PGP Desktop Version 9.5 for Mac OS X Release Notes

Thank you for using this PGP Corporation product. These Release Notes contain important information regarding this release of PGP Desktop for Mac OS X. PGP strongly recommends you read this entire document.

PGP welcomes your comments and suggestions. Please use the information provided in Getting Assistance to contact us.

Product: PGP Desktop for Mac OS X

Version: 9.5.3

Warning: Export of this software may be restricted by the U.S. government.

What's Included in This File

About PGP Desktop

PGP Desktop is a security tool that uses encryption to protect your data, both while it is on your system and while it is in transit.

Changes in This Release

This section lists the changes and new features in PGP Desktop in this release.

Changes between 9.5.2 and 9.5.3 include:

- **Resolved issue:** AIM proxy updated to support protocol changes made by AOL. [12598]

Changes between 9.5.1 and 9.5.2 include:

- This release includes resolution for minor issues.

Changes in 9.5.1 - Hotfix 1 include:

- There are no changes to PGP Desktop for Mac OS X in this release.

Changes between 9.5.0 and 9.5.1 include:

- **Localized for German and Japanese:** PGP Desktop for Mac OS X is available in German and Japanese.
- USB disks inserted during startup may not show up property as candidate disks for Whole Disk Encryption. This issue has been resolved. [10756]

What's New In PGP Desktop 9.5 for Mac OS X

Building on PGP Corporation's proven technology, PGP Desktop 9.5 for Mac OS X includes numerous improvements and the following new features:

Installation

- **Intel-based Mac support** PGP Desktop 9.5 is a Universal application that runs on both Intel- and PowerPC-based Macintosh computers.
- **PGP Universal Migration** allows PGP Desktop software stamped from PGP Universal Server to be installed on top of an unstamped installation of PGP Desktop; this stamped version of PGP Desktop will reset the policies and bind the existing installation to the policies set on the Server.

General

- **Unified Window Interface** adoption of Apple's new Unified interface provides a cleaner, more integrated look under Tiger.
- **Network Key and Group Selection** for PGP Zip, PGP Whole Disk, and PGP Virtual Disk has been completely redesigned to support selection of keys from all local keyrings, smart keyrings, and keyservers. Additionally, this new interface fully integrates with LDAP directories on both Windows and Mac OS X, enabling selection of groups or mailing lists – when configured for policy synchronization with PGP Universal 2.5. This provides easy encryption of files, messages, and disks to defined groups in your enterprise directory.
- **Notifier** enables direct user interface control over whether to send a message or block it. The Notifier feature displays the results of all automated key lookup operations and conveys exactly how the message will be sent to each recipient, enabling you to decide whether or not to send the message. The Notifier fades into view in a user-selected screen corner whenever a message is sent. Inbound messages also show notifications, including details about the signature on the message.

PGP Whole Disk Encryption

- **PGP Whole Disk Encryption** introduces encryption of entire hard disks for Mac OS X including multiple-user support and full compatibility with PGP Whole Disk Encrypted disks from PGP Desktop for Windows. This feature supports all removable and non-boot fixed disks, and is compatible with HFS+, FAT, and FAT32 filesystems. NTFS is also supported, as read-only.
- **Resizable Virtual Disks** now automatically expand to fit their contents. A PGP Virtual Disk can automatically expand as files are copied to it to the maximum size of the physical media on which the disk file resides. A PGP Virtual Disk can also be compacted down to the minimum size of the enclosed files.

PGP Zip

- **PGP Zip Editing** allows PGP Zip files to be opened after creation for editing. File contents and encryption recipients can be changed at any time.

PGP Messaging

- **Directory Authentication Enrollment** with PGP Universal is now supported in addition to the previous email enrollment process.

- **PGP Universal Server Messaging Policy** extends PGP Desktop messaging policy to support the new PGP Universal 2.5 content filtering system.
- **International Characters** in messages have received significant compatibility improvements in this release.
- **Messaging Policy Enhancements** introduces the following new policies in the Messaging Policy Editor:
  - **Send Signed** policy action has been added to support signing messages without encryption, even when a key is found.
  - **Message Size** policies are now available to execute actions based on whether a message is greater than or less than specific sizes.
  - **Search keys.domain and policy** has been added to allow implicit keys.domain lookup prior to searching any of the configured keyservers. This is now configured in all default policies.
  - **Managed Local Keyring**: Server policy now optionally allows the local keyring to be used for key lookups. The local keyring is queried when this option is on before all other key sources.
  - **PGP Universal Server HTTPS Proxy Support** enables policy connections from the client to PGP Universal through HTTPS proxies.
  - **Mailing List Expansion** automatically expands each mailing list to list all individual recipients for encryption, enabling creation of secured mailing lists when PGP Desktop is configured for policy synchronization with both PGP Universal Server 2.5 and a configured directory server.

PGP Keys

- **Signing Subkeys** treats your master key as a subkey authorizer, to authorize sets of signing and encryption subkeys over time.
- **Bundle Keys** allows you to import multiple X.509 certificates including those on smartcards, as subkeys onto a new PGP key so as to retain the integrated identity inherent in such certificate collections. Additionally, X.509 certificates can be imported from PKCS 12 or PFX files as subkeys of existing PGP keys. Export as certificates is also supported.
- **Preferred Encoding** is a new key property that can be configured on your private keys. Preferred encoding states whether you can receive PGP/MIME, PGP Partitioned, or both encoding formats. All components of the 9.5/2.5 product suite observe this property.
- **FIPS 140-2 Integrity Checking** provides a comprehensive test suite used to verify the PGP SDK for FIPS validation that can now be executed whenever PGP Desktop starts up. This test suite verifies PGP Corporation's signatures on each PGP SDK binary and verifies the algorithmic integrity of each FIPS validated cipher and public key algorithm.
- **FIPS 186-3 (Read-Only)** support for verification of signatures from the newly defined DSA key sizes of 2048 and 3072 has been added. A future release of PGP products will allow generation of such signatures.

System Requirements

- Mac OS X 10.4.x (Intel or PowerPC)
- 512 MB of RAM
- 64 MB hard disk space

Supported Email Client Software

PGP Desktop will, in most cases, work without problems with any Internet-standards-based email client that runs on Mac OS X 10.3.8.PGP Desktop for Mac OS X has been tested with the following email clients:

- Apple Mail
- Microsoft Entourage

- Qualcomm Eudora

Instant Messaging Client Compatibility

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

- iChat 2.1 and 3.0 - 3.1.5
- AIM 4.7

Other instant messaging clients may work for basic instant messaging, but have not been certified for use. Encryption of file transfers and direct connections requires AIM 5.9.3702 on Windows or iChat 2.1 or 3.0 on Mac OS X. Audio and video connections are not encrypted by PGP Desktop.

Continued interoperability with the AIM service may be affected by changes made to the underlying AIM protocols after PGP Desktop is released.

Anti-Virus Client Software Compatibility for Macintosh

PGP Desktop and PGP Satellite for Mac OS X have no known issues with any Mac OS X anti-virus software packages.

Installation Instructions

▸ **To install PGP Desktop on your Mac OS X system:**

1. Mount the PGP Desktop disk image.
2. Double-click `PGP.pkg`.
3. Follow the on-screen instructions.

Licensing

PGP Desktop uses a licensing system to determine what features will be active. You enter your PGP Desktop license using the Setup Assistant after installation. If you are in a domain protected by a PGP Universal Server, your PGP administrator may have configured your PGP Desktop installer with a license.

You can also use PGP Desktop without a license, but for non-commercial use only. Commercial use of PGP Desktop without a license is a violation of the End-User License Agreement (EULA). If you choose to use PGP Desktop without a license (and you are legally permitted to do so under the EULA for non-commercial use), most PGP Desktop features will not work; only basic functionality will be available.

For more information about PGP Desktop licensing and purchase options, go to the PGP Store **(**https://store.pgp.com/**)** .

Additional Information

This version of PGP Desktop replaces all older PGP products, as well as replacing PGP Universal Satellite 2.X. These products will be removed as part of upgrading to PGP Desktop. [NBN]

PGP Whole Disk Encryption

- Please make sure to remove any removable disks prior to uninstalling the product. [10120]
- PGP WDE is not functional until after the system is restarted. [9954]
- Secondary partitions physically located on your boot volume are not available for encryption on Intel-based Mac OS X machines. [11025]
- Hibernation: In recent maintenance releases of Mac OS X 10.4, “Sleeping” newer Mac OS X machines causes a "hibernate" effect, where potentially sensitive portions of memory are written to disk with severe security implications. This new behavior does not yet have a user interface to turn it off in Mac OS X. It is also not compatible with PGP Whole Disk Encryption. The PGP Desktop installer automatically disables this behavior for security and compatibility reasons. (Note that this behavior can also be turned off manually using "sudo pmset -a hibernatemode 0" from a shell.) [11320]
- PGP WDE and NitroAV PCMCIA/Firewire 800 Adaptors: Removable devices connected to a MacBook Pro using a NitroAV PCMCIA/Firewire 800 adapter are not currently supported. In addition, if you attempt to connect a device that had already been encrypted or partially encrypted, the disk will fail to mount after valid credentials are entered. [11936]

PGP Messaging

- Message Comments: To ensure proper display of comments added to secured messages per the "Add a comment to secured messages" option, PGP Corporation recommends using ASCII text in the Comment field. [11127]
- S/MIME-signed email messages: PGP may not process S/MIME signed emails if the signing X.509 certificate is not included in the email. The certificate is almost always included with the email unless the sender turns off this option. [9489, 9491]
- PGP Desktop is initially installed in Automatic mode. You may change this in the Preferences if necessary to accommodate your environment. Automatic mode uses Mac OS X’s built-in firewall functionality to redirect your email client connections through PGP Desktop. Some less common configurations may need to use Manual mode instead. If you fall into the categories below, you should switch to Manual mode in the PGP Preferences (**Messaging > Proxy Options > Email**). [NBN]

  These include:

  - Those with a requirement to use the built-in firewall for other purposes. Note that third-party applications can be installed to provide much more complete configuration options than the built-in user interface in System Preferences. These other solutions are compatible with PGP Desktop. Note that Norton Internet Security 3.0 does not use these methods, and is not compatible with Automatic mode.
  - Those who already redirect their email connections through, for instance, an SSH tunnel or VPN connection. Some VPN connections may cause problems with the connection diversion capabilities of PGP Desktop.
  - Automatic mode should *not* be used on a system which is also a mail server; use Manual mode instead.
- Multiple users and Automatic mode. If you fast user switch between multiple PGP Desktop users on a single Mac OS X machine, the first user to enable Automatic mode in PGP Desktop will be the only user who will be able to use Automatic mode; all other users must use Manual mode. If there are three or more users, each Manual mode user must bind to unique ports. [3335]
- Multiple messaging services for one email account. 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. PGP Desktop ships with wildcard support for common email services, such as *.yahoo.com and *.mac.com. If you see PGP Desktop create multiple services for a single email account, and you check the settings and see that the settings are the same except that 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, then you need to change the server name on the Server Settings screen for one of the services to mail*.example.com, then delete the other services. [5611]
- Mozilla Thunderbird: If you are using Mozilla Thunderbird as your email client, you should change your message forwarding preference to Inline to make sure that messages you forward as attachments display

correctly for Thunderbird IMAP users. To change the message forwarding preference to Inline, pull down the Tools menu and select Options. Click on the Composition icon, then choose Inline from the Forward Messages drop-down menu. [5982]

- AOL Mail 10.3.7: AOL Mail 10.3.7 is supported only if you disable the PGP AIM proxy. To work around this issue, quit PGP engine (option-click PGP menu) before running AOL or configure PGP to use manual proxy mode instead of automatic. (Click Messaging, click Proxy Options, and then select Manual Proxy.) [12057]
- Legacy users may have email stored that was encrypted with a version of PGP Desktop prior to 9.0. To decrypt such legacy email messages, PGP Desktop retains some of the decryption side of the plug-in technology used in previous versions of PGP Desktop.

  All PGP/MIME type emails (with or without attachments) are decrypted by the PGP Desktop plug-in, as are any plain text-formatted PGP Partitioned emails without attachments. However, HTML-formatted PGP Partitioned messages or any PGP Partitioned messages with attachments fail to decrypt with the PGP Desktop plug-in. You can rebuild your mailbox, as described below, to decrypt HTML-formatted PGP Partitioned emails with attachments.

  For encrypted IMAP mail to be proxied again, use the rebuild function in your mail application to re-download your email. For example in Mail.app, to rebuild your IMAP mailbox, choose **Mailbox > Rebuild**. Messages are again downloaded and decrypted by proxy. If proxying has stopped for some reason, reboot or quit and relaunch PGP Desktop before rebuilding your mailbox. [9730]

PGP Keys

- Key Reconstruction for PGP Desktop for Mac OS X users in a PGP Universal-managed environment is not supported in this release. [3505]

PGP Shred

- Shredding symbolic links on the Mac will shred the linked file or directory. [8922]

Getting Assistance

This section provides contact information and additional resources.

Contacting Technical Support

- To learn about PGP support options and how to contact PGP Technical Support, please visit the PGP Corporation Support Home Page (http://www.pgp.com/support).
- To access the PGP Support forums, please visit PGP Support (http://forums.pgpsupport.com).
- To access the PGP Support Knowledge Base or request PGP Technical Support, please visit PGP Support Portal Web Site (http://www.pgpsupport.com). **Note that you must have a valid support agreement to request Technical Support.**
- For any other contacts at PGP, please visit the PGP Contacts Page (http://www.pgp.com/company/contact/index.html).
- For general information about PGP, please visit the PGP Web Site (http://www.pgp.com).

Available Documentation

PGP Desktop documentation is located in the Documentation folder on the disk image from which PGP Desktop is installed. All documents are saved as Adobe Acrobat Portable Document Format (PDF) files. You can view and print these files with Adobe Acrobat Reader, available at the Adobe Web site (http://www.adobe.com).

This release also includes online help in Apple Help format.

Copyright and Trademarks