



Policy-based End Point Encryption

Echoworx Encrypted Documents

Product Overview

Encrypted Documents gives businesses the ability to manage the way that sensitive data is stored in their enterprise infrastructure. Data in an Encrypted Documents file or folder is encrypted so that only the owners of the data and individuals authorized by these owners have access to it. Businesses now have the flexibility of sharing information securely and easily with others, including individual and groups (such as finance, human resources or the legal department), and at the same time complying with the growing number of privacy and data protection laws and regulations.

Data Loss and Leakage Prevention

This fully-hosted solution gives businesses the ability to easily augment their data protection safeguards with the encryption of data at rest on their employees' desktops, laptops, removable storage media and file servers, as well as data in transit. IT Administrators can set policies to automatically encrypt data, reducing the risk that employees may forget to encrypt and protect sensitive data. For example, policies can be set to automatically encrypt data on an employee's computer; encrypt all office documents; and encrypt files stored on selected public file server folders.

Encrypted Documents automates the decision to encrypt data according to the business' defined data privacy policies. The encryption is completely transparent to the end users. IT Administrators are able to add and remove policies through the Administration Console, which fall under the following categories:

Encrypt by Folder – For example, encrypt all files in users' 'My Documents' folders.

Encrypt by File Type – For example, encrypt all Microsoft Office file types (.pptx, docx, .xlsx). Particular files (like .mp3 or .wma) can be added to an 'exclude list' so they are never encrypted.

Data Loss Prevention Management – Enforce data loss prevention through policies:

- Auto Encrypt - Unique policies can be configured based on file type or folder location.
- Data Loss Protection- Data cannot be copied to a USB device or can be copied based on authorization e.g., password.

Benefits

Enterprise Integration

No changes are required to existing storage or networking infrastructure

Simple to Use

Automatic policy-based encryption and data loss prevention enforcement are transparent to end users

Dynamic Product Labeling

White labeled version available for business to apply their branding and look-and-feel

Simple Deployment

Standard MSI package allows for quick and easy deployment of pre-configured client

Enterprise Architecture

Unlimited scalability and high availability service

Simple Administration

Administration Console provides easy access to manage end users and encryption policies

Standards Based

Industry standard encryption including digital signatures, PKI, RSA, and AES

Certificate Authority

No need to deploy and maintain expensive third party PKI or Certification Authorities

Always On Encryption

Files and folders remain encrypted at rest and in transit

Features

Data Loss Prevention

Control how users send, access, and store sensitive data over the network, through applications, and onto storage devices:

- User determined encryption
- Automated and transparent policy-based encryption
- Data loss prevention policies that prevent files from being moved to unauthorized devices such as USB

Enterprise-grade Administration

- Add and remove users
- Manage file, and folder automated encryption policies
- Manage data loss prevention strategies
- Control users' ability to change or add policies

Persistent File and Folder Encryption

- Files and folders remain encrypted when not in use
- Only authorized users are able to decrypt and access encrypted files and folders

Enterprise-Grade Device Encryption

- File and folder encryption support for standard algorithms, including AES-256 and the use of RSA-1024 bit keys

About Echoworx

Echoworx is a provider of security solutions for enhancing privacy and trust in digital communications. Echoworx privacy applications leverage the power of Echoworx Encryption Services (EES) platform, which is hosted at Secure Data Centers. All data is encrypted using industry trusted standard PKI (Public Key Infrastructure) and S/MIME technologies for strong encryption and digital signatures, relying on standard X.509 certificates. Echoworx data privacy applications include: Encrypted Mail, Policy-based Encryption Gateway, Encrypted Documents, Encrypted Document Presentment, and Encrypted Message eXchange. Echoworx products are currently offered by leading communication providers that include: AT&T, BT, LogicaCMG, Telus, and Verizon.

Technical Requirements

Administration Console

Operating System

Microsoft Windows XP 32-bit
 Microsoft Windows Vista 32-bit
 Microsoft Windows 2000
 For Windows Vista, XP and 2000, you are required to have administrative privileges.

Web Browser

Microsoft™ Internet Explorer® 6.0 or above

Internet Connection

LAN-based using standard TCP/IP
 DSL, ADSL, Cable Modem
Computer Hardware
 5-10 MB of hard drive space
 Pentium 233 MHz or greater
 128 MB RAM or greater

Encrypted Documents

Operating System

Microsoft Windows XP 32-bit
 Microsoft Windows Vista 32-bit
Web Browser
 Microsoft™ Internet Explorer® 6.0 or above

Internet Connection

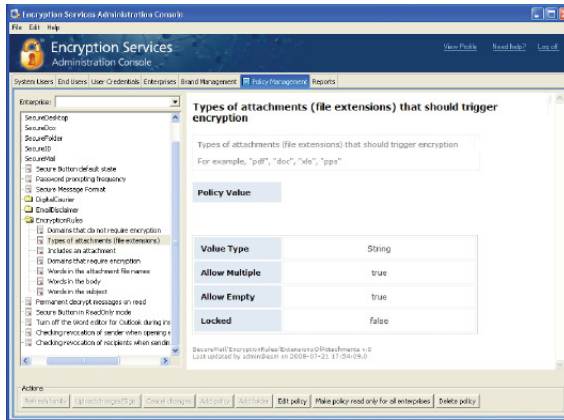
LAN-based using standard TCP/IP
 DSL, ADSL, Cable Modem

Computer Hardware

Pentium 1.6 GHz or greater
 1 GB RAM or greater
 10 MB of hard drive space for Encrypted Documents installation
 NTFS, FAT, FAT32 and CIFS

End User Experience

With Echoworx Encrypted Documents, businesses have the power to enforce encryption across all data whether it resides on a laptop, network drive or removable media device such as a USB key. All data in files and folders is protected at all times. Permissions for read and write privileges are controlled by the company's authorized IT administrator to further control data loss or leakage.

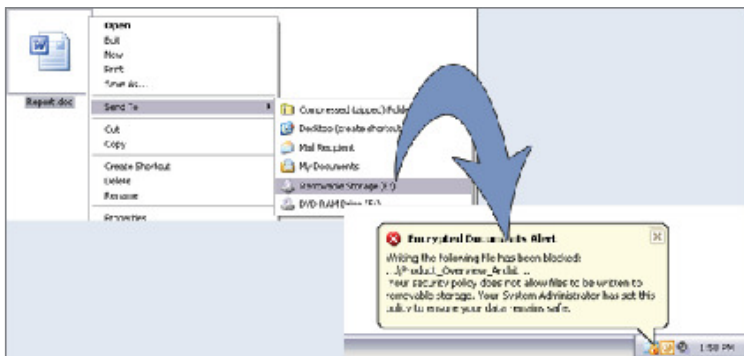
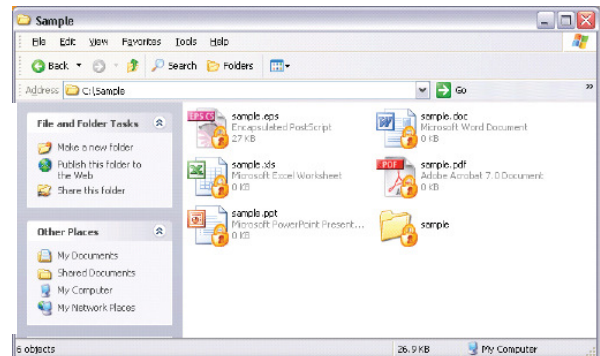


End User Management

With Echoworx Encrypted Documents, businesses have the power to enforce encryption across all data whether it resides on a laptop, network drive or removable media device such as a USB key. All data in files and folders is protected at all times. Permissions for read and write privileges are controlled by the company's authorized IT administrator to further control data loss or leakage.

End User Experience

Policy-based encryption is automatic and transparent to the user. Files and folders are encrypted automatically according to the policies and appear in the file system with a golden lock. The IT Administrator determines businesses encryption policies through the Administration Console.



DLP Management

Data Loss Prevention policies prevent users from copying files or folder onto authorized devices. When a user attempts to copy a file to a restricted device, a pop-up message appears with information on the related policy. The company enforces the DLP strategy through the Administration Console.

For more information contact Echoworx at 1.888.697.3246 or visit us at www.echoworx.com