it could prevent your system from booting. Prepare for this unlikely event by creating a recovery CD before you encrypt a boot disk or partition using PGP Desktop.

Caution: 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 9.5 recovery disk to decrypt a disk protected with PGP WDE 10.0 software, it will render the PGP WDE 10.0 disk inoperable.

This section includes procedures for creating a recovery compact disc. It also discusses their use. For more information, see *PGP KB article 1658* (http://support.pgp.com/?faq=1658).

To create a recovery CD

1. Download and save the recovery iso image to your system.
2. Burn the image to a CD-ROM using the Mac OS X Disk Utility. For information on how to do this, see the *Apple Support article HT2087* (http://support.apple.com/kb/HT2087).
3. Remove the recovery CD from the drive and label it appropriately.

To use a recovery disc or diskette

Caution: Once you have started to decrypt a disk or partition using a recovery disc or diskette, do not stop the decryption process. Depending on the size of the disk being decrypted, this process can take a long time. A faster way to decrypt the drive is to use another system that has the same version of PGP Desktop installed on it. For more information, see *Decrypting a PGP WDE-Encrypted Disk* (on page 152).

1. Boot the Macintosh system with the disc. To boot with the disk, hold down the Option key when rebooting the system and select to boot from the recovery disc. The PGP BootGuard screen is displayed.
2. To decrypt the disk, press D then press Enter.
3. Enter your passphrase when prompted and press Enter.

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).
- Connect a removable disk to a second system and decrypt from that system's PGP Desktop software. If the removable disk is formatted as a FAT drive, you can decrypt it using PGP Desktop for Windows or Mac OS X. If the disk is formatted as an HFS drive, you must use PGP Desktop for Mac OS X.

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

To use PGP Desktop to decrypt a disk

1. Open PGP Desktop, right-click on the disk you want to decrypt, and choose **Decrypt**. The Enter PGP Passphrase dialog box is displayed.
2. Enter the passphrase to unlock the disk and click **OK**. 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**.

Moving Removable Disks to Other Systems

You can move removable Windows-formatted disks to another Mac OS X system that has PGP Desktop 10.0 installed, and access the encrypted files on the other system.

You must be able to authenticate to access the contents of the disk.

Note: 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 Windows-formatted disk with PGP Whole Disk Encryption, you can use that removable disk on another computer with PGP Desktop 10.0 installed—even if the other system does not have a PGP Desktop license that supports PGP Whole Disk Encryption.

Accessing Data on Encrypted Removable Disks

If you use PGP Whole Disk Encryption for Windows to protect a removable disk—a USB flash disk, for example—you can move that disk to another Windows or Mac OS X system and access the encrypted files on that flash disk on the other system. Removable disks created using PGP WDE on Linux can be accessed using PGP Desktop version 10.0 or later only.

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

Note: 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 9.5.2 or later installed—even if the other system does not have a PGP Desktop license that supports Whole Disk Encryption.

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.

Passphrase Erasure

When you enter 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. Without this critically important feature, someone could search for your passphrase in your computer memory while you were away from the system. You would not know it, but they would then have full access to data 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 prevents a potential intruder from scanning the virtual memory file looking for passphrases.

Memory Static Ion Migration Protection

When you protect a disk or partition (on Windows systems) with PGP Whole Disk Encryption, your passphrase is turned into a key. This key is used to encrypt and decrypt the data on the encrypted disk or partition. While the passphrase is erased from memory immediately, the key (from which your passphrase cannot be derived) remains in memory.

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 encrypted disk or partition (on Windows systems) is decrypted 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 on with sensitive files open when you leave your desk, anyone can access that information—even if the disk or partition (on Windows systems) is protected using PGP Whole Disk Encryption.

Here are some tips for maintaining optimal security:

- When you are away from your desk, use a screen saver with a password to deter others from accessing your computer or viewing your screen.
- Make sure that your encrypted disks or partitions (on Windows systems) are not available to other computers on a network. You may need to arrange this with the network management staff within your organization. Once you have unlocked your disk or partition, PGP Whole Disk Encryption can no longer protect the files. They can be seen by anyone with network access to them. Consider the PGP Virtual Disk feature for storing files that need to be locked even while you are using your computer.
- Never write down your passphrase. 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, or a joke—just *do not write it down*.

- If you use PGP Desktop at home and share your computer with other people, they will probably be able to see your open files on a disk or partition (on Windows systems) that is protected using PGP Whole Disk Encryption. As long as you shut down a system with a whole disk encrypted 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.
- When you leave your computer for any length of time, PGP Corporation recommends that you shut down your Macintosh system, rather than putting the system to Sleep. This ensures that no one can access your encrypted system when returned from Sleep mode.

Technical Details About Encrypting Boot Disks

To support PGP Whole Disk Encryption of boot disks on Mac OS X, PGP Desktop creates a new partition (using GUID Partition Table) and puts a new boot loader onto the new partition.

Important: Versions of PGP Desktop prior to Version 10.0 supported APM partitions; this partitioning method does *not* support PGP Whole Disk Encryption of boot disks, so Version 9.9 and later use the GUID Partition Table (GPT) partitioning method. Because of this change, all disks that are PGP whole disk encrypted using versions of PGP Desktop prior to Version 9.9 need to be decrypted *before* installing Version 9.9 or above. Older PGP whole disk encrypted disks not decrypted prior to Version 9.9 being installed will not be accessible once Version 9.9 or later is installed.

The boot loader that is installed by PGP Desktop does several things: it authenticates users attempting to boot the disk and (when authentication is successful) it calls the Mac OS X boot loader and decrypts the files needed for normal booting of the disk. If authentication is not successful, it does not call the Mac OS X boot loader nor decrypt the necessary files, and thus the disk does not boot.

Caution: Apple's Boot Camp product works only when there are two partitions on the disk: one for Mac OS X and one for Boot Camp. Because PGP Desktop adds another partition, Boot Camp does not work on a Mac OS X system with PGP Desktop 10.0 or later. Other virtualization software (Parallels, for example) work normally on a Mac OS X system with PGP Desktop 10.0 or later. PGP Corporation strongly recommends uninstalling Apple Boot Camp before installing PGP Desktop.

12 Using PGP Virtual Disks

Use PGP Virtual Disks to organize your work, keep similarly named files separate, or keep multiple versions of the same documents or programs separate.

This section describes the PGP Virtual Disk feature of PGP Desktop.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

Note: 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.

About PGP Virtual Disks

A PGP Virtual Disk is an area of space, on any disk connected to your computer, which 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.

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 or the Mac OS X Finder, and it is inaccessible to anyone without proper authentication.

It is important to remember 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 Disks 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.

For information about the PGP options that affect PGP Virtual Disk volumes, see *Disk Options* (see "Disk Preferences" on page 196).

Caution: If you are using PGP Desktop in a PGP Universal Server-managed environment, you may be required to create a PGP Virtual Disk after installing PGP Desktop. If so, the size, file system, and algorithm may have been specified. For more information, see *Using PGP Desktop with PGP Universal Server* (on page 207).

Creating a New PGP Virtual Disk

▸ **To create a new PGP Virtual Disk**

1 Open PGP Desktop and select the **PGP Disk** item. The **PGP Disk** window is displayed.

Note: If you did not install PGP Whole Disk (an option available if you selected **Customize** during the installation of PGP Desktop) with an appropriate license, the only section displayed in this window is New Virtual Disk.

2 Click **New PGP Virtual Disk.** The New PGP Disk screen is displayed.

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

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

- To protect your PGP Virtual Disk with your keypair, select **Public Key**.

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

5 To view or change the advanced options settings, select the **Advanced Options** checkbox. The **Automatically resize PGP Virtual Disk as necessary** checkbox is displayed, as well as the **Cipher** and **Format** menus.

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

- Select the **Automatically resize PGP Virtual Disk as necessary** checkbox if you want PGP Desktop to manage the size of the new **PGP Virtual Disk** automatically. As you add or delete files, the disk size changes appropriately.

Caution: You can select (or not select) the **Automatically resize PGP Virtual Disk as necessary** option only when you are creating a PGP Virtual Disk. Once the disk is created, you can neither change a PGP Virtual Disk from a fixed disk to a resizable one, or vice-versa.

- From the **Cipher** menu, select the encryption algorithm that you would like to use to protect your PGP Virtual Disk: **AES-256 (256 bits)** or **CAST5 (128-bits)**. For more information about these encryption algorithms, see The PGP Virtual Disk Encryption Algorithms.
- From the **Format** menu, select the disk format that you would like to use with your PGP Virtual Disk:

  MS-DOS. Use if you intend to share this PGP Virtual Disk with someone using PGP Desktop 10.0 for Windows.

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

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

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

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

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

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

6 Click **Continue**.

7 The next step depends on whether you chose public key or passphrase authentication.

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

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

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

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

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

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

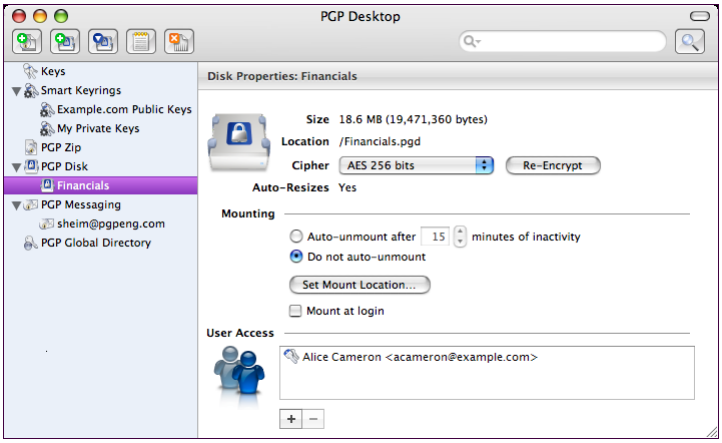
  In the **Confirm your passphrase** field, re-type the passphrase that you would like to use. Click **Continue.** The Save As dialog box is displayed. Continue with the next step.

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

9 Review the information on the PGP Disk Creation Summary screen. This screen displays the size of the PGP Virtual Disk, the volume name and location, the format, and so on. When you are finished, click **Create**.

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

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



Viewing the Properties of a PGP Virtual Disk

Once a PGP Virtual Disk has been created, information about the disk and settings you can change are accessible from the Disk Properties screen.

To view the properties of a PGP Disk volume

- Click on the name of the disk in the **PGP Disk** item. The Disk Properties screen is displayed.

Using a Mounted PGP Virtual Disk

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.

Caution: 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 to 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.

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:

- In PGP Desktop, select the PGP Virtual Disk you want to mount and select **Disk > Mount**.
- In PGP Desktop, select the PGP Virtual Disk you want to mount and then click **Mount** in the upper-right corner on Windows systems, or the **Mount** icon on the toolbar on Mac OS X systems.
- Change the properties of the PGP Virtual Disk so that it mounts when your computer starts.

On Windows systems only:

- 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 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 and Mac OS X Finder.

Unmounting a PGP Virtual Disk

You lock a PGP Virtual Disk by unmounting it. Once a PGP Virtual Disk is unmounted, its contents are locked in the encrypted file associated with the volume. Its contents are inaccessible until the volume is mounted once again.

Caution: You may lose data if you unmount a PGP Virtual Disk when some files that it contains are open. Specify options for unmounting disks by selecting **PGP > Preferences** and clicking the **Disk** icon. One option is **Allow PGP Virtual Disks to unmount even while files are still open**. If that option is selected, the option for **Don't ask before unmounting** also becomes available. **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:

- In PGP Desktop, select the PGP Virtual Disk you want to unmount under the PGP Disk item and select **Disk > Unmount** or click the **Unmount Disk** icon on the toolbar.
- Drag the icon of the mounted PGP Virtual Disk volume to the **Trash**.

Set Mount Location

You can specify where the PGP Virtual Disk is mounted (located).

To set the mount location

1. Select the PGP Disk control box, then select the PGP Virtual Disk for which you want to set the mount location.
2. Click **Set Mount Location**. The Set your PGP Disk's mount point dialog box is displayed.
3. Select one of the following:
   - **Desktop (Default)**. Select this option to mount your PGP Disk volume on the Desktop. This is where the PGP Virtual Disk is mounted if you do not specify another location.
   - **At the following location**. Select this option to mount your PGP Virtual Disk at a location that you specify. Click **Browse,** then navigate to the location at which you would like your PGP Virtual Disk mounted. Click **Open** to confirm your choice.
4. Click **OK**. The mount location for your PGP Virtual Disk is established.

Compacting a PGP Virtual Disk

To free up additional space on your PGP Virtual Disk, compact the disk. If the PGP Virtual Disk is mounted, you must unmount the disk first, before you can compact it.

To compact a PGP Virtual Disk

- Do one of the following:
  - In Mac OS X Finder, navigate to the location of the .pgd file. Right-click the file and select **PGP > Compact**.

    If you do not know where the PGP Virtual Disk is located, in PGP Desktop, right-click the name of the disk and select **Reveal in Finder**.

- In PGP Desktop, click the PGP Disk item on the left pane of the PGP Desktop main screen, select the PGP Virtual Disk you want to compact, and then select **Disk > Compact Disk**. You can also Ctrl+click (or right-click, if you have a two-button mouse) the PGP Virtual Disk in the PGP Disk control box and select **Compact** from the shortcut menu.

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 encrypt your PGP Virtual Disk again, but use a different underlying encryption key.

Caution: Adept users may be able to search the memory of a computer for the underlying encryption key of a PGP Virtual Disk. These users 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. Select the PGP Disk item on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk that you want to re-encrypt.
2. If the PGP Virtual Disk is mounted, unmount it.
3. Click **Re-Encrypt**. A confirmation dialog box is displayed.
4. Review the information it contains, then click **Re-Encrypt.** The Enter PGP Passphrase dialog box is displayed.
5. Type the passphrase for the PGP Virtual Disk administrator, then click **OK**. The PGP Virtual Disk is re-encrypted. A progress bar is displayed during the process.
6. When the current status displays Done, click **Next**.
7. Click **Finish** to complete the re-encryption process.

Working with Alternate Users

This section describes how to add, delete, and disable alternate user accounts for your PGP Virtual Disks. Also included is information on how to change the rights for users, including granting administrator rights to a user.

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 item on the left pane of the PGP Desktop main window, then select the name of the PGP Virtual Disk to which you want to add an alternate user.
2. Click the plus sign icon under the User Access list of the Disk Properties screen; select **Add Public Key User** or **Add Passphrase User,** depending on what kind of alternate user account you want to add.
   - If you clicked **Add Public Key User**, select the public key of the alternate user you want to add by dragging their key from the **Key Source** column to the **Keys to Add** column. You can add multiple alternate users if you like.
   - If you clicked **Add Passphrase User**, select the public key of the alternate user you want to add by dragging their key from the **Key Source** column to the **Keys to Add** column. The Add a user to your PGP Disk dialog box is displayed.

     In the **Name** field, type a name for the alternate user you are adding.

     In the **Enter a passphrase for this user** field, type a passphrase for the user.

     In the **Confirm user's passphrase** field, re-type the passphrase. The **Passphrase Quality** bar indicates the strength of the passphrase that you have typed. Select the **Show Keystrokes** check box if you want to see the characters you are typing.
3. Click **OK**. The Disk Properties screen is displayed again; the alternate public-key user or alternate passphrase user is displayed in the B list.

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 item on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk for the user account you want to delete.
2. In the User Access list, select the name of the alternate user whose account you want to remove. You cannot remove the Administrator.
3. Click the minus sign icon under the **User Access** list. A confirmation dialog box is displayed.
4. Click **Remove**. The alternate user is deleted.

Disabling and Enabling 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 or enable an alternate user account from a PGP Virtual Disk

1. Click the PGP Disk item on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk for the user account you want to change.
2. In the **User Access** list, select the alternate user you want to disable or enable. You cannot disable the Administrator.
3. Do one of the following:
   - To disable a user, select **Disk > Disable User**. A confirmation dialog box is displayed. Click **Disabled**. The alternate user is disabled. The user is greyed out in the **User Access** list.
   - To enable a user that you previously disabled, select **Disk > Enable User**. The alternate user is enabled.

Changing Read/Write and Read-Only Status

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 change the rights for a user of a PGP Virtual Disk

1. Click the PGP Disk item on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk for the user account you want to change.
2. In the User Access list, select the name of the alternate user whose read/write status you want to change.
3. Do one of the following:

- To change the user to read-only access, Ctrl+click (or right-click) the user's name and select **Set Read-Only Access**.
- To change the user to read/write access, Ctrl+click (or right-click) the user's name and select **Allow Write Access**.

Tip: These options are also available from the Disk menu when the user is selected.

4 The rights 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.

To grant administrator status

1 Click the PGP Disk item on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk for the user account you want to change.

2 In the User Access list, select the user you want to make administrator of the PGP Virtual Disk. Select either a passphrase user or yourself (if you are not the current administrator). Note that you cannot make a public key user an administrator of the PGP Virtual Disk.

3 Ctrl+click (or right-click if you have a two-button mouse) and select **Set as Disk Administrator** from the shortcut menu. The Enter PGP Passphrase dialog box is displayed.

Tip: You can also select **Disk > Set as Disk Administrator.**

4 Type the passphrase for the PGP Virtual Disk administrator, then click **OK**. The selected user account is changed to administrator.

Note: You can grant Administrator status to only 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 passphrase for a PGP Virtual Disk

1 Select 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 Select the name of a passphrase user from the User Access list, then select **Change User Passphrase** from the **Disk** menu. The Enter PGP Passphrase dialog box is displayed.

Tip: You can also Ctrl+click (or right-click if you have a two-button mouse) the user's name and select **Change User Passphrase** from the shortcut menu.

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

4 Type a new passphrase, type the passphrase again to confirm it, and click **OK**. The passphrase is changed.

Deleting PGP Virtual Disks

At some point you may decide you no longer need a particular PGP Virtual Disk and may choose to delete the disk entirely.

Caution: 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 want to save to another location *before deleting a PGP Virtual Disk*.

Make sure the selected PGP Virtual Disk is *not* mounted. You cannot delete the PGP Virtual Disk if the volume is mounted.

To delete a PGP Virtual Disk

1 Select the PGP Disk control box on the left pane of the PGP Desktop main screen, then select the PGP Virtual Disk you want to delete.

2 Select **Reveal in Finder** from the shortcut menu. A Finder window is displayed with the PGP Virtual Disk file selected. If you have opted to have Mac OS X display file extensions, the PGP Virtual Disk is a .pgd file.

3 Drag the file to the Trash, then select **Empty Trash** from the File menu in the Finder.

4 In PGP Desktop, Ctrl+click (or right-click if you have a two-button mouse) the PGP Disk volume you want to delete and select **Remove Item** from the shortcut menu. The PGP Disk is deleted from your system, as well as from PGP Desktop.

Maintaining PGP Virtual Disks

This section describes how to take proper care of the PGP Virtual Disk 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.

Note: 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 file system 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 in encrypted form

1. Unmount the PGP Virtual Disk.
2. In the Finder, locate the PGP Virtual Disk file. If you have opted to have Mac OS X display file extensions, the PGP Virtual Disk file name ends with `.pgd`.

   Tip: You can find the PGP Virtual Disk file easily by Ctrl+clicking (or right-clicking if you have a two-button mouse) the disk in the PGP Disk of the PGP Desktop side panel. Select **Reveal in Finder** from the shortcut menu.
3. Copy the unmounted encrypted PGP Virtual Disk file to a CD, DVD, tape, removable cartridge, or diskette just as you would any other file.

Even if some unauthorized person has access to the backup, they cannot decipher its contents.

When making backups of encrypted PGP Virtual Disk 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 from 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 vulnerable state.

Exchanging PGP Virtual Disks

You can exchange PGP Virtual Disk 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 Disk:

- 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.

Note: Public key is the most secure protection method when adding alternate users to a PGP Virtual Disk because: (1) You do not need to exchange a passphrase with the alternate user which, depending on your method, could be intercepted or overheard. (2) The alternate user does not 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.

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 enter 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. Without this critically important feature, someone could search for your passphrase in your computer memory while you were away from the system. You would not know it, but they would then have full access to data 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 prevents a potential intruder from scanning the virtual memory file looking for passphrases.

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.

13 Accessing Mobile Data with PGP Portable

Use PGP Portable to distribute encrypted files to users who do not have PGP Desktop software. Use PGP Portable to transport files securely to other systems that do not or cannot have PGP software installed.

PGP Portable provides:

- Portability of secured documents
- Ease of distribution of secured documents

There are two types of users of PGP Portable: the user who creates the PGP Portable Disk containing secured data, and the user who does not have PGP software but needs to access that secured data. You might also be both types of users: creating a PGP Portable Disk that you can take and use on a computer at a customer's site, for example.

On a Mac OS X system, you can *access* encrypted data that is stored on a PGP Portable Disk.

In This Chapter

Accessing Data on a PGP Portable Disk

The contents of a PGP Portable Disk can be accessed in three ways:

- By mounting the CD, DVD, or removable uSB drive on a Windows system, and running the PGP Portable Disk application (which launches automatically if autorun is enabled).
- By mounting the CD, DVD, or removable USB drive on a Mac OS X system, and running the PGP Portable Disk application.

When you access data on a PGP Portable Disk, remember that you are actually mounting two items: the removable device on which the PGP Portable Disk resides, and the PGP Portable Disk itself (which is mounted as a separate item). When you are finished, be sure to unmount thePGP Portable Disk before safely ejecting the removable device.

The steps to access data on a PGP Portable Disk are similar for Windows and Mac OS X systems.

Warning: Be sure that you properly unmount a removable device before physically removing it from the system. Failure to do so may result in corrupted file contents.

To access data on a PGP Desktop Disk using a Mac OS X system

1. Insert the removable device on which the PGP Desktop Disk is located. This can be a CD/DVD or a flash or removable drive.
2. Open the mounted removable device and browse for the PGP Desktop application (PGP Portable). Double-click the application. The PGP Portable dialog box is displayed.

3. Enter the passphrase for the PGP Desktop Disk.
4. When the correct passphrase has been entered, the PGP Desktop Disk is mounted. If the PGP Desktop Disk is mounted as a read-write device, you can add data to it. If the PGP Desktop Disk is mounted as a read-only device, you cannot add data.

   Note that the volume name is unique to PGP Desktop Disks and may not match the name of the volume when created.
5. When you are finished using the PGP Desktop Disk, unmount the PGP Desktop Disk (in the dock, click the PGP Desktop icon and then click **Unmount**. The drive that was mounted for the PGP Desktop Disk is unmounted.
6. Properly eject the USB device or disc from your computer.

Warning: Be sure that you properly unmount a removable device before physically removing it from the system. Failure to do so may result in corrupted file contents.

Changing the Passphrase for a PGP Portable Disk

There may be times when it is necessary to change the passphrase associated with a PGP Portable Disk. Note that you cannot change the passphrase on any PGP Portable Disk that is read-only (including PGP Portable Disks burned to CD/DVD media).

To change the passphrase on a PGP Desktop Disk using a Mac OS X system

1. Insert the removable device on which the PGP Desktop Disk is located. This can be a CD/DVD or a flash or removable drive.
2. Open the removable device and locate the PGP Desktop application (PGP Portable). Double-click the application, and enter the passphrase for the PGP Desktop Disk when prompted. When the correct passphrase has been entered, the PGP Desktop Disk is mounted.
3. Open PGP Desktop by clicking the icon in the dock and in the PGP Desktop dialog box, clicking **Change Passphrase**.
4. Enter the current passphrase, Enter and confirm the new passphrase, and click **Change**.

Unmounting a PGP Portable Disk

Be sure that you properly unmount a removable device before physically removing it from the system. Failure to do so may result in corrupted file contents.

To unmount a PGP Portable Disk

1. Open PGP Portable. To do this, do one of the following:
   - To open PGP Portable on a Windows system, right-click the system tray icon and choose **Unmount and Exit**.
   - To open PGP Portable on a Mac OS system, click the icon in the dock and choose **Unmount and Exit**.

   The PGP Portable Disk is unmounted.
2. Safely eject and remove the device from your system.

14 Using PGP Zip

Use PGP Zip to create, open, and edit encrypted and compressed packages, called PGP Zip archives. This section describes how to use the PGP Zip feature of PGP Desktop.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

Overview

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.

When you create a PGP Zip archive, you have the option of automatically deleting (shredding) the original files from your system when the archive has been created. When you receive a PGP Zip archive, choose to extract all of the files and/or folders in the archive or just the ones you want.

Create PGP Zip archives that are:

- **Encrypted to a public key**. If you are sending the PGP Zip archive to one or more persons whose public keys you have, you should encrypt the archive to their public keys; thus, only the intended recipients can open the archive. The recipients must have PGP Desktop installed.

- **Encrypted to a passphrase**. If you prefer to encrypt to a passphrase or you're sending the archive to multiple recipients, some of whom you don't have their public key, you can specify conventional encryption and encrypt the archive using a passphrase. In this case, you will need to communicate the passphrase to the recipients so they can open the archive. The recipients must have PGP Desktop installed.

PGP Zip archives are encrypted to the preferred cipher for PGP Desktop (if configured by a PGP administrator) or to AES256. PGP Zip Archives can be freely moved between Mac OS X and Windows platforms. PGP Desktop must be installed on the system to which the PGP Zip archive is being moved.

Creating PGP Zip Archives

To create a new PGP Zip archive

1. Open PGP Desktop and select the PGP Zip item. The PGP Zip screen is displayed.
2. Click **Create new PGP Zip**. The Untitled PGP Zip dialog box is displayed.
3. In the **Files** tab, specify what files and/or folders you want to be part of the PGP Zip archive you are creating. Do this by:
   - Dragging and dropping the files/folders into the list.
   - Clicking the plus sign icon below the list, then select the files and/or folders you want to be part of the PGP Zip archive in the dialog box displayed. Click **Add** to add the files to the list.

   If you add a file or folder you later decide you do not want, select the file or folder in the list and click the minus sign icon below the list. The file or folder is removed from the list.
4. Select **Shred original files** if you want to securely delete from your system the files/folders you are putting into the PGP Zip archive.
5. When you have specified the files/folder you want included in the PGP Zip archive, click the **Security** tab.
6. If desired, specify a private key from your keyring to provide a **Signature** for the PGP Zip archive you are creating.

   This specified private key is used to digitally sign the PGP Zip archive being created. The recipient(s) can verify who the archive is from by verifying the digital signature using the corresponding public key.
   - To view the properties of the selected signing key, click the Key icon to the right of the user ID of the key. Close the Key Info dialog box when you are done.
7. Select the type of encryption you want to use:

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

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

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

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

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

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

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

9 Click **Save**.

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

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

Opening a PGP Zip Archive

PGP Desktop must be installed on the system to open a PGP Zip archive.

To open a PGP Zip archive

1 Double click the archive file and do one of the following:

- If the archive was encrypted to your public key, you are prompted for the passphrase to your private key, which will be used to decrypt the archive (if the passphrase is cached, you do not need to enter it). Enter the appropriate passphrase and click **OK**.

- If the archive was encrypted to a passphrase, you are prompted for the passphrase. Enter the appropriate passphrase and click **OK**.

If the archive was also signed, PGP Desktop attempts to verify the signature; when verification is complete, a verification screen is displayed, displaying the results of the verification process.

2 If two or more files/folders were in the archive, a new folder is created that includes the files and/or folders that were in the PGP Zip archive.

If only one file was in the archive, just that file is created at the location of the PGP Zip archive.

Verifying Signed PGP Zip Archives

If you received a *signed* PGP Zip archive, you should verify it so that you know who it came from and that the archive was not tampered with before you got it. Files that are not signed cannot be verified.

To verify a signed PGP Zip archive

1 In PGP Desktop, select **View > Verification Info**. The Verification Info screen is displayed.

2 Drag the signed PGP Zip (.pgp) file you want verified onto the **Drag Signed Files Here** box. PGP Desktop verifies the signature and displays the verification information.

3 To clear the list of verified archives, click **Clear**. All listings on the Verification Info screen are removed.

15 Shredding Files with PGP Shredder

If you want to completely destroy sensitive files without leaving fragments of their data behind, use the PGP Shredder utility.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

Using PGP Shredder to Permanently Delete Files and Folders

If you want to destroy sensitive files or folders completely, use the PGP Shredder feature. When you delete files or folders using PGP Shredder, all traces of the item are removed.

The PGP Shredder feature works by overwriting your data with random text. It repeats this multiple times, or *passes*. You can set the number of passes that the PGP Shredder feature makes whenever it deletes a file—do that by opening the Disk panel of the Preferences screen. For more information about setting options and preferences, see *Disk Options/Preferences* (see "Disk Preferences" on page 196).

The shred session can be lengthy, depending on such factors as the number of passes you specified, the speed of the processor, and how many other applications are running.

Note: When set for three passes, PGP Shredder exceeds the media sanitization requirements specified in the Department of Defense 5220.22-M standard. While more passes are allowed, modern disk hardware does not require more than two passes. Security continues to increase up to approximately 28 passes. The PGP Shredder feature is capable of up to 49 passes, but remember that more passes means more time needed for secure deletion.

There are multiple ways to use PGP Shredder:

- Use the PGP Shredder icon. When PGP Desktop was installed, the PGP Shredder feature was installed into the same directory as the PGP Desktop application. Creating an Alias to the PGP Shredder icon, then moving the Alias to the Dock or Desktop makes the PGP Shredder convenient and easy to use.
- Use the PGP Shredder icon on the PGP Toolbar. Click the PGP Shredder icon in the Toolbar, then browse to the file/folder you want to shred.
- Select **File > Shred**, then browse to the file/folder you want to shred.
- Use the Finder shortcut menus (Ctrl+click, or right-click if you are using a two-button mouse, the file or folder and select **PGP > Shred**).

Caution: Some file systems use a feature called Journaling. Apple has introduced this feature for Mac OS Extended (HFS+) file systems in Mac OS X 10.2.2. Journaling causes a copy of everything written to disk to be written a second time in a private area of the file system. Thus, shredding the original file causes the original file to be shredded while the original file data is written to another part of the disk. To avoid this problem, *do not use the Journaling feature.* Journaling can be disabled using Apple's Disk Utility. For more information on file system journaling, see *Apple Support Technical Article 107249* (http://docs.info.apple.com/article.html?artnum=107249).

Tip: Many programs automatically save files in progress, so backup copies of the file you deleted may exist. After you delete the primary copy of a file, PGP Corporation recommends that you then use the PGP Shredder feature to delete any backup copies securely.

Shredding Files using the PGP Shredder icon

▸ **To shred a file or folder using the PGP Shredder icon**

1. Locate the file or folder you want to delete securely.
2. Drag the file or folder onto the PGP Shredder icon. A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.
3. Click **OK**. The file or folder is deleted from your system securely.

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

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

▸ **To shred a file or folder using the PGP Desktop Toolbar**

1. Click the **Shred Files** icon in the toolbar.
2. Locate the file or folder you want to Shred, then click **Shred**. A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.
3. Click **OK**. The file or folder is securely deleted from your system.

Shredding Files using the Shred Command from the File menu

▸ **To shred a file or folder using the Shred command**

1. Select **File > Shred.**
2. Navigate to the file or folder you want to Shred, then click **Shred**. A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.
3. Click **OK**. The file or folder is securely deleted from your system.

Shredding Files in the Finder

▸ **To shred a file or folder in the Finder**

1. In the Finder, locate the file or folder that you want to shred.
2. Ctrl+click the file or folder (or right-click it if you are using a two-button mouse) and select **PGP > Shred.** A confirmation dialog box is displayed, asking you to confirm that you want to shred (secure delete) the listed files and/or folders.
3. Click **OK**. The file or folder is securely deleted from your system.

16 Setting PGP Desktop Preferences

PGP Desktop is configured to accommodate the needs of most users, but you can adjust some settings to suit your requirements. This section describes the options you can set in PGP Desktop.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, your PGP Universal Server administrator may have disabled certain features. When a feature is disabled, the control item in the left side is not displayed and the menu and other options for that feature are not available. The graphics included in this guide depict the default installation with all features enabled. If your PGP Universal Server administrator has disabled this functionality, this section does not apply to you.

In This Chapter

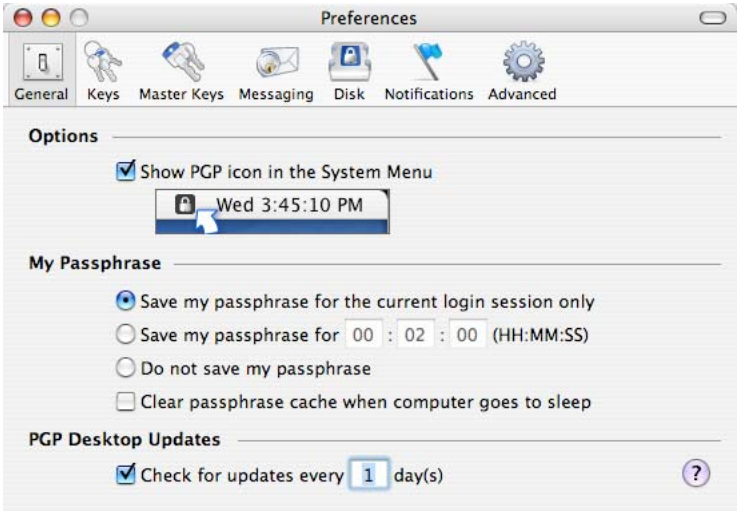
Accessing PGP Desktop Preferences

To access the PGP Desktop Preferences

1. Open PGP Desktop.
2. Select **PGP > Preferences**.
   - Move between different kinds of preferences by clicking the icons at the top of the Preferences dialog box
3. When you are done setting preferences, click the close button (the red circle in the upper left corner of the screen).

General Preferences

The General Preferences dialog box covers a variety of PGP Desktop settings.



The options on the General page of the Preferences dialog box are:

- **Show PGP icon in the System Menu.** When enabled, the PGP Desktop icon is displayed in the Mac OS X Menu Bar while PGP Desktop is active on the system. The PGP Menu Bar icon provides easy access to PGP Desktop functions.
  - To remove the PGP Desktop icon from the Menu Bar, deselect the checkbox.
  - To restore the PGP Desktop icon to the Menu Bar, navigate to the General preferences screen and select the **Show PGP icon in the System Menu** checkbox.

  Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, this option may be required.

  Removing the PGP Desktop icon from the Menu Bar does *not* shut down PGP Desktop services; they continue running.

  - To stop PGP Desktop services, press the **Option** key. In the Menu Bar, click the PGP Desktop icon, then select **Quit**.

  Note: PGP Corporation suggests that you not stop PGP Desktop services unless required to do so.

- **My Passphrase**. Provides options to save your passphrase.

- **Save my passphrase for the current login 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 enter it again for the same key until you log off your computer.

Caution: When this option is enabled, it is very important that you log off your computer before leaving it unattended. (You can log out by selecting **Log out [your name]** from the Apple menu.) If you never log off, your passphrase can remain cached for weeks, 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**. 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 enter it again until the specified time has elapsed. The three number fields are for **hours, minutes, seconds,** respectively. The default setting is two minutes.
- **Do not save my passphrase**. Prevents your passphrase from being stored in memory. If you enable this option, you must enter your passphrase each time it is needed.
- **Clear passphrase cache when computer goes to sleep**. Enable this preference to have PGP Desktop clear any saved passphrases from memory when your computer goes into Sleep mode. (Not all computers have a Sleep mode.)

- **Check for updates every X day(s).** When enabled, PGP Desktop checks for software updates automatically at the specified interval. The default interval is one day. If a newer version of PGP Desktop is available for download, a notification screen is displayed to notify you of the new version and help you download it. When this option is disabled, PGP Desktop does not automatically check for software updates.

  This option requires an available Internet connection to work correctly.

  Once you have downloaded the update, install the update by following the prompts.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, this option may be required. PGP Desktop then searches for updates on its associated PGP Universal Server.

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

Keys Preferences

The Keys Preferences dialog box contains settings that apply to PGP Desktop keys.

The options on the Keys page are:

- **Synchronization**. These settings specify how you want keys on your keyrings synchronized with public servers.
  - **Synchronize with keyservers daily**. When selected, PGP Desktop performs a daily synchronization of the public keys on your keyring with your list of keyservers. This list includes the PGP Global Directory.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, this option may be required.

If changed versions of the keys are available, they are downloaded automatically. If the keyserver notifies PGP Desktop that a key is removed from the keyserver, PGP Desktop disables that key on the local keyring.

If you use PGP Desktop to make a change to a public key on your keyring, that change is not automatically uploaded from your computer to any keyserver. You must manually upload the changed key to the desired keyserver. PGP Desktop prompts you to upload changed keys when you quit. Otherwise, to send the key to the keyserver, right-click the changed key, select **Send To** from the shortcut menu, and then select the desired keyserver from the list.

- **Automatically lookup keys on keyservers when verifying signatures.** When this option is enabled, you can specify that PGP Desktop should search the configured keyservers for the necessary public key if you receive an email message signed by a private key and you do *not* have the corresponding public key on your local keyring.

Note: If you are using PGP Desktop in a PGP Universal Server-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 Server-managed environment are never saved to your keyring.

If the public key *is* found on the keyserver, there are three options:

- **Do not save to my keyring.** Any key(s) found on the configured keyservers are used only once, to verify the signature with which you are currently working. The key is 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 my keys with other computers using MobileMe**. (MobileMe is Apple's new version of .Mac.) Check this box to synchronize your keys using your MobileMe account. (You must have a valid account to use this option.) When this option is selected, the synchronization engine runs and copies your key files to a local cache that MobileMe uses for updating.
- To synchronize your keys with your MobileMe account immediately, click **MobileMe**. The System Preferences MobileMe panel is displayed. Log in, click the Sync panel, select the PGP Keys item in the list, and click **Sync Now**.

- **Backup**. These settings specify when and where you want your keys backed up.
  - **Backup keys upon exiting PGP Desktop.** 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.
    - **to this location.** When selected, your keys are backed up to the location on your computer that you specify. Click **Browse** to set a location.

Master Keys Preferences

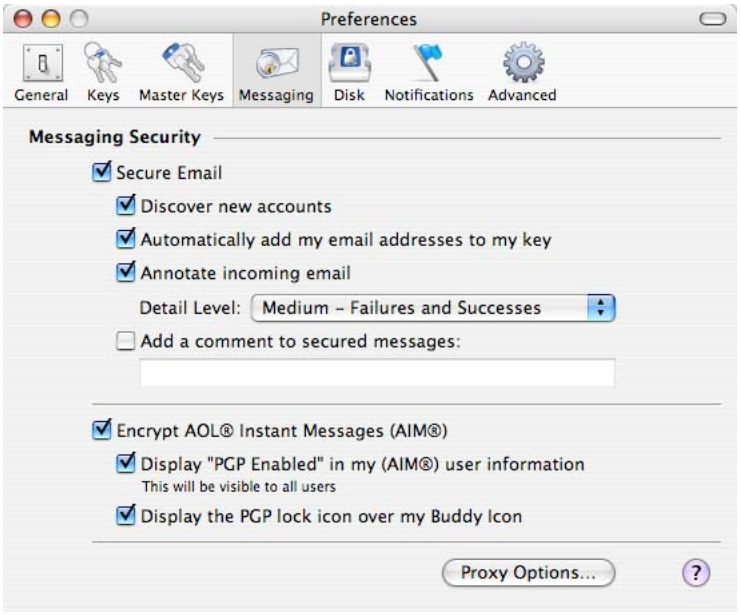
The Master Key List is a set of keys that you want added by default any time you are selecting keys for messaging, disk encryption, and PGP Zip. This saves you the step of dragging the keys that you regularly use into the **Recipients** field.

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.

Note: If you generated your key using the Setup Assistant, your key is automatically added to the Master Key list. If you skipped key generation and imported your key into PGP Desktop, your key is not automatically added to the list.

Messaging Preferences

The **Messaging** Preferences panel contains settings that apply to your messaging security. It also provides access to email and IM settings.



The **Messaging** preferences are:

- **Secure Email.** Select the **Secure Email** checkbox if you want PGP Desktop to automatically secure all your email accounts. 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. It then secures messages sent using those accounts.

Note: If you are using PGP Desktop in a PGP Universal managed environment, the use of a wildcard (*) binding causes this function to be no longer active due to all mail services will match the binding of *. Therefore all new accounts will automatically match policy and be created even if this option is deselected.

- **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.

  Deselect this checkbox to prevent email addresses from being automatically added to your key. This has privacy value; for example, if you want 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 from 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 an 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 enter here is always included in messages you encrypt or sign. Comments entered 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.

Note: If you are using PGP Desktop in a PGP Universal Server-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 compatible instant messaging clients. The other participant in the IM session must also be using PGP Desktop.

  AOL® Instant Messenger™ and iChat software applications are compatible.

  - **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 is displayed 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 is displayed with your buddy icon, so others can see that the IM session is protected. When disabled, your icon is displayed normally.

- Click **Proxy Options** to access advanced messaging settings.

Proxy Options

Click **Proxy Options** for advanced email and IM preferences.

Email Preferences

If your computer needs to have a proxy manually configured so that you can send and receive email, you would use this feature.

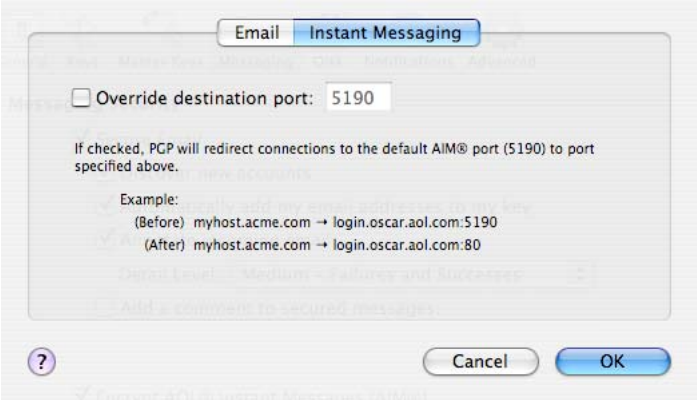
PGP Desktop works between your email application and the mail server that provides your mail. This configuration enables PGP Desktop to filter, or *proxy,* your email traffic for you automatically. PGP Desktop can protect your messages, based on the applicable policy, without interrupting your work.

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.

Instant Messaging Preferences

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.



- **Override destination port.** 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 port number to use.

Disk Preferences

The **Disk** Preferences panel contains settings that apply to volumes protected using the PGP Virtual Disk and the PGP Shredder features.

Note: If you are using PGP Desktop in a PGP Universal Server-managed environment, these preferences may already be configured.

The **Disk** preferences are:

- **Allow PGP Disks to unmount even while files are open.** Normally, you cannot automatically unmount a PGP Virtual Disk if any of the files in that volume are open. Enabling this option allows unmounting even with open files, a practice known as a forcible unmount.

  Warning: 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 automatically unmounts any mounted PGP Virtual Disk volumes when your computer goes into Sleep mode.

  - **Prevent sleep if disk(s) cannot be unmounted.** This setting is inactive until you select the **Unmount when computer goes to sleep** checkbox. This setting prevents your computer from sleeping if a PGP Virtual Disk volume cannot be unmounted.

- **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 (up to a maximum of 49 passes).

  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.

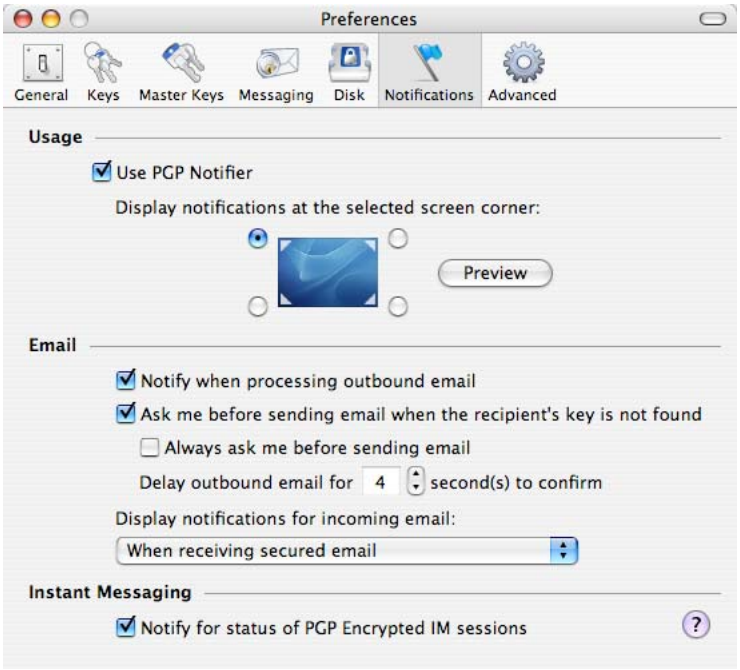
  The recommended guidelines for number of passes are:

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

- **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 to be shredded. This option is selected by default.

Notifications Preferences

The **Notifications** Preferences panel 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 PGP Desktop disk features.



The **Notifications** preferences are:

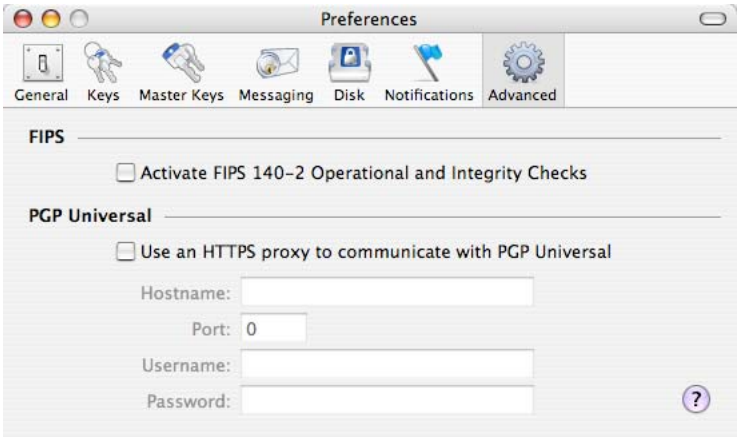
- **Use PGP Notifier:** PGP Desktop Notifications can appear at any of the four corners of your screen. Select a button to indicate the corner that you would like PGP Desktop Notifications to appear. Click **Preview** to see how the PGP Desktop Notification alert box looks in the specified corner.
- **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 Notifications 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 PGP Desktop Notification 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 91).

- **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 PGP Desktop Notification, and either send or block the email.
- **Delay outbound email for n second(s) to confirm** (where *n* is a number from 1-30; the default is 4 seconds). If you would like a PGP Desktop Notification 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 PGP Desktop 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 PGP Desktop Notification, move your cursor over it. The PGP Desktop Notification changes from translucent to opaque in appearance, and the outbound email is delayed while you review the PGP Desktop Notification information. You can then allow the email to be sent, or block it.
- **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 PGP Desktop Notification box is displayed 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 PGP Desktop Notification box 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 PGP Desktop Notification box as you receive email, select this option. This option does not affect PGP Desktop Notifications for outgoing mail.
- **Notify for status of PGP Encrypted IM sessions**: Select this checkbox if you would like a PGP Desktop Notifier box to appear briefly when you begin a secure instant message chat, and appear briefly again when the chat ends.

Advanced Preferences

The **Advanced** Preferences panel provides settings that most users will not need to change.



The **Advanced** preferences are:

- **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.
- **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 Server 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.

A Working with 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.

This section 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.

In This Chapter

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 enough to justify the effort. 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 255 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 reduces 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.

For more information about Diceware, see the *Diceware Passphrase Home Page* (http://world.std.com/~reinhold/diceware.html).

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.

  Caution: 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:

- Do not write down your passphrase.
- Do not give your passphrase to anyone.
- Do not let anyone see you entering your passphrase.
- Do not use "password" or "passphrase."
- Do not use patterns. Not "abcdefgh" or "12345678" or "qwertyui" or "88888888" or "AAAAAAAA."
- Do not 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.
- Do not 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.
- Do not 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.

- Do not use any of the above backwards, or with a preceding or following single digit.

What if You Forget Your Passphrase?

If you forget your passphrase, 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 key restoration policy for your company. For more information, see *PGP Key Reconstruction* (see "Reconstructing Keys with PGP Universal Server" on page 82, "If You Lost Your Key or Passphrase" on page 82) and contact your PGP administrator.

Saving Your Passphrase in the Keychain

If desired, you can cache your key passphrases using the Mac OS X Keychain. When you are prompted to enter a passphrase, select the box to **Save passphrase in Keychain**. You can then access all PGP Desktop features without needing to enter your passphrase each time.

Subkeys are also saved in the Mac OS X keychain, so actions by subkeys are automatic once the keychain has been unlocked.

B Using PGP Desktop with PGP Universal Server

PGP Universal Server 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. For more information about the PGP Universal Server, see *PGP Universal Server on the PGP website* (http://www.pgp.com/products/universal/index.html).

Using PGP Desktop in a PGP Universal Server-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.

To use PGP Desktop in a PGP Universal Server-managed environment, you must install PGP Desktop using an installer application you receive from your PGP administrator.

If you are using a version of PGP Desktop you purchased for home use, and are not using it in a corporate environment, you are likely using a standalone version, and this section does not apply to you.

Caution: If you are using PGP Desktop in a corporate environment and you obtained your PGP Desktop installer from a different source other than your PGP administrator, you should check with your PGP administrator **before** installing or using that version of PGP Desktop.

This section describes how using PGP Desktop is different in a PGP Universal Server-managed email domain.

In This Chapter

Overview

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.
- You may have certain features disabled, such as PGP Messaging or PGP NetShare (on Windows systems), or you may have a customized PGP Whole Disk Encryption BootGuard screen (on Windows systems). For more information, see *Features Customized by Your PGP Universal Server Administrator* (on page 4).

Those features of PGP Desktop that can be managed by a PGP administrator in a PGP Universal Server-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 Server-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.

Manually binding to a PGP Universal Server

If you manually bind to a PGP Universal Server using PGP Desktop (when viewing a Messaging Service, click **Server Settings**) and enroll, you will download only the email policy and not the consumer policy. Your PGP Universal Server administrator may have specified other options in the consumer policy (such as key modes, forcing the encryption of disks, and so on). To be fully managed and enforce consumer policy you need to use a PGP Universal Server "stamped" installation. Contact your administrator to obtain a stamped installation if you do not have one.

In addition, when you manually bind to a PGP Universal Server, the file `PGPtrustedcerts.asc` does not exist in C:\Documents and Settings\AllUsers\Application Data\PGPCorporation\PGP. If you want to manually bind to a PGP Universal Server, you will need to create this file and ensure that the user ID of the organization key in that file matches the server specified by the PGPSTAMP (the domain name and IP address must match).

Index

F

G

H

I

K

R

S

T

U

V

W

X