

Save Secure, Send Secure with SecureZIP®

Files that contain sensitive data need to be protected. Whether stored on a PC or sent via email, SecureZIP® makes securing these files an effortless task. SecureZIP is the industry-leading security and compression utility, combining encryption and digital signing functionality with ZIP file management and compression. The additional benefit of cross-platform compatibility makes it the ideal solution for exchanging data within the enterprise.

Save and send files securely from Microsoft Office

SecureZIP's integration with Microsoft Office allows you to save zipped and encrypted files directly to your storage media from Word, Excel, or PowerPoint. By simply selecting "Save as Secure ZIP File," your files are compressed and encrypted automatically.

SecureZIP's integration with Microsoft Office and Outlook also allows users to send zipped and encrypted files as email attachments directly from Office applications.

Maintain control of organizational data*

Files that have been encrypted must remain accessible to an organization. When end-users are given the ability to encrypt sensitive data, SecureZIP's contingency key capabilities ensure that whatever is encrypted is accessible for audit or data recovery purposes.

Contingency key processing ensures SecureZIP customers can meet the need of auditors, compliance officers, or regulators to inspect or recover encrypted data - even if a passphrase is forgotten or a decryption key lost - while still strongly protecting the data.

Centrally administer security policies*

SecureZIP's policy manager functionality enables organizations to lock down encryption controls to reflect their data security policies and practices in a manner that users cannot circumvent.

Administrators can create and manage multiple SecureZIP policies via the familiar Microsoft Management Console (MMC). This provides more flexibility with less effort, ensuring organizational encryption policies are adhered to.

Encrypt files using passphrases, X.509 digital certificates, or both

SecureZIP supports both passphrase- and X.509 digital certificate-based encryption, offering flexible security that meets varying requirements within business environments. In comparison to passphrases, digital certificates offer higher levels of security, are easier to use, and allow secure communication with larger numbers of recipients. Passphrases provide a good alternative when someone doesn't have a digital certificate.

In addition, when run in "FIPS mode," SecureZIP allows government agencies and their business partners to meet FIPS 140 compliance

Features and Benefits

Save and send files securely from Microsoft® Word, Excel®, and PowerPoint® via seamless integration with Microsoft Office®

Automatically compress and secure emails and attachments in Microsoft Outlook®

Centrally administer security policies, ensuring organizational encryption policies are adhered to*

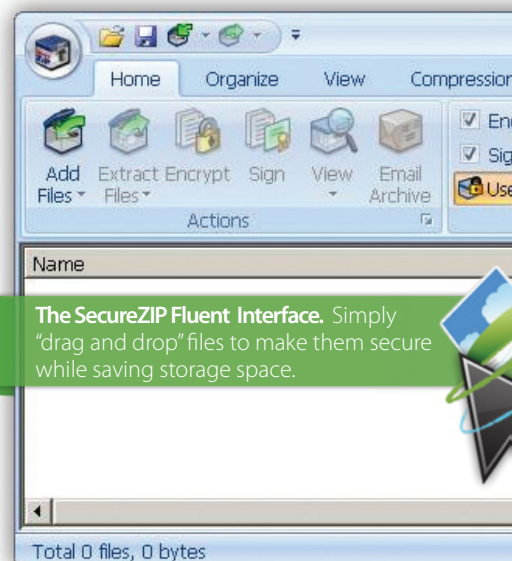
Maintain control of organizational data for audit and recovery purposes with contingency key*

Encrypt files using passphrases, X.509 digital certificates, or both

Includes easily deployable digital certificate (license purchase up to 200 users)*

Operates on all major computing platforms, allowing seamless data transfer between operating systems, including z/OS®, i5/OS®, UNIX®/Linux® server, and Windows® server and desktop

*Feature available in SecureZIP Enterprise Edition



requirements by protecting sensitive data using cryptographic modules.

Includes easily deployable digital certificate*

SecureZIP makes acquiring and using a digital certificate simple, allowing you to exchange files and emails securely. Upon installation, SecureZIP will automatically request and install (if desired) a digital certificate from one of the industry's leading certificate authorities, Comodo®.

Once a user's digital certificate is installed, people can send protected files and emails, securing them with the recipient's public key. Once the secure communication is received, SecureZIP uses the recipient's private key for decryption. Digital certificates are also used for signing, which assures recipients that the communication can be trusted.

? How does a digital certificate work?

Digital certificates attest to the identity of a person and are usually associated with an email address and a key pair, referred to as public and private key. A public key is used to encrypt and a private key is used to decrypt.

Public Key

- Encrypts
- Validates



- Decrypts
 - Authenticates
- #### Private Key

When someone sends a message or file, they use the recipient's public key to encrypt it. When the message or file is received, the recipient's private key automatically decrypts it. A private key is also used to "sign," or authenticate a message or file to ensure that a recipient knows it came from a trusted sender.

Note: SecureZIP Enterprise Edition includes a free digital certificate with a license purchase of up to 200 users.

The SecureZIP Global Directory is a depository of public keys for SecureZIP users, making it easy to send secure files with digital certificates. When a secure email is sent using a digital certificate, SecureZIP checks the Directory for the public key associated with the recipient's email address. If the recipient doesn't have a digital certificate, the message can still be secured with a passphrase.

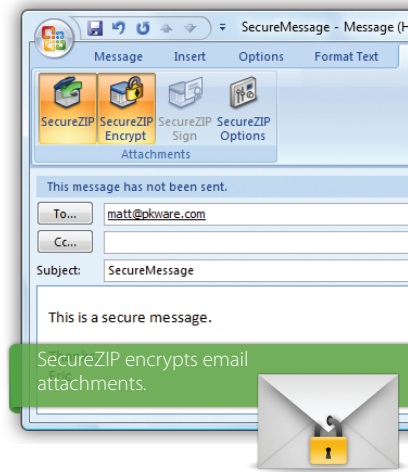
Automatically compress and secure emails and attachments

SecureZIP integrates with Microsoft Outlook; emails and attachments sent using this application are secured automatically or on an individual basis. Users can also re-encrypt messages and attachments when forwarding emails to others.

In addition, SecureZIP's advanced compression reduces file size, eliminating the problems associated with sending large email attachments that exceed mail system size limits. Sending secure emails is simple: write an email, attach files, and with a click of a button users can quickly and efficiently send secure messages.

About PKWARE

PKWARE, Inc., the creator and continuing innovator of the ZIP standard, is a global market and technology leader providing data-centric, cross-platform data security and compression software. The SecureZIP & PKZIP product families are used by over 30,000 corporate entities and over 200 government agencies to ensure data security, portability, and cross-platform computing exchange - both internally and externally with partners. Organizations use PKWARE products daily for their unmatched scalability, ease of use, and rapid deployment. PKWARE, a privately held company, is based in Milwaukee, WI with additional offices in New York and the United Kingdom.



System Requirements

Operating System	Memory (RAM)	Hard Disk Space	Additional
SecureZIP Standard Edition			
Windows 2000 SP4 and higher with IE 6.0 or above	128 MB RAM (256 MB recommended; 512 MB on Vista & Windows 7)	For 32-bit versions: 28 MB of free HD space For 64-bit versions: 33 MB of free HD space	For seamless Office/Outlook integration – Office/Outlook 2002 or later
SecureZIP Enterprise Edition			
Windows 2000 SP4 and higher with IE 6.0 or above	128 MB RAM (256 MB recommended; 512 MB on Vista & Windows 7)	For 32-bit versions: 28 MB of free HD space For 64-bit versions: 33 MB of free HD space	For seamless Office/Outlook integration – Office/Outlook 2002 or later Microsoft Management Console v1.2 or later Windows 2000 SP4 and higher with IE 6.0 or above or Windows Server 2003 or later

United States
 648 N. Plankinton Ave.
 Suite 220
 Milwaukee, WI 53203
 1.888.4.PKWARE
 www.pkware.com

UK/EMEA
 Crown House
 72 Hammersmith Road
 London W14 8TH
 United Kingdom
 +44 (0) 207 470 2420

