FAQs - Unix / Linux Server

Generated: 2016-04-27 22:26:09.205000

Latest Version

V14.50.0010 released March 2019

Version	Release Date
14.50.0010	3/2019
14.41.0008	6/2016
14.40.0035	3/2015
14.40.0027	5/2014
12.5	8/2010
8.7	8/2007

Compatibility

Yes, native 64-bit programs are now available for Windows Server, Linux, and HP-UX on Itanium.

Yes, a problem was detected in the operation of this option setting in versions prior to V12.0. Content of ZIP files created using this option setting was similar to that of either the "-dir" or "-dir=current" options with leading folder information retained that would not be expected if the "specify" sub-option was used. This issue was resolved in V12 and "-dir=specify" now operates correctly.

To avoid problems that can result when files and folders may have the same name, the allowed syntax for specifying a folder to exclude has been updated. Now folders to exclude should be specified using the syntax folder*.**. For example, a folder previously excluded using the folder name of TEMP, now should be specified for exclusion as \TEMP*.**.

In most cases, No. SecureZIP does support using OpenPGP encryption using the standard program syntax of PKZIP / SecureZIP. However, to simplify the transition from your legacy OpenPGP software, you can run SecureZIP in an OpenPGP compatible mode. Two modes are provided that emulate the most common OpenPGP commands. Using one of these modes of operation allows SecureZIP to use your existing scripts for OpenPGP encryption. SecureZIP can emulate EBS.EXE and PGP.EXE command switches.

PKZIP / SecureZIP is supported on Solaris (UltraSPARC and x86), HP-UX (Itanium-only), and IBM AIX. Support for HP-UX on PA-RISC is discontinued beginning with V14.10.0011.

PKZIP / SecureZIP is supported on x86 processors running Ubuntu, RedHat Enterprise Linux and SUSE Linux Enterprise. The Linux version is also available for Linux on z System.

PKZIP / SecureZIP Server is supported on Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2003 R2, and Windows Server 2003. It is not formally supported, but is known to run without issues on Windows Server 2016, Windows Vista and Windows 7 / 8 / 10.

The PKWARE Server products are not formally supported on Desktop operating systems, however they are extensively tested and no known issues exist on most Windows OS's, including Windows 10. We are aware of one issue for users of Windows 8.1 that also have Microsoft Internet Explorer 11 installed. The FTP integration in PKZIP / SecureZIP on this platform does not operate due to an issue reported by Microsoft in the publication 808279 .

No, Currently PKZIP / SecureZIP do not run on this new pre-release operating system from Microsoft.

The PKZIP / SecureZIP Server program itself is a single threaded application. Using system process management functions, separate instances of PKZIP / SecureZIP can be run simultaneously.

No, PKZIP / SecureZIP Server itself does not impose any specific CPU configuration requirements. PKZIP / SecureZIP Server is designed to run under the minimum recommended hardware configuration of the supported operating system.

Basics of Zipping and Unzipping

ZIP (including files with the .zipx extension), TAR, RAR, Gzip, Bzip2, JAR (Java Archive), UUencode, XXencode, BinHex, ARJ, Z, and LHA / LZH. On Windows, CAB files can also be extracted. PKZIP / SecureZIP provides the same interface for extracting from all of these archive types.

ZIP, TAR, Gzip, Bzip2, UUencode, and XXencode.

PKZIP / SecureZIP tries to change the settings of your terminal. When it runs in the background, PKZIP is not able to change the settings, and waits until it can. Using the -silent option will change that behavior, as well as suppress all output. Please read Appendix E of the Users Manual, for more hints and tips on running PKZIP / SecureZIP in the background or from a script.

PKZIP / SecureZIP returns a value to the shell to indicate error status. On UNIX or Linux, one normally checks this by checking the value of $? immediately after running the command. If $? is 0, then everything was all right. On Windows, one checks the errorlevel. If the errorlevel is set to 0, then everything was all right. Please read Appendix B of the Users Manual for more information.

There are several operations for which PKZIP / SecureZIP creates temporary files:Updating an archive: When you update an archive, PKZIP / SecureZIP first creates and updates a temporary copy of the archive. When the update is completed, the original archive is replaced with the updated copy. Data in the temporary file is encrypted if it was encrypted in the archive you are updating. Similarly with new or updated files for the archive: they are encrypted in the temporary file if they are to be encrypted in the updated archive.Creating a spanned archive: A temporary file is created to span an archive in segments across multiple discs or other media. Data in the temporary file is encrypted if it is to be encrypted in the final archive.Extracting an embedded archive: An archive can be embedded in another archive. For example, a ZIP file can contain another ZIP file, or a GZIP archive can contain a TAR archive. The embedded option can be used to extract the files in an embedded archive file directly instead of first extracting the embedded archive itself. In this case, the embedded archive is extracted into a temporary file before its files are extracted. The data in the temporary file is encrypted only if the archive is encrypted. Example1: if outside.zip contains inside.zip, the data in the temporary file is encrypted only if it was encrypted in inside.zip. Example2: if outside.zip contains inside.tar, the data in the temp file is NOT encrypted, as TAR doesn't allow for encryption.Creating streamed archives: When you write an archive to a data streamfor example, to STDOUT (see chapter 3 of the Users Manual for the Server or Command Line productsPKZIP compresses and (if encryption is specified) encrypts the data before writing it to the temporary file. The temporary file is needed to get size information for local headers, which are written out before file data. But the data is already compressed and encrypted when its placed in the temporary file; it never appears on disk unencrypted.

This option appears in V14 help screens when using the -help option. This option is not operational in the software at this time. Please watch for future versions that will enable this capability.

Security and Digital Certificates

When the -shred option is selected in V14 and higher, PKZIP / SecureZIP will first rename the file to be shredded to a temporary name. The name reported during a shred operation will be the renamed temporary file name.

There is a documented issue with using certificates signed using SHA2 if you are using Microsoft Windows 2003 R2 or a 64-bit version of Windows XP. You will need to obtain and apply a Hotfix from Microsoft to resolve this problem. Additional information on this issue is available directly from Microsoft using the following URL, http: / / support.microsoft.com / default.aspx?scid=kb;EN-US;938397. PartnerLink customers providing new Software Distribution Packages (SDP) to their partners should inform them to obtain and apply this Hotfix from Microsoft if they will be using SHA2-signed certificates on the affected platforms.

Your files are only as secure as your password, but that can be a problem sometimes. It is important to make your passphrase easy for you to remember, but hard for anyone else to guess. PKZIP / SecureZIP does not store an archive's passphrase anywhere but inside the file. PKWARE has no special means for getting around the encryption and is not able to assist in the recovery of an encrypted file.

There are several reasons you may be asked to enter a password even though you are using a digital certificate. One reason is that your digital certificate may be protected with two-factor authentication. One form of two-factor authentication uses a password you define to control use of your certificate. This means that in order to use your certificates private key for signing or decrypting, software applications such as PKZIP / SecureZIP can only use it if you grant access to your private key. Providing your password when prompted grants PKZIP / SecureZIP access to use your private key. If you are using a password to protect the private key for your digital certificate, make sure you remember this password just as you would if you were using a password to encrypt a .zip file without a digital certificate.Another reason you may be asked for a password is that your private key is not available. To open a .zip file using your digital certificate, your private key must be available on the machine where you are working.

Your digital certificate resides on the computer where you use it to encrypt and decrypt your .zip files. To ensure you are able to use your certificate after replacing or repairing your computer, you must make sure you have a protected backup of your digital certificate, including your certificates private key. On UNIX and Linux make sure you include your certificates.db files with your routine system backup steps. You can also use the PKCertTool utility to export your certificate in UNIX / Linux. See "The PKCertTool export Command" in Chapter 6 of the User Manual for more information. On Windows, use the Certificate Export Wizard in Windows Internet Options to export your digital certificate. Be sure to export your private key.

No. Both the certificate and private key must be installed to your local system.

Only SecureZIP Enterprise supports using LDAP digital certificates to encrypt archives. See "Accessing Recipients in an LDAP Directory" in Chapter 3 of the Users Manual for more information.

No. A V12 certificates.db file cannot be used directly with V14. Options to assist with migrating your certificates include exporting and importing using the pkcerttool command. Alternatively, the "-upgrade" option to pkcerttool can be used to convert. Use the -help option for more information. Version 14 includes a helper script to assist with this conversion. Run PKCertTool-upgrade.sh. Always backup your V12 certificates file before performing a conversion.

OpenPGP

No, the format for the files used to store encryption group data is inconsistent across vendors and in many cases is not documented by those vendors. Groups used with other OpenPGP products can be easily configured using SecureZIP.

SecureZIP defaults to using AES for OpenPGP (and .ZIP) file encryption. If you have a pre-existing OpenPGP key from your partner, it may not support AES. Try changing the algorithm setting from AES to either CAST5 or IDEA and then resend the file to your partner.

When using the recipient option in V14.0 to specify an encryption key(s), the prompt to enter a passphrase may appear unexpectedly when no password / passphrase was required for the operation. Use the --passphrase setting on the command line to suppress this prompt. Alternatively, this setting can be set within the configured options using:pkzipc config archivetype=pgp --passphrase

PKZIP and SecureZIP support adding file and archive comments for .ZIP files. The OpenPGP format does not natively provide the same capabilities. Using the -header or -comment options when creating an OpenPGP file will not place a comment into the resulting file as they would for a .ZIP file. Including either of these options on your command line when creating an OpenPGP file will not be reported as an error condition and your OpenPGP file will be created, however comment entries will be silently ignored.

When creating a signed OpenPGP or .ZIP file, only one digital signature can be applied to the file. When using the .ZIP format, individual files in the .ZIP archive can include multiple signatures.

Microsoft Crypto API (CAPI) provides storage for X.509 digital certificates which are not required for use with OpenPGP encryption. However, CAPI also provides access to cryptographic algorithms used by PKZIP / SecureZIP regardless of the type of key used. Users of PKZIP / SecureZIP must have appropriate access to Crytopgraphic Server Providers available through CAPI.

Legacy Applications

PKZIP / SecureZIP Windows Server Standard Edition is no longer offered by PKWARE. We recommend that you use PKZIP / SecureZIP Windows Server Enterprise Edition. If you were using Standard Edition on Windows Desktop, and need command line capabilities, you may also try PKZIP / SecureZIP Command Line Interface.