McAfee eBusiness Server Command Options in SecureZIP Enterprise

If you are transitioning from the McAfee eBusiness Server (EBS), you can use SecureZIP command line Enterprise Edition in OpenPGP Mode to run many of your existing EBS scripts with minimal editing. The commands include ***decrypt***, ***encrypt***, and ***sign***.

You can do this if you're using the legacy PGP.exe application as well, See "Using Legacy PGP Mode."

Using OpenPGP Mode

To enable OpenPGP Mode:

1. Install SecureZIP
2. Copy or Link `pkzipc.exe` to the program name `ebs.exe`.
   To copy and rename pkzipc.exe to ebs.exe:
   copy pkzipc.exe <path/>ebs.exe

   To use a symbolic link for pkzipc.exe:
   mklink <path/>ebs.exe <path/>pkzipc.exe

3. If you have the McAfee eBusiness Server in your PATH, either remove the PATH statement altogether, or replace the pointer to the McAfee ebs.exe program with the PKWARE program defined in step 2.
4. Make sure any running scripts have the PATH set to use the ebs.exe program from step 2.

Name/Description	***Shortcut***	***Value(s)***	***Example usage***	***Used with***
armor Create ASCII armored file	-a	No sub-options. --- No default value.	***ebs --encrypt --armor save.pgp***	encrypt, sign
authenticate Verifies that an archive is signed.		No sub-options. --- No default value.	***ebs --decrypt --authenticate signed.pgp***	decrypt
Conventional Trigger use of symmetric passphrase encryption	-c	No sub-options. --- No default value.	***ebs --encrypt --conventional save.pgp***	encrypt
conventional-passphrase Provide symmetric encryption passphrase		<passphrase>	***ebs --encrypt --conventional --conventional-passphrase <passphrase>***	encrypt
decrypt Specify decryption operation	**-d**	No sub-options. --- If no other command is entered, ***ebs*** will default to ***decrypt***.	***ebs --decrypt [passphrase <passphrase>]*** [***--preserve-name]*** ***save.pgp***	standalone
dry-run Prints out messages to preview the results of a set of commands or options without actually performing the tasks	**-n**	No sub-options. --- No default value.	***ebs --encrypt --dry-run save.zip***	encrypt
encrypt Specify encryption operation	**-e**	No sub-options. --- No default value.	***ebs --encrypt --conventional [--conventional-passphrase <passphrase>] save.pgp *.doc***	standalone
help Displays help screen	**-h**	**<command or option>** - Any command or option for which help is desired. No default value.	***ebs --help*** Display help for the decrypt command: ***ebs --help --decrypt***	standalone
output Sets OpenPGP output file name.	**-o**	**<filename>**	***ebs --decrypt --output save.pgp save.zip*** ***ebs --encrypt --output save.zip encrypt.pgp***	decrypt, encrypt , sign

overwrite Specifies whether to overwrite existing files with files being added or extracted. By default, PKZIP prompts before overwriting when extracting but not when adding.	-ow	No sub-options. --- No default value.	***ebs --decrypt --overwrite save.zip***	encrypt, decrypt
passphrase Specify private-key passphrase	**-z**	**<passphrase>** - The passphrase. --- No default value.	***ebs --encrypt --passphrase beowulf9 save.zip***	encrypt, decrypt
preserve-name Ignore any internal file name and use OPGP filename when decrypted		No sub-options. --- Default = off.	***ebs --decrypt -preserve-name sample.txt.pgp***	decrypt
sign Specify signing operation.	**-s**	No sub-options. --- No default value.	***ebs --encrypt -sign --sign-with "John Smith <johns@example.com>" save.zip***	encrypt, standalone
signed-by Specifies the sender's key. Decrypt this file only if the file is signed with this key. The option can appear more than once in the same command line, to specify multiple keys.		**<email address>** - Email address of the person associated with the OpenPGP key pair. **User name** - The name of the person associated with this OpenPGP key pair. **UserID** - This value can contain a name, email address and comment; such as: Tom <tom@example.com>. **@<file name>** - Specifies a text file which contains a list of certificates, one on each line. **keyID** - Long or short version of unique key identifier. --- No default value.	***ebs --decrypt --signed-by "john.public@nowhere.com" save.zip*** ***ebs --decrypt --signed-by "John Public" save.zip*** ***ebs --decrypt --signed-by "John Public <john.public@nowhere.com>" save.zip*** ***ebs --decrypt --signed-by "john.public@nowhere.com" save.zip*** ***ebs --decrypt --signed-by "0x12345678" save.zip*** ***ebs --decrypt --signed-by* @recipients.txt *save.zip***	decrypt
sign-with Specifies the key to use to sign an OpenPGP file.		**<email address>** - Email address of the person associated with the OpenPGP key pair. **User name** - The name of the person associated with this OpenPGP key pair. **UserID** - This value can contain a name, email address and comment; such as: Tom <tom@example.com>. **keyID** - Long or short version of unique key identifier.	***ebs --encrypt --sign-with "john.public@nowhere.com" save.zip *.doc*** ***ebs --encrypt --sign-with "John Smith" save.zip *.doc*** ***ebs --encrypt --sign-with "Jon Public <john.public@nowhere.com>" save.zip *.doc*** ***ebs --encrypt --sign-with "0x12345678" save.zip *.doc***	encrypt
text Translate line endings to UNIX	**-t**	Default = **UNIX**	***ebs --decrypt -text save.zip*** ***ebs --encrypt --text scripts.zip *.pl***	decrypt, encrypt
user Specifies the UserID that will sign the OpenPGP-encrypted file. You can include this option more than once to specify multiple users.	**-u**	**<email address>** - Email address of the person associated with the OpenPGP key pair. **User name** - The name of the person associated with this OpenPGP key pair. **UserID** - This value can contain a name, email address and comment; such as: Tom <tom@example.com>. **@<file name>** - Specifies a text file which contains a list of certificates, one on each line. **keyID** - Long or short version of unique key identifier. --- No default value	***ebs --encrypt --user "John Smith" save.zip *.doc*** ***ebs --encrypt --user "john.public@nowhere.com" save.zip *.doc*** ***ebs --encrypt --user "Jon Public <john.public@nowhere.com>" save.zip *.doc*** ***ebs --encrypt --user "john.public@nowhere.com" save.zip *.doc*** ***ebs --encrypt --user "0x12345678" save.zip *.doc*** ***ebs --encrypt --user @recipients.txt save.zip *.doc***	encrypt
version Gives information about the version of the release. Displays complete version information; also returns to the shell particular version numbers specified by sub-options.		No sub-options. --- No default value.	The command line: ***ebs --version*** outputs two lines like the following after the usual header information: ***Program File Version(pkzipc): 14.30.1181*** Product Version: 1.00.0047	standalone

wipe Overwrites PKZIP temporary files and files deleted by PKZIP to prevent recovery of their data	**-w**	No sub-options. ---------- No default value.	***ebs --encrypt --wipe myfiles.zip **	decrypt, encrypt

Using Legacy PGP Mode

PKWARE offers support to users of the McAfee Legacy PGP application. This application supports the limited command set of PGP v2.63 described in the accompanying table. Other key differences between OpenPGP mode and Legacy PGP include:

- PGP mode commands only use the single-letter Command Switch, rather than the full command name.
- You can combine multiple commands with one switch. For example, to decrypt a PGP file and preserve the encrypted file's name, type:

  pgp -dp sample.txt.pgp

- Use ***+force*** to accept all requests from the program.

To enable Legacy PGP Mode:

1. Install SecureZIP
2. Copy or Link `pkzipc.exe` to the program name `pgp.exe`.

   To copy and rename `pkzipc.exe` to `pgp.exe`:

   copy pkzipc.exe <path/>pgp.exe

   To use a symbolic link for `pkzipc.exe`:

   mklink <path/>pgp.exe <path/>pkzipc.exe

3. If you have the McAfee eBusiness Server in your PATH, either remove the PATH statement altogether, or replace the pointer to the McAfee pgp.exe program with the PKWARE program defined in step 2.
4. Make sure any running scripts have the PATH set to use the pgp.exe program from step 2.

Name/Description	***Command Switch***	***Value(s)***	***Example usage***	***Used with***
armor Create ASCII armored file	-a	No sub-options. ---------- No default value.	***pgp –ea save.txt <userID> <userID>***	encrypt, sign
cypher Provide symmetric passphrase	-c	No sub-options. ---------- No default value.	***pgp –c save.txt [–z <passphrase>]***	encrypt
decrypt Specify decryption operation	**-d**	No sub-options. ---------- If no other command is entered, ***pgp*** will default to ***decrypt***.	***pgp –d save.txt.pgp [–z <passphrase>]***	standalone
encrypt Specify encryption operation	**-e**	No sub-options. ---------- No default value.	***pgp -e save.pgp <userID> <userID>***	standalone
+force Force YES to all responses		No sub-options. ---------- No default value.	***pgp -e +force save.pgp <userID> <userID>***	Encrypt, decrypt, sign
help Displays help screen	**-h**	No sub-options. ---------- No default value.	***pgp -h***	standalone
outputfile Sets OpenPGP output file name.	**-o**	**<filename>**	***pgp –d save.txt.pgp –o new.txt*** ***pgp –e save.txt –o new.txt.pgp***	decrypt, encrypt, sign

passphrase Specify private-key or symmetric passphrase. If you specify the passphrase twice, the first item entered is assumed to be associated with the public key (for decryption) or the private key (for encryption). The second item entered is assumed to be the cypher passphrase for the file.	**-z**	**<passphrase>** - The passphrase. ---------- No default value.	***pgp -e save.txt -z beowulf9***	encrypt, decrypt
preserve-name Restores the original name of the encrypted file inside the archive. If this switch is not used, the decrypted file will use the archive filename minus ".pgp".	-p	No sub-options. ---------- Default = off.	***pgp -dp sample.txt.pgp***	decrypt
sign Specify signing operation.	**-s**	No sub-options. ---------- No default value.	***pgp –es save.txt –u <sign id> [<userid>]***	encrypt, standalone
text Considers all PGP plaintext files to be text files. Preserves the internal text structure and converts to local text conventions.	**-t**		***pgp -dt save.zip***	decrypt, encrypt
user Specifies the person (recipient) permitted to decrypt your OpenPGP-encrypted file.	**-u**	**UserID** - This value can contain a name, email address and comment; such as: Tom <tom@example.com>. ---------- No default value	***pgp –es save.txt –u <sign id> [<userid>] *.doc***	encrypt
wipe Erase the original plaintext file after encryption. May also be used on its own for secure file deletion.	**-w**	No sub-options. ---------- No default value.	***pgp -ew myfiles.zip ****	decrypt, encrypt