PGP® Desktop Version 9.8 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: 9.8.3

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* (https://support.pgp.com/?faq=589).

What's Included in This File

About PGP Desktop for Windows

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 version 9.8.3 and version 9.8.2

- **Resolved issue:** Resolved a rare issue where PGP NetShare could introduce an inconsistency in the file encryption keys, preventing the file from properly decrypting when performing administrative update operations on complex folder structures with differing memberships. [16905, 17833]
- **Resolved issue:** Resolved an issue where upgrading PGP Whole Disk Encryption could, in rare cases, cause disk inconsistencies. [17726]
- **Resolved issue:** Resolved an issue with PGP NetShare with Windows Vista when using copy or xcopy commands to copy PGP NetShare-protected data from a folder on a Windows 2003 or Windows 2008 server to another folder on the same server. [17910]

Changes between version 9.8.2 and version 9.8.1

- **Resolved issue:** PGP BootGuard now properly displays on an external monitor (Analog or digital) when the laptop lid is closed including when using a docking station. [16341, 17501]
- **Resolved issue:** Users are no longer required to enter Key Reconstruction information again if that information was previously entered and is currently stored on the PGP Universal Server [17001, 17173]
- **Resolved issue:** Resolved issues with WDRTs and encrypting multiple removable disks. [17258]

Changes between version 9.8.1 and version 9.8

- **Resolved issue:** PGP Universal-generated certificates now contain all email aliases of the key within the Subject Alternative Name property of the certificate [13138, 16372]
- **Resolved issue:** Security of keyboard-typed passphrases at boot time for a PGP WDE-encrypted drive has been improved. [16869]
- **Resolved issue:** Improved PGP NetShare interoperability with Novell 4.91 SP4. [16326]
- **Resolved issue:** Issues with PGP Whole Disk Encryption when upgrading an encrypted disk from previous versions, including version 9.0.6, have been resolved. [16904]

Changes between version 9.8 and version 9.7.1

- **Localized for German and Japanese:** PGP Desktop for Windows is available in German and Japanese.
- This release also includes bug fixes and improvements.
- **Resolved issue:** A new Whole Disk Recovery Token (WDRT) is now sent to the appropriate PGP Universal Server in cases where the client was unable to contact the server when the original WDRT was used. [10730]
- **Resolved issue:** Rare cases where Microsoft Office macros conflicted with PGP Desktop have been fixed. [15035]
- **Resolved issue:** A conflict between Microsoft SoftGrid and PGP Desktop has been fixed. [15665]
- **Resolved issue:** Improvements have been made to token handling when tokens are removed from a system. [15758, 16242]

Changes between version 9.7.1 and version 9.7

- **Resolved issue**: PGP NetShare files initially encrypted by PGP Desktop 9.7.1 on 64-bit versions of Windows used an incorrect file format. Such files should be decrypted using 9.7.1 on the 64-bit system prior to upgrade. This release ensures proper PGP NetShare formatting on 64-bit systems. [16381]

What's New in PGP Desktop for Windows Version 9.7

Building on PGP Corporation’s proven technology, PGP Desktop 9.7 for Windows includes numerous improvements and the following new features:

PGP Desktop General Features

- **Additional platform support.** PGP Desktop is now available for Microsoft Windows Vista 64-bit and Mac OS X 10.5 (Leopard).
- **Feature deployment control.** Administrators can now enforce policy by providing end users only with authorized client features, enabling or disabling client capabilities before distributing PGP client software to end-users. Disabled features are then unavailable in the PGP Desktop user interface.
- **Intel AMT support.** PGP Desktop supports Intel Active Management Technology (AMT) Agent Presence on those computers with properly configured Intel AMT-equipped motherboards. PGP Desktop reports its current status via AMT to enable Enterprises to query configuration information even when a system is turned off.
- **Updated key reconstruction user interface.** The PGP Desktop Key Reconstruction user interface has been significantly improved in this release. Primary new features include the ability to select and

customize a set of provided questions, a visually more appealing experience, and a new Assistant to help guide the user through the process.

- **Local key reconstruction.** Standalone installations of PGP Desktop support Local Key Reconstruction. The Key Reconstruction Assistant saves Key Reconstruction information in a file that can be used later to reconstruct the user key.
- **PGP Log message filtering.** The PGP Log feature of PGP Desktop now provides a menu option to filter local log messages by topic to facilitate troubleshooting (for example, displaying messages related only to Email, IM, NetShare, or WDE).
- **Passphrase quality evaluation improvements.** Passphrase quality evaluation has been significantly enhanced both visually and functionally in this release.

PGP Whole Disk Encryption Features

- **Advanced centralized event logging.** PGP Universal now provides significantly expanded reporting on PGP Whole Disk Encryption usage on client systems. This logging feature itemizes events such as which systems have been encrypted, the progress of encryption or decryption for an individual system, errors encountered during encryption, the status of recovery tokens, removable storage usage, and failed/successful login attempts. Administrators can set thresholds that raise alerts in PGP Universal on the PGP Daily Status Email or dashboard screen after a configured number of failed logins has been exceeded.
- **Extended pre-boot smart card support.** PGP Whole Disk Encryption has greatly expanded pre-boot authentication to a variety of smart cards.
- **Customizable WDE BootGuard screens.** Administrators in a PGP Universal-managed environment can configure the PGP Whole Disk Encryption boot screen to display the text and graphics of their choice.
- **Group administration access tokens.** PGP Whole Disk Encryption admin accounts can be added, allowing an administrator with a smart card key to override the BootGuard prompt. This key can be specified separately for each Internal User Policy. Using a single keypair copied to multiple smart cards (each with its own PIN), an organization can enable multiple administrators for each Policy.
- **Domain administrator restart bypass.** Windows System and Administrator account(s) may now engage a mode to bypass WDE authentication on the next restart by utilizing the privileges of the administration account to act as the authenticated user. This feature enables administrators to perform remote software installations requiring a restart of the target computer. Use of this feature is logged to the PGP Universal server.
- **Partition encryption deployment.** Administrators in a PGP Universal-managed environment may now configure encryption of only the boot partition or only Windows partitions rather than always encrypting entire disks.
- **PGP WDE Single Sign-On for Novell environments.** The PGP WDE Single Sign-On (SSO) feature is now available for Windows systems running in Novell network environments.
- **User Interface modifications for ADA compliance.** As part of our expanding support for the Americans with Disabilities Act (ADA) standards for accessible design, the PGP WDE BootGuard screen has been modified to provide audible feedback when the screen is ready for user input, when a user types in an incorrect password, and when a user types a correct password. This audio feedback is optional, configurable using PGP Universal for managed clients.
- **Lenovo laptop Recovery button.** PGP Whole Disk Encryption now provides complete support for the Lenovo Rescue and Recovery software (version 3.x and 4.x) including using the “Access IBM” blue button for boot-level recovery of the OS even when the disk (or partition) is encrypted.
- **Microsoft Windows PE support.** PGP Desktop provides administrators with the ability to create a Windows PE (Preinstallation Environment) boot disk containing a subset of PGP Whole Disk Encryption. This bootable disc can be used to perform a variety of management and recovery tasks.
- **Trusted Platform Module (TPM) support for PGP WDE.** PGP Desktop supports using the Trusted Platform Module as an additional authentication device for PGP Whole Disk Encryption if present on the motherboard and enabled via proper driver installation for your hardware. When use of the TPM is specified prior to encryption, the user can authenticate to the disk only on that particular machine, locking the disk to the machine hardware and thus deterring attacks such as hard disk theft. This feature works with passphrase users only and is compatible with the PGP WDE Single Sign-On feature.

PGP NetShare Features

- **PGP NetShare per-folder administration.** PGP NetShare administrative granularity has been extended to restrict administrator control to a per-folder level, thus limiting administrative access to exactly where it is needed.
- **Whitelists and blacklists.** Administrators can now centrally define PGP NetShare policy to protect files stored in specific directory locations, enforcing security policy without impacting user behavior. Conversely, administrators can also force specific directories to prevent encryption.
- **Directory roles.** There are now three roles for PGP NetShare-protected directories: Admin, with full rights over the directory; Group Admin, who can add/remove users that are not Admins or Group Admins; and Users, who can only access content, and have no administration abilities.
- **Centralized PGP NetShare logging.** Centralized logging on PGP Universal provides visibility into the activity of PGP NetShare deployments to satisfy management and auditing requirements.
- **PGP NetShare Command Line.** Most PGP NetShare functions can now be scripted. This utility is documented in the PGP NetShare Command Line Programmer's Guide.

PGP Desktop Email Features

- **MAPI support for PGP/MIME formatted messages.** PGP Desktop now provides the ability to encrypt PGP/MIME messages in Outlook clients using MAPI. PGP/MIME decryption has also been significantly improved in this area.
- **Microsoft CAPI integration.** PGP Desktop supports the use of Microsoft Cryptographic Application Programming Interface (CAPI) credentials, enabling the user to make use of existing X.509 certificates directly from the Microsoft operating system certificate store. PGP Universal administrators can specify automatic enrollment of such certificates as well.
- **IMAP speed improvements.** This release of PGP Desktop contains significant IMAP performance improvements. Users will experience quicker responses and shorter downloads, particularly when accessing large mailboxes, switching between folders, and checking for new messages.
- **Out-of-the-mail-stream support.** PGP Desktop and PGP Universal Satellite will selectively send email messages directly to the PGP Universal Server via a SOAP connection if required by policy, such that the server does not need to be in the mail stream to support Web Messenger or Smart Trailer functionality.
- **Weak-cipher decryption.** PGP products now decrypt S/MIME encoded messages encrypted with weak 40-bit RC2 encryption for backwards compatibility with older email clients. Additional warnings are added to messages decrypted using that algorithm. Note that PGP Desktop will not *encrypt* using weak ciphers.

System Requirements

- Microsoft Windows 2000 (Service Pack 4), Windows Server 2003 (Service Pack 1), Windows XP (Service Pack 1 or 2; 32-bit versions only), Windows Vista (all 32-bit and 64-bit versions), Microsoft Windows XP Tablet PC Edition 2005 (requires attached keyboard)

  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 client versions of Windows 2000 (Service Pack 4) and Windows XP (Service Pack 1 or 2), and on Windows Vista; it is *not* supported on Windows 2000 Server or 2003 Server.
- 512 MB of RAM
- 64 MB hard disk space

Supported 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 (Outlook 12)
- Microsoft Outlook 2003 SP2
- Microsoft Outlook XP SP3
- Microsoft Outlook 2000 SP3
- Windows Mail 6.0.6000.16386
- Outlook Express 6
- Mozilla 1.7
- Thunderbird 1.0 or later
- Lotus Notes 5.0.11, 6.x, and 7.0.1
- Novell GroupWise 6.5.1 or later

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 (https://support.pgp.com/?faq=713) as more information becomes available.

Instant Messaging Client Compatibility

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

- AOL AIM 5.9.x
  - Encryption of file transfers and direct connections requires AOL Instant Messenger 5.9.3702 on Windows (with the Firewall preference set to “AOL proxy server only”) or Apple iChat 3.1.5 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 version 9.8 is released.
- AOL AIM 6.5
  - To encrypt instant messages with AIM 6.5, you must change the default port that AIM uses from 493 to 5190.
- Trillian 3.1

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.

Computer Associates Internet Security Suite 2007

- 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).

McAfee VirusScan 7.x

- No special configuration required.

Panda Platinum 2005 Internet Security 9.x

- No special configuration required.

Sophos Anti-Virus

- No special configuration required.

Symantec Norton AntiVirus 11.x through 12.x, Symantec Norton Internet Security 2005, Symantec Norton Internet Security 2006

- 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.

Symantec Norton AntiVirus 9.x through 10.x, Symantec Norton Internet Security 2003, Symantec Norton Internet Security 2004

- 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.

Symantec Norton AntiVirus 8.x

- PGP Corporation does not recommend using PGP software with this version of Norton AntiVirus. PGP Corporation recommends that you upgrade to Norton AntiVirus version 10.x or later. [10419]

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

- No special configuration required.

Personal Firewall Compatibility

- **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 9.8 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]

Citrix and Terminal Services Compatibility

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

- Citrix Presentation Server 4.0
- 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 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.
- PGP NetShare is not supported.

Supported Smart Cards and Tokens for PGP WDE BootGuard Authentication

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

Supported Smart Card Readers for PGP WDE Authentication

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

Generic smart card readers

Any CCID smart card reader is supported. 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)

CyberJack smart card readers

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

ASE smart card readers

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

Supported Smart Cards or Tokens for PGP WDE Authentication

PGP Whole Disk Encryption supports the following smart cards for pre-boot authentication:

- ActiveIdentity ActivClientCAC cards, 2005 model
- Aladdin eToken 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)

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

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

  Note: The Athena tokens are supported only for credential storage.

- EMC RSA SecurID SID800 Token

  Note: This token is supported only for credential storage. SecurID is not supported.

- Charismathics CryptoIdentity plug 'n' crypt Smart Card only stick
- S-Trust StarCOS smart card

  Note: S-Trust SECCOS cards are not supported.

- Rainbow iKey 3000

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.

To upgrade from previous versions of PGP Desktop

- If you are upgrading your computer to Windows Vista and want to use this version of PGP Desktop, be sure to uninstall any previous versions of PGP Desktop *before* upgrading to Windows Vista 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. 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 9.8 includes PGP Desktop Email and PGP Whole Disk Encryption.
- PGP Desktop Storage 9.8 includes PGP Whole Disk Encryption and PGP NetShare.
- PGP Desktop Enterprise 9.8 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 (https://store.pgp.com/).

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 Net Nanny software:** Net Nanny software from ContentWatch does not properly handle Windows networking under Windows Vista with PGP Desktop. Contact ContentWatch for updates to their software. [14178]
- **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. [16286]

PGP Messaging

- **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]
- **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:**
    - **RC2 128-bit S/MIME messages:** PGP Messaging does not support the decryption of RC2 128-bit S/MIME-encrypted email. [12140]

- **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. 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:**
  - **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 2000 MAPI:** Composing messages while in offline mode when using Outlook 2000 with MAPI is not supported. [8165]
  - **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**: After upgrading from Windows XP to Windows Vista without reinstalling PGP Desktop, MAPI messages are sent in the clear and existing encrypted messages are not decrypted. When you upgrade your operating system to Windows Vista, PGP Corporation recommends that you first uninstall PGP Desktop, upgrade your operating system, and then reinstall PGP Desktop. [13119]
- **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]
  - **Encrypted attachments:** When sending an encrypted attachment without also encrypting the message, the encrypted attachment is not automatically decrypted when received by Lotus Notes. [11969]
  - **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:**
  - **AIM Pro:** PGP Desktop does not support AIM Pro. To use AIM Pro with unencrypted instant messages, change the port it uses to communicate with the AOL server from the default port 5190. Other standard ports used by AOL are 5191-5193. [11334]
  - **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**: The German and Japanese versions of AIM 6.5 that are currently in beta are not compatible with PGP Desktop. PGP Desktop will not secure instant messages with these beta versions. In addition, PGP Desktop does not secure instant messages when the English (released) version of AIM 6.5 is run on German or Japanese operating systems. [16393]

PGP NetShare

- **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]
- **Overlay Icons**: PGP NetShare overlay icons are not displayed on 64-bit Windows Vista. The PGP NetShare properties tab is not available on 64-bit Windows Vista. [15042]
- **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. [12506]
- **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]

PGP Whole Disk Encryption

- **PGP WDE Authentication**: The ActiveIdentity ActivClientCAC model 2002 smart card is not supported in this release. To use the ActiveClient CAC card, use model 2005. [16259]
- **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:** When using a smart card reader with a built-in PIN pad, the correct PIN may not be accepted the first time and you will be prompted to provide the password again. When this message appears, click OK without entering the password. This will either allow the password to be accepted or will transfer control to the PIN pad of the smart card reader, where you can enter the password. [16143]
- **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 encypting 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]
- **Single Sign On**: If you are using PGP WDE in Single Sign On mode, changes to your Windows domain password may be accepted by PGP WDE even if the Windows domain rejects that password change. [15685]
- **Using WDRT after hibernation**: If the WDRT is used at the PGP BootGuard screen to resume a system after hibernation, you must reboot the system to generate a new WDRT. [15276]
- **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]

- **Upgrading**: The PGP BootGuard screen is not updated immediately after you upgrade to PGP Desktop 9.8. To display the updated PGP BootGuard screen (containing new login and keyboard options), reboot your system a second time. [NBN]
- **GPT partition style disks:** PGP Whole Disk Encryption does not support encryption for a disk based on the GUID partition table (GPT) partition style. [12722]
- **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]
- **Supported passphrase characters**: The following characters are supported:

  `abcdefghijklmnopqrstuvwxyz`

  `ABCDEFGHIJKLMNOPQRSTUVWXYZ`

  `0123456789`

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

  Any other characters, including accented characters (such as ç é è ê ë î ï ô û ù ü ÿ) or symbols (such as ¢ ® œ), are not supported. [12947, 11551]

  Additionally, when using the following language keyboards, these characters are not supported in passphrases:

  - Japanese: \ or | or _
  - Spanish: \
  - German: | or ^
- **Using PGP WDE-Protected Disks with PGP Desktop 9.x and 9.7:** Disks encrypted with PGP Desktop 9.0, 9.5, or 9.6 can be used on a PGP Desktop 9.7 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 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 9.5, 9.6, or 9.7 software, it will render the PGP WDE 9.5, 9.6, or 9.7 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]

- **Dell USB SK-8125 keyboard:** Do not use the Dell USB SK-8125 keyboard if you are encrypting your boot drive using the PGP Whole Disk Encryption feature. The keyboard inserts extra characters under these circumstances and thus you can't authenticate correctly. [5686]
- **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:
  - Utimaco Safeguard Easy 3.x. [8010]
  - Absolute Software's CompuTrace laptop security and tracking product. PGP Whole Disk Encryption is compatible only with the BIOS configuration of CompuTrace. Using CompuTrace in MBR mode is not compatible. [10884]
  - 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.
- **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]
- **Whole Disk Recovery Token and Aladdin eTokens:** If you need to use a Whole Disk Recovery Token to log in to a drive that has been PGP Whole Disk Encrypted, be sure to remove any Aladdin eTokens from the system before you attempt to log in. [7505]
- **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://technet.microsoft.com/en-us/library/bb456994.aspx
  - http://support.microsoft.com/kb/305293

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]

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**. [14067]
- **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 Zip

- **Adding Files**: The PGP Zip Assistant may appear to stop when adding large files. Please allow additional time to create a PGP Zip file when adding large files. [14591]

- **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 boxess that appear; file names and the content of the SDA are not affected. [7144]
- **Shred Original option and SDAs:** When creating an SDA via PGP Zip in PGP Desktop and selecting the **Shred Originals** option, if the operation contains any folders, neither the folder nor its contents are shredded after the SDA is created. [11832]

PGP Shred

- **PGP Shred on Windows Vista:** When shredding a folder containing files on Windows Vista, the PGP Shredder shreds the files but does not remove the folder. [12786]
- **Wiping small files:** Wiping 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 freespace even after deleting a file, and thus they also will not be wiped using PGP Desktop's Freespace Wipe feature. In addition, NTFS supports Journaling, which can save wiped file data in an internal operating system cache. For the highest security wiping on NTFS disks, we recommend starting your system from an OS on a different partition and using PGP Desktop's option in the Freespace Wipe feature to overwrite these NTFS data structures (the **Wipe NTFS internal data structures** checkbox). This does not affect FAT32 or other supported file systems. [NBN]

Getting Assistance

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

Available Documentation

Prior to installation, complete Product Documentation is available through the PGP Support Knowledge Base (https://support.pgp.com/?faq=589).

PGP Desktop documentation is installed onto your computer during the installation process. To view it, select **Start > Programs > PGP > Documentation**. All documents are saved as Adobe Acrobat Portable Document Format (PDF) files. You can view and print these files with Adobe Acrobat Reader, available on the Adobe Web site (http://www.adobe.com). PGP Desktop also includes integrated Windows online help.

Copyright and Trademarks