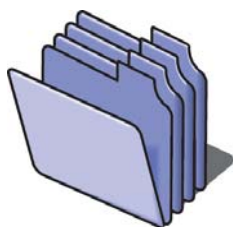


# Encryption Plus® Folders

*Powerful security. Simple to use. Superior service & support.*



**folders**

Encryption Plus® Folders protects data in administrator- and user-selected folders and subfolders. It includes centralized administrative tools for managing user passwords and provides administrators with multiple methods of recovering encrypted data when necessary.

Encryption Plus Folders is easy to configure, distribute, and modify over a network. The software supports Single Sign-On, allows multiple users to share encrypted folders on a single computer, and encrypts folders on removable media.

Also Encryption Plus Folders features GuardianEdge's unique Authenti-Check® self-service password reset program, which eliminates administrative costs due to forgotten passwords.

## **BENEFITS OF ENCRYPTION PLUS FOLDERS**

---

**Protect Your Data With a Powerful Algorithm**—Encryption Plus Folders uses the durable and trusted Blowfish algorithm, a fast block cipher, and includes a strong 192-bit encryption key.

**Removable Media**—In addition to protecting folders on the hard drive, users can encrypt folders on removable media. This capability is especially valuable when two or more users need to securely exchange or share data, as well as for backing up data and encrypting it for safe, long-term storage.

**Easy Installation & Use**—Encryption Plus Folders requires minimal administration and user training. It is completely transparent to users, requiring no change in the way they work.

**Maximize Security, Minimize Risk**—Encryption Plus Folders transparently protects data with a true on-the-fly encryption process that decrypts only the specific portion of a file that is in use. Other products that claim to be “on the fly” decrypt an entire file and load it into memory, creating significant security risks.

**Expand to Multi-User Encryption on Single Computers**—Encryption Plus Folders enables two or more users to share encrypted folders on a single computer. With an easy point-and-click method, a user can choose to share selected folders with any of the other users listed on that computer.

**Simplify the Login Process**—Once integrated into the network login, Encryption Plus Folders no longer requires users to separately login to Encryption Plus Folders.

**Full Key Recovery**—Encryption Plus Folders' key recovery feature ensures that system and local administrators can easily restore any encrypted files—even if the password has been forgotten.



**Encryption Plus Folders User Main Menu**

## Typical Installation and Usage

- 1 The administrator installs Encryption Plus Folders Administrator on his or her workstation, sets user settings, creates a User Install Program, and identifies folders that must be encrypted.
- 2 Users install Encryption Plus Folders on their workstations and select, if desired, additional folders for encryption on the hard disk.
- 3 Each day, EP Folders prompts the user for a user name and password. Alternatively, the password login process can be integrated with network login (Single Sign-On).
- 4 As files located in the encrypted folder are accessed, they are automatically decrypted with no user intervention. Likewise, the files are automatically re-encrypted as they are written back to the hard disk.

## Password Management

Administrators can configure how users manage their Encryption Plus Folders passwords using the software's optional Password Management features. Password Management allows administrators control over Password Expiration, Minimum Password Length, and

Password Re-Use. Also, administrators can require the use of Special Characters in passwords to make them more difficult to guess.

Administrators can set Encryption Plus Folders to automatically "lock out" users after a predetermined number of unsuccessful logon attempts.

## Forgotten Passwords

When users forget passwords, they can easily and securely regain access to their computers with GuardianEdge's Authenti-Check® challenge/response self-service password recovery feature. Authenti-Check can be set to require users to answer up to three secure questions, which can be defined by the administrator, the user, or both.