PGP(R) Desktop Version 10.0 for Windows Release Notes

Thank you for using this PGP Corporation product. These Release Notes contain important information regarding this release of PGP Desktop for Windows. 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 Windows

Version: 10.0.0

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 Windows

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.

What's New in PGP Desktop for Windows Version 10.0

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

General

- Additional supported operating systems. PGP Desktop for Windows can now be installed on Windows 7.
- New localized versions. PGP Desktop has been localized and can now be installed in French (France) and Spanish (Latin America).
- Support for new smart cards. For both pre- and post-boot in PGP Desktop for Windows:
  - Axalto Cyberflex Access 32K V2 smart card
  - Giesecke and Devrient Sm@rtCafe Expert 3.2 personal identity verification cards
  - Oberthur ID-One Cosmo V5.2D personal identity verification cards
  - SafeNet iKey 2032 USB token
  - T-Systems Telesec NetKey 3.0 and TCOS 3.0 IRI cards
- Redesigned interface. The main user application window in PGP Desktop for Windows has been redesigned.
- 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.

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.

- **Keyring location.** In PGP Desktop for Windows, you can use environment variables to specify the location of your keyrings.

- **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.

- **Lotus Notes.** PGP Desktop now provides the ability to encrypt mail messages using Lotus Notes native encryption if PGP Desktop is configured to do so and the recipient is an internal Notes user.

- **Lotus Notes.** PGP Desktop now provides the ability to encrypt Lotus Notes RTF-formatted email messages using PGP/MIME, S/MIME, or PGP Partitioned formats.

- **Lotus Notes.** PGP annotations in messages now honor the regional settings for date and time stamp.

- **Microsoft Outlook buttons added.** Buttons enable you to manually add encryption and/or your digital signature to your Outlook emails. This new feature provides compliance with digital signature laws that require showing intent to sign.

- **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 Portable**

- Previously available as a standalone option, PGP Portable is now included in PGP Desktop. PGP Portable Disks can be created on Windows systems. This functionality requires a separate license.

**PGP Whole Disk Encryption**

- **Additional smart card compatibility.** New cards added for pre-boot authentication in PGP Whole Disk Encryption for Windows include Axalto Cyberflex Access 32K V2, Marx CrypToken USB token, SafeNet iKey 2032 USB token, and T-Systems T-Telesec NetKey smart card.

- **Personal Identity Verification (PIV) card support.** Support has been added in PGP Whole Disk Encryption for Windows for users with Giesecke and Devrient Sm@rtCafe Expert 3.2 and Oberthur ID-One Cosmo V5.2D personal identity verification cards.

- **Additional Keyboard Compatibility (Windows).** A total of 50 international language keyboards can now be used to log in at PGP BootGuard. For a list of all compatible keyboards, see the PGP Desktop for Windows User's Guide or online help.

- **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.

- **Local self recovery.** PGP Desktop for Windows now provides a way for you to access your encrypted drive from the PGP BootGuard screen if you have forgotten your passphrase. When configured, you won't have to contact your administrator for assistance.

- **Multi-user enhancements.** In an environment where multiple users may access a group of computers, the PGP Universal Server administrator can define a PGP WDE Admin password. When you enter this password at the PGP BootGuard screen on a PGP Desktop for Windows system, you are prompted to enter your Windows passphrase and the disk is decrypted.

- **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.

- **Additional token support for PGP BootGuard.** The Marx CrypToken USB token can now be used at the PGP BootGuard for PGP Desktop for Windows.

- **Extended ASCII character support.** Extended ASCII characters can now be used when creating PGP WDE users.

- **Kanji characters.** Kanji characters are now displayed correctly in the PGP BootGuard screen.

- **Windows Server operating systems.** PGP WDE can now be installed on Windows Server operating systems (Windows
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


**Note:** The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

PGP Whole Disk Encryption (WDE) is supported on all client versions above as well as the following Windows Server versions:

- Windows Server 2003 SP 2 (32- and 64-bit editions)
- Windows Server 2008 SP 1 and 2 (32- and 64-bit editions)
- Windows Server 2008 R2 (32- and 64-bit editions)

For additional system requirements and best practices information on using PGP WDE on Windows Server systems, see PGP KB article 1737.

- 512 MB of RAM
- 64 MB hard disk space

Compatible Email Client Software

PGP Desktop for Windows will, in many cases, work with Internet-standards-based email clients other than those listed here. PGP Corporation, however, does not support the use of other clients.

PGP Desktop for Windows has been tested with the following email clients:

- Microsoft Outlook 2007 SP1 (Outlook 12)
- Microsoft Outlook 2003 SP3
- Microsoft Outlook XP SP3
- Microsoft Windows Mail 6.0.600.16386
- Microsoft Outlook Express 6 SP1
- Windows Live Mail version 2009
- Mozilla Thunderbird 2.0
- Lotus Notes 6.5.6, 7.0.3, 8.02, 8.5
- Novell GroupWise 6.5.1

PGP Corporation Compatibility Status with Microsoft Exchange Server 2007

PGP Corporation is pleased to announce compatibility with Microsoft's new Exchange Server 2007. PGP Desktop 9.6 introduced support for Microsoft Exchange Server 2007 and Microsoft Office 2007. When used with Internet-standard PGP/MIME (RFC 3156) messages, full message fidelity is preserved for all secured messages.

With Exchange Server 2007, Microsoft has introduced a change in functionality that converts all messages to its internal MAPI format immediately upon processing, unlike previous versions of Exchange that supported the MIME standard for email. Exchange Server 2007, when both sending and receiving via non-MAPI clients, destroys MIME structures in email. However, PGP/MIME-encoded messages are fully compatible with this Microsoft transition even when MAPI is not in use. All messages sent between PGP Corporation's MAPI clients are also fully compatible.
Please note that messages encoded using the legacy "PGP Partitioned" format may not always display HTML message content properly, and foreign character sets in such messages may not reproduce correctly when processed through Exchange Server 2007. If such messages are processed from non-MAPI clients, the server may delete some encrypted HTML body parts and remove non-ASCII character set information, thus resulting in messages that do not preserve full fidelity. If your organization currently uses the legacy PGP Partitioned encoding with non-MAPI clients, PGP Corporation recommends not upgrading to Exchange Server 2007 at this time. PGP Corporation is working with Microsoft to seek additional solutions for compatibility between Exchange Server and the MIME standard.

PGP Corporation will update the Support Knowledge Base Article #713 as more information becomes available.

Instant Messaging Client Compatibility
PGP Desktop is compatible with the following instant messaging clients when encrypting AIM instant messages, file transfers, and direct connections:
- AOL AIM 6.5.5
  - To encrypt instant messages with AIM 6.5, you must change the default port that AIM uses from 493 to 5190.
  - 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 version 10.0 is released.
- Trillian 3.1 (Basic and Pro)

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

Anti-Virus Software Compatibility for Windows
In all anti-virus programs, enabling real-time scanning detects any viruses as the email or attachments are opened. Therefore, although it is recommended to disable email scanning for some of the anti-virus products listed below, your email is still being scanned and you are still being protected by your anti-virus product from viruses spread via email.

BitDefender Internet Security
- When using SMTP, POP, or IMAP, disable the Real-Time Protection feature or uninstall BitDefender. [13687]

Computer Associates eTrust EZ-Antivirus 7.x
- Selective scanning is not compatible with PGP Desktop.

- This product is incompatible with PGP Desktop and should not be installed on the same system as PGP Desktop. [12023]

McAfee Internet Security Suite 2006, McAfee Internet Security Suite 2005, McAfee Internet Security 8.0, McAfee VirusScan 8.x through 10.x
- If email scanning is enabled, the email will not be processed by PGP Desktop. Disable email scanning in the McAfee product and enable real-time scanning.
- No additional special configuration requirements for MAPI email.
- When using McAfee VirusScan Enterprise 8.0i, disable Prevent mass mailing worms from sending mail in the Access Protection Properties dialog box of the VirusScan console. If this option is enabled, SMTP email will be blocked. To disable this option, right-click the McAfee icon in the System Tray and choose VirusScan Console. Double-click Access Protection. In the Access Protection dialog box, under Ports to block, deselect the box to Prevent mass mailing worms from sending mail (this option is enabled by default).
- When using McAfee Security Center 9.3, email will not be processed by PGP Desktop. Stop and disable the McAfee Proxy Service. This disables the McAfee Personal Information Protection and Parental Control but allows the PGP email proxy to process your email.

Panda Platinum 2005 Internet Security 9.x
- No special configuration required.

Sophos Anti-Virus
- No special configuration required.

- No special configuration required for MAPI email.
- When using POP email, enable Auto-Protect and disable the Anti-Spam and Email Scanning options. Auto-Protect, which is enabled by default, provides protection against viruses in email messages when the message is opened.
- Disable SSL/TLS in Server Settings in PGP Desktop or PGP Universal Satellite. (In PGP Desktop, select the PGP Messaging Control Box and then choose Messaging > Edit Server Settings. For SSL/TLS, select Do Not Attempt. In PGP Universal Satellite, on the Policies tab, select Ignore SSL/TLS.) These versions of Norton AntiVirus prevent all mail clients from using SSL/TLS, regardless of the use of PGP software.


- Disable email scanning.
- For Norton Internet Security users, disable Norton Privacy Control and Spam Alert.
- Disable SSL/TLS in Server Settings in PGP Desktop and PGP Universal Satellite. (In PGP Desktop, select the PGP Messaging Control Box and then choose Messaging > Edit Server Settings. For SSL/TLS, select Do Not Attempt. In PGP Universal Satellite, on the Policies tab, select Ignore SSL/TLS.) These versions of Norton AntiVirus prevent all mail clients from using SSL/TLS, regardless of the use of PGP software.

Trend Micro Antivirus 12.x, Trend Micro PC-cillin Internet Security 2005

- No special configuration required.

Personal Firewall Compatibility

PGP Desktop for Windows has been tested with the following personal firewall software:

- **Zone Alarm:** The Zone Alarm firewall, by default, restricts access to localhost. Because PGP Desktop redirects connections to localhost, this stops PGP Desktop from working correctly. To fix this, add localhost (127.0.0.1) as a trusted IP address in Zone Alarm (on the Firewall/Zones screen). Email proxying by PGP Desktop will work normally once this is accomplished. [6446]

- **CyberArmor Personal Firewall:** PGP Desktop 10.0 is not compatible with InfoExpress CyberArmor Personal Firewall versions 2.6.050802 or 3.2.050802 or prior. Before you install PGP Desktop, you must upgrade these versions: contact your helpline or the vendor (InfoExpress at support@infoexpress.com) for more information. [7010]

- **Webroot Desktop Firewall:** PGP Desktop is compatible with Webroot Desktop Firewall Version 5.8 only. Earlier versions of Webroot software are not compatible with PGP Desktop.

Citrix and Terminal Services Compatibility

PGP Desktop for Windows has been tested with the following terminal services software:

- Citrix Presentation Server 4.0
- Citrix Metaframe XP
- Windows 2003 Terminal Services

The following features of PGP Desktop for Windows are available in these environments, as specified:

- Email encryption is fully supported.
- PGP Zip functionality is fully supported.
- PGP Shred functionality is fully supported.
- PGP NetShare is fully supported.
- PGP Virtual Disks cannot be mounted at a drive letter over Citrix/TS, but can be mounted at directory mount points on NTFS volumes.
- PGP Whole Disk Encryption is not supported.
- Smart cards are not supported.

For information on how to install PGP Desktop on a Citrix server, see PGP Support KB Article 832.
Compatible Smart Cards and Tokens for PGP WDE BootGuard Authentication

This section describes the system requirements (compatible smart cards/tokens and readers).

Compatible Smart Card Readers for PGP WDE Authentication

The following smart card readers are compatible when communicating to a smart card at pre-boot time. These readers can be used with any compatible removable smart card (it is not necessary to use the same brand of smart card and reader).

Generic smart card readers

Most CCID smart card readers are compatible. The following readers have been tested by PGP Corporation:

- OMNIKEY CardMan 3121 USB for desktop systems (076b:3021)
- OMNIKEY CardMan 6121 USB for mobile systems (076b:6622)
- ActivIdentity USB 2.0 reader (09c3:0008)
- SCM Microsystem Smart Card Reader model SCR3311

CyberJack smart card readers

- Reiner SCT CyberJack pinpad (0c4b:0100).

ASE smart card readers

- Athena ASEDrive IIIe USB reader (0dc3:0802)

Embedded smart card readers

- Dell D430 embedded reader
- Dell D630 embedded reader
- Dell D830 embedded reader

Compatible Smart Cards or Tokens for PGP WDE Authentication

PGP Whole Disk Encryption is compatible with the following smart cards for pre-boot authentication:

- ActivIdentity ActivClientCAC cards, 2005 model
- Aladdin eToken PRO 64K, 2048 bit RSA capable
- Aladdin eToken PRO USB Key 32K, 2048 bit RSA capable
- Aladdin eToken PRO without 2048 bit capability (older smart cards)
- Aladdin eToken PRO Java 72K
- Aladdin eToken NG-OTP 32K

**Note:** Other Aladdin eTokens, such as tokens with flash, should work provided they are APDU compatible with the compatible tokens. OEM versions of Aladdin eTokens, such as those issued by VeriSign, should work provided they are APDU compatible with the compatible tokens.

- Athena ASEKey Crypto USB Token for Microsoft ILM
- Athena ASECard Crypto Smart Card for Microsoft ILM

**Note:** The Athena tokens are compatible only for credential storage.

- Axalto Cyberflex Access 32K V2
- Charismathics Cryptoidentity plug 'n' crypt Smart Card only stick
- EMC RSA SecurlD SID800 Token (v1 and 2)

**Note:** This token is compatible only for key storage. SecurlD is not compatible.

- EMC RSA Smart Card 5200
- Marx CrypToken USB token
- Rainbow iKey 3000
- S-Trust StarCOS smart card

**Note:** S-Trust SECCOS cards are not compatible.

- SafeNet iKey 2032 USB token
- T-Systems Telesec NetKey 3.0 smart card
- T-Systems TCOS 3.0 IEI smart card

**Personal Identity Verification (PIV) cards**
- Oberthur ID-One Cosmo V5.2D personal identity verification cards using ActivClient version 6.1 client software.
- Giesecke and Devrient Sm@rtCafe Expert 3.2 personal identity verification cards using ActivClient version 6.1 client software.

**Installation Instructions**

To install PGP Desktop on your Windows system

1. Locate the PGP Desktop installer application and double-click it.
2. Follow the on-screen instructions.
3. If prompted to do so, restart your system.

For additional information, including upgrade instructions, see the *PGP Desktop for Windows User's Guide*.

**Licensing**

PGP Desktop uses a licensing system to determine what features will be active. Depending on the license you have, some or all PGP Desktop features will be active. Consult your PGP administrator if you have questions about what features are available with your license.

Use the Setup Assistant to enter your PGP Desktop license 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.

The PGP Desktop features that will be active on your system depend on the type of license you have:

- PGP Desktop Professional 10.0 includes PGP Desktop Email and PGP Whole Disk Encryption.
- PGP Desktop Storage 10.0 includes PGP Whole Disk Encryption and PGP NetShare.
- PGP Desktop Enterprise 10.0 includes PGP Desktop Email, PGP Whole Disk Encryption and PGP NetShare.

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**

- **Japanese characters and Current Window/Clipboard processing:** The Current Window/Clipboard encryption and decryption features do not support ISO-2022-JP. [7489]

- **Compatibility with Oracle applications:** If you encounter problems with Oracle application using Oracle JInitiator you may be able to use the latest version of the Sun Java Runtime Environment to run your Oracle applications. [15543]

- **Compatibility with Google Desktop:** PGP Desktop is compatible with Google Desktop installed if you disable the option in Google Desktop to index mail. For more information, see PGP Support KB Article 958. [16286, 18499]

- **Windows XP Password Changes:** PGP Desktop relies on the Microsoft Data Protection API (DPAPI) to secure user enrollment data. Windows XP SP2 users may lose access to this enrollment information due to a known issue in SP2. Users affected by this Microsoft issue should upgrade to Windows XP SP3 and re-enroll. For more information, see Microsoft KB article 890951. [20852]
- **Windows Password Changes**: To ensure proper operation for a variety of PGP functions, including SSO and SKM keys, Windows passwords should never be changed using the "net user" command in Windows command prompt. [22825]

**PGP Keys**
- **RSA SecurID SID800**: The RSA SecurID SID800 only supports SHA-1. When generating a key on the RSA SecurID SID800, modify the key properties by clicking the Advanced button, and under Hashes select only SHA-1. If a key has already been generated, get the Key Properties, edit the set of supported Hashes, and select only SHA-1. [14861]
- **GemPlus Smart Cards**: GemPlus smart cards only support SHA-1. When generating a key on GemPlus smart cards, modify the key properties by clicking the Advanced button, and under Hashes select only SHA-1. If a key has already been generated, get the Key Properties, edit the set of supported Hashes, and select only SHA-1. [15681, 16603]
- **Athena Tokens**: When creating 2048-bit PGP keys to be used with Athena tokens, you cannot copy the PGP key to the token. You can, however, create the 2048-bit key directly on the token. [24861]

**PGP Messaging**
- **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]
- **MAPI and Message policies**: Policies based on the condition "Message is <x>" are not currently supported with MAPI. [9448]
- **Legacy Messages Encrypted to Non-Roman Character Sets**: The Current Window and Clipboard decryption functionality has been enhanced to detect a UTF-8 character set conversion failure. In that event, the content will be decrypted to the system's local code page instead. Note that legacy messages from PGP Desktop version 8 and below did not support proper character set identification, and thus the local code page may not be correct either. If you encounter such legacy messages decrypting to an incorrect character set from the clipboard, you may need to use third-party tools to convert the resulting character set to the correct one. [11889, 19679]
- **PGP Desktop 8.x and international characters**: Note that PGP Desktop 8.x did not support international characters in message body content. To use languages other than English in your message content, please ensure your correspondents are using at least PGP 9.0.0 or above. In some cases, you may be able to cause PGP Desktop 8.x or below to create a proper message by forcing the use of the UTF-8 character set. [11257, 11888]
- **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 Messages:**
  - **S/MIME-signed email messages**: PGP Messaging 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. If the message is not processed by PGP, it may still be processed by the mail client application. [9489, 9491]
  - **S/MIME and MAPI**: S/MIME users who intend to use S/MIME with MAPI should ensure that they have an X.509 certificate attached to their keys; otherwise, it is possible that these messages when saved in the Sent Items folder cannot be processed by PGP Desktop. [9858]
- **Microsoft Outlook**:
  - **Microsoft Outlook**: Messages that have been processed by PGP Desktop cannot be modified from the Microsoft Outlook Outbox. [20269]
  - **Microsoft Outlook and ESET Antivirus**: When using Microsoft Outlook on a system on which ESET Antivirus is installed, you may encounter a delay when opening Outlook. [22192]
  - **MAPI/Exchange users and inline objects**: If you are a MAPI/Exchange user, and you are sending messages containing embedded content in a proprietary format (inline objects), PGP Desktop will secure the complete message. This will cause inline objects to be readable/viewable only by recipients in a MAPI/Exchange environment. [5530]
  - **Outlook MAPI**: If you are using Outlook in a MAPI environment, use the PGP Log to confirm the validity of PGP signature annotations in message bodies unless the message was decrypted by your PGP Universal Server, which will do this for you. [6819, 7304]
  - **Outlook Connector for Notes**: The Outlook Connector for Notes that allows an Outlook client to emulate a Lotus Notes client is not supported. [7567]
  - **MAPI Email on Windows Vista or Windows 7**: After upgrading your operating system to Windows Vista or Windows 7 without reinstalling PGP Desktop, MAPI messages are sent in the clear and existing encrypted
Lotus Notes:
- Lotus Notes and disabled users: When a user has been disabled, email sent by the user is initially blocked. To work around this issue, send the email again and email is sent in the clear, as expected. [12234]
- Lotus Notes and disabled users: When a user has been disabled, and then re-enabled, the user must restart Lotus Notes to send encrypted email. [12236]
- Japanese Notes IDs: Due to the way that Lotus Notes creates SMTP addresses from the user ID, accounts with Japanese user IDs may display incorrectly or be truncated in some dialog boxes in PGP Desktop. This does not interfere with the operation of PGP Desktop or delivery of the user's email. [12913]

POP: Verizon POP accounts return an incorrect response when connecting to the POPS/SMTPS ports if you have not purchased Verizon's Silver/Gold services. In this situation you must set the ports manually to 110/25 in the Policy user interface for the account, respectively, to avoid connecting to the normal ports. [NBN]

SMTP: Activate SMTP AUTH in your email client if it is not currently active. [NBN]

PGP Messaging license change: If you change the license for PGP Desktop from a license that does not support the PGP Messaging feature (PGP Whole Disk Encryption for Enterprises, for example) to a license that does support PGP Messaging, you must stop and restart the PGP Services once the new license is accepted. This ensures that PGP Desktop can properly protect your messages. To stop the PGP Services, click the PGP Tray icon and choose Exit PGP Services. To restart the services, choose Start > Programs > PGP > PGP Desktop. [8107, 12200]

Instant Messaging:
- Multiple AIM connections: If your system has multiple ways to access the AIM service (LAN and wireless network accesses, for example), and you lose your connection to AIM but the AIM server doesn't see the connection as lost, and your IM client accesses the AIM service again using the other network access, the AIM server will see you as signed in to the same AIM account from two locations. This will cause PGP Desktop to disable the AIM proxy because of the error condition and the AIM server will display a message telling you that your account is logged in from two different locations. To solve this problem, simply reply to the message from the AIM server with a 1. The old AIM session will be discontinued and PGP Desktop will encrypt the remaining AIM session. [NBN]
- Compatibility with AIM 6.5: PGP Desktop does not secure instant messages when the English (released) version of AIM 6.5 is run on 64-bit Windows XP or Windows Vista operating systems, or any German or Japanese operating systems. [16393]

PGP NetShare

Compatibility with SmartFTP: SmartFTP from SmartSoft Ltd. cannot be used to download files into a folder protected by PGP NetShare. Use the built-in Windows FTP client instead. [17942]

Windows Links. PGP NetShare does not follow Windows links ( .lnk files), including such links as "My Network Places". Adding a folder to PGP NetShare that is actually a link will protect the link file and not the desired location. [13339]

Using PGP NetShare with Windows Vista: On Windows Vista systems, adding new folders to a PGP NetShare Protected Folder using the drag-and-drop method is not supported in this release. This issue does not occur with Windows Vista SP1. [12506]

Using PGP NetShare with Windows Vista 64-bit: The PGP NetShare properties tab is not available on 64-bit versions Windows Vista. [17622]

Software incompatibility with the PGP NetShare feature: The following programs are incompatible with PGP NetShare:
- Securewave Sanctuary Device Control 3.0.3. To use PGP Desktop with Sanctuary Device Control, it is necessary to upgrade the Securewave software to version 4.1 or later. [12850]
- CommVault System Data Migrator. To use PGP Desktop with Data Migrator, it is necessary to unregister the PGP NetShare DLL (at the command prompt, type regsvr32 /u PGPfsshl.dll). [12016]

Whitelisted Applications: Application whitelists are applications that your PGP Universal Server administrator has defined so that all files created by the application are forced to be encrypted. Files created by these whitelisted applications are locked (requiring authentication to access) after you log off or shut down your system. [17491]

Using PGP NetShare and SharePoint with Windows Vista 64-bit: The PGP NetShare shortcut menu is not available on 64-bit versions Windows Vista systems when viewing a folder within SharePoint. To access the shortcut menu, view the folder using Windows Explorer. [19421]

PGP Portable

Accessing Data on Windows 2000 systems. When mounting a PGP Desktop Disk on a Windows 2000 system, the contents are available only through a Web Browser, and the data is read-only. [21446]
PGP Portable and Microsoft Office 2003. PGP Portable is compatible with Microsoft Office 2003 when Office Service Pack 3 is installed. [21854]

PGP Portable and Microsoft Office 2003. Microsoft Office 2003 documents cannot currently be added to a PGP Portable Disk when the disk is being created on a Windows Vista system. [21697]

Accessing Data on Windows XP systems. Mounting a PGP Portable Disk on Windows XP will fail with a "Not Connected" error if another process is already using port 80. [21869]

Creating new Word documents on a PGP Portable Disk. When creating a new Microsoft Word file on a mounted PGP Desktop Disk on Windows XP (right-clicking the mounted PGP Desktop Disk and selecting New > File > Microsoft Word Document), the resulting zero-byte Word file is read-only. To edit the file, save it as a new name (on the PGP Desktop Disk). [21680]

Adding Data on Windows XP Systems. In order to add data to a PGP Portable Disk on a Windows XP system, set the local security policy for Allowed to format and eject removable media to Administrator and Interactive Users. [21975]

Disk Space Requirements. When copying large files to a PGP Portable disk, ensure that you have sufficient space available on your local drive. The amount of space needed is equivalent to the amount of data being copied to the PGP Portable disk. [21595]

PGP Portable Passphrases: Japanese characters are not currently supported for passphrases when creating a new PGP Portable Disk or changing the passphrase on an existing disk. [21717]

PGP Portable Disk File Names. When creating a PGP Portable Disk, the combination of file name and folder name(s) cannot exceed 240 characters. [21816]

PGP Portable Disk size: In this release, you can create NTFS-formatted PGP Portable disks up to 4 GB only. [25414]

PGP Shred

Shredding (wiping small files): Shredding small files (under 1 K) on some NTFS-formatted disks can leave remnants of the file behind due to an NTFS optimization that stores file data in internal data structures for very small files. These structures are not considered free space even after deleting a file, and thus they also will not be shredded using PGP Desktop's Shred Free Space feature. In addition, NTFS supports Journaling, which can save shredded file data in an internal operating system cache. For the highest security shredding on NTFS disks, we recommend starting your system from an OS on a different partition and using PGP Desktop's option in the Shred Free Space feature to overwrite these NTFS data structures (the Shred NTFS internal data structures checkbox). This does not affect FAT32 or other supported file systems. [NBN]

Shredding sparse files: Sparse files, commonly used for disk images, database snapshots, log files and in scientific applications, cannot be securely deleted using PGP Shred. [21255]

Automatic shredding: Automatically shred when emptying the Recycle Bin/Trash is not compatible with the Windows built-in CD burning software. [22794]

PGP Viewer

Lotus Notes: 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. [23384]

Viewing Sign-Only Emails with Shift-JIS: Outlook Express or Windows Mail messages signed using Shift-JIS cannot be verified using PGP Viewer. This issue does not occur if the message was encrypted and signed. [22870]

S/MIME Messages: S/MIME-encrypted messages cannot be decrypted by PGP Viewer in this release. [22022]

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]

Copying Email Messages to Inbox: When copying a Microsoft Outlook 2003 email message to your inbox using PGP Viewer, the date/time stamp on the message is changed to the current date/time. [24355]

Viewing MAPI Email: Microsoft Outlook messages opened within PGP Viewer will display Unmatched Address in the From: field. [24703]

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]

PGP Virtual Disk

Using with Personal Certificate-based Keys: In order to mount a PGP Virtual Disk that is secured with a personal certificate-based key, note that you should not enter a passphrase when prompted in the PGP Enter Passphrase dialog box, but instead click Enter. [14762]
Existing NTFS PGP Virtual Disks and Windows Vista: NTFS disks created under Windows XP may not be properly handled by Windows Vista. For best results, create NTFS disks in Windows Vista. A future Microsoft update is expected to resolve this Windows issue. [12644]

PGP Whole Disk Encryption

- **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]
- **PGP WDE Evaluation Licenses.** If you are using PGP WDE with an evaluation license in a managed PGP Universal Server environment, please ensure you obtain a valid license prior to the expiration of your evaluation license. This will prevent the automatic decryption of your disk upon expiration of the evaluation license. [16445]
- **PGP WDE Authentication:** The Activeldentity ActivClientCAC model 2002 smart card is not compatible in this release. To use the ActiveClientCAC card, use model 2005. [16259]
- **Passphrase Recovery:** Token users who use passphrase recovery when authenticating at PGP BootGuard will be prompted to change their passphrase. This prompt can be ignored as your PIN will not be changed even if you enter text in the dialog or click Cancel. [24335]
- **Passphrase Recovery:** Passphrase recovery is only available for encrypted boot disks. [24510]
- **Passphrase Recovery:** If you use the Forgot Passphrase option at the PGP BootGuard screen and enter an incorrect user name, you will need to click Cancel to return to the PGP BootGuard screen and then select Forgot Passphrase again. [24825]
- **PGP WDE and Smart Card Readers:** When using a smart card reader with a built-in PIN pad, the correct PIN may not be accepted the first time it is entered on the pad, and you will be prompted to provide the PIN again. When this message appears, click OK without entering the anything. This will either allow the PIN to be accepted or will transfer control to the PIN pad of the smart card reader, where you can enter the PIN again. [16143]
- **PGP WDE and Smart Card Readers:** Pre-boot authentication using a smart card reader is not currently supported on Panasonic Toughbook and Sony Vaio P-Series Mini systems. [20638]
- **PGP WDE and GemXpresso:** PGP Desktop is not compatible with the GemXpresso family of smart cards. Keys on the GemXpresso smart card can be used for encrypting PGP Virtual Disks and PGP NetShare protected folders, but cannot be used to encrypt a disk or removable disk. [16415]
- **OHCI USB Controllers:** PGP BootGuard does not currently work with OHCI USB controllers. As a result of this, tokens do not work in PGP BootGuard on such systems. [15800]
- **Encrypting drives:** Any drives with a sector size other than 512 bytes are not supported by PGP WDE and cannot be encrypted. [21126]
- **PGP WDE and SSO:** If you encounter problems with synchronizing a Windows password change on a Windows XP system, follow the steps below to correct the issue: [17269]
  1. On your Windows Desktop, right-click My Network Places and select Properties from the shortcut menu.
  2. Select Advanced > Advanced Settings.
  3. Select the Provider Order tab.
  4. Rearrange the order of the providers so PGPpwflt is listed above the Intel card.
  5. Click OK.

You can also modify the .msi installation file. Use the PGP_SET_HWORDER=1 command to place PGPpwflt in the first of the list. For example, run the .msi installation file using the following command:

```command
msiexec /i pgpdesktop.msi PGP_SET_HWORDER=1
```

- **PGP WDE SSO on Novell Networks:** The Single Sign-On feature of PGP WDE does not work on Windows Vista systems running Novell Network Client. Once you have authenticated at the PGP Bootguard screen you will need to enter your password again to start Windows Vista. [16688]
- **PGP WDE SSO on Novell Networks:** When using the Single Sign-On feature of PGP WDE on Windows Vista systems running Novell Network Client, offline users receive a Novell Security Message stating the "tree or server cannot be found." To continue logging in to Windows, click Yes, and the login proceeds normally. [16995]
- **TPM Support:** We are in the process of validating many different TPM implementations. We are interested in your test results on any additional TPM systems. [14666]
- **Token Authentication:** Token authentication in PGP BootGuard requires pressing CTRL+ENTER instead of just Enter. Users may also experience some delay during the authentication of tokens in PGP BootGuard. [14792, 16466]
- **PGP WDE and USB Two-Factor Authentication:** If you have created a passphrase user with a USB flash drive and
encrypted your boot disk, when you reboot you may find that the USB device is not recognized at the PGP BootGuard screen. You can still authenticate at the PGP BootGuard screen using just the passphrase, however. If you want to use two-factor authentication, you will need to decrypt your disk, then create another passphrase user using another USB flash device, and then re-encrypt your boot disk. [16577]

- **External Disks and Two-Factor Authentication**: If you have encrypted an external disk with both a passphrase user and a token user, you must insert the token prior to connecting the external disk. [19013]

- **Aladdin Smartcards**: Aladdin Smartcards do not properly generate 2048-bit keys using Aladdin software version 4.5.52, and such keys cannot be used for PGP WDE pre-boot authentication. PGP Corporation is working with Aladdin to correct this issue. Note that Aladdin tokens do not have this issue. [16699]

- **Athena ASECard Crypto Cards**: The Athena ASECard Crypto Card is not compatible with OmniKey readers for pre-boot authentication. Use a different compatible reader with Athena smart cards for pre-boot authentication.[18283]

- **Upgrading**: The PGP BootGuard screen is not updated immediately after you upgrade to PGP Desktop 10.0. To display the updated PGP BootGuard screen (containing new login and keyboard options), reboot your system a second time. [NBN]

- **Removable drive encryption**: Certain types of removable flash devices cannot be encrypted with the vendor-supplied format. They must be formatted within Windows prior to encrypting. [12362]

- **Removable drive encryption**: If both Automatically Encrypt Boot Disk Upon Installation and Force Encryption of Removable Disk are enabled by policy, you may encounter an error when inserting a USB disk while a fixed disk is being encrypted. To work around this issue, wait until the encryption process has completed on the fixed disk. [12167]

- **PGP WDE and Hibernation**: When resuming from Hibernation, an extra domain password prompt may appear even if Single Sign-on is active. [9935]

- **Using PGP WDE-Protected Removable Disks with PGP Desktop 9.x and 10.0**: Disks encrypted with PGP Desktop 9.0, 9.5, or 9.6 can be used on a PGP Desktop 9.7 or later system, and work as expected. However, if you make any changes to the disk using PGP Desktop 9.5 or 9.6 software (such as changing the passphrase, adding or removing users, and so on), the disk will no longer function on the PGP Desktop 9.0 system. [11610, 11845]

- **Disk Recovery**: As a best practice, if you need to perform any disk recovery activities on a disk protected with PGP Whole Disk Encryption (WDE), PGP Corporation recommends that you first decrypt the disk (by using the PGP Desktop Disk > Decrypt option, your prepared PGP WDE Recovery Disk, or by connecting the hard disk via a USB cable to a second system and decrypting from that system's PGP Desktop software). Once the disk is decrypted, proceed with your recovery activities. [NBN]

- **Using PGP WDE with Norton Ghost 9 or 10**: Ghost is compatible with fully encrypted disks. Ghost sometimes exhibits errors when used to make backups within the Windows OS of partially encrypted disks. To recover from an error like this, reboot the system and perform a Windows chkdsk when the system restarts. Ghost should be functional again. [13004]

- **Compatibility of older-version PGP WDE recovery disks**: PGP WDE recovery disks are compatible only with the version of PGP Desktop that created the recovery CD. For example, if you attempt to use a 9.0 recovery disk to decrypt a disk protected with PGP WDE version 9.5 or later, it will render the PGP WDE disk inoperable. [10556]

- **Preparing for disk encryption**: Errors when attempting to encrypt your disk are often caused by bad sectors on a hard disk. These can frequently be corrected with third-party products which repair and ensure the health of your disk. The Windows CHKDSK program may resolve the issue in some instances, but more comprehensive programs such as SpinRite from Gibson Research Corporation (http://www.grc.com) are often required. Additionally, if your disk is seriously fragmented, PGP Corporation recommends that you defragment your disk prior to encryption using the Windows Disk Defragmenter. [10561]

- **PGP WDE and Dell systems boot diagnostics**: (Dell systems only) Advanced boot diagnostics that are normally accessible by pressing F12 during the boot process are not available on disks encrypted with PGP WDE. To run advanced boot diagnostics using F12, first decrypt the disk, and then run diagnostics. [12120]

- **Software incompatibility with the PGP Whole Disk Encryption feature**: Certain programs are incompatible with the PGP Whole Disk Encryption feature; do not install these products on a system with PGP Desktop, and do not install PGP Desktop on a system with these products installed:
  - Faronics Deep Freeze (any edition) [15443]
  - Utimaco Safeguard Easy 3.x. [8010]
  - Hard disk encryption products from GuardianEdge Technologies: Encryption Anywhere Hard Disk and Encryption Plus Hard Disk products, formerly known as PC Guardian products. [12005, 12065]
  - Safeboot Solo co-exists on the system but blocks PGP WDE.
  - SecureStar SCPP co-exists on the system but blocks PGP WDE.
  - Wave Systems' Dell Embassy Trust Suite co-exists on the system but causes the system to slow down. [19297]

- **PGP WDE Recovery Tokens**: In a Universal-managed environment, if a disk is encrypted with PGP Whole Disk
Encryption prior to enrollment with PGP Universal, the Automatically Encrypt boot disk upon installation must be selected on the PGP Universal Server for the Whole Disk Recovery Token (WDRT) to be uploaded to the PGP Universal Server; otherwise the token will not be automatically uploaded when the system is enrolled with PGP Universal. [12183]

- **IBM Fingerprint Software:** PGP Desktop is compatible with the IBM ThinkVantage fingerprint software version 5.6.1 or later. [13786]

- **PGP WDE SSO:** When using PGP WDE SSO, PGP Corporation recommends that organizations enable the Microsoft Group Policy option Always wait for the network at computer startup and logon. This ensures that password expiration and forced changes happen as soon as possible. For more information regarding this setting, see the following Microsoft Knowledgebase articles. [14142]
  - http://support.microsoft.com/kb/305293

- **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.

- **Using CHKDSK:** CHKDSK may report errors in a file called PGPWDE01 when checking a disk that has been encrypted with PGP Whole Disk Encryption. This file is protected by PGP Whole Disk Encryption and such errors can be ignored. [20197]

- **Using Maximum CPU Usage to encrypt removable disks:** Removable disks cannot be encrypted using the Maximum CPU Usage option even though this option can be selected. [24286]

- **PGP WDE on Lenovo Ideapad systems:** PGP WDE is incompatible on Lenovo Ideapad S10-2 systems running Microsoft Windows XP. PGP WDE is compatible when running Windows 7 on these systems. [24082]

- **Recovering data from an encrypted disk:** If you have an encrypted disk that cannot be recovered using the ppwde --recover command, you can recover the disk using a Windows PE disc or a previous version of the recovery disc. For more information on how to recover the encrypted disk, see PGP KB article 1826. For information on how to create a Windows Pre-installation Disc, see PGP KB article 807. [25425]

**PGP Zip**

- **PGP Zip and PGP NetShare:** On Windows Vista, creating a PGP Zip archive of a folder added to PGP NetShare is not supported. [17058]

- **Self-decrypting archives:** When the recipient of a self-decrypting archive (SDA) decrypts it, all dialog boxes that PGP Desktop displays are in English, regardless of what version of PGP Desktop—English, German, or Japanese—was used to create the SDA and regardless of what language your system is currently running. This applies only to the dialog boxes that appear; file names and the content of the SDA are not affected. [7144]

- **Compatibility with AVG Anti-Virus:** To create a PGP Zip SDA on systems running AVG Anti-Virus software, you must be using AVG Anti-Virus version 8.0 or later. If you are using an earlier version of AVG Anti-Virus, disable heuristic analysis in the RESIDENT SHIELD if you want to create PGP Zip SDAs. [16488]

**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 the [PGP Contacts Page](#).
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.

Copyright and Trademarks

Copyright © 1991-2009 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.