

Using the Administrative Module to Implement an Options Lockdown Policy

PKZIP offers an add-on Administrative Module that enables a PKZIP administrator to enforce policies that govern how PKZIP is used—particularly with respect to compressing, encrypting, and digitally signing files and email attachments. The module is available for both PKZIP for Windows and SecureZIP™ for Windows.

Installing the module adds to the PKZIP Options dialog a Policy category with a Lock Options tab. The tab contains controls to lock PKZIP configuration options to specified settings. Once locked, the options cannot be changed until the settings are unlocked on the Lock Options tab. Controls to unlock settings (or lock additional ones) are protected by password: only someone with the password can enable the controls to set or remove locks.

To access the tab in PKZIP, choose **Options...** from the Tools menu to open PKZIP Options; then choose the Policy category.

Locks on options affect all users of PKZIP on the machine on which the locks are set.

The PKZIP help explains how to use the controls on the Lock Options tab. The sections below repeat some of that information and add details—about file names and registry keys—that is intended only for PKZIP administrators who configure locks on PKZIP options for other users.

You Must Have a Feature to Lock It

The copy of PKZIP or SecureZIP that you work in when you lock options must support all the options that you want to lock: you cannot lock an option that your copy of PKZIP does not have.

For example, the option to sign files with digital signatures requires SecureZIP: PKZIP does not have this option. Consequently, you cannot select the option to sign files in PKZIP, and the Lock Options tab in PKZIP does not offer a control to lock it.

You can, however, lock options that not all affected users have. For example, working in SecureZIP, you can lock the option to sign files even though some users whose options are affected by the locks you set only have PKZIP. Users who do not have an option that you lock are unaffected by that

particular locked setting, but locks you set on options that they do have are enforced.

The Lock Settings Configuration File

Locked option settings are recorded in a configuration file. The path and name of this file are displayed in the *Policy file* field in a dialog that opens from the **Policy File...** button on the Lock Options tab. Lock settings are saved to the path and file specified in the *Policy file* field.

Unless a different location for this file is specified (see “Specify a Location for the Configuration File on Installation,” below), PKZIP maintains configuration settings in a file called `pkzipw_policy.xml` in a `PKWARE` folder in the `COMMON_APP_DATA` system folder. The actual path to this folder varies among versions of Windows, but a typical path on Win2000 and XP is this:

```
C:\Documents and Settings\All Users\Application Data\PKWARE\  
pkzipw_policy.xml
```

Save a Registry Pointer to the Configuration File

For greater security, you can specify a custom file name and location for a master copy of the configuration file and have PKZIP save the name and location to a registry key that PKZIP checks for the location of the file. Because PKZIP uses the registry key to locate the file, you can save the file anywhere, including to another machine on the network.

PKZIP automatically saves the name and location of the configuration file to the registry if you change either the default path or file name of the local copy of the file (see the preceding section) when you save new lock settings on the Lock Options tab.

When PKZIP starts, it checks the registry key for a pointer to a configuration file. If it finds one, PKZIP uses that file to configure locks on options in PKZIP. If no registry pointer is found or if PKZIP cannot access the file, PKZIP uses the local copy of the configuration file to configure locks.

The registry key where PKZIP saves the name and location of a configuration file other than the default local copy is:

```
HKEY_LOCAL_MACHINE\Software\PKWARE\PKZIP70\Policy
```

Under this key, PKZIP saves the pathname to the string value `PKZIPW` for lock settings that apply to PKZIP for Windows.

Users who lack administrator privileges cannot change values in `HKEY_LOCAL_MACHINE` on Windows NT, 2000, or XP, but users who have administrator privileges can. To best ensure the security of the configuration file, restrict write access to the file on the network and keep confidential its location and the registry key that points to it. Also, do not give PKZIP users

administrator privileges that might enable them to change the pointer in the registry.

Windows 9x systems (98 and ME) are inherently insecure in that they do not make it possible to prevent changes to the registry. You cannot reliably enforce PKZIP policies on systems running any of these versions of Windows.

Lock PKZIP Options on Multiple Machines

You can lock the same option settings for multiple users of PKZIP throughout the enterprise by causing their copies of PKZIP to configure locks from the same configuration file.

To do this, open PKZIP and configure the locks you want. Save the configuration file to a secure location on the network. (The location must be accessible to the machines on which you want to configure PKZIP option locks.) Then add to the registry of each machine the key described above, containing the path and name of the configuration file.

Specify a Location for the Configuration File on Installation

You can specify a custom location for the configuration file on installation by installing PKZIP from the command prompt. Enter a command line like the following:

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

In this sample command line, `/s` is a switch that tells InstallShield® to run silently and not to display various initial screens (that say, for example, *Preparing to install...*). The `/v` command passes to the Windows installer the `PKPOLICY` property containing the specified name and location of the configuration file. (The path and file name shown above are just a sample. You can use any path and file name.)

Because this location is (presumably) different from the default location (described in “The Lock Settings Configuration File,” above) for the configuration file on the local machine, PKZIP creates a pointer to the file in the registry of the local machine when PKZIP is run.

Maintain Locks for Disconnected Users

Each time PKZIP is run, it copies any configuration file pointed to in the registry to a local file saved by default to this location:

C:\Documents and Settings\\Application Data\PKWARE\
pkzipw.xml

If a user is disconnected from the network (and therefore cannot access a configuration file on another machine), PKZIP uses the previously saved local copy of the file to configure locks. The local copy is automatically refreshed from the master file the next time PKZIP is run when the user is reconnected to the network.

Contact PKWARE Technical Support

Phone: (414) 354-8699

http://www.pkware.com/support/supportform_small.html