Protect data exchange and archiving processes

Files that contain sensitive data, whether stored or being transmitted, need to be protected. SecureZIP® makes securing these files an effortless task. SecureZIP is the industry-leading security and compression utility that greatly reduces transmission times and required storage space while securely protecting data, in transit and at rest. The additional benefit of cross-platform compatibility makes it the ideal solution for exchanging data within the enterprise.

ACCESS ENCRYPTED FILES FOR AUDIT AND RECOVERY PURPOSES WITH CONTINGENCY KEY*

Files that have been encrypted must remain accessible to the organization. When files have been encrypted with PKI and/or passphrases, SecureZIP's contingency key capabilities ensure that encrypted data is accessible for audit or data recovery purposes.

EXCHANGE DATA SECURELY ACROSS DESKTOP, SERVER, MIDRANGE, AND MAINFRAME SYSTEMS

SecureZIP is available on all major platforms and supports secure data exchange between Windows® desktops, UNIX®/Linux® and Windows servers, i5/OS midrange, and z/OS mainframe operating systems. SecureZIP automatically converts data to the appropriate format based on the type of system it is being transferred to.

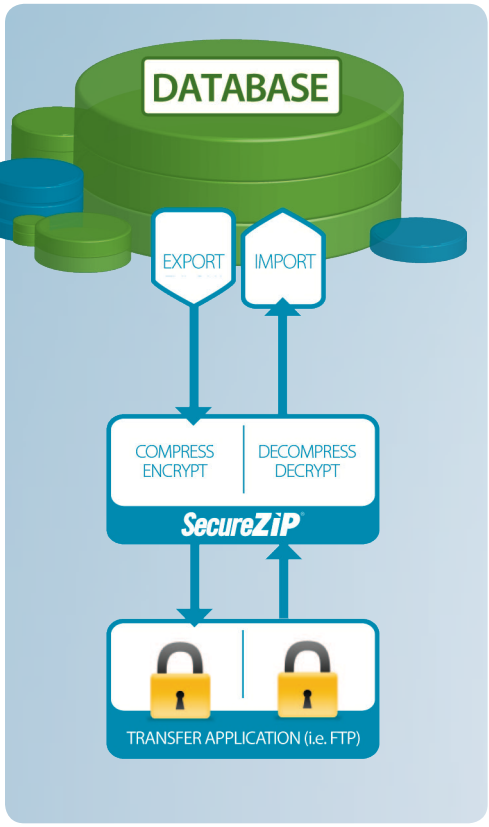
PKWARE is the only single-source vendor for data compression and security products across all major enterprise operating systems.

AUTOMATICALLY DISTRIBUTE FILES FROM SERVER TO DESKTOP

By creating self-extracting files (PKSFX®), encrypted and compressed archives sent from servers are automatically decrypted and decompressed onto desktops. This process is simple for desktop users, requiring just a few clicks, allowing for quick and easy transfer of files to desktop systems. Note: PKSFX is licensed for internal use only.

PROCESS ENCRYPTED DATA WITHOUT STAGING DECRYPTED DATA TO DISK

SecureZIP with Application Integration decrypts data and streams it directly to the application without staging it to disk. After the application completes processing, it can then stream the data to SecureZIP for encryption – once again, unprotected data is never staged to disk.



FEATURES AND BENEFITS

- Conserve storage space and reduce file transfer time
- Process encrypted data without staging decrypted data to disk
- Access encrypted files for audit and recovery purposes with contingency key*
- Encrypt data using passphrases, PKI, or both
- OpenPGP support ensures data can be easily shared with business partners regardless of the partners' data security preference or computing platform
- Apply added data protection by using smart cards and smart tokens (available on Windows server only)
- Automatically distribute files from server to desktop
- Verify documents have not been altered by using digital signatures
- Operates on all major computing platforms, allowing seamless data transfer between operating systems, including z/OS®, IBM i, UNIX®/Linux® server, and Windows® server and desktop

*Feature included with SecureZIP Server Enterprise Edition

ENCRYPT DATA USING PASSPHRASES, PKI, OR BOTH

SecureZIP supports both passphrase- and PKI-based methods of 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 an alternative when the intended recipient does not have a digital certificate.

VERIFY DOCUMENTS HAVE NOT BEEN ALTERED BY USING DIGITAL SIGNATURES

SecureZIP enables users to sign files with their unique digital certificates. Recipients of signed files can validate the signature to ensure the sender is who they claim to be and verify that the document has not been altered or tampered with since signing. In addition, digital signatures offer non-repudiation - the signer cannot later claim that the signature is invalid.

APPLY ADDED DATA PROTECTION BY USING SMART CARDS, SMART TOKENS, AND TIMESTAMPING

SecureZIP's support for smart cards and smart tokens (available for Windows server) enables security professionals to apply an added layer of data protection by storing the user's private decryption key on a small portable device. Smart cards and smart tokens also enable two-factor authentication, requiring the user to present two credentials before they can access protected data, such as a passphrase and a private key stored on a portable device.

About PKWARE, Inc.

The PKWARE Solution is the only complete system for reducing, moving, storing and securing data across the extended enterprise, both internally and externally, from mainframes to servers to desktops and into the cloud. Used by more than 30,000 corporate entities and over 200 government agencies, PKWARE is the industry standard for portability, ensuring data security and cross-platform computing. PKWARE, a privately held company, is based in Milwaukee, WI with additional offices in New York and the United Kingdom.

For additional information and resources, please visit our website: www.pkware.com

To speak with a PKWARE Specialist in the U.S., call toll free: 1.866.583.1795

To speak with a PKWARE Specialist outside the U.S., visit www.pkware.com/contact for specific country offices and contact information

SYSTEM REQUIREMENTS

WINDOWS

Enterprise Edition Note: SecureZIP Server for Windows is only available in Enterprise Edition.

- Windows 2003 and higher with IE 6.0 or above
- 256 MB RAM (512 MB recommended)
- 15 MB available disk space
- **Enterprise Edition:** Microsoft Management Console v2.0 running on Windows Server 2003 or later

SOLARIS®

- Solaris 8 or greater on UltraSPARC
- Solaris 10 or greater on x86
- 64 MB RAM (128 MB recommended)
- 20 MB available disk space
- **Enterprise Edition:** Microsoft Management Console v2.0 running on Windows Server 2003 or later

IBM-AIX®

- 5L Version 5.3 (5300-08) or higher
- 6L Version 6.1 (6100-00) or higher
- 7L Version 7.1 (7100-00) or higher
- **Required xlC packages:** xlC.aix50.rte 11.1.0.2 or later, xlC.rte 11.1.0.2 or later
- 64 MB of RAM (128 MB recommended)
- 28 MB available disk space
- **Enterprise Edition:** Microsoft Management Console v2.0 running on Windows Server 2003 or later

HP-UX®

- 11iv1 (PA-RISC processor only) with patches: PHCO_29903, PHCO_30238, PHCO_33582, PHCO_35743, PHCO_36503, and PHSS_22535
- 11iv2 or higher with patches: PHSS_39821, PHSS_39897 and PHSS_40537
- 11iv3 or higher with patches: PHSS_39822 and PHSS_40538
- For all HP-UX versions, please install the patches prior to installing PKZIP
- 64 MB of RAM (128 MB recommended)
- 40 MB available disk space
- **Enterprise Edition:** Microsoft Management Console v2.0 running on Windows Server 2003 or later

LINUX®

- RedHat 4 and greater
- SuSE 9 and greater on x86, x86_64, s390, or s390x
- Ubuntu 10.04 (LTS) and greater on x86 and x86_64
- x86_64 requires the 32-bit compatibility libraries for that Linux distribution.
- 64 MB of RAM (128 MB recommended)
- 20 MB available disk space
- **Enterprise Edition:** Microsoft Management Console v1.2 running on Windows Server 2003 or later