SecureZIP for Mac OS

Additional Info

Minimum Requirements

Minimum OS X supported versions

OS X Name	Version
All prior versions	10.8
Mavericks	10.9
Yosemite	10.10
El Capitan	10.11

Supported	Not Supported

Installers / Maintenance Updates

- SecureZIP for OS X 2.00.0011

- SecureZIP for Mac OS Knowledge base

Getting started with SecureZIP for Mac OS

SecureZIP for Mac from PKWARE, Inc., lets you create ZIP archives and open them, even if they are encrypted or digitally signed. When a file is encrypted, you must have an appropriate credential (either a passphrase or digital certificate) to open it.

About Strong Encryption

You can encrypt files using either strong encryption or traditional ZIP encryption. Strong encryption is far more secure than the older, traditional ZIP encryption.

You can use strong encryption by identifying a passphrase, using digital certificates and a recipient list, or both.

- With passphrase-based encryption, the same passphrase is used to encrypt and to decrypt, and anyone who has the passphrase can decrypt.
- With certificate-based encryption, a certificate's public key is used to encrypt, and the certificate's private key is used to decrypt. The public and private keys are a pair of numbers associated with a digital certificate that together function like a very long, highly random passphrase.

The public key can be distributed to anybody who may want to use it to encrypt data and share this data specifically for the certificate's owner. Share your public key so that others can authenticate your digital signature. The private key, on the other hand, is never shared. Your digital signature is authenticated by your private key. If someone sends you data encrypted with your public key, the private key associated with that public key must be present for you to view that encrypted data.

The advantage of certificate-based encryption is that you can encrypt for just the people you want to see your files, provided those

people have a digital certificate with a public and private key. Only these people, whose certificates you use to encrypt, can decrypt the files.

The list of people for whom you encrypt using certificates is called a recipient list. The term is also used for the list of certificates.

The Mac Keychain Access application manages certificates and their keys for you. When a recipient runs SecureZIP to extract files encrypted using the recipient's certificate, SecureZIP finds and applies the certificate's private key to decrypt the files.

Before you can do certificate-based encryption, you must have access, for each intended recipient, to a copy of a digital certificate containing the public key.

Note: Some older ZIP utilities cannot decrypt files encrypted using SecureZIP strong encryption.

Using SecureZIP for Mac

SecureZIP for Mac from PKWARE, Inc., lets you create ZIP archives and open them, even if they are encrypted or digitally signed. When a file is encrypted, you must have an appropriate credential (either a passphrase or digital certificate) to open it.

Installing SecureZIP for Mac

SecureZIP for Mac installs from a standard disk image file (.dmg). This file is available for download from PKWARE. It contains the SecureZIP for Mac files needed to run the application.

System Requirements: You must be running MacOSX 10.9 or later, and have administrative privileges to install SecureZIP for Mac.

1. Download or copy the .dmg file to your Mac.
2. Double-click the .dmg file to start the installation. You will see the SecureZIP application icon.
3. Drag the SecureZIP icon and drop it in your Applications folder.

First Time Run

The first time you run SecureZIP for Mac, you may see a message dialog that says:

"SecureZIP" is an application downloaded from the Internet. Are you sure you want to open this application?

Choose **Open.**

SecureZIP Preferences

Setting SecureZIP Preferences

When you have placed SecureZIP in the Dock, you can use the Preferences dialog box to associate a variety of archive types with SecureZIP, define a default location for extracted files and enable encryption and signing for enhanced security.

To open SecureZIP Preferences, double-click SecureZIP in the Dock, then choose **SecureZIP > Preferences**.

Associating File Types with SecureZIP

SecureZIP can open these types of archives. By default, SecureZIP associates itself to all these archive types:

- ZIP
- ZIPX
- 7-Zip
- ARJ
- BinHex
- BZip2
- TAR BZip2
- GZip
- TAR GZip
- LHA

- RAR
- TAR
- UNIX Compressed (Z)
- UUEncode
- XXEncode

If you have another application that can open archives on your system, you may clear any box to disassociate that file type from SecureZIP. Use your preferred application to associate an archive type with that application.

Selecting a Location for Unzipped Files

When you first install SecureZIP, newly extracted (that is, unzipped) files are placed in the same directory as the original archive. If another file with the same name is located in that same directory in Finder, the newly-extracted file is added as a copy of the original file.

The **Extraction** tab in SecureZIP Preferences allows you to select a new default folder, or be prompted for a destination folder each time you open an archive. Choose from these options:

- Original archive folder (default)
- Your **Desktop**
- **Other** folder. This option opens a Finder box. Choose any folder for all extracted files to be extracted to.
- **Prompt for folder**. When you select this option, you will be asked where to put the extracted files each time you extract an archive with SecureZIP.

Enabling Digital Signatures

Before you can digitally sign files, use SecureZIP Preferences to identify your digital certificate:

1. With SecureZIP open, go to the **SecureZIP** menu.
2. Choose **Preferences**.
3. Click the **Security** tab.
4. Check **Sign files**.
5. Use the box to identify your digital certificate.

If you don't have a certificate with a private key installed in Keychain, the Certificate box in Preferences will be dimmed.

If you have more than one certificate installed in Keychain, use the arrows to identify the correct certificate to use.

Once you have enabled digital signatures, each archive you create (and the files inside) will be signed. People who receive a signed file will know that it comes from you and is unchanged since you signed it.

Enabling Encryption

Before you can encrypt ZIP files, use SecureZIP Preferences to identify your preferred encryption method and digital certificate:

1. With SecureZIP open, go to the **SecureZIP** menu.
2. Choose **Preferences**.
3. Click the **Security** tab.
4. Check **Encrypt files**.

If you intend to use a recipient list at any point in the future, use the box to identify your digital certificate.

If you don't have a certificate with a private key installed in Keychain, the Certificate box in Preferences will be dimmed.

If you have more than one certificate installed in Keychain, use the arrows to identify the correct certificate to use.

Using SecureZIP for Mac

Unzipping ZIP Files

To open (also known as extract) a ZIP archive and put the files in a folder:

Note: All SecureZIP functions are available from the Services menu within Finder.

1. Open Finder.
2. Double-click the ZIP you want to open OR control-click on the file and select **SecureZIP: Extract Archive**. Clicking the gear icon in Finder will also lead to the **SecureZIP: Extract Archive** menu item.
3. If the archive is encrypted with a passphrase, you will be prompted to enter the passphrase. If the archive is encrypted with the public key of your digital certificate, it should open automatically. The Mac Keychain Access application manages certificates and their keys

for you. When a recipient runs SecureZIP to extract files encrypted using the recipient's certificate, SecureZIP finds and applies the certificate's private key to decrypt the files.

4. The uncompressed contents of the archive appear in the same folder.

Zipping Files into a New Archive

Compress and (optionally) encrypt one or more files or folders with SecureZIP for Mac. If you have enabled encryption, you may encrypt with a passphrase, for a recipient list, or both.

SecureZIP doesn't just create ZIPs! You can also create archives of various types. See Associating File Types with SecureZIP for all the archive formats you can use.

Follow these steps to create a new ZIP archive:

1. Open Finder.
2. Select the file(s) or folder(s) you want to compress.
3. Choose the gear icon in Finder. Select **SecureZIP: Create Archive**.
4. (optional) If you have enabled encryption, choose an encryption method:
    - To encrypt with a passphrase, check the box. Add a passphrase of at least eight (8) characters. Re-type to confirm passphrase.
    - To encrypt for recipients, check the box. Select a recipient from the list of available digital certificates.
    - You may choose both methods.
5. The first time you create a ZIP after enabling signing, you may be asked to allow SecureZIP access to your private key. You should choose to always allow.
6. Click OK to create your ZIP archive.

Security with SecureZIP for Mac

Encrypting a file encodes its contents so that the file cannot be read until it is decrypted. Decrypting removes the encryption and restores the file to its original form.

Signing a file provides assurance that the file is really from you and has not been tampered with.

Encrypting with SecureZIP

Generally speaking, the easier an encryption standard is to use, the less secure it is. With SecureZIP you have a choice in what standard to use. Traditional ZIP encryption with relatively simple passphrases is almost certainly good enough to preserve the secret family cookie recipe from the neighbors, but the initial business plan for your unique new product needs to get to your patent attorney with SecureZIP strong encryption. Strong encryption is much more secure, but older ZIP utilities can only decrypt files encrypted with the traditional method. Your recipients may need SecureZIP or the free ZIP Reader by PKWARE to decrypt files that you encrypt with strong encryption.

You can use a passphrase or a key from one or more digital certificates (or both passphrase and certificate) to encrypt files in SecureZIP. A passphrase uses letters, numbers, spaces and other non-alphanumeric symbols to allow your recipient to open your encrypted file or message.

If you use a passphrase to encrypt, anyone who has the passphrase can decrypt. If you use a key from a digital certificate, only the owner of the certificate can decrypt. You can choose to encrypt with both a passphrase and a certificate. If someone sends you an archive containing files encrypted with your digital certificate, SecureZIP attempts to decrypt the files automatically when you (and only you) extract them.

SecureZIP does not extract files that cannot be decrypted. Someone who wants to extract encrypted files must either be able to supply a correct passphrase or else own a digital certificate used to encrypt the files.

You can encrypt files with SecureZIP when you add them to a ZIP archive.

Signing Files

You sign a file, or an entire archive, by attaching a digital signature derived from a digital certificate that you own. Other people use your certificate's public key to verify that the signature is yours. You can sign files either when you add them to an archive or later.

SecureZIP always authenticates digital signatures on files that you receive, but you must have a certificate to attach a digital signature of your own.

Specify a Passphrase and/or Recipients

If you use encryption, SecureZIP opens a dialog to get a passphrase and/or recipient list from you when you add files.

- If you encrypt using only a passphrase, only people who have the passphrase can decrypt.
- If you encrypt using only a recipient list, only recipients can decrypt, using the private keys from the certificates whose public keys you used to encrypt.
- If you encrypt using both a passphrase and a recipient list, anyone who has the passphrase or is on the recipient list can decrypt the files.

Specify a Passphrase to Encrypt

To specify a passphrase:

1. Enter the passphrase in the Passphrase field. The passphrase must be at least eight characters long.
2. Enter the same passphrase again in the Confirm field to confirm that you typed what you thought you did.
3. Click OK to encrypt the selected file(s).

Encrypt for a Recipient List

When you use a recipient list to encrypt, SecureZIP decrypts the files automatically when unzipping them for someone on the list. Recipients on the list do not need to supply a passphrase. You need access to a public key for a digital certificate for each recipient to encrypt for a recipient list.

Create a recipient list by picking certificates for recipients from the Certificates list.

The Certificates list shows all the X.509 certificates you have for people on your system. You can have multiple certificates for the same person. The list states when each certificate expires.

To pick recipients for the recipient list, check the boxes for individual recipients you want to add. If there are more certificates than fit in the window, use Search to locate the person(s) you want to add.

Be sure to select one of your own Personal Certificates to add yourself as a recipient so that you can decrypt the files without entering a passphrase.

Skip Encrypting Files

You can skip encrypting the selected files and add them without encryption by clicking **Skip**. The files are added to the archive without being encrypted.

Enterprise Features

SecureZIP Enterprise Features

System administrators and those responsible for data security in an enterprise environment can use SecureZIP Enterprise Edition to implement security and access measures through policy definitions.

About Policy

Enterprise versions of SecureZIP (and PKZIP for Windows) enables an administrator to control how SecureZIP is used—particularly with respect to encrypting and digitally signing files—by creating a policy file. By applying a policy, an administrator can lock selected SecureZIP options to desired settings. These policies will apply to computers running SecureZIP for Mac.

Policy settings are saved to a policy file, which is digitally signed by an authorized administrator. SecureZIP checks the policy file at startup and locks any settings specified in the file.

For example, to ensure that zipped files are always encrypted, an administrator can apply a policy that locks the Encrypt files settings. SecureZIP will then always zip and encrypt files until those options are unlocked and turned off.

How Locks Are Set

Locks on options are set by defining a policy in SecureZIP Enterprise. Policy locks are not set from SecureZIP for Mac.

Contingency Keys

Enterprise versions of SecureZIP (and PKZIP for Windows) enable an administrator to control how SecureZIP is used—particularly with respect to encrypting and digitally signing files—by creating a policy file. These policies will apply to computers running SecureZIP for Mac.

Administrators can also define one or more contingency keys in a policy file. Contingency keys enable an organization to decrypt files encrypted by anyone in the organization, whether the files were passphrase-encrypted or were encrypted for specific recipients. Contingency keys are a safeguard to be sure that important information belonging to the organization does not become inaccessible because no one in the organization can decrypt it.

SecureZIP for Mac in Reader Mode

Enterprise customers who regularly exchange compressed and encrypted data with users on Macintosh OS X may find situations where a partner does not already have SecureZIP for Mac and is unable to open encrypted files they receive. These partners can easily obtain their own copy of SecureZIP for Mac from PKWARE.

If your partners are unable to obtain their own copies of SecureZIP for Mac, Enterprise customers can contact PKWARE for information on options for providing their partners with a “Reader-only” license of SecureZIP for Mac. This license allows a user to install SecureZIP to extract and decrypt archives. This installation disables the compression and encryption features but allows them to receive and open encrypted files they receive.

In Reader mode, SecureZIP will open the same variety of archive types as the complete application. If an archive is encrypted using traditional ZIP encryption or strong encryption (passphrase- and certificate-based), Reader mode will handle these as well.