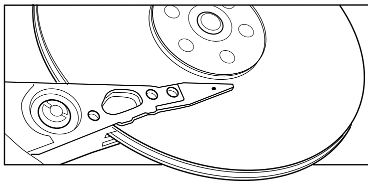

WD Sync™ Synchronization and Encryption Software

Improved Data Security for WD Passport™ Hard Drives

WD Sync synchronization software with Advanced Encryption Standard (AES) 128-bit encryption turns any PC into your own protected workspace. Beginning May 30, 2006, WD Sync is included with every new WD Passport Portable and Pocket hard drive.

WD Sync lets you save your critical data, personalized computer settings, and all your personal files on a WD Passport drive. When you travel, you can use WD Sync to plug your WD Passport drive into any PC to access and edit your Microsoft® Word documents and Excel spreadsheets, MP3, and even Internet Explorer favorites in a cybercafé, on a friend's laptop, or in a colleague's office. You can even send and receive e-mail securely from your WD Passport drive using WD Sync. After you're back from your travels, WD Sync synchronizes all your changes to your home or office computer keeping your files up to date.

WD Sync leaves no files behind and keeps your information secure regardless of the system you're using. With WD Sync, your personal files and Microsoft Outlook® data remain on your WD Passport and are not copied to the computers you visit. WD Sync also provides a secure browsing function so that all data related to internet surfing (cookies, cache, history) is stored on the WD Passport and deleted afterwards.

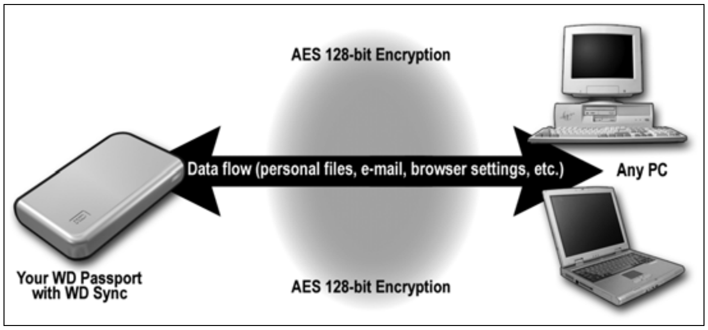
AES 128-bit Encryption
Data flow (personal files, e-mail, browser settings, etc.)
Any PC
Your WD Passport with WD Sync
AES 128-bit Encryption

Figure 1. WD Passport-to-PC Data Flow

Increased Data Security with AES

WD Sync's encryption function uses AES 128-bit encryption technology to protect you from data exposure as a result of a lost or stolen unit. WD Sync does not provide a means to recover a lost password—the only way to use a WD Passport without a password is to delete the contents of the drive and reset it with a new password. In this way, WD Sync serves as a deterrent to data theft.

AES 128-bit encryption also makes WD Passport data more difficult to hack via the "empirical" method (i.e., guessing the encrypt key pattern set by your password).

AES vs. DES

AES was developed to replace the single Data Encryption Standard (DES), which is being phased out of use and is currently permitted only in legacy systems. Both AES and DES use keys (passwords or tables needed to decipher encoded data) for encryption. DES keys are 56 bits long, meaning that there are approximately 7.2×10^{16} possible DES keys. By contrast, AES keys used for WD Passport drives are 128 bits long, providing a possible 3.4×10^{38} key numbers. Thus, there is somewhere in the neighborhood of 10^{21} times more possible AES 128-bit keys than DES 56-bit keys.

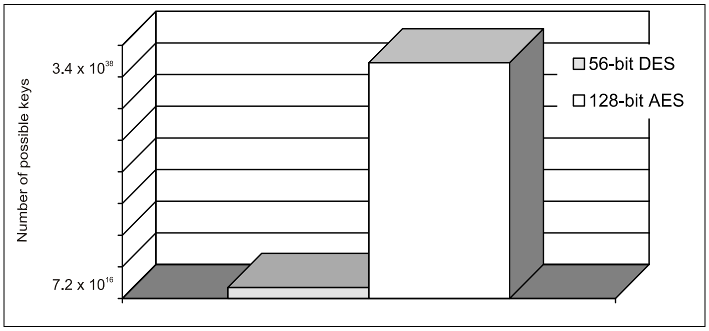

Figure 2. 128-bit AES vs. 56-bit DES

Western Digital is a registered trademark; and WD, the WD logo, WD Passport, and WD Sync are trademarks of Western Digital Technologies, Inc. Other marks may be mentioned herein that belong to other companies. Product specifications subject to change without notice.

Western Digital
20511 Lake Forest Drive
Lake Forest, California 92630

2579-701178-A00 May 2006

For service and literature:
support.wdc.com
www.westerndigital.com

800.ASK.4WDC	North America
949.672.7199	Spanish
+800.6008.6008	Asia Pacific
+31.20.4467651	Europe/Middle East/Africa

WD Western Digital®