

## Encryption Plus<sup>®</sup> Hard Disk Full-Featured Data Security for Enterprise PCs

<b>Encryption Plus<sup>®</sup> Hard Disk Features Checklist</b>	
<b>Encryption Technology</b>	
Current version:	7.1.0
Operating systems supported:	Windows XP, 2000, NT (Service Pack 6 and later) Windows Server 2000 and 2003
Disk encryption algorithm used:	Advanced Encryption Standard (AES) in Cipher Block Chaining mode
What is the minimum encryption key length?	256-bit
Other cryptographic algorithms used:	RSA, Elliptic Curve Diffie-Hellman, OpenSSL, SHA1, Random Number Generator
Has the AES algorithm been FIPS 140-2 certified?	Yes
Is EP Hard Disk Common Criteria certified?	Yes
Is EP Hard Disk FIPS 140-2 compliant?	Yes
<b>Core Features</b>	
What is the maximum disk size that can be encrypted?	1 terabyte (up to 8 partitions)
Does EP Hard Disk provide mandatory pre-boot access control?	Yes
Does EP Hard Disk provide boot sector protection?	Yes
Is EP Hard Disk compatible with anti-virus software?	Yes
Is EP Hard Disk compatible with all applications that run on Windows?	Yes
Does EP Hard Disk offer 100% protection of the Windows operating system?	Yes
Does EP Hard Disk offer 100% protection of applications and data?	Yes
Can EP Hard Disk be configured to encrypt the full disk, including unused sectors?	Yes
Can EP Hard Disk be configured to encrypt only the sectors of the disk that are in use?	Yes
Can EP Hard Disk encrypt temp, swap and page files in addition to all unused space?	Yes
Can EP Hard Disk encrypt separate partitions?	Yes (up to 8 partitions)
Does EP Hard Disk support Single Sign-On for Windows?	Yes
Does EP Hard Disk support Single Sign-On for Novell?	Yes
Does EP Hard Disk support Single Sign-On for Active Directory, NT Domains and PW Sync?	Yes
EP Hard Disk support hibernation?	Yes

<b>Administration</b>	
Does EP Hard Disk include an enterprise component that permits centralized configuration and management of security policy?	Yes. The console is called the Administrator Program.
Does the Administrator Program permit remote, centralized control over users' security settings, both individually and globally?	Yes
Can the EP Hard Disk Administrator remotely change any Corporate or Local Administrator's privileges?	Yes
Does the Administrator Program allow the administrator to remotely change any user's privileges, including expiring a user's account?	Yes
Is a separate server program required to run the Administrator Program?	No
If desired, is an <i>optional</i> server program available that will automate management of the user community?	Yes. <b>Encryption Plus Management Console</b>
Are professional or engineering support services required to configure or deploy the User Program or updates?	No
Are <i>optional</i> Professional Services available from PC Guardian Technologies Inc?	Yes
<b>Encryption Keys and Key Recovery</b>	
Does EP Hard Disk create a unique encryption key for every computer?	Yes
Does EP Hard Disk store the user's encryption key or password in plain text on the hard drive?	No
Does the EP Hard Disk Administrator Program generate unique encryption keys for every local administrator?	Yes
Does EP Hard Disk store the computer's encryption key on the hard drive in plain text?	No
Does EP Hard Disk provide different levels of administrative recovery?	Yes
Does the program offer Remote Web-based administrative recovery?	Yes
Does the program offer remote One-Time Password administrative recovery?	Yes
Is any additional software or hardware required to take advantage of Remote Web-based recovery?	No
Does EP Hard Disk allow users to securely authenticate themselves to their PCs to recover forgotten passwords, requiring these users to reset these passwords (self-service key recovery)?	Yes
Can rescue disks be created for each user to support emergency recovery?	Yes

<b>Installation</b>	
Can the User Program be deployed using common electronic distribution tools (i.e., SMS, Tivoli, etc.) to multiple users, simultaneously?	Yes
Are other installation methods available?	Yes These include local, command line or script and pre-encrypting PCs before they have been distributed
Can EP Hard Disk be configured to force the installation of EP Hard Disk onto any user's PC, no matter where the user is on the network?	Yes
Can the User Program be installed while users are working on their PCs, regardless of location (i.e., <b>Background Encryption</b> )?	Yes
Is there a noticeable degradation in performance when EP Hard Disk is running?	No
Can the User Program be installed without requiring users or administrators to be present to respond to installation and reboot prompts?	Yes
Can users adjust initial encryption speeds during installation in order to draw upon more CPU resources while initial encryption takes place?	Yes
Can initial encryption withstand power interruptions without data loss?	Yes
Will the initial encryption process resume where it left off after power interruptions?	Yes
Can users shut down their computers during Initial Encryption without having to re-initiate the encryption process when they re-boot their PCs?	Users never have to re-initiate the Initial Encryption process. Initial Encryption will always pick up where it left off.
<b>Updates and Version Upgrades</b>	
Can updates and version upgrades be deployed using common network installation tools?	Yes
Can updates and upgrades be installed without requiring the drive to be decrypted and without uninstalling the previous version?	Yes
<b>Miscellaneous</b>	
Does EP Hard Disk generate audit logs for each user?	Yes
Can Administrators view EP Hard Disk log files from a central location?	Yes.
Is there a version of EP Hard Disk that supports Japanese language?	Yes
Does EP Hard Disk offer multi-language keyboard support?	Yes, including variants: English, Danish, Finnish, French, German, Italian, Japanese, Spanish, Norwegian, Swedish, Portuguese