

## Administer Security Policy with SecureZIP for Windows Enterprise Edition

SecureZIP Enterprise Edition enables you to implement, deploy, and enforce security policies affecting any data your end users work with in SecureZIP.

PKWARE Policy Manager is a Microsoft Management Console (MMC) snap-in. It provides a command center from which you can bring to bear SecureZIP's arsenal of security features to improve efficient transfer of data and help maintain regulatory compliance whenever SecureZIP is used by anyone in your organization.

**Note:** This document mostly refers to SecureZIP. Users of PKZIP Enterprise Edition can only set policies and define standards for passphrase-based strong encryption.

### Glossary

Some terms associated with PKWARE Policy Manager can be confusing. Table 1 clarifies the most important.

**Table 1: PKWARE Policy Manager Glossary**

<i>Term</i>	<i>Definition</i>
Contingency Key	Contingency keys enable an organization to decrypt files encrypted by anyone in the organization, whether the files are passphrase encrypted or 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.
Policy	A particular set of SecureZIP configuration options that specifies contingency keys and determines how SecureZIP compresses, encrypts, or digitally signs files or email attachments.
Policy Certificate	Digital certificate selected by an administrator for PKWARE Policy Manager to sign policy files. SecureZIP authenticates a policy file by checking that it is signed by a policy certificate.
Policy File	When a policy is defined and a policy certificate is associated to that policy, Policy Manager saves that information to a policy file with a .szp extension. This file can then be applied to any PKZIP or SecureZIP Enterprise installation.

## Policies

Working in PKWARE Policy Manager, you can create, manage, and distribute multiple policies appropriate for different organizational roles.

At the user level, SecureZIP enforces a policy by configuring and locking options to the settings the policy specifies. For many SecureZIP options, policy administrators can:

- Define a setting and prevent users from changing that setting (locking)
- Define a preferred default setting that users can change (new defaults), or
- Allow users to define their own choices

## Locking Options

When SecureZIP options are locked by a policy, the controls (such as check boxes) for setting the options on client systems are disabled and grayed, preventing the end user from changing the settings. Controls for options that are incompatible with locked settings are also disabled.

## Create New Default Settings

As an alternative to locking options, a policy can also change native SecureZIP default option settings to new defaults. This gives administrators a more flexible way to influence how SecureZIP is used.

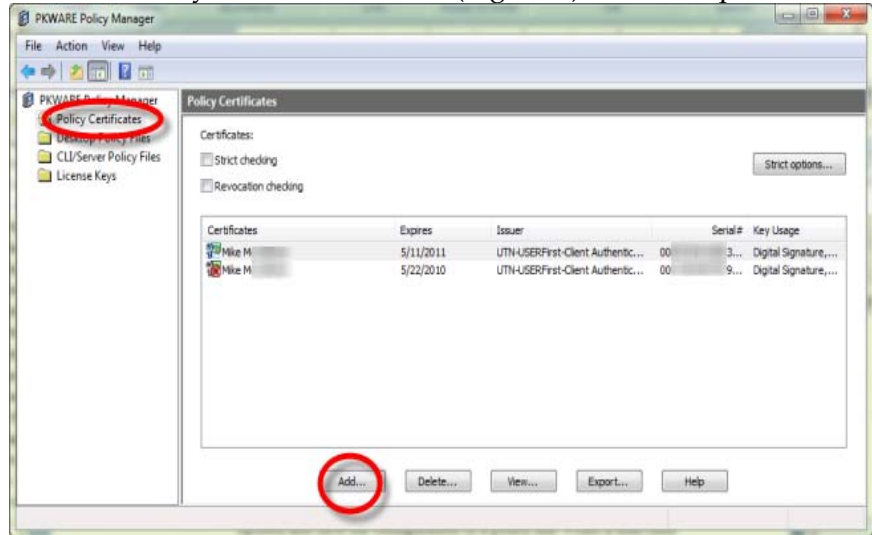
For example, the installation default setting for the *Sign files* option is Off. If you prefer that users sign files, but you do not want to force them to, you can change the setting to On in a policy but not lock it. This turns the option On by default so that SecureZIP ordinarily signs files, but users can change the setting.

## Identifying Policy Certificates

To ensure that policy files are authentic, SecureZIP Enterprise Edition requires all policy files to be digitally signed with a policy certificate. A policy certificate is simply a digital certificate selected by a SecureZIP Enterprise administrator to sign policy files. You can add multiple certificates to Policy Manager, but only one certificate is associated with each policy file. Before activating a policy file on a user's machine, SecureZIP authenticates a policy file by checking that it is signed by a policy certificate.

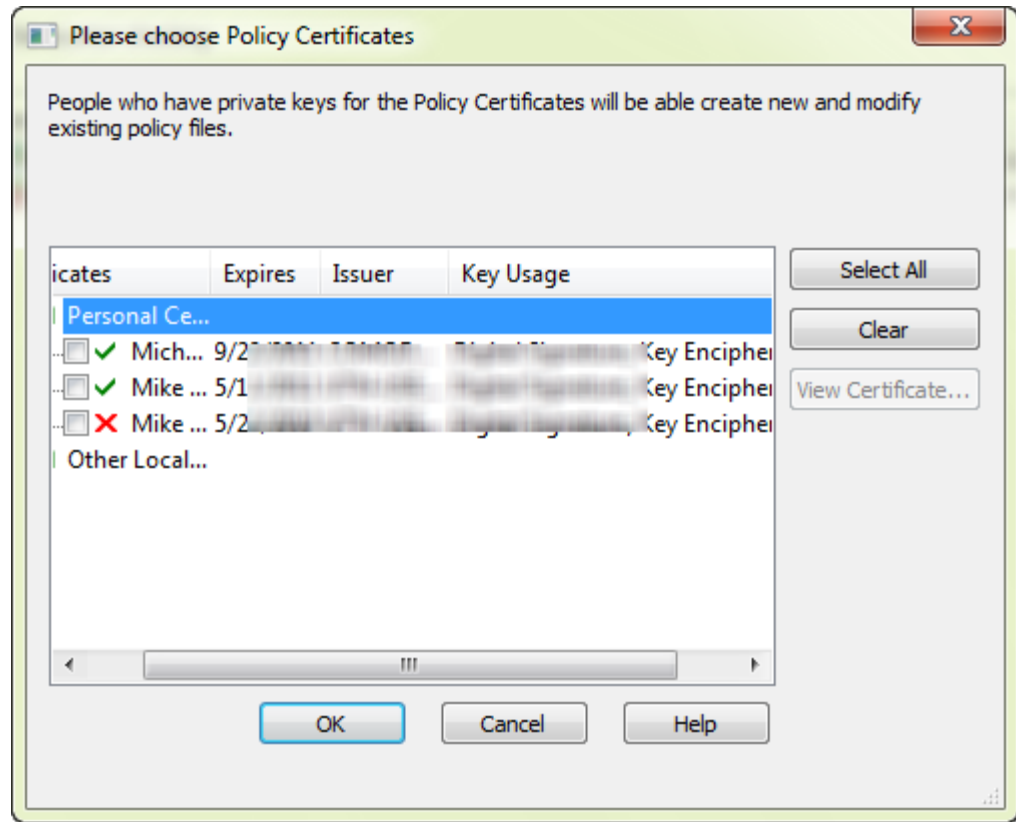
Below is a summary of the steps to add a policy certificate.

1. Open PKWARE Policy Manager.
2. Click the Policy Certificates folder (Figure 1) in the left pane.



**Figure 1 Add digital signatures to authenticate policy files.**

3. Choose **Add** to define a certificate to use to sign a policy file. Figure 2 appears.
4. Select the certificate(s) to use as policy certificates and choose **OK**.



**Figure 2 Add a digital certificate from the list.**

While still in the Policy Certificates view, choose **Export** to export all policy certificates to a .reg file. This will allow policies to be applied to, and enforced on, PKZIP and SecureZIP Desktop clients. See *Creating and Applying a Policy* to learn more about this process.

Once Policy Certificates are configured, you can proceed to creating policy files.

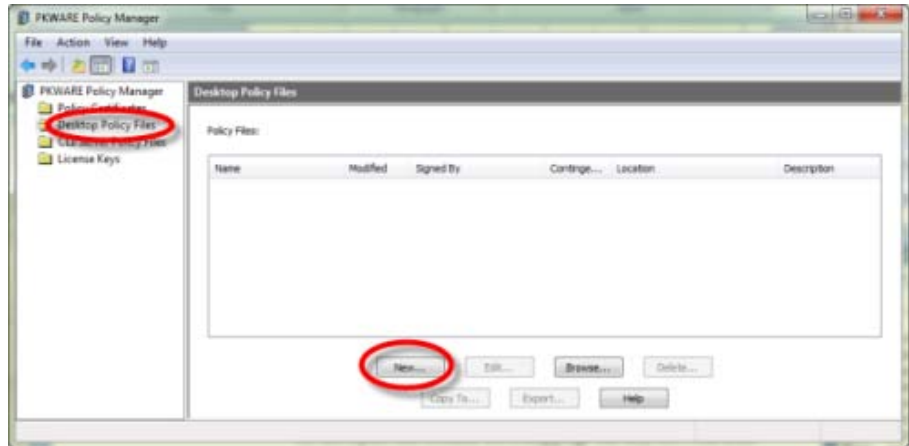
## Creating and Applying a Policy

To create a policy, an administrator uses the PKWARE Policy Manager to set options and save the configuration to a policy file. When a user runs SecureZIP, SecureZIP checks for a policy file and configures the user’s options according to the settings in the file.

Follow these steps to create a new policy file for PKZIP/SecureZIP for Windows Desktop:

**Note:** These steps describe using PKWARE Policy Manager to create .reg files as a mechanism for importing policy certificates and policy file location into the registry on client machines. You can also push the registry settings to user desktops using standard administrative tools, including SMS.



1. In the Desktop Policy Files view (Figure 3), choose **New** to open the Policy Editor to set and lock the options you want the policy to enforce, or specify contingency keys .

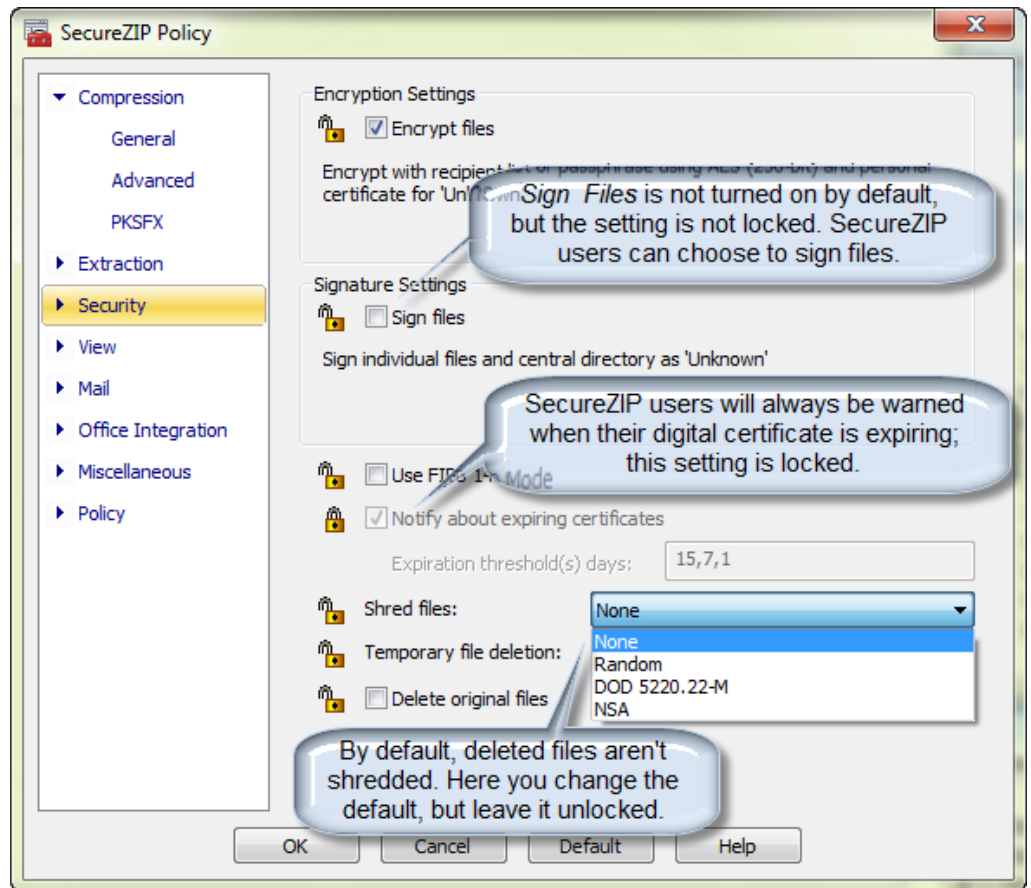


**Figure 3 Click New to create a policy file.**

**Note:** The CLI/Server Policy Files folder is used to specify contingency keys for use with SecureZIP Server. If you wish to use SecureZIP in a server environment, please contact PKWARE Sales for more information.

2. In the Policy Editor, configure the options according to your organization's requirements. Most pages in this dialog have some lockable settings; you can configure compression, security, and mail options including specifying contingency keys.

Options that can be locked display a padlock icon to the left in the Policy Editor. The padlock shows whether the option is currently locked  or unlocked . To *lock* an option to its current setting, click its padlock icon. If the option is already locked, click the padlock to unlock it before changing the setting. Figure 4 describes the three types of settings.



**Figure 4 Administrators have options when creating policies.**

To replace installation default settings with your own settings for options that are *not* locked, check the box, *Use unlocked options as defaults* (on the General tab of the Policy category).

3. (Optional) Click **Policy**, then **Contingency Keys** to add a contingency key for this policy file. This dialog box works the same way as the Policy Certificate dialog box described in the “Identifying Policy Certificates” section, and performs a similar function. You should not, however, use the policy certificate as a contingency key.
4. After you configure option settings, choose **OK** to save your settings to a policy file. Save the file to a location on the network where the file can be imported later. In the *Sign by* dropdown menu of the Save As dialog, select a policy certificate to use to sign the file.

When saving the file, use its full, universally accessible pathname. Do not use a path that contains drive mappings that may not work from client machines.

5. Back in the Policy Files view from which you opened the Policy Editor, choose **Export** to export a pointer to the location of the (selected) policy file to a .reg file.
6. On each client machine, run the certificates .reg file and then the policy file location .reg file to import the policy certificates and the pathname of the policy file into the registry. When these registry files are imported to the client system, SecureZIP then knows where to look for both the policy file and the authenticating signature.

### ***Editing an Existing Policy File***

Once you have created a policy file, you can change any settings inside PKWARE Policy Manager. Select the file from the Desktop Policy Files folder, and click **Edit**. Complete Steps 2-4 above to make the changes and apply them to the client machine(s). Users must log off their system and log on again before the new policy goes into effect.

If you use a different certificate from the original (or most recently edited) policy file to authenticate the new policy file, you will need to import both the certificates and policy .reg files on the client machine.

## Policy Files

PKWARE Policy Manager saves policy settings and information about contingency keys to a policy file with a .szp extension. You can save a policy file to a location of your choice.

To tell Windows systems where to find a policy file, export a Windows registry key that points to it and import the key into the registry on Windows end-user systems (see Steps 5 and 6 in *Creating and Applying a Policy*).

On Windows systems, when SecureZIP starts, it checks the HKLM\Software\PKWARE\PKZIP80\Policy registry key for the location of a policy file. Under this key, SecureZIP saves the pathname to the string value SecureZIPW for policy files that apply to SecureZIP for Windows Desktop. If a pointer to a policy file is found, SecureZIP uses that file to lock options in SecureZIP.

When run, SecureZIP Desktop additionally saves a copy of the policy file to the local system. If no pointer is found, or if SecureZIP cannot access the file, SecureZIP Desktop uses the previously saved local copy to configure locks.

If a pointer is found but SecureZIP cannot locate any previously saved policy file, SecureZIP goes into read-only mode and does not let users create or modify archives.

## Windows Command Line Installation

You can install SecureZIP for Windows Desktop from the Windows command-line prompt or a batch file. In the command line, you can specify a policy file and set various other properties to customize the installation.

The command line looks like this:

```
<name of SecureZIP installation file> /S
/v"<properties>"
```

where:

- /S (case-sensitive) is a switch that tells the installation program to run silently and not to display various initial screens (that say, for example, *Preparing to install...*)
- /v is a switch that must be used to pass any specified SecureZIP properties to the Windows installer.
- <properties> is a list of property settings. Available properties are listed later in this guide.

You can also optionally pass in a switch to specify either the Basic UI, that displays a dialog containing only a **Cancel** button to stop the installation; or No UI, that displays no dialog. Both Basic UI and No UI can run unattended. The default is the full, graphical UI, which is interactive and so cannot run unattended.

<b>Switch</b>	<b>Specifies</b>
<b>/qb</b>	Basic UI
<b>/qn</b>	No UI

Any quotes (") in the parameters must be escaped with a backslash (\).

Examples:



```

<name of SecureZIP installation file> /S /v/qb

<name of SecureZIP installation file> /S /v"/qb
PKCABASSOC=0"

<name of SecureZIP installation file> /S
/v"PKCABASSOC=0 LICENSE_KEY=<Your license key>"

<name of SecureZIP installation file> /S
/v"INSTALLDIR=\\\"My Programs\PKWARE\" "

```

The properties you can set are described in the following sections.

### ***Specify a Policy File***

You can set the PKPOLICY property to specify a policy file on installation. Enter a command line like the following:

```

<name of installation file> /S
/v"PKPOLICY=\\network\share\pkzipw_policy.szp"

```

The command line sets the PKPOLICY property to the specified name and location of the policy file. (The path and file name shown above are just a sample. You can use any full path and file name. Do not use a relative path.)

For the policy file to be usable, you must also import into each user's registry a key that contains the certificate used to sign the file. See "Creating and Applying a Policy" to learn how to create a .reg file that imports policy certificates to the right key in the Policy Certificates view of SecureZIP Enterprise. To use such a .reg file, do one of the following:

- Set the SecureZIP POLICY\_CERTS property to point to and run the .reg file when SecureZIP is installed (see "Import Policy Certificates" below).
- After installation, run the .reg file on each end-user machine to import its certificates.

### ***Import Policy Certificates***

You can set the POLICY\_CERTS property to point to a .reg file that imports policy certificates (used to sign policy files) when SecureZIP is installed. For example:

```

<name of installation file>
/v"POLICY_CERTS=\\network\share\pkpolicycerts.reg"

```

or, using a local address:

```
<name of installation file>
/v"POLICY_CERTS=\"C:\Documents and
Settings\jq_public\My
Documents\PKWARE\pkpolicycerts.reg\" "
```

Note the quotes preceded with backslashes around the address in the example above. The quotes (and backslashes) are necessary because the address contains spaces.

You can use PKWARE Policy Manager to create a .reg file that contains the key and certificates to import. Use the **Export** button in the Policy Certificates view.

### ***Set Installation Directory***

If you want SecureZIP to install somewhere other than the system's Program Files directory, use the INSTALLDIR property and set it to the new location. For example:

```
<name of installation file> /S /v"INSTALLDIR=\"\My
Programs\PKWARE\" "
```

### ***Set the License Key***

SecureZIP checks the PKWARE license key each time the program runs. Use the LICENSE\_KEY property to set the license key on users' systems. For example:

```
<name of installation file> /S /v"LICENSE_KEY=<Your
license key>"
```

### ***Associate File Types with SecureZIP***

By default, the installation associates with SecureZIP the types of files listed in the following table. These file associations enable you to open a file of any of these types in SecureZIP by double-clicking it in Windows Explorer.

<i>File Type</i>	<i>Property</i>
<b>ZIP</b>	PKZIPASSOC
<b>UUEncode/XXencode</b>	PKUUEASSOC
<b>GZIP and Tar</b>	PKGZASSOC
<b>BZIP2</b>	PKBZ2ASSOC
<b>ARJ</b>	PKARJASSOC
<b>RAR</b>	PKRARASSOC
<b>LZH</b>	PKLZHASSOC
<b>JAR</b>	PKJARASSOC
<b>CAB</b>	PKCABASSOC

If you do not want a particular file type associated with SecureZIP, set its corresponding property to 0 in the command line. For example:

```
<name of installation file> /S /v"PKCABASSOC=0"
```

### **Shortcuts**

By default, the installation creates shortcuts to SecureZIP. If you do not want a shortcut created in one of the places listed in the table below, set the corresponding property to 0.

<i>Location</i>	<i>Property</i>
<b>Program group in Start menu</b>	PKSTARTMENU
<b>Desktop</b>	PKDESKTOP

### **SecureZIP Attachments Status**

The SecureZIP Attachments tool tray icon runs in the system tray. If you want it to run each time you start your computer, set the START\_PKTRAY property to 1. Otherwise set it to 0. (You can also control display of the tool tray icon from the Start menu command **SecureZIP Attachments Status**.)

### **Do Not Install SecureZIP Attachments**

SecureZIP Attachments, the extension module for zipping email messages and attachments, installs by default if Outlook is detected. To not install SecureZIP Attachments, set the PK\_PKZIP\_ATT property to No using a command line like this:

```
<name of installation file> /S /v"PK_PKZIP_ATT=\"No\""
```

**Set Whether Certificate Request Wizard Runs Automatically**

With license purchases up to 200 users, a digital certificate is included that will automatically install with the software. SecureZIP users who do not have a PKWARE (Comodo) certificate can click **Get a Digital Certificate** in the Help menu to run a certificate request wizard.

You can set SecureZIP to automatically run this wizard when the user launches the program the first time by setting the PK\_CERT\_AUTORUN property. Set the property to 1 to enable the wizard to run automatically; set it to 0 to disable auto-run. For example:

```
<name of installation file> /S /v"PK_CERT_AUTORUN=1"
```

**Do Not Install Certificate Request Wizard**

With license purchases up to 200 users, a digital certificate is included that will automatically install with the software. SecureZIP users who do not have a PKWARE (Comodo) certificate can click **Get a Digital Certificate** in the Help menu to run a certificate request wizard.

You can disable installation of the wizard, and prevent the wizard from ever running, by setting the PK\_NO\_CERT\_REQUEST property to 1:

```
<name of installation file> /S /v"PK_NO_CERT_REQUEST=1"
```

**Do Not Install SaveSecure Feature**

The SaveSecure feature adds an Office Integration tab to Miscellaneous options that contains options to automatically open an archived file in the file's associated application program, and to enable Office Integration.

The SaveSecure Office Integration option adds menu commands and toolbar buttons to some Microsoft Office applications to make it possible to open documents of appropriate types in the application directly from ZIP files. Documents can also be saved directly to ZIP files using these commands.

To not install the SaveSecure functionality, set the SAVESECURE property to 0:

```
<name of installation file> /S /v"SAVESECURE=0"
```

**Do Not Install Key Backup Feature**

By default, the Encryption and Signing tabs of Security options contain a **Backup...** button that enables the user to export a backup copy of a private key to a .pfx file. The user can also export a private key by checking a box in

the certificate request wizard, which can be run from the command **Get a Digital Certificate...** in the Help menu.

To hide these controls and not install the key backup functionality, set the PK\_KEY\_BACKUP property to 0:

```
<name of installation file> /S /v"PK_KEY_BACKUP=0"
```

## Disconnected Use on Windows

Users can run the program when disconnected from the network if they have their own local copy of the program. Policies and contingency keys are applied during such disconnected use by means of local copies of the policy file.

Each time SecureZIP is run, it copies any policy file pointed to in the registry to a local file saved on the user's system.

If a user is disconnected from the network (and therefore cannot access a policy file on another machine), SecureZIP uses the previously saved local copy of the file. The local copy is automatically refreshed from the network the next time SecureZIP is started when connected on the network.

A user must start SecureZIP once when connected to the network to access the master policy file and get a local copy in order for SecureZIP to apply the policy settings and contingency keys when the user is disconnected.