

McAfee Endpoint Encryption for Files and Folders

Encrypt data automatically for secure sharing, transporting, and storing

Digital files and folders often contain vast amounts of confidential company and compliance related data. In their digital format, this valuable data is easy to share, store, and, unfortunately, lose or leak to unauthorized parties. The risk of a data breach is real, and the consequences can be expensive and far-reaching, including loss of competitive advantage and intellectual property. McAfee® Endpoint Encryption for Files and Folders delivers policy enforced, automatic, transparent encryption of files and folders stored or shared in PCs, file servers, emails, and removable media (for example, USB drives and CD/DVDs).

The McAfee ePolicy Orchestrator® (McAfee ePO™) management infrastructure works with McAfee Endpoint Encryption for Files and Folders and enables centralized deployment, management, policy administration, password recovery, monitoring, reporting, and auditing from a single console. McAfee ePO software works for endpoint encryption, data loss prevention (DLP), and other McAfee security products for ease of management, consistent protection, holistic visibility, and low total cost of ownership.

Key Features and Benefits

Multiple storage and sharing options

Encrypts data on local disks, file servers, removable media, and in email attachments (whether or not the recipient has McAfee encryption software), providing storage and sharing options to meet a wide range of needs.

Policy-based, scalable encryption

Encryption is automatically deployed in accordance with the organization's information security policy and can be set differently for separate individuals, groups, or entire companies. Encryption policies are created using McAfee ePO software and can be assigned to users based on information from Microsoft Active Directory. Encryption keys are generated and managed centrally using McAfee ePO software. Users can not override policies.

Automatic, always on encryption

Encryption follows the document when transferred between storage media which ensures that the data remains secure without user interaction. The encryption information travels with the file in a "file header." Files are encrypted when they are created which prevents hidden data leakage through plaintext temp files or system page files (virtual memory from the hard disk), for example. Encryption is retained when copying, moving, and editing files on supported storage media.

Transparent end-user experience

Encrypted documents keep original file extension and still appear as "normal" to the authorized end-user with a minimum of user interaction. The user authentication is fully integrated with the Microsoft Windows logon, meaning that any authentication token used for the Windows logon is automatically supported by McAfee Endpoint Encryption for Files and Folders, yielding a completely transparent and simplified end-user experience.

Granular flexibility

Granular options to encrypt individual documents, entire folders, locations, and/or file types provides more effective selection of valuable data to encrypt based on policies, while also allowing the end user to encrypt additional files on demand.

Encrypted document sharing

Authorized users can easily share encrypted documents among individuals or within groups due to the centralized key management in McAfee ePO software. The encryption and decryption happens on the fly on the client side when accessing and saving protected documents. Self-extracting files can be used for email attachments so the recipient doesn't need to install any software in order to read the encrypted attachment.

Removable media encryption

Data on the portions of or entire standard off-the-shelf USB and other removable storage devices can be encrypted, modified, and saved on the device with separate authentication and retained encryption yet without needing any software installation or local administrative rights on the device host. No files are left on the host PC because wiping is built in. Multiple, configurable protection, authentication (password, CAC, or PIV smart cards), and recovery methods can be used. Separately, McAfee also offers hardware-encrypted USB flash and hard drives.

How It's Used

Protect removable media

Off-the-shelf USB devices are small and inexpensive, so they're easy to misplace or lose. With policy-based encryption and McAfee ePO software, it's quick and easy to enforce organization-wide encryption policies for removable media to mitigate the risk of data loss. Encrypting removable media still permits the media to be used by the authorized owner outside the organization for retained portability.

Protect local data

McAfee Endpoint Encryption for Files and Folders offers PCs an extra level of protection for sensitive data stored on a PC's hard disk, whether the computer is on or off.

Protect data on network shares

If a cybercriminal somehow gets into your network, having files and folders separately encrypted provides an extra layer of protection, so even if they get the file or folder, the data it contains is unreadable and unusable to unauthorized parties. If that isn't enough, you can even stack separately encrypted files in separately encrypted folders for even more security.

Securely share data with third parties

When collaborating with partners, contractors, or other third parties, use encrypted files and folders—just in case they aren't quite as careful with your company's confidential data as you are.

Summary

Without proper authentication, an encrypted document is unreadable (encrypted "X&@W*E#x3") instead of easily readable ("the key secret ingredient in our formula is ..."). When files, folders, removable media, or email attachments contain company confidential or compliance-related data, one of the best ways to protect that data wherever it goes is with encryption.

McAfee offers a wide range of endpoint encryption solutions plus centralized management and much more to provide comprehensive, managed data protection that is easily customized to protect your company's most valuable data assets.

System Requirements

McAfee ePolicy Orchestrator 4.5 P4 or higher

Supported client platforms:

- Microsoft Windows XP, 32-bit
- Windows Vista 32-bit
- Windows 7, 32/64-bit

Supported algorithms:

- AES 256 bits, FIPS 140-2

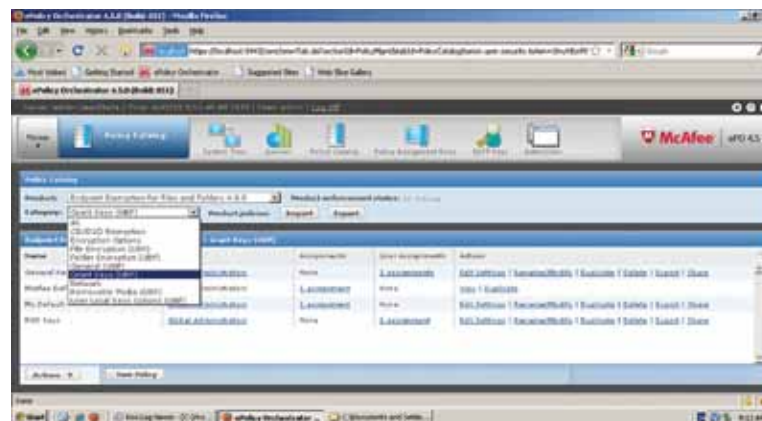


Figure 1. Policy options in the McAfee ePO management console.

