PGP Desktop

PGP Desktop

> ⚠ PGP is no longer being offered on the software grid. Support is being phased out and will discontinue at the end of 2016.

On this page:

- About
- Enable PGP Desktop
- FAQ
  - Do I need to encrypt my computer using PGP Desktop?
  - How does PGP Desktop protect my data?
  - Is my computer protected when it is in sleep mode or when the screen saver is active?
  - Can PGP Desktop be installed on desktop computers or only on laptops?
  - Does PGP Desktop work on a Mac?
  - Can I install PGP Desktop on multiple workstations using an image?
  - Can I use MIT's PGP Desktop on my home computer?
  - Does PGP work on mobile devices?
  - If I change my Kerberos password, will my PGP passphrase also change?
  - Can I share my passphrase with Desktop Support?
  - What is the difference between PGP key, password, passphrase and recovery token?
- Support
  - Uninstalling
  - Troubleshooting
  - Passphrase issues
  - How to...
- See Also

About

PGP (Pretty Good Privacy) is a piece of software that offers, primarily, whole disk encryption capabilities. Because of its proven reliability, ease-of-use and time-tested security features, PGP Desktop was chosen by IS&T to protect MIT's high-risk data.

PGP Desktop 10 Whole Disk Encryption (WDE) is currently being distributed for individuals who need to protect data on laptops and portable storage devices against physical loss or theft. It is the recommended solution for encryption on a Windows computer.

Enable PGP Desktop

> ⚠ PGP and Mac OS X 10.8 (Mountain Lion) users: IS&T recommends that users who handle sensitive data on Macs and use PGP for encryption wait to upgrade to Mountain Lion or to switch to FileVault the native encryption system on Macs. To make the switch from PGP to FileVault, first uninstall PGP, and then use these instructions to enable FileVault.

1. First run Identity Finder to see if there are sensitive data files on the computer. If possible, take action to remove any sensitive information. If no sensitive data resides on the computer, there is no need for full-disk encryption.
2. Check compatibility issues.
3. Obtain a copy of PGP Desktop (MIT faculty and staff only).
4. Back up your data before you install PGP Desktop or encrypt your computer, using a backup tool such as Code42.
5. Install PGP Desktop on your computer and initiate encryption.
6. (Optional) Encrypt an external drive.

FAQ

Do I need to encrypt my computer using PGP Desktop?

Not everyone who has sensitive data on their computers needs to encrypt their computer. You should first identify and inventory the data you have on your computer, and Identity Finder is a software utility that does just that. Currently, laptops and other portable storage devices (i.e. portable hard drives, USB memory sticks) that contain personal information requiring notification (PIRN) are required to be encrypted.

If you want to use PGP Desktop, check in first with your system administrator. Local IT policy may require additional safeguards to ensure that - should you leave MIT, be unavailable, or forget your password - someone from your business area can still access the important business files on the encrypted computer.

How does PGP Desktop protect my data?

PGP protects the data only when the computer is turned off (learn more about whole disk encryption).

PGP offers no protection for malware (computer virus) infections. Users must maintain their operating system and practice good computing hygiene (applying patches, security updates, creating strong passwords, and staying away from dubious links and web sites).

PGP Desktop also does not encrypt email or attachments. Users must look to other tools for protecting data in transit, such as PGP Zip.

Is my computer protected when it is in sleep mode or when the screen saver is active?

No. Your sensitive data is only protected by PGP whole disk encryption when your computer is turned off. Once you boot your computer and enter your password, your disks are mounted even when a screen saver is active or your computer hibernates. This means data can still be accessed on your computer when you don't have a screen saver or a wake-from-sleep password. We therefore recommend you protect your computer by also putting your computer to sleep with a strong password.

Can PGP Desktop be installed on desktop computers or only on laptops?

PGP protects the data only when the computer is off, so it is most useful on machines that are likely to be lost or stolen (e.g. laptops and USB drives). Since certain desktops can also be stolen, PGP can certainly be installed on desktops as well.

Does PGP Desktop work on a Mac?

Because there have been delays by Symantec (the company that owns PGP Desktop) to provide compatible versions of PGP Desktop for Mac OS X, IS&T does not recommend using PGP Desktop on a Mac computer. Instead, we recommend using FileVault 2. The current version of PGP Desktop on the IS&T software grid does not run on Mac OS X 10.8.

Can I install PGP Desktop on multiple workstations using an image?

No. As each workstation must be enrolled with the PGP Universal Server using the individual's credentials - for recovery purposes - there isn't an easy way to do this. The install takes a minimal amount of time, so individual installations do not pose a major time-sink to deploy.

Can I use MIT's PGP Desktop on my home computer?

No. MIT's PGP license does not allow for installation on home computers.

Does PGP work on mobile devices?

No. PGP does not currently support mobile devices (smartphones or tablets). See more about encryption on mobile devices here.

If I change my Kerberos password, will my PGP passphrase also change?

No, the two are not connected. Although you may have originally used your Kerberos password as your PGP passphrase when you installed PGP, if you change your Kerberos password later on, this does not also change your PGP passphrase.

Can I share my passphrase with Desktop Support?

You should not need to, and doing so may violate state laws that require you to protect personal information that is on your computer.

What is the difference between PGP key, password, passphrase and recovery token?

- PGP password & PGP passphrase: these two terms can be used interchangeably. This is what needs to be entered when your computer boots up to bypass the PGP protection screen.

- Whole Disk Recovery Token: if you forget your password, a recovery token can be generated to regain access to your system. The token acts as a one-time password.
- Keys: your hard disk is encrypted using what's called a symmetric key; that is, the same key is used to both encrypt and decrypt the data on your hard drive. The security of the system comes from the key being kept secret. In PGP Desktop's case, the key is kept secret using your password.

Support

Uninstalling

- From a Mac or Windows prior to an operating system upgrade
- Manually from a Mac

Troubleshooting

- A boot error on certain Win 7 computers
- Receiving a Blue Screen of Death

Passphrase issues

- Forgot your PGP passphrase
- Change your PGP passphrase
- Your PGP passphrase doesn't work
- Bypass the PGP passphrase

How to...

- Backup PGP keys and keyrings
- Use PGP Zip
- Decrypt prior to system upgrades

See Also

- Encryption Landing Page

Users in need of further assistance can contact the Help Desk at 617.253.1101, helpdesk@mit.edu, or by submitting a request online (http://ist.mit.edu/help).