

## Save Secure, Send Secure with SecureZIP

Files that contain sensitive data, whether stored or sent via email, need to be protected. SecureZIP makes securing these files an effortless task. SecureZIP is the industry-leading security and compression utility that zips and unzips files, greatly reducing email and FTP transmission times while securely protecting data in transit or at rest.

### SecureZIP for Windows

- Seamlessly integrates with Microsoft Office<sup>®</sup> - save and send files securely
- Automatically compress and secure emails and attachments in Microsoft Outlook<sup>®</sup>, Outlook Express<sup>®</sup>, and Windows Mail<sup>®</sup>
- Access encrypted files for audit and recovery purposes with contingency key
- Supports passphrases and X.509 digital certificates
- Includes easily deployable digital certificate<sup>1</sup>

### Automatically Compress and Secure Emails and Attachments in Microsoft Outlook, Outlook Express<sup>®</sup>, and Windows Mail<sup>®</sup>

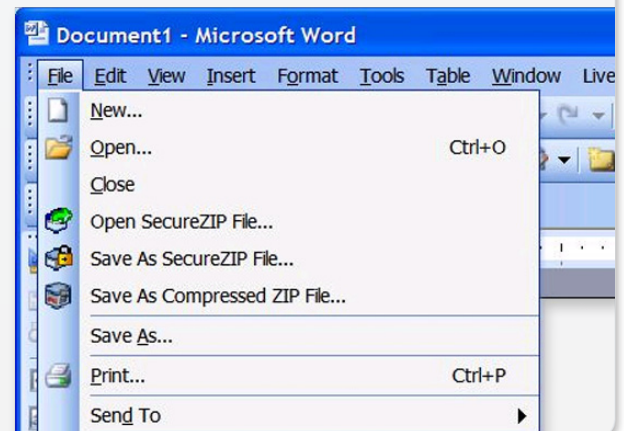
SecureZIP makes Outlook a secure email application. Emails and attachments are secured automatically or on an individual basis. You can also re-encrypt messages and attachments when forwarding emails to others. In addition, SecureZIP's advanced compression eliminates the problems associated with sending large email attachments that exceed mail system size limits. Sending secure emails is simple: write your email, attach your files, and with a click of a button you can quickly and efficiently send secure messages.

### Access Encrypted Files for Audit and Recovery Purposes with Contingency Key

Files that have been encrypted must remain accessible to your 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.

### Seamlessly Integrates with Microsoft Office - Save and Send Files Securely

SecureZIP's integration with Microsoft Office allows you to save secure files directly to your storage media from Word<sup>®</sup>, Excel<sup>®</sup>, or PowerPoint<sup>®</sup>. By simply selecting "Save as SecureZIP File," your files are compressed and encrypted automatically.



### Available for All Major Computing Platforms

PKWARE, the inventor and innovator of the ZIP standard, is the industry leader in delivering scalable compression and security solutions for the enterprise, supporting all major computing platforms including desktop, server, midrange and mainframe systems.

## Supports Passphrase and X.509 Digital Certificates

SecureZIP supports both passphrase and digital certificates, 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.

## Includes Easily Deployable Digital Certificate

SecureZIP makes acquiring and using a digital certificate simple and easy, allowing you to exchange files and emails securely. Upon installation, SecureZIP will automatically request and install (if desired) a digital certificate<sup>1</sup> from one of the industry's leading certificate authorities, Comodo.

Once your digital certificate is installed, people can send you secure files and emails, securing them with your public key. When you receive the secure, encrypted communication, SecureZIP uses your private key to decrypt. Digital certificates are also used for signing, which assures recipients that the communication has come from you and can be trusted.

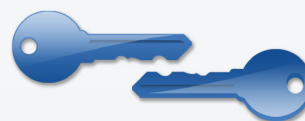
The SecureZIP Global Directory is a depository of public keys for SecureZIP users, making it easy to send secure files with digital certificates. When you send a secure email using a digital certificate, SecureZIP checks the Directory for the public key associated with the recipient's email address.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

### How Does My 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



#### Private Key

- Decrypts
- Authenticates

When someone sends you a message or file, they use your public key to encrypt it. When you receive the message or file, your private key automatically decrypts it. Your private key is also used to "sign," or authenticate a message or file to ensure that a recipient can trust it came from you.

	Standard Edition	Enterprise Edition
Save and send secure documents directly from Microsoft Office	✓	✓
Outlook, Outlook Express, and Windows Mail email integration encrypts emails and attachments	✓	✓
Encrypt using passphrases, digital certificates, or both	✓	✓
Contingency key capabilities for data recovery and audit purposes		✓
LDAP directory support		✓
LZMA and PPMd Support	✓	✓
SecureZIP Global Directory support	✓	✓
Supports x.509 digital certificates	✓	✓
Includes digital certificate for higher security and ease of use <sup>1</sup>		✓
Policy management and rules enforcement		✓

<sup>1</sup>SecureZIP Enterprise Edition includes easily deployable digital certificate with license purchase up to 200 users. Software versions are available that let the user automatically install the digital certificate when prompted.

### System Requirements

#### SecureZIP

13 MB of free HD space  
 128 MB RAM (256 MB recommended; 512 MB on Vista)  
 Windows 2000 SP4, XP SP2, or Vista running Internet Explorer 6.0 or later  
 For seamless email integration – Outlook 2002 or later (Outlook 2002 requires Office XP SP1)  
 For seamless Office integration – Office 2002 or later

#### SecureZIP Enterprise Edition

SecureZIP requirements, including the following for policy management:  
 Microsoft Management Console v1.2 or later  
 Windows 2000 SP4, XP SP2, Vista or Windows Server 2003