



Encrypting Files using WinZip

Documents, spreadsheets, databases, and other files that contain personal information or other sensitive information should be encrypted when saved on hard drives, CDs, Floppies, USB drives, and other non-central media.

One of the easiest ways to do this on a Sinclair Imaged PC is to use the WinZip application. WinZip can compress single files, multiple files, and entire folders as *archives*.

NOTE: Encrypting files with WinZip requires that you have WinZip version 9 installed on your PC. Instructions for installing WinZip 9 and for encrypting files with WinZip are below.

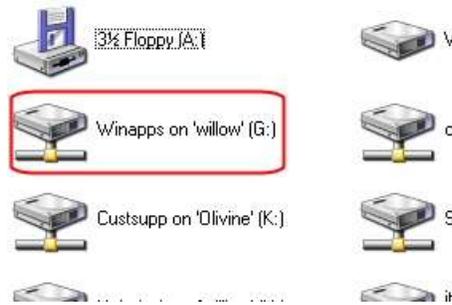
NOTE: While WinZip works well for many users, some people have experienced problems when transmitting WinZip encrypted files to off-campus users. An alternative free software encryption program, that is compatible with most computer systems, is AxCrypt. Instructions on using AxCrypt are found on it.sinclair.edu under in the Service section under Policies and Security Information.

Installing WinZip:

1. Double-click on the **My Computer** icon on your PC's Desktop.



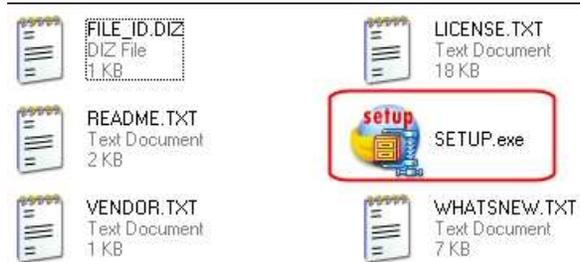
2. Double-click on the **Winapps on 'willow' (G):** icon.



3. Double-click on the **WinZip 9 SR-1** folder.

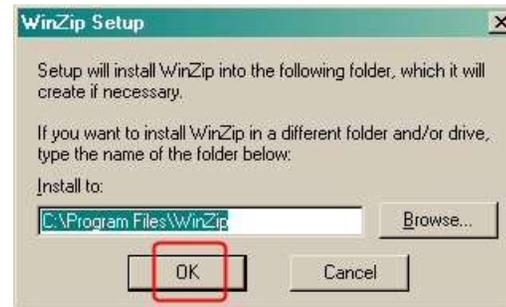


4. Double-click on the **SETUP.exe** file.

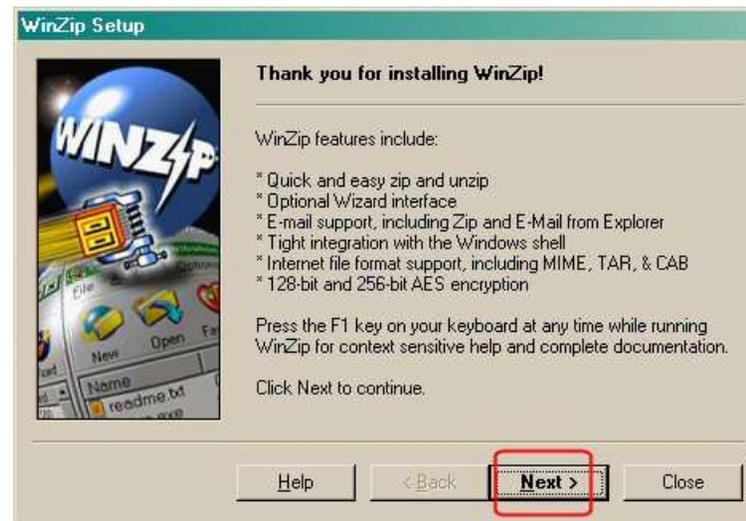


5. The installation setup window will open.

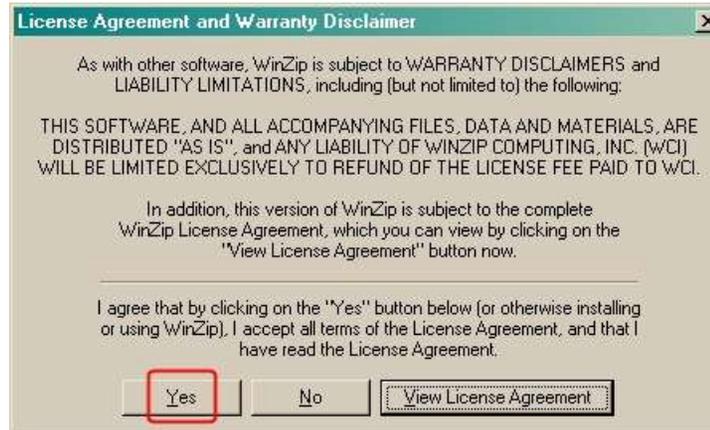
Click on **Next**.



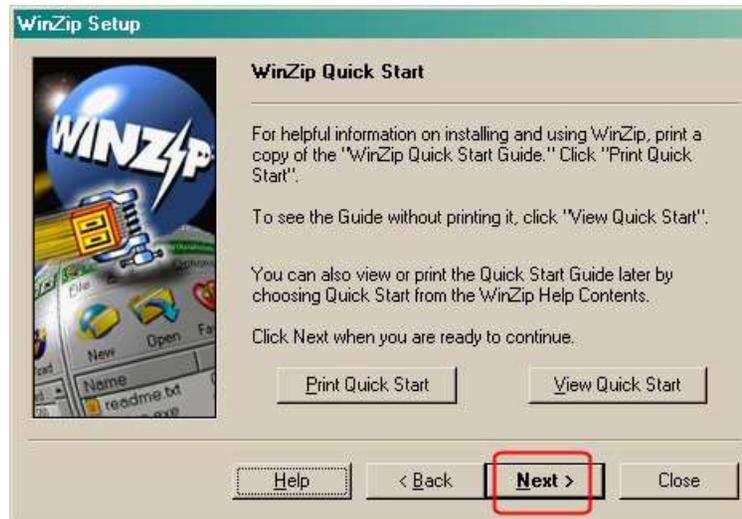
6. Click **Next**.



7. Click **Yes** to accept the license agreement.

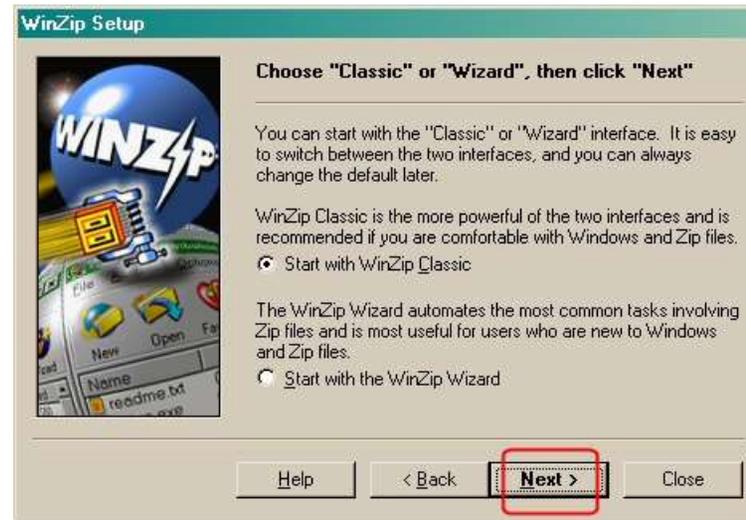


8. Click **Next**.



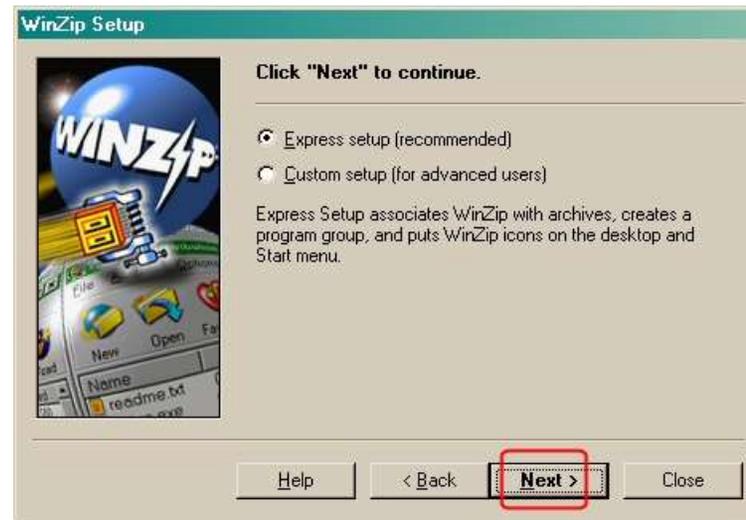
9. Choose **Start with WinZip Classic**.

Then click on **Next**.

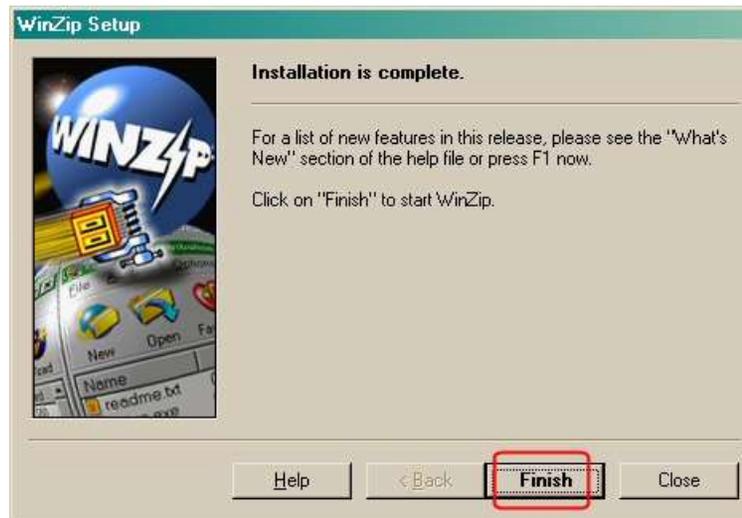


10. Choose **Express setup**.

Click on **Next**.



11. Click on **Finish**.

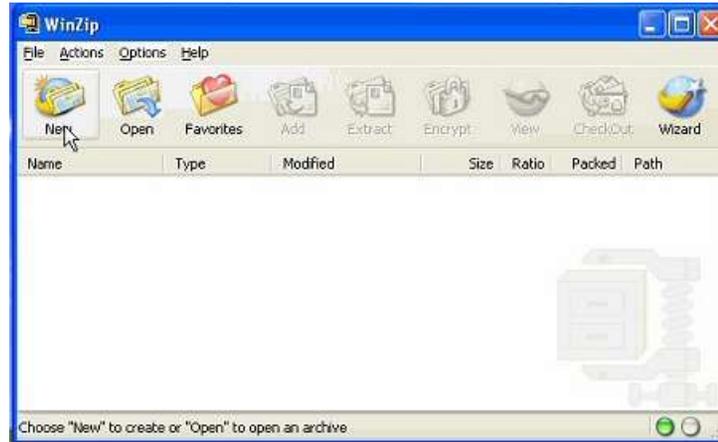


To create a new encrypted archive:

1. Open the WinZip application from your **Start>All Programs>WinZip** menu



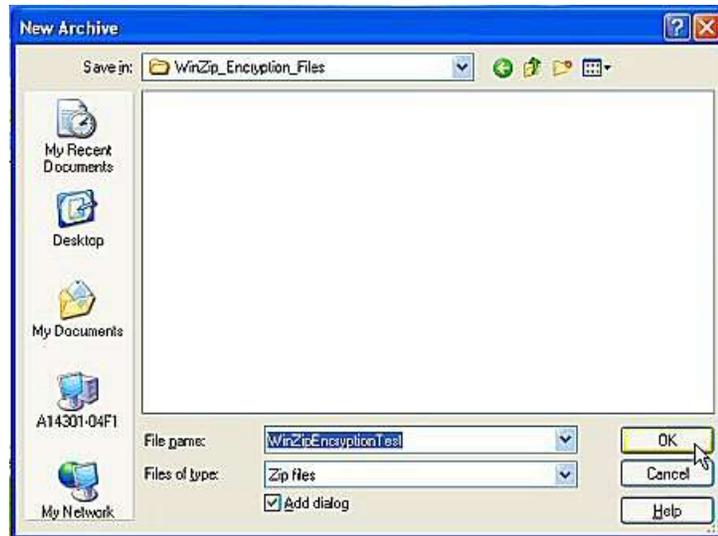
- When the application opens, select **New**.



- In the **Save in** dialogue box, browse to the folder or disk where you want to create the new archive, then type a name for the archive in the **File name** dialogue box.

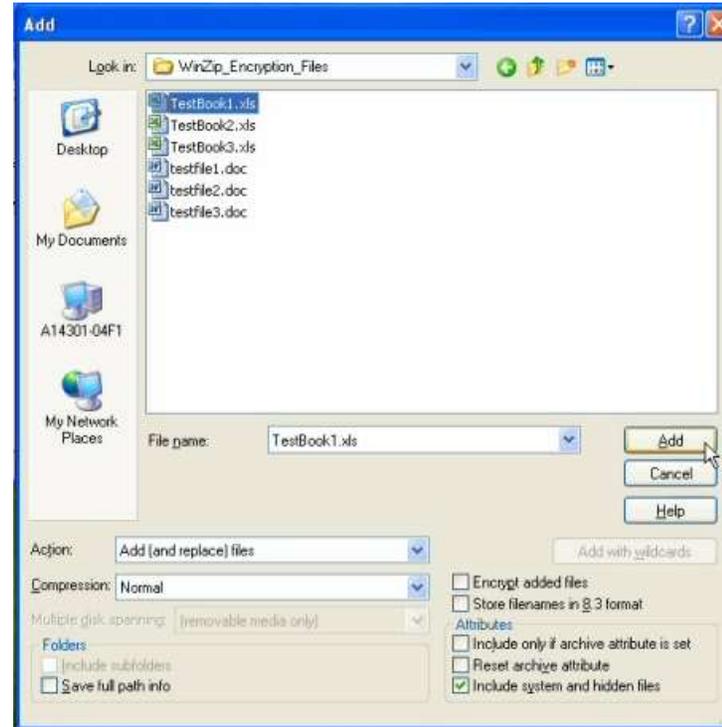
In this example, the archive is named WinZipEncryptionTest, and is stored in the folder WinZip Encryption Files.

Then click **OK**.

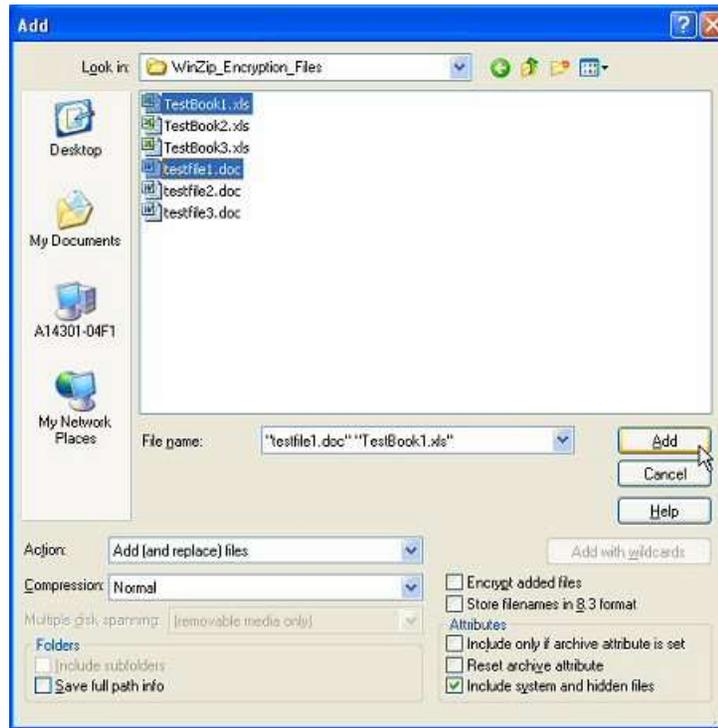


- The **Add** window should appear after you click OK. This is where you select the file or files that need to be encrypted.

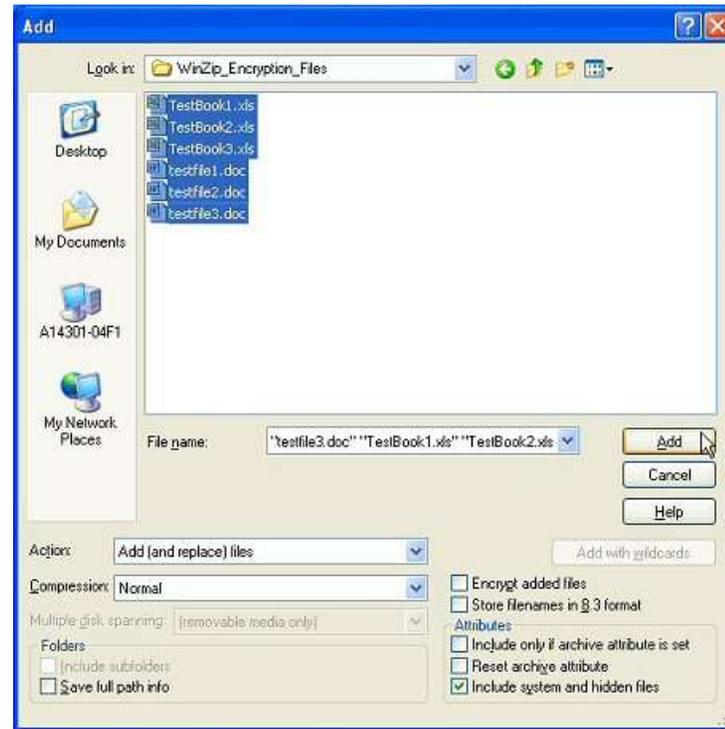
NOTE: If a single file needs to be encrypted, simply select it and click **OK**.



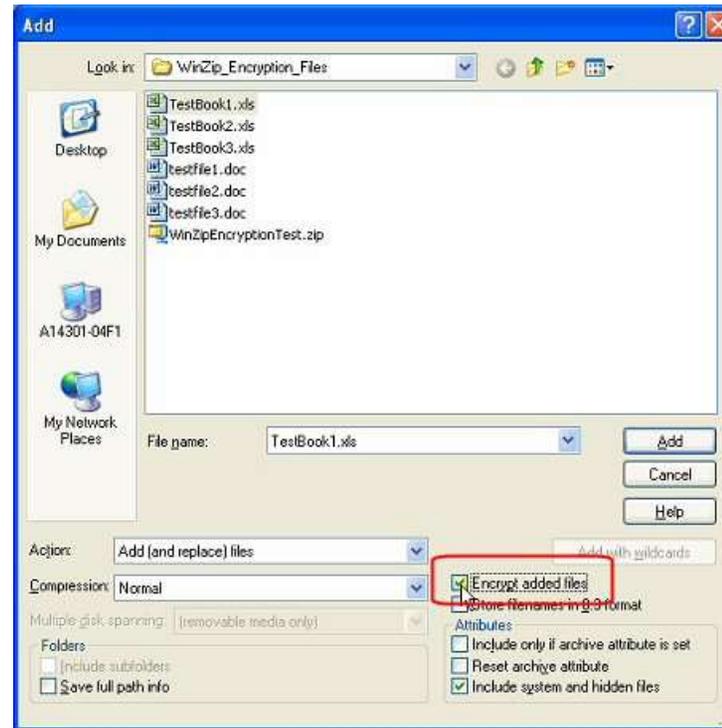
NOTE: If multiple files need to be encrypted, hold down the **Ctrl** key as you select each with your mouse.



NOTE: If a range of files need to be encrypted, click the first file in the range, then hold the **Shift** key and click on the last file in the range.



5. Make sure the Encrypt added files checkbox is checked, then click **Add**.



6. A WinZip Caution warning pops-up if this is the first time you have used WinZip to encrypt a file.

If you do not want to be warned each time you encrypt a file, check the box next to "Do not display this dialogue box in the future."



Click **OK** to close the box.

- Next, select the encryption method to use and create the password required to decrypt the archive.

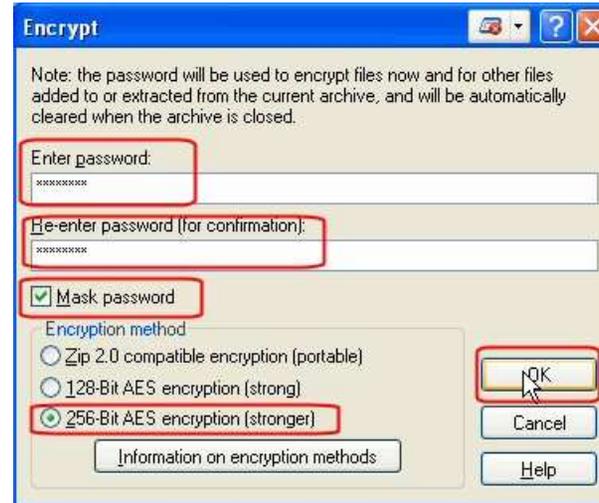
For most purposes, 256-Bit AES encryption should be selected.

The password is a critical part of this process, the stronger the password, the better protected the archive.

The longer and more complex the password is, the greater the protection.

As a minimum, select a password at least 8 characters long that contains upper- and lower-case letters, numbers, and special characters.

Click **OK**.



8. **NOTE: The final step is to ensure the original files (added to the encrypted archive) are properly protected or deleted.**

If the files are on a network storage device such as your “H-drive” or a department shared folder, the files may be left unencrypted. Security of network storage devices is managed by ITS.

If the original files are on a PC hard drive, portable device, or removable media such as CD, DVD, or USB drive, the unencrypted files should be deleted.



Use Windows Explorer to delete the original files.

Sending encrypted files:

If you need to send or the encrypted file to someone else, **do not send the password with the file**. Instead, transmit the password separately using another communication method. Examples include:

- If emailing the file, use phone to transmit the password.
- If mailing the file via CD, use phone to send the password.

Since this encryption is based solely on the password, including the password with the file completely defeats the security the encryption provides.

For questions or additional information, contact the IT Help Desk at 937-512-HELP (4357) or at helpdesk@sinclair.edu.