FAQs - zLinux Server

Generated: 2016-04-28 14:47:58.044000

Latest Version

Version 14.40.0027

Compatibility

PKZIP / SecureZIP is supported on RedHat Enterprise Linux 4 or above and SUSE Linux Enterprise 9 or above.

PKZIP / SecureZIP on Linux for z System provides all the same features that are available on x86 Linux servers. Linux software builds and license keys are hardware-specific; therefore, x86 Linux software and licenses will not work on z System, and vice-versa.

Basics of Zipping and Unzipping

ZIP (including files with the .zipx extension), OpenPGP, TAR, RAR, Gzip, Bzip2, JAR (Java Archive), UUencode, XXencode, BinHex, ARJ, Z, and LHA / LZH

ZIP, OpenPGP, 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.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 doesnt 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.

Security and Digital Certificates

Yes, SecureZIP supports standard OpenPGP keyrings and keys. You can use your existing OpenPGP keyrings for creating and opening OpenPGP encrypted files on Linux for z System.

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 archives 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

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.