PGP(R) Desktop Version 10.0 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 Corporation strongly recommends you read this entire document.

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

Product: PGP Desktop for Mac OS X
Version: 10.0.3

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

Note: To view the most recent version of this document, please go to the PGP Support Portal and view the Knowledge Base article PGP User Guides, Administrator Guides, Quick Start Guides, and Release Notes.

What's Included in This File

- About PGP Desktop
- Changes in this release
- System Requirements
- Installation Instructions
- Licensing
- Additional Information
- Getting Assistance
- Copyright and Trademarks

About PGP Desktop for Mac OS X

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

Changes in This Release

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

Changes between 10.0.3 and 10.0.2

- This release of PGP Desktop includes resolution for minor issues. No new features are included in this release.

Changes between 10.0.2 and 10.0.1

- Resolves an issue with PGP Desktop version 10.0.0/10.0.1 for Mac OS X. Upgrading to that release on a system encrypted with PGP Desktop 9.10/9.12 and then subsequently encrypting an external disk caused the system to hang and become unresponsive and caused further attempts to authenticate the disk to fail.

Changes between 10.0.1 and 10.0.0

- This release of PGP Desktop includes resolution for minor issues. No new features are included in this release.
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 features.

General

- **Additional supported operating systems.** PGP Desktop for Mac OS X can now be installed on systems running Mac OS X 10.6.
- **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.
- **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.

Resolved Issues

For a list of issues that have been resolved in this release, please go to the PGP Support Portal and view Knowledge Base Article 1014.

System Requirements

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

Compatible 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 10.5.x or Mac OS X 10.6.x.
- Apple Mail 2.1.1, 3.4, 4.1
- Microsoft Entourage 2008
  - Entourage is compatible for POP/IMAP only. "Exchange Mode" is supported when using the Entourage Scripts included with PGP Desktop. Automatic proxying is not supported with the scripts. For more information on using the scripts, see "Integrating with Entourage 2008" in the PGP Desktop for Mac OS X User's Guide.

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.

Anti-Virus Client Software Compatibility for Macintosh
- Norton Antivirus 11 and Norton Internet Security 3.0: To use PGP Desktop with email and instant messaging, you must disable the Vulnerability Protection option in Norton. To do this, select Auto Protection and then disable the option for Vulnerability Protection. [18130]
- ClamXav: ClamXav is not compatible with PGP WDE on Mac OS X systems. [25682]

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.
4. If prompted to do so, restart your system.

For additional information, including upgrade instructions, see the PGP Desktop for Mac OS X User's Guide.

Note: If you are upgrading your computer to a new major release of Mac OS X (such as from 10.5.x to 10.6.x) and want to use this version of PGP Desktop, be sure to uninstall any previous versions of PGP Desktop before upgrading to the new version of Mac OS X 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.

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.

Additional Information

General

- **Installation**: 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]

- **Upgrading the Mac OS X software**: If you are upgrading your computer to a new major release of Mac OS X (such as from 10.5.x to 10.6.x), be sure to uninstall any previous versions of PGP Desktop before upgrading to the new version of Mac OS X. 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 decrypt your disk before you can uninstall PGP Desktop. Once you have upgraded your version of Mac OS X, you can then reinstall PGP Desktop.

- **Upgrading to PGP Desktop ver 10.0**: When upgrading from a previous version of PGP Desktop (such as version 9.10), after rebooting the Mac OS X system the system may appear to stop with a message "updating boot cache." If this issue occurs, restart the system with hard reboot. The system will boot correctly then. [23955]

- **Enabling shortcut functions from the Finder**: In Mac OS X 10.6, Apple changed the way shortcuts are available from the Finder. In order to enable shortcuts to encrypt or sign files, or mount disks, you must first enable the keyboard shortcuts in the Services preferences. To do this, open System Preferences and open the Keyboard option. Select the Keyboard Shortcuts panel and verify the PGP shortcuts are there. Then, to perform any encrypt or sign functions, select the file, choose Finder > Services, and select the appropriate option. [18872]

- **Using RAID volumes**: There is a known issue with RAID drives and Mac OS X systems (Apple confirms this issue). When PGP Desktop is installed on a system with a RAID volume, you will not be able to properly shut down the system. Note that if you unmount the volume prior to shutting down the system, the shutdown will complete properly. [25694]

PGP Messaging

- **Adding new Exchange email accounts**: When you add a Microsoft Exchange account in Mail.app, Mail.app automatically selects its server type and uses Exchange Web Service with Port 80 for that email account. As a result, PGP Desktop cannot proxy email through the account. To work around this issue, when you add a new Microsoft Exchange account in Mail.app, hold down the Option key after you click Continue when setting up the email account. You can then select IMAP as the Account type. You will not encounter this issue if you have upgraded from Mac OS X 10.5 to Mac OS X 10.6 and you already have an IMAP account that you want to keep, or if you are using Thunderbird for your email client on Mac OS X.

- **Thunderbird Email Sent to BlackBerry Users**: If your Thunderbird email client is set to send email in HTML-only format, and the message is encrypted by either PGP Universal Server or PGP Desktop before it arrives at the BES gateway, the recipient will be unable to view the email message on his or her BlackBerry. To work around this issue, configure your Thunderbird email client so that it does not send HTML-only messages. [16273]

- **Adding comments to secured messages**: 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]

- **Automatic mode**: 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]

- **AOL Mail 10.3.7**: AOL Mail 10.3.7 is compatible 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]

- **Instant Messaging**: Encrypted file transfers fail on Intel Macintosh systems when the intended recipient is using a .Mac account. This applies only for file transfers sent to a .Mac recipient and only if both sender and recipient are using an Intel-based Macintosh. [13190]

**PGP Shred**

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

**PGP Viewer**

- **ASCII-armored text**: PGP Viewer does not support pasting in ASCII-armored text. To decrypt an email containing ASCII-armored text, drag 'n drop the entire email message into PGP Viewer. [23202]

- **Displaying Decrypted Messages**: If you drag an item to PGP Viewer and the message does not appear, restart PGP Viewer and drag the item again. [22215]

- **Cancelling the passphrase prompt**: If you drag an item to PGP Viewer and then click Cancel when prompted to enter your passphrase, you will need to restart PGP Viewer again. This is required so that you can then enter your passphrase in order to decrypt messages. [25390]

- **Using PGP Viewer with Mozilla Thunderbird v3**: If you are using Thunderbird version 3, be sure that you have created a folder named "Inbox" in your Thunderbird Local Folders collection. The Inbox is not necessarily created automatically for new installations of Thunderbird. [25604]

- **Viewing attachments with PGP Viewer**: Dragging and dropping signed-only messages with attachments directly from Mail.app's IMAP folder is not supported in this release. To view messages with attachments, drag and drop the message to your desktop first before dragging and dropping into PGP Viewer. You can also save the message as an .eml file and drag and drop that file into PGP Viewer. [22806]

**PGP Virtual Disk**

- **Unmounting disks on Sleep**: The option to prevent sleep if PGP Virtual Disks cannot be unmounted is not working in this release. The system will sleep even if disks cannot be unmounted. [24818]

- **Compacting PGP Virtual Disks**: Dynamically sized PGP Virtual Disks created using PGP Desktop for Windows cannot be compacted using PGP Desktop for Mac OS X on Mac OS X 10.6 systems. [25293]

**PGP Whole Disk Encryption**

- **Upgrading to PGP Desktop 10.0.2 with Apple Boot Camp installed**: Apple Boot Camp users running Mac OS X who upgrade from PGP Desktop 10.0.0/10.0.1 to PGP Desktop 10.0.2, may encounter an issue when attempting to boot to the Windows partition. After reboot and successful authentication at the PGP BootGuard screen, Windows might not load and instead, a black screen with a blinking cursor
appears. No data loss has been encountered with this issue. For information on a workaround, see PGP Support KB article 1989. [26871]

- **Pausing encryption and decryption processes**: Do not reboot, or shut down your Mac OS X system while PGP Desktop is encrypting or decrypting your disk. If you do so and are unable to reboot your system, you will need to start the system using target disk mode. [25451]

- **Erasing/reformatting encrypted disks**: Do not erase or reformat a PGP WDE-encrypted disk without decrypting the disk first. [24999]

- **Apple Boot Camp**: PGP Corporation recommends that you read the PGP KB Article 1697 prior to installing PGP Desktop on a system with Apple Boot Camp. [23997]

- **Apple Boot Camp**: If you have booted into the Windows partition on a system on which Boot Camp is installed, and you want to boot into the Mac OS X partition, you will need to hold down the Option key during the reboot process. Then choose the OS X partition from the Startup Manager. This is a known Apple issue (see Apple support article HT1310). [23299]

- **Using Apple French keyboards with Boot Camp**: When you boot into the Windows partition on a system running Apple Boot Camp, the # and @ keys on the Apple French AZERTY keyboard cannot be used. These keys can be used when you enter the passphrase when booting into the Mac OS X partition. [24752]

- **Backwards compatibility**: Disks encrypted with this version of PGP WDE can only be accessed with this same version of PGP WDE for Mac OS X or versions 9.9.0 and up of PGP WDE for Windows. [19875]

- **Backwards compatibility**: Disks that use the MBR partition scheme and are encrypted with this version of PGP WDE cannot be accessed using previous versions of PGP WDE. [19875]

- **Fast User Switching**: This release of PGP Desktop is not compatible with fast user switching on Mac OS X. [23655]

- **Kernel panic**: In rare circumstances, when you reboot your system you may experience a kernel panic. If you receive a kernel panic, simply reboot the system again using the Power on/off button. [21509]

- **External Devices**: When plugging in a Samsung Omnia I900 phone to be used as an external storage device, you will receive a kernel panic and the device will not be mounted. [24353]

- **Universal File System**: Disks formatted as UFS are not supported. [23595]

- **Entering Japanese characters**: Although the PGP Desktop interface allows it, do not use Japanese characters when creating PGP WDE passphrases as they will not work for authentication at PGP BootGuard. [18139]

- **Encrypting boot disks with both Mac OS X 10.5 and 10.6 installed**: Systems booted into Mac OS X 10.5 cannot encrypt a Mac OS X 10.6 disk. To work around this issue, you can boot from Mac OS X 10.6 first and then encrypt the Mac OS X 10.5 disk. [20807]

- **Safe Boot**: The Mac OS X Safe Boot feature does not work on a boot disk that has been whole disk encrypted; if you hold down the Shift key to enter Safe Boot, after authenticating at the PGP BootGuard screen, the system will fail to boot. [17770]

- **PGP WDE and Recovery Applications**: Be sure you decrypt your disk before you run any disk recovery applications (such as DiskWarrior from Alsoft). [18157]

- **Previously Encrypted Partitions or Disks**: If you used the PGP Whole Disk Encryption feature of previous versions of PGP Desktop for Mac OS X, you must decrypt those non-boot partitions or disks (including USB flash drives) before installing version 10.0 or you will no longer be able to access the data on them. You can re-encrypt the partitions/disks with PGP Desktop 10.0 for Mac OS X once it is installed. [NBN]

- **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.

- **Supported passphrase characters**: [12947, 11551, 18871] The following characters are supported:

```plaintext
abcdefghijklmnopqrstuvwxyz
ABCDEFGHIJKLMNOPQRSTUVWXYZ
0123456789
```


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

Note that in this release, the ç character cannot be entered at boot time at PGP BootGuard.

- **Using a Mac Mini with Apple Keyboards.** The Mac Mini does not have boot time support for the new thin aluminum Apple keyboards. The PGP WDE passphrases cannot be entered at boot time using these keyboards with the Mac Mini.

- **Partition Formats:** APM-formatted disks are not available for encryption. GPT and MBR disks are supported. [11025]

- **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. [11936]

- **Encrypting Non-Journaled File Systems:** PGP WDE for Mac OS X does not support "non-journaled" file systems. You will receive an error when trying to encrypt a non-journaled file system. *Important note:* Previous versions of PGP WDE for Mac OS X incorrectly allowed the encryption of non-journaled file systems. These disks should be decrypted, backed up, and converted to the Mac OS X default of journaled (non-case sensitive). [19866]

- **Adding keys to removable drives.** To add a public key to a removable drive, be sure to add that key to your keyring first. You cannot add public keys to a removable drive if that key is not on your keyring. [20396]

- **Operating system updates during encryption:** While your disk is encrypting, do not accept any operating system updates if they are offered. If the update occurs automatically, do not restart your computer until the encryption process has completed. [25451, 25612]

### Getting Assistance

#### 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](#).

- To access the PGP Support Knowledge Base or request PGP Technical Support, please visit [PGP Support Portal Web Site](#). *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](#). 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](#).

**Contacting Other Departments**

- For any other contacts at PGP Corporation, please visit [PGP Contacts Page](#).

- For general information about PGP Corporation, please visit the [PGP Web Site](#).

#### Available Documentation

Prior to installation, complete Product Documentation is available through the [PGP Corporation Support Portal](#).

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](#).
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://www.pgp.com/support/knowledge_base).

**Copyright and Trademarks**

Copyright © 1991-2010 PGP Corporation. All Rights Reserved. "PGP", "Pretty Good Privacy", and the PGP logo are registered trademarks and PGP Universal is a trademark of PGP Corporation in the U.S. and other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.