How do I use MIT's PGP Desktop for Windows to whole disk encrypt external storage drives?

Q: How do I use MIT's PGP Desktop for Windows to whole disk encrypt external storage drives?

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

Answer

PGP Desktop allows you to encrypt disks, other than just your computer's internal hard drive, using Whole Disk Encryption. This includes USB flash drives and external portable storage devices. It is especially important to encrypt these devices if they contain sensitive information, as they are easy to misplace or have stolen and, in the case of external portable hard drives, may be used for backup of sensitive information that you have on your encrypted computer, so they must be encrypted as well.

A Warning: After an external portable hard drive or USB memory stick is encrypted using PGP Whole Disk Encryption, any computer that you want to use to access your portable storage MUST have PGP Desktop installed.

To create an encrypted disk:



3. Select the device you want encrypted in the Disk Properties window.



4. Click New Passphrase User...



 Enter a username and a strong passphrase. A whole sentence is best. Remember, this is the only thing that keeps the data protected. You will not see the password as you type it unless you select "Show Keystrokes". Click OK.

PGP Disk New User	
PGP Desktop	Create New User If your users do not have keys available you need to create passphrases for them. Keep in mind that this is not as secure as encrypting to public keys.
	Enter a new usemane
	Mike
	Enter a Passphrase for new user
	Passphrase Quality T00-%
	Re-enter Passphrase
	Show Keystrokes
	OK Cancel Help

6. Once the device you want encrypted is selected and a Passphrase User has been created, click the **Encrypt** button in the upper right corner of the window.



Result: PGP Desktop will begin encrypting the disk. The status of the encryption progress will be shown, as well as an estimated time to completion. When finished, the entire contents of the disk will be encrypted.



See Also

Encryption Landing Page

Additional Information More information on PGP can be found on the PGP Desktop page. If you don't find your answer, contact pgp-help@mit.edu.