Frequently Asked Questions

(Please note that this document will be frequently updated with new questions and answers to all of the PGP products being released from Xerox Services Encryption Services)

PGP General Questions

Q. What is PGP?

Q. Why is PGP required?

Q. Who is required to have PGP installed (i.e., a PGP license)?

Q. Is PGP required on Xerox Services desktops/laptops supported by non-Xerox Services locations?

Q. Who is called for support when I have issues with PGP?

Q. Does PGP affect the performance of my computer?

Q. Does PGP have to be “patched” or “upgraded” periodically?

Q. Does PGP affect my ability to work remotely?

Q. How do I reset my passphrase if I lose it?

Q. Does my passphrase require changing periodically?

Q. Is PGP dependent of a network connection to reset my passphrase?

Q. Is anything required when a Xerox Services employee terminates?

Q. How does help desk verify my identity when passphrase reset is requested?

Q. If my computer is re-imaged will my old passphrase still work?

Q. If I change jobs within the company will that have any impact on PGP installation?

Q. If I change email servers will that have any impact on PGP installation?

Q. Will PGP work with my wireless router at home?

Encrypting Removable Media

Q. Do I have to encrypt all of my external drives?

Q. What happens if I forget my passphrase?

Q. If I had a flash drive encrypted and forgot the passphrase, but did not have information on the drive I needed can just re-format the drive?

Q. I no longer needed the information on my flash drive and could not remember my passphrase so I just reformatted. The drive is now showing that it is encrypted but I have full access to the drive. How can I fix this?

Q. What happens if my power goes out when I am encrypting my drive?

Q. When encrypting my external drives can I use a different password or passphrase?

Q. I've encrypted my drive and now I want to decrypt it, but the software is not showing the decryption option?

PGP Zip - Self Decrypting Archive (SDA)

Q. What is PGP Zip?

Q. What is a Self Decrypting Archive?
Q. What is a passphrase?
Q. When should I create a SDA?
Q. How can I set Windows to show file extensions?

PGP General Questions

Q. What is PGP?

Pretty Good Privacy (PGP) is the first product on the market to implement Public Key Cryptography. Public Key Cryptography is a technology that uses two keys, one to encrypt (i.e., scramble a message so it cannot be read by any one) and another to decrypt (i.e., unscramble so it can be read by its intended recipient). PGP can be used to encrypt an individual file or an entire hard drive as well as individual e-mail messages.

Q. Why is PGP required?

Laptops are becoming a commodity and desktops are shrinking in size each year. More and more client Personally Identifiable Information (PII) and Xerox Services financial information is being stored on these computers. We want to make sure that should any of these computers be removed from our own control, that data will not be viewable by anyone else. **All laptops must be encrypted.**

Q. Who is required to have PGP installed (i.e., a PGP license)?

The Xerox Services CSG Security Standard states that every laptop/desktop that may come in contact with client PII, or Xerox Services financial information should have PGP installed.

Q. Is PGP required on Xerox Services desktops/laptops supported by non-Xerox Services locations?

If it is a client controlled workstation on a client controlled network then they are responsible for protecting its contents. We suggest that you might wish to give them the chance to make use of the added protection but that is strictly up to you.

Q. Who is called for support when I have issues with PGP?

In the event of a problem the ITO employee will call the Dallas Help Desk. They will open a ticket and try to help the employee. If they cannot solve the problem the ticket will be referred to the employee's local Desktop Support person. If the Local Desktop person cannot solve the problem the ticket will be routed to Global Shared Services Help Desk (i.e., PGP Server Support) for resolution. If they cannot fix the problem the ticket will be referred it to PGP Technical Support to resolve.

Q. Does PGP affect the performance of my computer?

No. As far as the speed of the actual machine is concerned once PGP Whole Disk is in place on a machine the performance will depend almost entirely on the hard drive speed, since PGP Whole Disk uses a symmetric key stored in cache and the processor to do encryption and decryption. PGP Whole Disk can do those operations much faster than the drive can write so most of the time PGP Whole Desk just ends up waiting for the hard drive to spin to write or read data. Typical 5400 RPM hard drives for laptops work just great. However, encryption may affect system performance up to 4 hours after installation because PGP is encrypting your drive. Please note that encryption times may vary depending on the size of the harddrive and not the amount of data stored.

Q. Does PGP have to be “patched” or “upgraded” periodically?

PGP does **NOT** have to be patched or upgraded, however, we will try to keep it updated if vulnerabilities are discovered or performance improvements are developed.

Q. Does PGP affect my ability to work remotely?

No! PGP will not effect performance or the ability to do anything you are currently doing with your computer.

Q. How do I reset my passphrase if I lose it?

If you forget your passphrase you will call the Help Desk just as you do for forgotten Network Passwords today. The Help Desk will provide a one time use passphrase to start your computer. You will then be asked to choose a new passphrase for on-going use.

Q. Does my passphrase require changing periodically?

No, your passphrase does not expire.

Q. Is PGP dependent of a network connection to reset my passphrase?

You do not need to be connected to the Internet to boot your computer. However, you will need to be connected to change your passphrase.

Q. Is anything required when a Xerox Services employee terminates?

When a Xerox Services employee is terminated he or she will be required to turn in all Xerox Services assets, as well as all system login information, i.e. all passwords and passphrase's. If an employee is rehired he or she will be issued a new password and passphrase. If moving to another group within Xerox Services the employee, per Xerox Services policy, will take their Xerox Services assets with them.

Q. How does help desk verify my identity when passphrase reset is requested?

When someone asks for a new passphrase the Dallas Help Desk will open a ticket and refer the ticket to the employee's Local Desktop Support person. The Local Desktop Support person will generate a one time use passphrase they will hand deliver the employee.

If the employee is traveling, or working remotely, the Local Desktop Support person will contact the employee's Manager for confirmation, or if that is not feasible contact the employee directly asking enough personal information to be sure they are talking to the right employee. Then, and only then, the Local Desktop Support person will generate a one time use passphrase that they will hand deliver the employee verbally communicating the one time use passphrase directly to the individual over the phone.

Q. If my computer is re-imaged will my old passphrase still work?

If your computer is re-imaged everything, including PGP, will have to be re-installed. At that point you would be asked to select a new passphrase.

Q. If I change jobs within the company will that have any impact on PGP installation?

Your PGP installation will stay with your computer; if you are issued a new system you should establish a new PGP passphrase that is different from your former passphrase."

Q. If I change email servers will that have any impact on PGP installation?

No! The PGP Server is reachable over the Internet and for PGP to fully function your computer will only need to communicate with the PGP Server from time to time. However, in the future we will be expanding the functionality of PGP to automatically encrypt e-mail. At that time there may be more details about this question.

Q. Will PGP work with my wireless router at home?

Yes! The data on your hard drive is encrypted while at rest. Once you access that data it is decrypted. If you move a file to another computer it is moved in the clear. It matters not if you are doing a file transfer or e-mail transfer.

Top

Encrypting Removable Media

Q. Do I have to encrypt all of my external drives?

If your drive contains client Personally Identifiable Information (PII) or Xerox Services financial information you must encrypt the drive. Remember, your personal drives must **NOT** contain this type of information.

Q. What happens if I forget my passphrase?

You must call the help desk to access your drive.

When using the Whole Disk Encryption (WDE) application to encrypt an external drive, a WDRT (recovery token) is still always generated for any drive (internal or a removable drive, like usb/flash) as you’re accustomed to when you encrypt a normal system. The device name, as identified by windows, is tagged to the device and if you call the Help Desk, they will be able to use a WDRT to unlock the device, where they can potentially create a new passphrase or decrypt the device.

Q. If I had a flash drive encrypted and forgot the passphrase, but did not have information on the drive I needed can just re-format the drive?

No, contact the Help Desk to decrypt the drive properly and then you can re-format the drive if necessary.

Q. I no longer needed the information on my flash drive and could not remember my passphrase so I just reformatted. The drive is now showing that it is encrypted but I have full access to the drive. How can I fix this?

Your drive is no longer encrypted properly. You will need to call the Help Desk to decrypt your drive to get rid of the encryption information. Once your drive is decrypted you will need to reformat the drive again to clean it up. When you are complete you will be able to re-encrypt your drive.

Q. What happens if my power goes out when I am encrypting my drive?

You can potentially lose your data. It is recommended that you take all of the necessary safety precautions before backing up your drives. If you think that power failure is a possibility for you select the Power Failure Safety option when encrypting your drive. Also, please refer to the PGP Best Practices Guide on InfoBank.

Q. When encrypting my external drives can I use a different password or passphrase?

No you will need you use the passphrase that is associated with that user key.

Q. I've encrypted my drive and now I want to decrypt it, but the software is not showing the decryption option?

You will probably need to reseat you drive. You will need to properly remove your drive from your computer and then reconnect it. Now, when you go back into PGP desktop the drive should show up with the updated status.

Top

PGP ZIP - Self Decrypting Archive (SDA)

Q. What is PGP Zip?

PGP Zip is a tool for securely archiving your sensitive data, whether you want to distribute it to others or back it up. You can add any combination of files and folders to an encrypted, compressed, portable archive.

Q. What is a Self Decrypting Archive?

A Self-Decrypting Archive (SDA) is an executable containing a file that has been encrypted using a passphrase. A recipient of an SDA runs the executable and enters the passphrase to decrypt the file. SDA's are especially useful when the sender must send an encrypted file to a recipient who does not have PGP software installed.

Q. What is a passphrase?

A passphrase is similar to a password, but is generally longer and uses a wide variety of characters. The stronger your passphrase is, the more secure your files are.

Q. When should I create a SDA?

Create an SDA when you want to share sensitive files and/or folders or if you want to encrypt files with PI that are attached to Internal Emails.

Q. How can I set Windows to show file extensions?

1. *Double click* on your **My Computer** icon on your computer's desktop.
2. *Go* to the **Tools** menu and *select* **Folder Options**.
3. *Click* on the **View** tab.
4. *Uncheck* the box for “**Hide extensions for know file types**” and *click* **OK**.

Top