WinZip® 27
ENTERPRISE

INSTALLATION AND CONFIGURATION GUIDE

Introduction

This Installation and Configuration Guide will help you plan, configure, and successfully install WinZip® 26 Enterprise.

Note: WinZip Enterprise is available in two editions: WinZip Enterprise Government and Regulated edition (restricted) and WinZip Enterprise (unrestricted). **The default settings described in this guide apply to the WinZip Enterprise Government and Regulated edition**, in which the features are turned off, leaving only basic zipping and unzipping available by default. Although this guide is written from the perspective of enabling features, it can also be used to learn how to turn off features in the unrestricted edition.

WinZip is FIPS 140-2 compliant and is WIP (Windows Information Protection) aware. Examples of a few Enterprise environments are included later in this guide to show specific configurations and to help you determine what might be best for your organization's privacy and security policies.

Resources

Resource	Description
WinZip website http://www.winzip.com/	Information about WinZip Computing and its award-winning applications
WinZip Knowledge Base http://kb.winzip.com/kb/	Indexed and searchable articles with information about WinZip, its uses, and more
WinZip Support help@winzip.com	Contact email for help using WinZip, along with sales and service information
Microsoft Orca.exe http://msdn.microsoft.com/en-us/library/aa370557.aspx	Information on how to use the MSI file editing tool, along with download information
Microsoft Support – Group Policy http://support.microsoft.com/kb/816102	Microsoft article concerning the use of Group Policy for installing applications
MS System Center Configuration Manager http://technet.microsoft.com/library/gg682129.aspx	Technical information on the use of SCCM, including deploying and updating applications
VMware website http://www.vmware.com/	Information and software for virtualization
Microsoft Technet – FIPS 140 Validation https://technet.microsoft.com/en-us/library/security/cc750357.aspx	Information about Microsoft FIPS 140 compliance and validation
Microsoft Technet – Create a WIP policy: https://technet.microsoft.com/itpro/windows/keep-secure/overview-create-wip-policy	Information about using Windows Information Protection (WIP) to deploy an enterprise data protection policy

Contents

Planning the Installation

Customizing the WinZip MSI file

How the WinZip Enterprise MSI file differs from other WinZip versions

Enterprise lets you select the features you want to install, rather than requiring you to disable unwanted ones. WinZip® Express for SharePoint add-on information is covered later in the guide.

Choosing WinZip features

If WinZip® Enterprise is installed without any modifications, it will essentially be a zipping and unzipping tool with no shortcuts and no user configurable options. The following information concerns entries in the MSI file **Property** table that can be configured to add features or change the behavior of WinZip. Additional information in the Conversions, Cloud Services, and Social Media section and the Example Usage Scenarios section of this guide can help you select features.

Property	Description
ADDDESKTOPICON	Default=0, No WinZip shortcut on the Desktop; on=1. Settings apply to WinZip and applets.
ADDFILEASSOCIATION	Default=2, all supported file types will be associated with the appropriate applet (Image or PDF); 0=no associations; 1= WinZip Image Manager is added to the Open With menu for all supported image files.
ADDMENUGROUP	Default=0. No WinZip group available at Start -> All Programs for users; on=1
ADDSTARTMENU	Default=0, No WinZip shortcut at the top of the Start menu; on=1 Settings apply to WinZip and applets.
ALWAYSENCRYPT	Default=DEFAULT, off (or FALSE); TRUE forces the use of encryption
AUTOOPENREADONLY	Default=1, Contents of Zip files opened from the Temp folder, such as when received as an attachment, will be Read Only; off=0
CONTACTSOURCE(1-4)	Default=NONE. No preset email contacts to be used by the WinZip emailer; up to 4 different sources can be defined. See Configuring a combined address book for Contacts.

DEFAULTCLOUDSERVICE	Specify one of the available cloud services to act as the default. Default = no service selected.
DEFAULTLANGID	Default=1, WinZip language is set to language of OS at installation; 0=No default language. If conditions are met, WinZip language will follow the language of the current OS (ALLLANGS must = 1, AUTOLANG must = 0). A locale ID can also be used to specify the language. See Language options.
DEFAULTSHARESERVICE	Specify one of the available cloud services to be the default for sharing files. Default = no service selected.
DEFAULTUIMODE	Default=1, Ribbon starts in expanded mode; 0=Ribbon starts minimized
DEFCOMPICK	Default=Legacy, create .zip files; Best = create .zipx files
DISABLECLOUDSERVICES	Default=ALL, disables all cloud services; other options are NONE; ALIBABACLOUD, AMAZONS3, AZUREBLOB, BOX, CENTURYLINK, CLOUDME, DROPBOX, FTP, GOOGLECLOUD, GOOGLEDRIVE, IBMCLOUD, IONOS, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, OVH, RACKSPACE, S3COMPATIBLE, SHAREPOINT, SUGARSYNC, SWIFTSTACK, TEAMSSHAREPOINT, WASABI, WebDAV, and/or ZIPSHARE
DISABLECONVERSIONS	Default=ALL, disables all conversion features; other options are NONE; IMAGERESIZE, CONVPHOTOS, REMOVEPERSDATA, DOCTOPDF, PDFTODOC, WATERMARK, ENLARGEREDUCEIMAGE (File Management tool only), COMBINEPDFFILES and/or SIGNPDFFILES
DISABLEDIPUS	Default=2. Installs both stub and applet exe (no user download necessary, applets not automatically updated); 0=Installs only stub exe (user must download); 1=Installs both stub and

	applet exe (no user download necessary, applets automatically updated);
DISABLEFILEEXPIRATION	Default=0. Schedule for Deletion option (file expiration) is available; off (controls hidden; functionality unavailable)=1
DISABLEFIPSPOLICYWARNING	Default=0; Warning that displays when FIPSComplianceMode is set to RELAXED is not disabled; on=1
DISABLEIMGUTIL	Default=1, no image applet available; off=0
DISABLENOTIFICATIONSERVICES	Default=ALL, disables all Social Media options; other options are NONE; FACEBOOK, LINKEDIN, SLACK, TWITTER, YOUTUBE, GTALK, FACEBOOKCHAT, JABBER, YAHOOMESSENGER, OFFICE365GROUPS, TEAMS, and TWITTERMESSAGE
DISABLEPDFUTIL	Default=1, no PDF applet available; off=0
DISABLEPERSONALCONTACTS	Default=1, personal email addresses cannot be used in the WinZip emailer; off=0
DISABLERECENTARCHIVES	Default=1, recently used archives are not recorded; off=0, they are recorded
DISABLERECENTJOBS	Default=1, recently used jobs are not recorded; off=0, they are recorded
DISABLERECIPIENTSERVICES	Default=ALL. No email address recipient services will be available; other options are NONE, EXCHANGECONTACTS, GOOGLECONTACTS, LDAPCONTACTS, OUTLOOKCONTACTS, OUTLOOKPOCONTACTS, SLACKCONTACTS, and YAHOOCONTACTS
DISABLESBKUPUTIL	Default=1, no backup applet available; off=0
DISABLESETTINGSFROMCLOUD	Default=1, WinZip settings cannot be saved to or retrieved from a cloud service; off=0
DISABLESHAREDFILES	Default=1, Shared files folder will not display; off=0
DISABLESHORTLINKS	Default=1, Link shortening options are disabled; on=0
DISABLEVIRTUALZIP	Default=1, Zip virtualization for On-demand Downloading is disabled; on=0

DISABLEVIRTUALZIPMETRICS	Default=1, Zip virtualization metrics is disabled (default); on=0. The metrics save and retrieve Zip file directory size and location information to optimize the speed of loading cloud-based Zip files.
DISABLEZIPANDSHARE	Default=1, No Zip and Share (WinZip Express) context menu entry and a disabled Zip and Share button on the Tools tab; both available=0
ENABLEEXPRESSFEATURES	Default=0, WinZip Express features (Zip and Share, Snap and Share, and Scan and Share) are not available; on=1
ENCRYPTDISABLEMETHODS	Default=DEFAULT, all are on; options: ZIP20, AES128, and/or AES256
ENCRYPTREPLACEMENTS	Default=0, Unlocked: User can set preference to enable or disable the requirement to use a password when updating or deleting encrypted files (WinZip Options > Advanced). 1=Locked by admin to on (password always required; option hidden from user). 2=Locked by admin to off (password not required; option hidden from user).
ENCWIPEDELETE	Default=0, A caution message will display when certain files cannot be wiped, they are then deleted normally; on=1 (the caution message is suppressed, files of this type will be deleted only)
FIPSComplianceMode	Default=DISABLED (disables FIPS mode use in WinZip); other options are DEFAULT (WinZip follows the compliance setting of the computer), STRICT (allows only approved FIPS operations), RELAXED (shows warnings before executing unapproved FIPS operations)
HIDEREGINFO	Default=1, the link in the About WinZip dialog is hidden; off=0
HIDESECMENU	Default=0, display the Show WinZip Security Menu options; off=1
INSTALL[*cloud service]	Default=1, the named cloud service files will be installed; off=0, the named cloud service files will not be installed; cloud service names are NONE; ALIBABACLOUD, AMAZONS3,

	AZUREBLOB, BOX, CENTURYLINK, CLOUDME, DROPBOX, FTP, GOOGLECLOUD, GOOGLEDRIVE, IBMCLOUD, IONOS, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, OVH, RACKSPACE, S3COMPATIBLE, SHAREPOINT, SUGARSYNC, SWIFTSTACK, WASABI, WebDAV, and/or ZIPSHARE; example: INSTALLZIPSHARE
INSTALLBGBIN	Default=0, the Recycle Bin background tool will not be installed; on=1. See Cleaner tool configuration for options.
INSTALLBGCUST	Default=0, custom cleaner tool option is hidden; on=1 (custom cleaner tool displays). See Cleaner tool configuration for options.
INSTALLBGDD	Default=0, Duplicate File Cleaner will not be installed; on=1. There are no other configuration options for the tool (user chooses settings).
INSTALLBGDNLD	Default=0, the Downloads background tool will not be installed; on=1. See Cleaner tool configuration for options.
INSTALLBGDOCS	Default=0, the Documents background tool will not be installed; on=1. See Cleaner tool configuration for options.
INSTALLBGOP	Default=0, the Organize Photos tool will not be installed; on=1. There are no other configuration options for the tool (user chooses settings; the tool cannot be locked).
INSTALLBGPICS	Default=0, the Pictures background tool will not be installed; on=1. See Cleaner tool configuration for options.
INSTALLBGQA	Default=0, the Quick Access Folder Cleaner background tool will not be installed; on=1. See Cleaner tool configuration for options.
INSTALLBGTEMP	Default=0, the Temporary files background tool will not be installed; on=1. See Cleaner tool configuration for options.
INSTALLBGZS	Default=0, the ZipShare Folder Cleaner background tool will not be installed;

	on=1. See Cleaner tool configuration for options.
INSTALLCMD	Default=/noc4u /noaod /disableaod /autoinstall; add/remove switches as desired - see below
INSTALLEDP	Default=0, Enterprise Data Protection support, also called WIP, is turned off; on=1
INSTALLEXPRESSOFFICE	Default=0, WinZip Express for Office will not be installed; on=1
INSTALLFAH	Default=0, File Association Helper will not be installed; on=1
INSTALLJOBFILES	Default=0, no preconfigured job files installed; install=1
INSTALLOMNI	Default=1. In-app analytics tracking is enabled; off=0
INSTALLPREVIEWER	Default=0, no WinZip file preview feature for Explorer; install=1
INSTALLUPDATENOTIFIER	Default=0, an update notifier that displays alerts about updates when WinZip is not in use will be installed; on=1
INST_EXPL_SHELL	Default=1, WinZip context menu available; prevent the install of the shell extension (context menu)=0
LOCKADDONS	Default=0, Express Add-ons (if installed) are not locked); on =1
LOCKSECMENU	Default=0, the selection for Show WinZip Security Tools Menu will not be locked; on=1
MAXUPSZ_[*service]	Default=0, maximum allowed by the service; number value sets a maximum upload size in megabytes; there are ten separate properties, such as MAXUPSZ_AMAZON.
NOEDITMAILACCTS	Default=0, allows adding/editing email accounts for the WinZip email feature; prevent=1
NOEDITMAILSVCS	Default=0, allows adding/editing email services for the WinZip email feature; prevent=1
NOINTERNALEMAILER	Default=1, no WinZip email feature (not available and No Email tab in WinZip Options; available=0

NOUSERCLOUDDEFAULT	Default=DEFAULT, off (same as FALSE) users can specify a default cloud service; *TRUE=users cannot specify a default cloud service
PASSWORDLENGTH	Default=8, 8 character encryption password length policy; values from 1 to 99 are allowed
PASSWORDREQLOWER	Default=DEFAULT, off (same as FALSE); TRUE requires at least one lower case letter character in encryption passwords
PASSWORDREQNUMBER	Default=DEFAULT, off (same as FALSE); TRUE requires at least one number in encryption passwords
PASSWORDREQSYMBOL	Default=DEFAULT, off (same as FALSE); TRUE requires at least one symbol character in encryption passwords
PASSWORDREQUPPER	Default=DEFAULT, off (same as FALSE); TRUE requires at least one upper case letter character in encryption passwords
PASSWORDRESTRICT	Default=TRUE, on (users cannot change password policies and no Passwords tab in WinZip Options); DEFAULT or FALSE - users will have a Passwords tab in WinZip Options and can change password policies
SECMENU	Default=1, enables the "Show WinZip File Security Menu" checkbox; off=0
SHOWZIPSHARETRACKINGFOLDER	Default=1, on. Shared Files folder is visible in Files pane; off=0
USAGECOLLECTLOCK	Default=1, on, users cannot change the data collection setting, off=0
USAGEPICK	Default=Usage_No, turns data collection off; on=Usage_Yes
WRITABLE_FOLDER_[*service]	Default="\"(root); Path entered will be used for Share upload operations, acts as the user root folder location in which the "ZipShare" folder, "timestamp" folder, and files are written
ZIPSHARETRACKINGENABLED	Default=1, on. Tracking of shared files using ZipShare enabled; off=0

*Note: When setting **NOUSERCLOUDDEFAULT** to TRUE, a default service should be provided in both **DEFAULTCLOUDSERVICE** and **DEFAULTSHARESERVICE** if both are to be available.

Additional Features

You can add these properties to the MSI file Property table.

Property	Description
INSTALLDIR	Value should be a drive letter and path to the intended install location
USER_WZMUL_LOCATION	Value should be the path to a shared folder in which the registration file (WinZip.wzmul) is stored; a UNC path works best

Configuring Customizations

After you select the features you want, you need to customize the installation. You can use an MSI file editor, such as Microsoft Orca, either to edit the Property table directly or to create one or more transform files (.mst). Properties described in the tables above can be added to a Windows Installer command line as install options. The basic syntax for such a command is:

msiexec /Option <Required Parameter> [Optional Parameter]

For more on this, see Command line usage for installing with the WinZip MSI file.

The INSTALLCMD Property

INSTALLCMD can be edited to remove or include switches. The default value is **/noc4u /noaod /disableaod /autoinstall**. The **/autoinstall** switch must be included and it must be last. Each switch must be preceded by the forward slash (/) and must have a space between it and the next switch. The table below explains the purpose of each switch.

Switch	Description
noc4u	Disable and remove the **Check for Update** feature
nojobrunprompt	Prevent the prompt dialog from appearing when running WinZip jobs (**Caution:** Be sure to consider the security implications of allowing your users to run WinZip Job files automatically before using this parameter.)
altext "XXX"	The **altext** property will associate the file extension you specify with WinZip. In other words, if you double click a file with the extension specified, it will open in WinZip.
noaod	Prevent WinZip from automatically opening MS Office files when you double click a Zip file
disableaod	Prevent users from changing the **auto-open for Office files** feature*

*Note: Using the **/disableaod** switch by itself will **not** disable "auto-open". The **/noaod** switch must also be used to both disable this and to prevent configuration changes.

Language options

You can choose the application language using the **DEFAULTLANGID** property. The value set for this property determines the value assigned to the **InstalledUILangID** registry key. As described in the property table, you can choose one of the following options:

- **0**=No specified language. WinZip will update so that it always matches the current OS language. There are two conditions:
    - The language must be supported by WinZip (if not, WinZip defaults to English).
    - The following values must be set: **ALLLANGS**=1 (to install all language assets), **AUTOLANG**=0
- **1**=WinZip locks to the language of the OS during installation, as long as the language is supported (if not, WinZip defaults to English).
- Locale code: You can enter one of the following language codes to specify the application language.

1031 - German	**1040** - Italian	**1046** - Brazilian Portuguese
1033 - English	**1041** - Japanese	**2052** - Chinese Simplified
1036 - French	**1043** - Dutch	**3082** - Spanish

Password Policy properties

The table at the top of this article lists and describes the available Password Policy properties. Listed alphabetically, the properties are: **ALWAYSENCRYPT**, **ENCRYPTDISABLEMETHODS**, **PASSWORDLENGTH**, **PASSWORDREQLOWER**, **PASSWORDREQNUMBER**, **PASSWORDREQSYMBOL**, **PASSWORDREQUPPER**, and **PASSWORDRESTRICT**.

ENCRYPTDISABLEMETHODS can be used to disable one, two, or all three encryption methods. When disabling more than one method, use a comma to delimit the values. For example, if 256-bit AES encryption is the only method desired, the value for **ENCRYPTDISABLEMETHODS** should read **ZIP20,AES128**.

Each of the password policy properties creates a registry setting. These registry settings and their values are described in Registry settings for WinZip; Policies and more.

Configuring a combined address book for Contacts

You can use the combined address book feature to gather contacts from multiple sources if you are using the WinZip emailer. The WinZip emailer is an internal email feature for email services if your organization does not use a MAPI client (such as Outlook). The WinZip emailer can be set up from **File** > **WinZip Settings**. In the **WinZip Options** window, click **Email** in the **Settings** list. You must configure the **NOINTERNALEMAILER** property to have a value of "0" if you wish to use the WinZip emailer.

If you click **Contacts** in the **WinZip Options** window, you can find the controls for setting up the combined address book. **Contact sources** can be configured during the install by making use of the four

CONTACTSOURCE properties in the MSI file. When this is done, the feature will be "locked", that is, users will be unable to add any other contact sources on their own. Contact sources that can be configured include **GOOGLECONTACTS**, **LDAPCONTACTS**, **OUTLOOKCONTACTS**, **OUTLOOKPOCONTACTS**, **SLACKCONTACTS**, and **YAHOOCONTACTS**. For example, if you want all users to have their Google contacts available, you could set this: **CONTACTSOURCE1=GOOGLECONTACTS**. You can also provide an LDAP contact source (LDAPCONTACTS) and/or an Exchange contact source (EXCHANGECONTACTS). Additional parameters are required for the latter contact sources. For example:

CONTACTSOURCE2=EXCHANGECONTACTS:url=https://10.35.1.10/QRST/Exchange.asmx
The parameter to be supplied is the Exchange server URL.

CONTACTSOURCE3=LDAPCONTACTS:ip=10.35.1.62,domain=mybusinessinc.com
The parameters to be supplied are the IP address and Domain name.
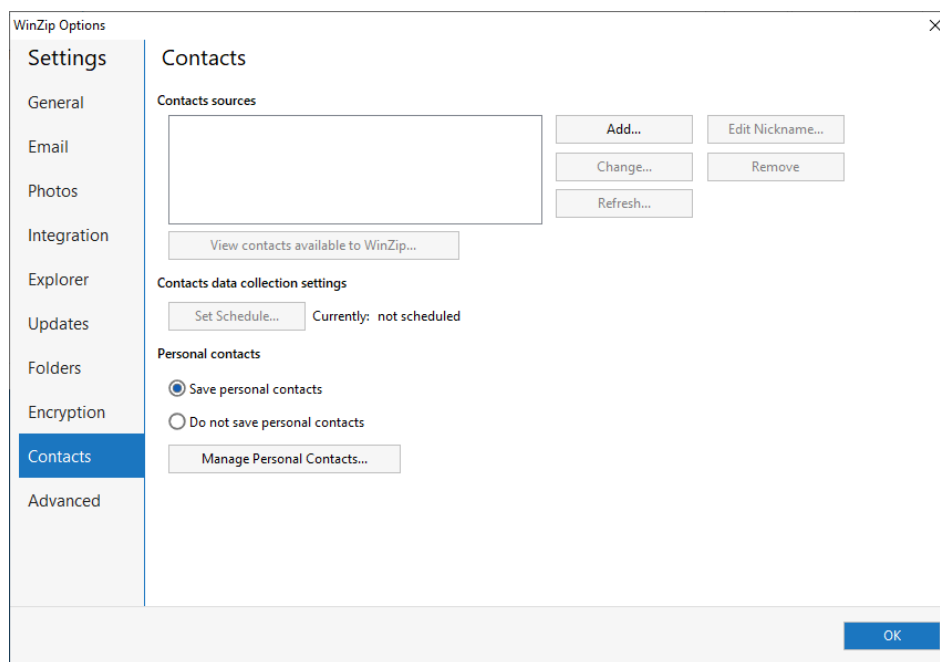
When contact sources are configured in this way, the user is asked to sign in to the services the first time they use the address book.

If you have not configured any of the **CONTACTSOURCE** properties and have enabled any or all of the contact sources by means of the **DISABLERECIPIENTSERVICES** property (i.e. set to **GOOGLECONTACTS** or **NONE**), users will be able to click the **Add** button on the **Contacts** page of **WinZip Options** window and add the services they want.
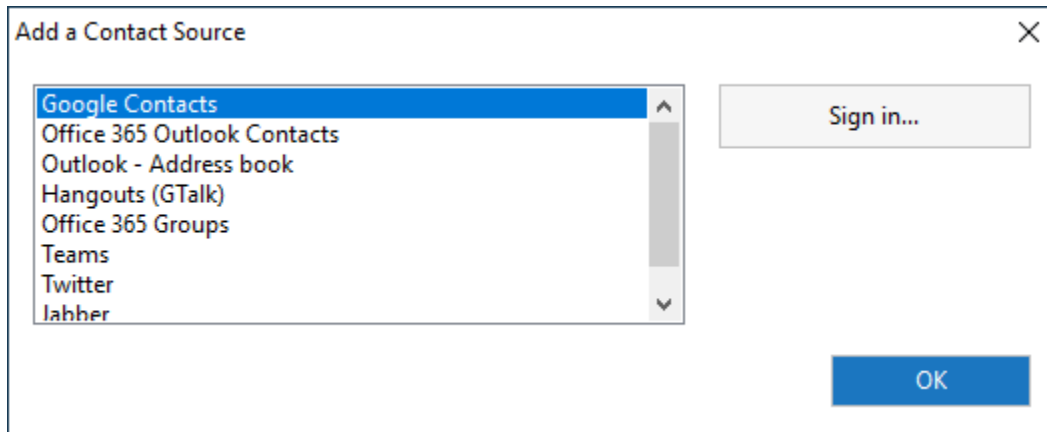
When the user adds a contact source in this way, they are prompted to sign in to the service before it is added to the address book.
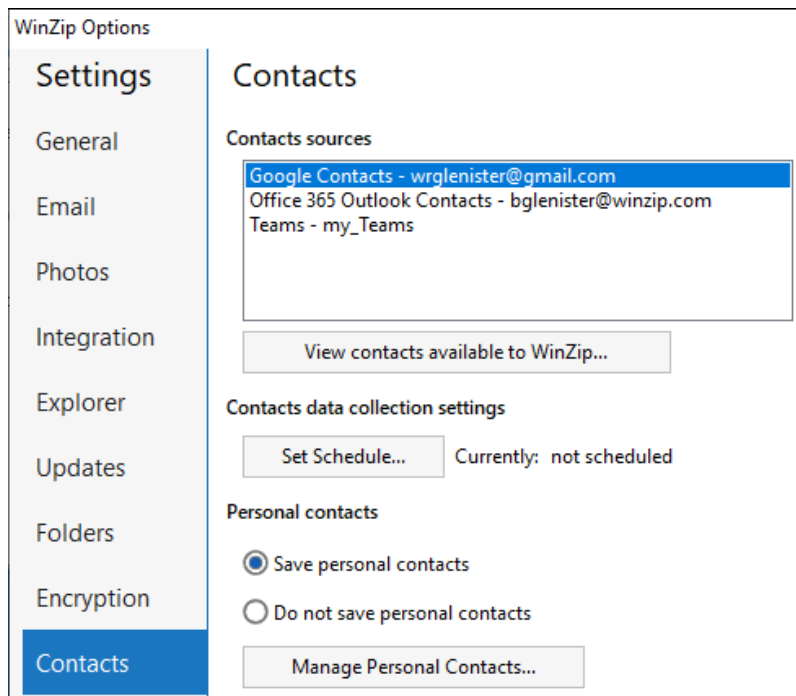
Users can add individual contacts manually to the combined address book if the **DISABLEPERSONALCONTACTS** property is set to the value **0**.

If you choose to view your entries **By Source**, you will find tabs for each source including **Personal**. You can choose to save or not save your personal contacts on **Contact** page of the **WinZip Options** window.
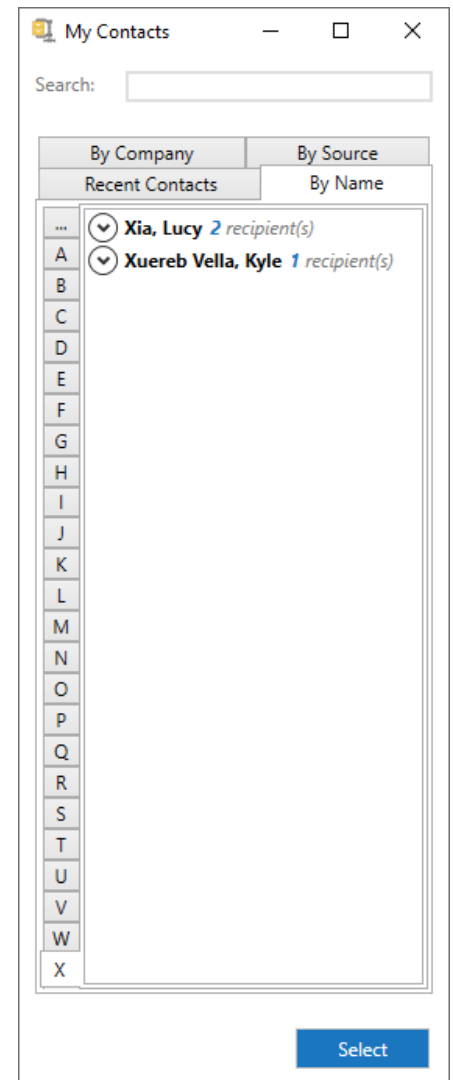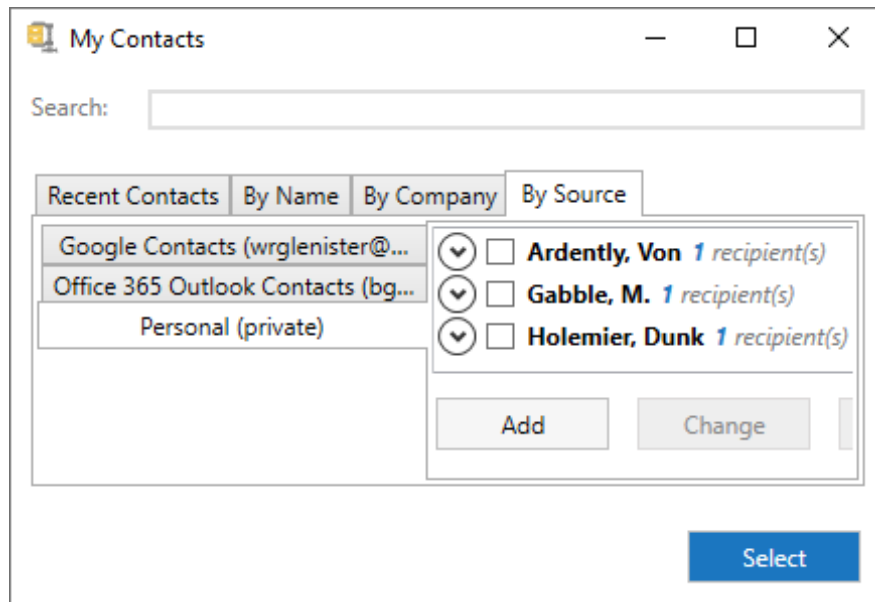
Cleaner tool configuration

You can set configuration options for the cleaner tools, including **Documents File Cleaner** (INSTALLBGDOCS), **Downloads File Cleaner** (INSTALLBGDNLD), **Pictures File Cleaner** (INSTALLBGPICS), **Quick Access Folders Cleaner, Recycle Bin Cleaner** (INSTALLBGDNLD), and **Temporary File Cleaner** (INSTALLBGTEMP), **ZipShare Folder Cleaner** (INSTALLBGZS).

If enabled in the application, you can find the settings in the **WinZip Options** window, under **Tools**.

By default, cleaners are not installed (MSI value is set to 0). If the one or more cleaners are installed (MSI value set to 1), you can configure them with the settings described below. Note: The cleaner tasks are scheduled after WinZip is first run for the user account associated with the first run.

- **minDays**: Lets you set a minimum age for files that you want to clean, based on the file's access date. You can set a number between 1-99998. For example, a setting of 4 would mean that no files that have been accessed within 0-3 days will be cleaned. You can use it in conjunction with **maxDays** to create a range. The default value if not specified is 30. Note that the **minDays** setting does not affect the **Temporary File Cleaner** and **Recycle Bin Cleaner** tools.
- **maxDays**: Lets you set a maximum age for files that you want to clean, based on the file's access date. You can set a number between 1-99999. The setting must be higher in value than the **minDays** setting. For example, a setting of 21, in conjunction with a **minDays** setting of 4 would mean that only files that have been accessed within the last 4-21 days will be cleaned. The default value if not specified is 99999. Note that the **maxDays** setting does not affect the **Temporary File Cleaner** and **Recycle Bin Cleaner** tools.

- **locked**: Determines if the user is able to change the cleaner tool settings. By default, tool settings are unlocked (value = 0). If the value is set to 1, the settings are locked. **Note:** A schedule must be set before you lock the settings.
- **sched**: Lets you choose a daily, weekly, or monthly schedule by using the following settings:
  - **daily:** Lets you schedule a cleaner by day.
    - Use **freq** to set a value from 1-30 days. For example, a value of 10 will run the task every 10 days. If the parameter is present but no value is set, the default is 1. If a schedule is set with no freq, the default is 2.
  - **weekly:** Lets you schedule weekly cleaners.
    - Use **freq** to set a value for a minimum of 1 (once per week) and a maximum of 4. If no value is set (or if the value is invalid), "1" is used.
    - Use **dow** to select days of the week by choosing values between 1-7, where 1 is Monday and 7 is Sunday (if no value is set, the current day of the week is used). For multiple days of the week, use the "+" sign between values.
    - For example, to run a cleaner Tuesday, Thursday, and Sunday, you would use the following setting: **sched=weekly,freq=3,dow=2+4+7**.
  - **monthly-dom:** Lets you set a monthly schedule by days of the month.
    - Use **months** to schedule a cleaner by choosing values between 1 and 12, where 1 is January, and 12 is December. Multiple months can be specified by using the "+" sign between values, or you can set the value to "all" to choose all months (if "all" is present, it overrides any other values). If no value is set (or if all values are invalid), then "all" is used.
    - Set a value for **dom** to select a day of the month, from 1 to 31, or "last" (to choose the last day of a month). For multiple dates in a month, use the "+" sign between values.
    - For example, to schedule a cleaner to run in January and July, on 15th day of the month, use the following setting: **sched=monthly-dom,months=1+6,dom=15**
  - **monthly-dow:** Lets you set a monthly schedule by the day of the week.
    - Use **months** to schedule a cleaner by choosing values between 1 and 12, where 1 is January, and 12 is December. Multiple months can be specified by using the "+" sign between values, or you can set the value to "all" to choose all months (if "all" is present, it overrides any other values).
    - Use **weeks** to schedule which weeks in the months to run the cleaner by choosing values from 1-4. Multiple weeks can be specified by using the "+" sign between values, or you can set the value to "all" to choose all weeks.
    - To select days of the week, use **dow** values between 1-7, where 1 is Monday and 7 is Sunday (if no value is set, the current day of the week is used). For multiple days of the week, use the "+" sign between values.

- ▪ For example, to schedule a cleaner to run on Mondays of the first and third week of every month, use the following setting: **sched=monthly-dow,months=all,weeks=1+3,dow=1**
- **start**: Lets you set the date of first run for a cleaner. For example, to start on May 15, 2020, enter 20200515 (yyyymmdd).
- **time**: Lets you schedule the cleaning task by setting a time of day in HHMM (hours and minutes, using the 24-hour clock format). For example, to start a cleaning task at 9:00 am, use 0900. To start a task at 10:30 pm, use 2230. If no value is set (or if the value is invalid), the time defaults to the next half hour from the time of installation (if installed at 09:17 am, the time is set to 09:30 am).

Example: Full cleaner configuration:

INSTALLBGDOCS: 1,minDays=90,maxDays=99999,locked=1,sched=daily,freq=10,start=5,time=0600

In this example, the options affect the Documents folder cleaner. The unnamed setting '1' (which must appear first) installs the cleaner. The minDays and maxDays values indicate that files that have not been accessed in 90 days are candidates for cleaning. The locked=1 setting prevents users from modifying the cleaner settings. The tool will be run every 10 days (sched=daily,freq=10) on Fridays (start=5) at 6 AM (time=0600).
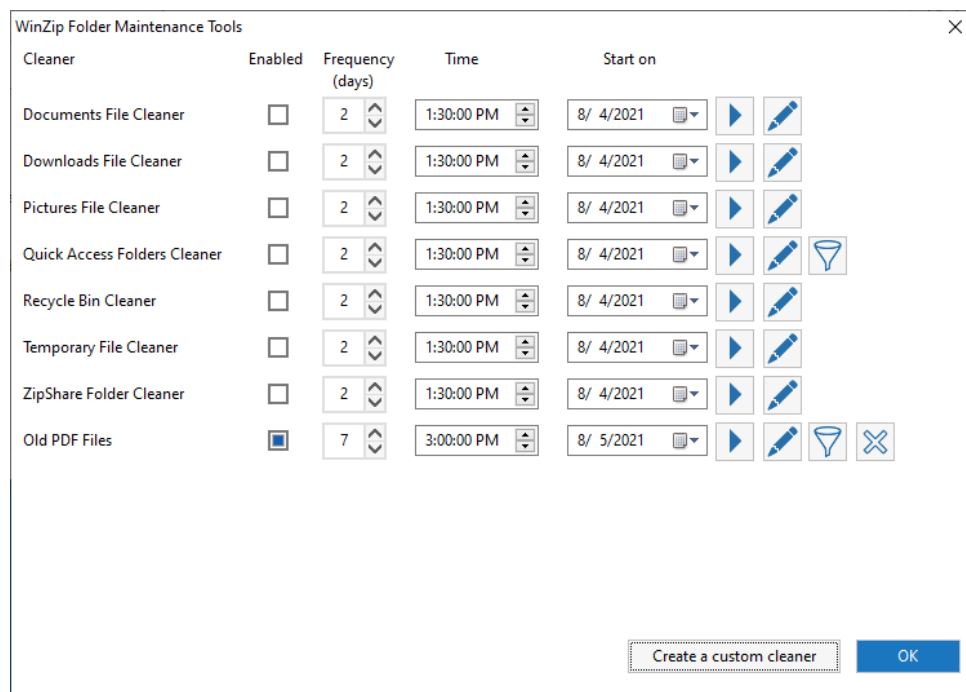
A custom cleaner, Clean old PDFs, was added to the Cleaner list.

Custom cleaner: You can add custom cleaners to **Tools**. The custom cleaner function (INSTALLBGCUST) is hidden by default (0), but can be made visible by setting the property value to 1. INSTALLBGCUST is configurable in the same way as the other tools. When visible, you can create a custom cleaner in the application by clicking **Settings** > **WinZip Options** > **Tools**, and clicking the **Create a custom cleaner** button. Follow the instructions in the **New Custom Folder Cleaner** window and click **OK**. If you want to set a filter for

the custom cleaner, in the **Cleaner** list, click the filter button 🔽 for your cleaner, ensure the **Include** tab is open (default), click **Add a pattern**, and enter the wildcard and file information that you want to use. For example, if you want to clean all PDFs, enter ***.PDF**. Alternatively, you can filter out some file types by clicking the **Exclude** tab, and adding a pattern for a file name or file type that you never want to clean.

Using WinZip with WIP (Windows Information Protection)

WinZip 25 Enterprise is a WIP-aware application. WIP (Windows Information Protection) is used to create an EDP (Enterprise Data Protection) policy.

What problem does WIP/EDP solve?

Users systems are set up by listing the domains and network locations that a user has access to. This means that you can end up with a network location that contains files that are managed by different domains. The result is that users might have access to files that they shouldn't. WIP/EDP (Enterprise Data Protection) restricts users from opening these files if they have not been given permission by the domain that manages the files.

The solution: Designated work files and personal files

In WIP/EDP (Enterprise Data Protection), files are separated into either work or personal. Work files are associated with a managing domain. Work files can reside only in secure locations. Although personal files can reside in the same location, the files are treated differently—actions are restricted when dealing with files tagged as work, but there are no restrictions on personal files.

For detailed information about using WinZip with WIP, see WinZip Enterprise and Windows Information Protection (WIP).

Important things to know about using WinZip with WIP

- WinZip is unable to wipe temporarily extracted files if it is deployed in a WIP environment. To prevent dialog boxes that state this fact from displaying, it is recommended that you configure the **ENCWIPEDELETE** property to have the value **1** before you deploy. With this setting, WinZip will simply delete the temporarily extracted files and no dialog box about wiping will display.
- Users are not allowed to save or extract work files to unsecure locations like non-corporate clouds, social media, or instant messaging.
- Users cannot copy and paste or drag-and-drop work files from WinZip to a WIP-unaware application.
- Any file tagged as a work file must maintain that tag unless specifically changed by the user. This includes any files run through WinZip file converters, such as **Convert to PDF**.
- All secure network resources and client devices are formatted NTFS and have the encrypted file system (EFS) enabled.
- Corporate clouds can be added to the secure resource list so that they can be used in the office and remotely.

Enterprise-wide password management

WinZip Enterprise lets administrators set up an enterprise-wide key that can be used to unlock .zip and .zipx files that individual employees have encrypted with WinZip. The goal is to prevent data loss by ensuring that files can be decrypted in the event the original encryption password is lost or not available. The system uses Windows digital certificates to create a private/public key pair to encrypt passwords associated with individual .zip and .zipx files. The private enterprise key can then be used to retrieve and decrypt the corresponding file passwords. The enterprise key can be updated without losing the password information. Administrators can set up more than one enterprise key.

The Enterprise-wide password feature does not alter or impact the way users encrypt or decrypt files in WinZip—no additional user interaction is required after the administrator configures user systems with the public key.

Important: Administrators should review security protocols for their environment carefully before considering an enterprise-wide password implementation.

Options for user certificate access

The following values can be used to determine user certificate access:

- **SS=NM: My** — WinZip will find a certificate installed in **Current User**, Personal (user-specific access)
- **SS=NM: Root** — WinZip will find a certificate installed in **Current User** or **Local Machine**, Trusted Root Certificate Authorities
- **SS=NM: Trust** — WinZip will find a certificate installed in **Current User** or **Local Machine**, Enterprise Trust
- **SS=NM: CA** — WinZip will find a certificate installed in Current User or Local Machine, Intermediate Certification Authorities

Example: If you want to deploy the .cer to all users of a single machine, it should go in Enterprise Trust, Intermediate Certificate Authorities or Trusted Root Certificate Authorities.

Administrator setup

Administrators can use the following instructions to set up an enterprise-wide public key cryptography (**PKC**) for WinZip.

Note: When you import a certificate (tool: Microsoft Management Console (MMC), Certificate Import Wizard), ensure that the following Import option is enabled: **Mark this key as exportable**.

Set up certificates and registry

1. Generate a Windows digital certificate with your tool of choice. The X.509 certificate for the Windows Certificate Store must use the following parameters:
    - o Subject must contain **WinZip** as part of the name

  o CerStoreLocation

    ▪ For individual users = **cert:\CurrentUser\My**

    ▪ For multiple users on a single machine = **cert:\Root** or **cert:\Trust**, or **cert:\CA**

  o KeySpec **= KeyExchange**

  o KeyUsage **= KeyEncipherment**

2. Copy and save the **Thumbprint** code for the certificate.
3. Set up user access to the public certificate (either on local user system or remotely).
4. After you install WinZip Enterprise on the user systems, update the following Registry key (use method of your choice):

   - **Registry location:** HKEY_LOCAL_MACHINE\SOFTWARE\Nico Mak Computing\WinZip\Policies
   - **Name:** EntX509Certificate
   - **Data value:** SS=NM:My;FT=SHA1:[Thumbprint code]. For example, *SS=NM:My;FT=SHA1:710B6D9F61977FB12604FD238845E4459EA9081A*

     Note: *My* is replaced by a different value if creating a multi-user setup.

5. In WinZip Enterprise, verify that the password encryption system is working on the user's computer by clicking **Help** > **About**. A lock icon appears in the upper left corner of the dialog box if the system is configured correctly.
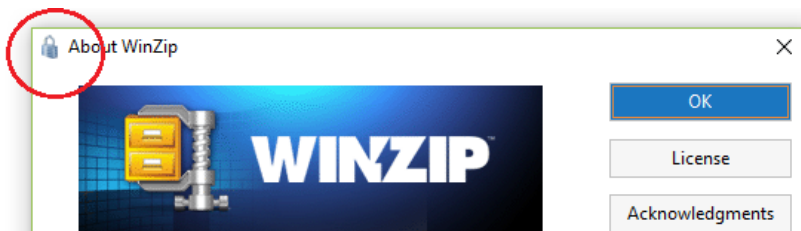
Retrieving passwords and updating enterprise certificates

To retrieve passwords and manage the enterprise certificates, the administrator uses a WinZip Enterprise Snap-in for the Microsoft Management Console (MMC).

Install the WinZip Enterprise Snap-in on the administrator system

1. On the administrator system that has the private key installed, copy **EWP MMC Snap-in.msi** to the computer and install the component.
2. Open the **Microsoft Management Console** (MMC).
3. Click **File** menu > **Add/Remove Snap-in**.
4. In the list of available snap-ins, select **WinZip Enterprise-Wide Password Snap-in** and click **Add**, and **OK**.

Retrieve passwords

1. In the navigation pane on the left side of the MMC window, click **Decrypted zip files list**.
2. In the **Actions** pane on the right side of the MMC window, click **Get user's passwords.**
3. Select the files that you need to decrypt and click **Open**.

4. In the **Windows Security** window, select the corresponding enterprise certificate (if you have more than one certificate set up).
5. The password decryption results are displayed in the middle pane.

Update the enterprise certificate for encrypted files

1. After generating a new certificate (see requirements in *Administrator setup*), open the **Microsoft Management Console** (MMC).
2. In the left pane, choose **WinZip Enterprise Wide Password** > **Update key records**.
3. In the **Actions** pane on the right, click **Use a different enterprise key**.
4. Select the folder that contains the files for which you want to change the key and click **OK**.
5. In the **Windows Security** window, select the current certificate, and click **OK**.
6. In the second **Windows Security** window, select the new certificate, and click **OK**.

WinZip Express

WinZip Enterprise includes all of the available WinZip Express features and add-ons, except WinZip Express for Outlook. In its place, the feature-rich WinZip® Courier™ is included, offering the potential for the most useful and powerful WinZip installation ever.

Although each extension can each improve user productivity, you may not wish to install them all. Please note that any customization made to the WinZip installation will also affect WinZip Express. For example, if one or more of the available cloud services is disabled, it will also be unavailable when zipping actions are done through WinZip Express.

Along with WinZip Courier, you can choose to install any of the following:

- WinZip Express features
    - WinZip Zip and Share
    - WinZip Snap and Share
    - WinZip Scan and Share
- WinZip Express for Office
    You can also install the following add-on:
-

Installing features

The WinZip Express features can be installed by setting the appropriate property in the MSI file with the value "**1**".

Installing add-ons

WinZip Express for SharePoint brings the power and convenience of WinZip Express directly to the **SharePoint Documents** web interface. This add-on must be installed on the SharePoint server in order for **Zip and Share**

to be available in the SharePoint web interface as a drop-down menu entry. WinZip does not need to be on the server, but it must be installed and registered on each targeted client computer.

Note: When WinZip Enterprise is installed, it includes a SharePoint cloud service. When enabled, WinZip Enterprise users can use this in much the same way that they would use other cloud services, such as Dropbox, Google Drive, etc.

Overview of WinZip Express Features

The WinZip context menu, used for zipping files or folders, remains very useful. WinZip Express extends and improves the context menu functionality, providing many new and useful features. Each of the WinZip Express features and add-ons makes use of the WinZip Express dialog. Some features will change or be omitted depending on which WinZip Express component you use. Here is the WinZip Express for Explorer dialog along with descriptions of each element:
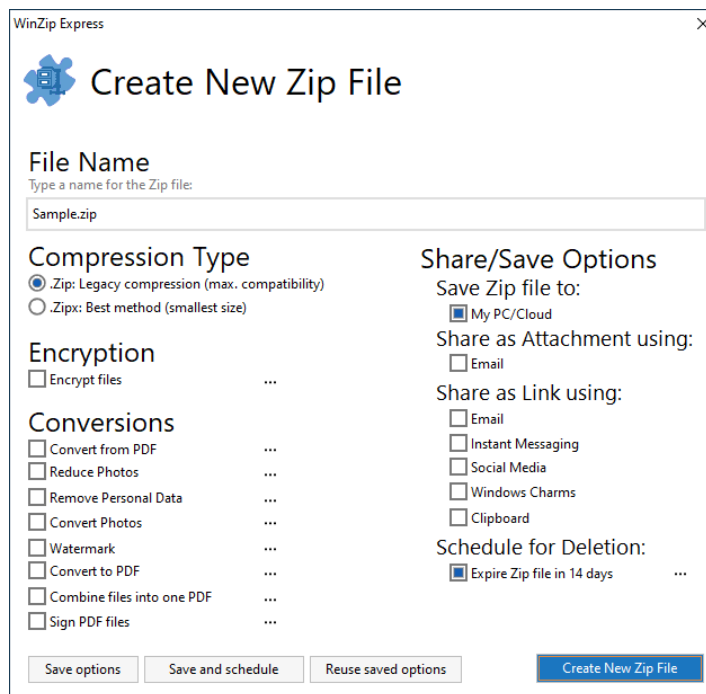
File Name

A default file name appears in this text box when WinZip Express opens. Click this box to type a different Zip file name.

Compression Type

WinZip Express preselects your default compression. Unlike the legacy WinZip context menu, WinZip Express allows you to change the compression type from .Zip to .Zipx or vice versa depending on what is best for each use.

Encryption

Files being zipped can also be encrypted using the **Encryption** strength set in the <u>WinZip Settings</u> tab. This option will be checked and grayed if the **Always Encrypt** property has been administered. If all three encryption strengths have been disabled, a dialog will display explaining the lack of availability. WinZip Express will comply with FIPS 140-2 if that has been configured.

Conversions

Any or all conversion options can be selected. These will be applied only to the appropriate file types. The conversions available are:

- **Reduce Photos** — Image files (BMP, DIB, EXIF, GIF, JPG, PNG, and/or TIF) will be resized to the smaller physical size that has been configured
- **Remove Personal Data** — Remove EXIF metadata from files (DOC, DOCX, GIF, JPG, PDF, PNG, PSD, PPT, PPTX, XLS, XLSX). See <u>Remove Personal Data</u> for details and exceptions.
- **Convert Photos** — Convert image files (BMP, GIF, JPG, JP2, PNG, PSD, TIF, and WEBP) from one file format to another
- **Watermark** — Image files (BMP, GIF, JPG, PDF, PNG, and/or TIF) will have a watermark phrase placed on them where and how it has been configured
- **Convert to PDF** — Document files (DOC, DOCX, XLS, XLSX, PPT, and/or PPTX files) will be converted to PDF files as they are added to a Zip file
- **Combine PDFs —** Combine two or more PDF files into a single PDF file
- **Sign PDF Files** — Sign PDF files for added security

Share/Save Options

WinZip Express provides multiple options for sharing and saving Zip files. Those options are:

Save Zip file to:

- **My PC/Cloud** — Save the Zip file to a local drive, external drive, network location, or any configured cloud service

Share as Attachment using:

- **E-mail** — Send the Zip file by email

Share as Link using:

- **E-mail** — Share via email; upload the Zip file to a cloud service and send a link to the receiver to download the file
- **Instant Messaging** — Upload the Zip file to a cloud service and place a link in one of the supported instant messaging services

- **Social Media** — Upload the Zip file to a cloud service and place a link to download the file on Facebook, LinkedIn, or Twitter
- **Windows Charms** — Upload the Zip file to a cloud service, and share the link by using a Windows Charm (app). For example, Windows Charms are available for Mail, OneNote, Skype, and other social media.
- **Clipboard** — Upload the Zip file to a cloud service; the link to download the file will be copied to the clipboard allowing you to paste it into the media of your choice.

Schedule for Deletion

Lets you set an expiration date for the Zip file, at which time the file will be deleted. This is particularly valuable with shared files that need to be available only for a given period of time so they don't accumulate.

Automation options

These buttons let you save and reapply your WinZip Express settings, as well as schedule WinZip Express to perform a saved set of operations automatically.

- **Save options** — Save the current WinZip Express settings to an options file that you can use later
- **Save and schedule** — Save the current WinZip Express settings and set a schedule for a single or recurring WinZip Express operation (uses Windows Task Scheduler)
- **Reuse saved options** — Apply WinZip Express settings from a previously saved options file

Note concerning cloud services
If a Zip file destination is selected that requires uploading to a cloud service, a dialog will display allowing the user to select a destination from those services that are enabled.

WinZip Zip and Share

If WinZip has been installed with the ENABLEEXPRESSFEATURES property set to "1" and the DISABLEZIPANDSHARE property set to "0", a root level context menu entry for WinZip Express will be available. Submenu entries for the legacy WinZip context menu are still available and will still be useful. However, WinZip Express provides many additional features compared to the context menu. Please see the [Overview](#) above for details.

WinZip Snap and Share

The **WinZip Snap and Share** feature streamlines the photo downloading process by reducing the number of dialogs to two (from five with the WinZip Camera Wizard). As with the WinZip Camera Wizard, **WinZip Snap and Share** allows users to retrieve images from a digital camera, compress them, and store them in a Zip file.

WinZip Snap and Share is activated when a camera is plugged into a USB port after **Zip from camera** is selected in the AutoPlay dialog or when **Photos** on the **Backup** tab is clicked.

The first page of the dialog displays the camera that has been detected, provides the options for retrieving pictures, and the options for removing pictures from the camera. The default settings can be used, or items can quickly and easily be changed.
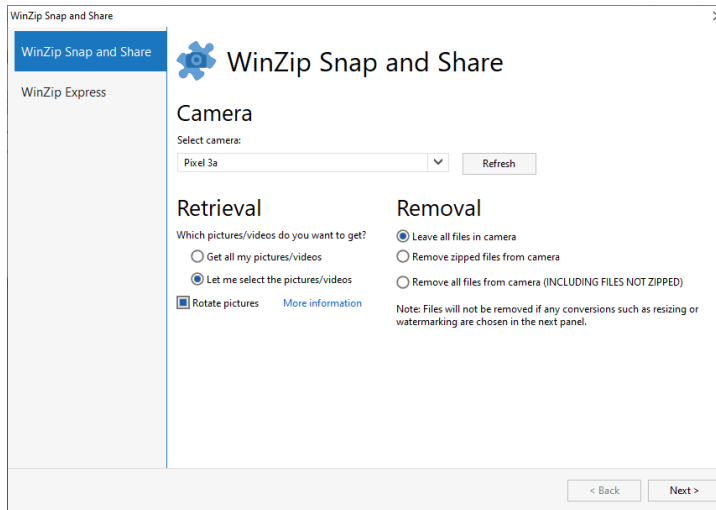
The second page of the dialog is very similar to the one used for WinZip Express for Explorer with these changes:

- A suggested name based on the date (yyyymmdd) and time (hhmmss) prefills the **File Name** text box
- No PDF conversion option is offered because it does not apply to photos
- An additional save option, **Current Zip File**, is available and can be used when a Zip file has been opened and the person wants to use WinZip Express to add more photos to that Zip file
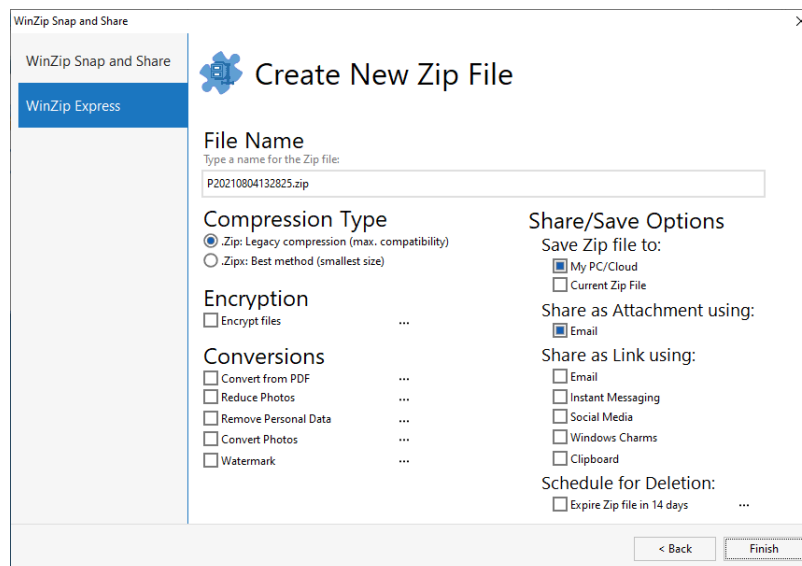
WinZip Scan and Share

The **WinZip Scan and Share** feature lets you capture and share images directly from a scanner. You can compress and store the scanned images in a Zip file. **WinZip Scan and Share** is available in WinZip when a scanner is plugged into a USB port.

The first page of the dialog displays the scanners that have been detected, lets you type a name for the scanned image, and provides image format options.
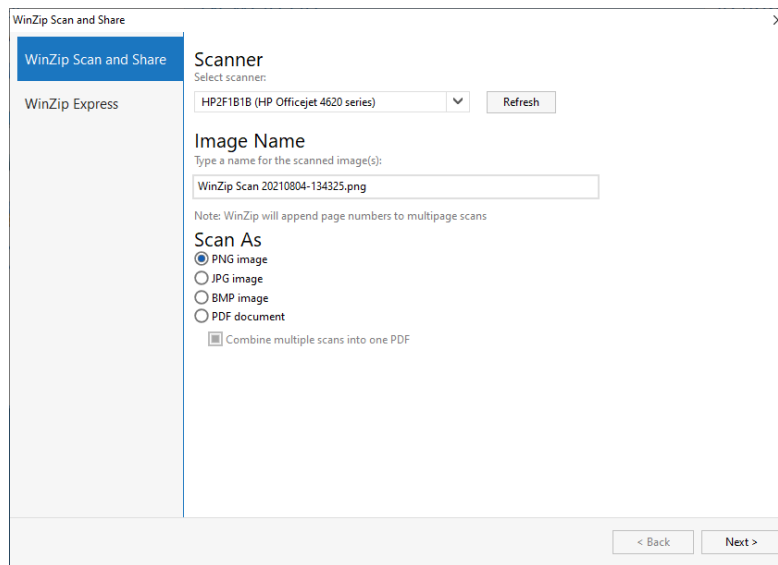

The second page of the displays the same options that appear on the **Snap and Share** WinZip Express page.
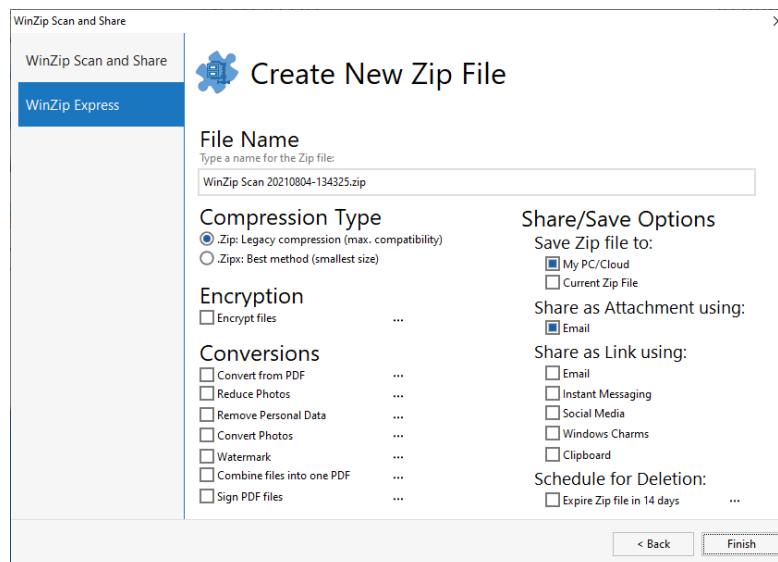
WinZip Express for Office

The WinZip Express for Office feature adds Zip and Share functionality to the File menu in Microsoft Word, Microsoft PowerPoint, and Microsoft Excel. You can share the Zip file through email, upload it to a cloud service, and share a link from a cloud service or social media, depending on the services that are enabled. WinZip Express for Office is compatible with Microsoft Office 2007 or higher.
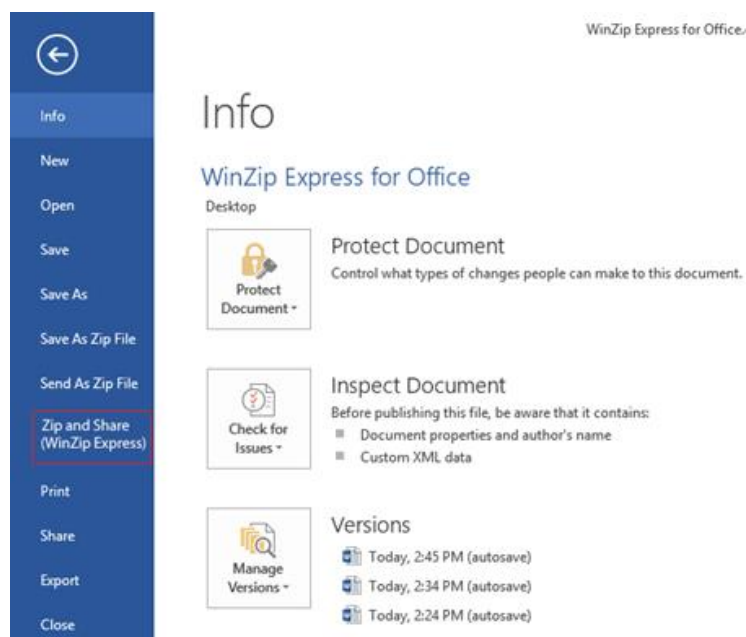
WinZip applets: WinZip PDF Express, WinZip Image Manager, and WinZip Secure Backup

Applets are utilities that can be launched from within **WinZip Enterprise** or used completely independently. For example, you can add, delete, or extract pages from a PDF file or add a watermark in **WinZip PDF Express** without opening **WinZip**. The applets consolidate and expand upon tools used for specific workflows. WinZip Enterprise includes the following applets:

- **WinZip PDF Express**: Consolidates a broad range of PDF tools that let you create, convert, edit, lock, and sign PDF files. To access the applet from WinZip, click **Tools**, and in the ribbon click **PDF Files** or click the **PDF** button in the **Actions** panel. Settings can be found in **File** > **PDF Settings**.
- **WinZip Image Manager**: Consolidates a broad range image image management tools that let you convert and edit image files. To access the applet from WinZip, click **Tools**, and in the ribbon click **Image Files** or click the **Image** button in the **Actions** panel. Settings can be found in **File** > **Settings**.
- **WinZip Secure Backup**: Consolidates Backup and Restore features, including scheduling and encryption options. To access the applet from WinZip, click **Backup/Clean**, and in the ribbon click **Folder** or click the **Backup** button in the **Actions** panel.

Enterprise users can manage the applets through several properties:

- **DISABLEIMGUTIL:** Specifies if WinZip Image Manager is available or not.
- **DISABLEPDFUTIL:** Specifies if WinZip PDF Express is available or not.
- **DISABLESBKUPUTIL:** Specifies if WinZip Secure Backup is available or not.
- **DISABLEDIPUS**: Controls updates for applets.
- **ADDDESKTOPICON:** Lets you add a desktop icon (applies to WinZip and the applets)
- **ADDFILEASSOCIATION:** Provides options for file format associations and the Open With menu.
- **ADDSTARTMENU:** Lets you add the applets to the Start menu (applies to WinZip and the applets)

For more information about the properties listed above, see [Customizing the WinZip MSI file.](#)

Conversions, Cloud Services, and Social Media

The three feature sets discussed in this section might be less familiar. All of them can be very useful when enabled. The features are available through WinZip Express and the WinZip user interface. Please consider this information when planning a WinZip Enterprise installation.
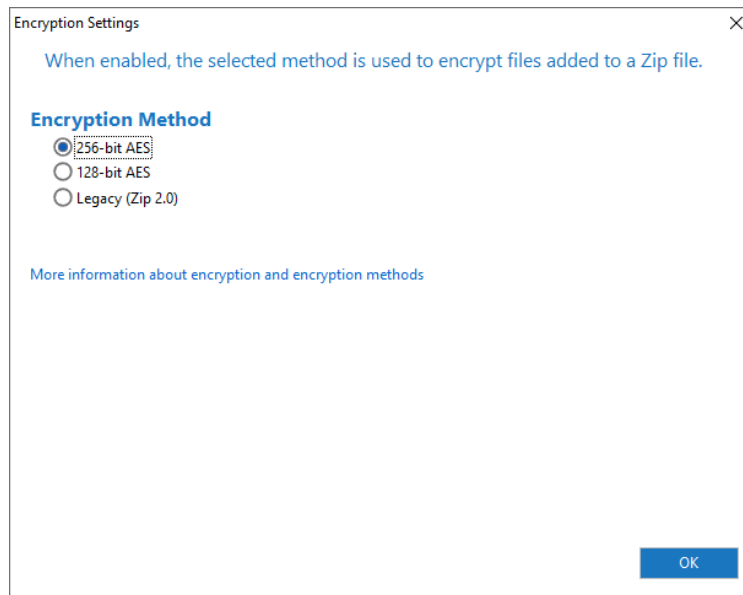
Conversions

Conversions are actions that make a lasting change to files that are contained in the Zip file. Encryption is a special type of conversion. It converts the file from its original format into an encrypted format. Encryption, however, can be undone by providing the correct password when unzipping, which produces an exact duplicate, unzipped file if no other conversions were used. Information about the other conversions follows.

The choice to convert files being zipped can be made in the WinZip user interface on the **Zip** ribbon, and in the **Send Selected Files** dialog when sharing files from an open Zip file, or in WinZip Express. The **Reduce Photo Size** conversion is also offered when Zip and Email or Zip and Email Plus is used, if any of the files being zipped are picture files.

Encryption

This conversion option lets you set the encryption method for the Zip file. In the Encryption Method area, choose one of the following:

- 256-bit AES
- 128-bit AES
- Legacy (Zip 2.0)

Reduce Photos

This conversion option can be used with the following supported picture/image files: BMP, DIB, EXIF, GIF, JPG, PNG, and/or TIF. Reducing creates physically smaller pictures, which will also be significantly smaller files. Reducing a picture's size also reduces its resolution. This is usually fine for sharing, but not for printing. You should not reduce pictures when their quality is of major importance.
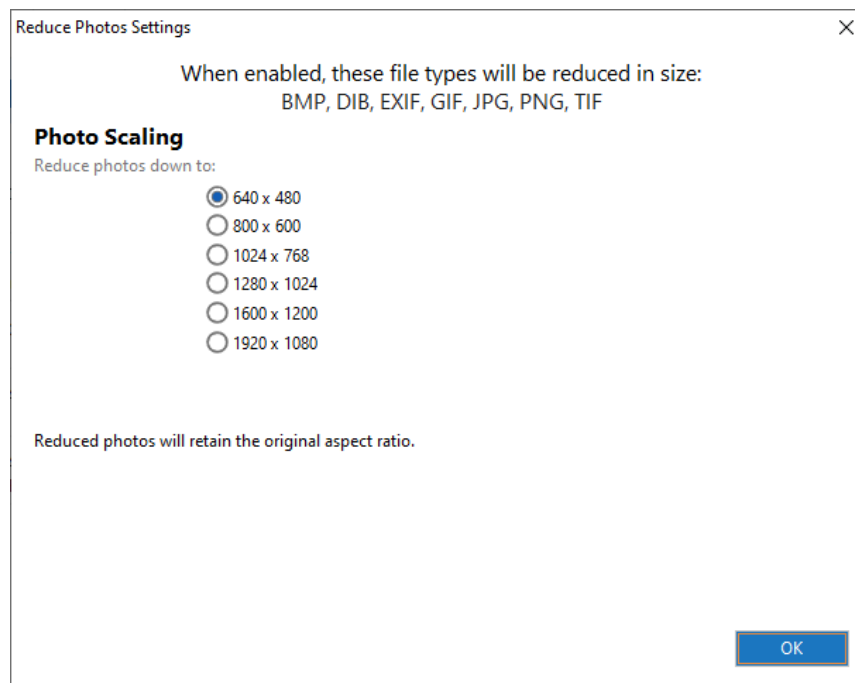
Remove Personal Data

This conversion option is used to remove EXIF metadata from files. Supported file types are: DOC, DOCX, GIF, JPG, PDF, PNG, PSD, PPT, PPTX, XLS, XLSX. Different file types include different types of metadata. When this option is enabled, all metadata is removed from files, with the following exceptions:

- Copyright
- Rights
- Producer

Convert Photos

This conversion option is used to convert image files, such as photos, from one file type to another. In some cases, converting to another file type can result in smaller file sizes. It is also useful in converting images to a common file format for sharing. Supported file types are: BMP, GIF, JPG, JP2, PNG, PSD, TIF, WEBP, and SVG.
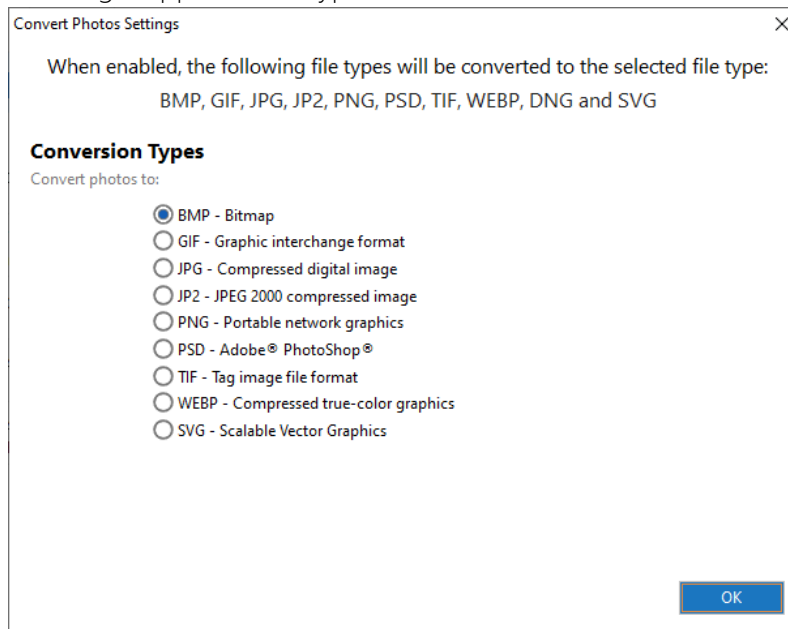

Watermark

This conversion option is used to protect pictures and PDF files by stamping them with a sentence or text phrase, such as **Confidential, do not copy**. Supported file types are: BMP, GIF, JPG, PDF, PNG, and TIF.

The **Watermark Settings** dialog will open when this option is first selected and can be edited in the user interface. The following options are available:

- **Placement** – Choose where the watermark appears; this is shown graphically
- **Direction** – Choose from four directions in which your text will appear
- **Transparency** – Determine how solid or transparent the text will be
- **Text** – Default text can be left or changed as desired

- **Font** – Choose the type and size font to be used. **Note:** When a "shrink to fit" view is used with a very large picture that has a watermark applied, that watermark might seem quite small.
- **Include a date stamp**
- **Include a time stamp**
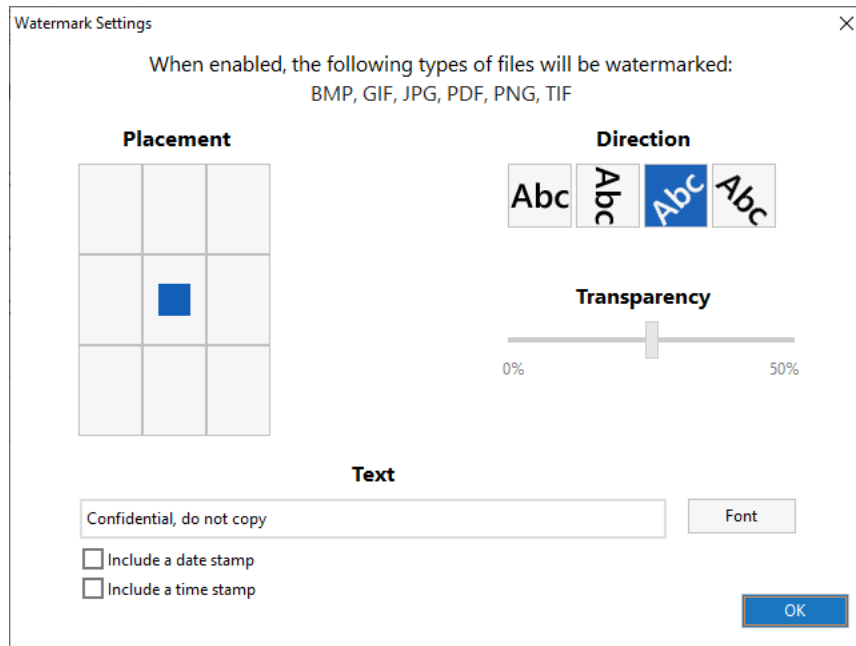
Convert from PDF

This conversion option lets you convert a PDF file to DOCX, DOC, BMP, JPG, PNG or TIF format. At the first use, the **PDF Convert from PDF Settings** dialog will display with the list of file formats.
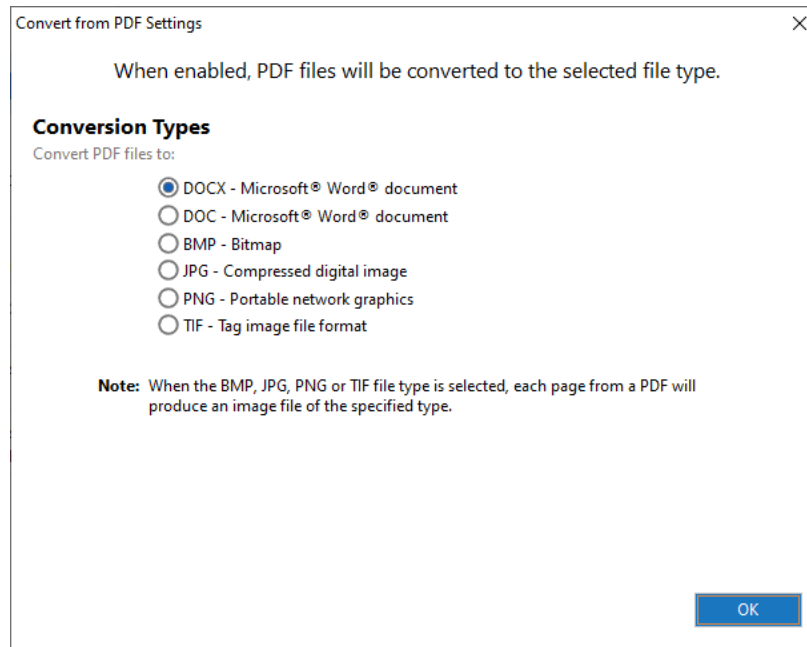
Convert to PDF

This conversion option works with Microsoft Word files, Excel files, and PowerPoint files, as well as some standard image and metadata file formats. At the first use, the **PDF Conversion Settings** dialog will display. The full list of supported file formats appears in the dialog.

By default, PDF files that allow text editing and copying are created. Other options include removing Word comments and/or creating read-only PDF files.
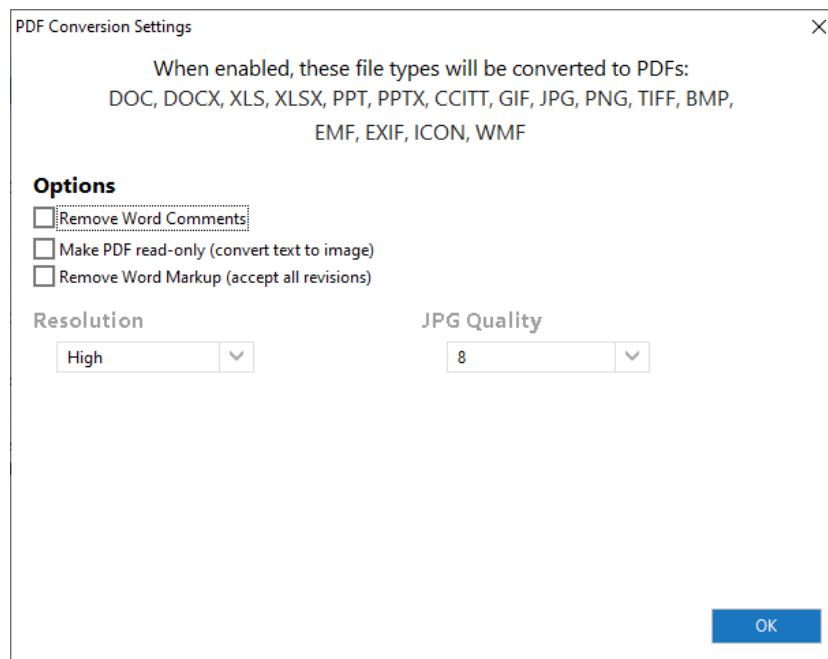
Read-only PDF files include options for PDF resolution and for JPG quality. If a document that is mostly text is converted to a read-only PDF, the file size after conversion will likely be significantly larger. However, the contents are more difficult to copy, relieving a security concern.

Combine Files into a PDF

This conversion lets you combine two or more PDF files into a single PDF file. The following default settings can be selected:
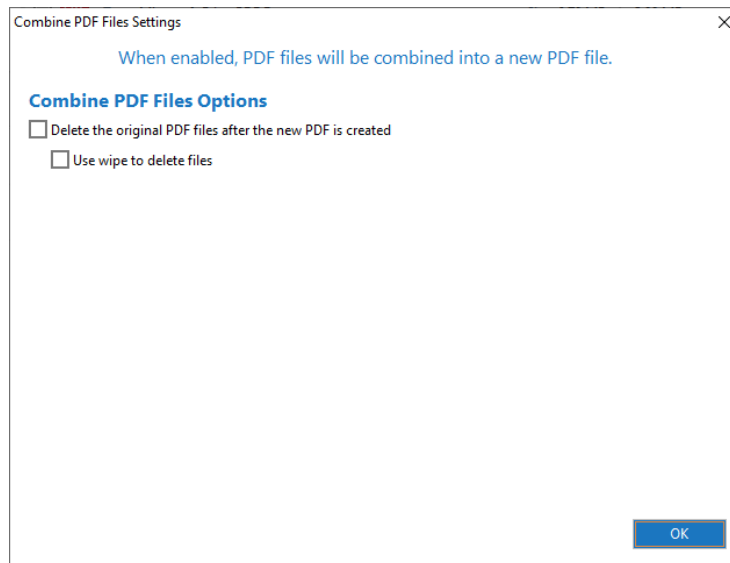
- **Delete the original PDF files after the new PDF is created**: Enable if you want to delete the source PDF files after the new combined PDF is created.
    - **Use wipe to delete files:** Enable this check box if you want to ensure the deleted files cannot be recovered (wiping is sometimes thought of as the electronic version of shredding a document).

When you use the feature, a dialog box opens with the following options:

- **Set the order of the PDF files**: Drag the thumbnails to set the order of the PDFs in the new file.
- **New PDF File name**: Type a name for the combined PDF.
- **Destination**: Choose where you want to save the file.
- **Additional Options**: These options are also available as default settings. See descriptions above.
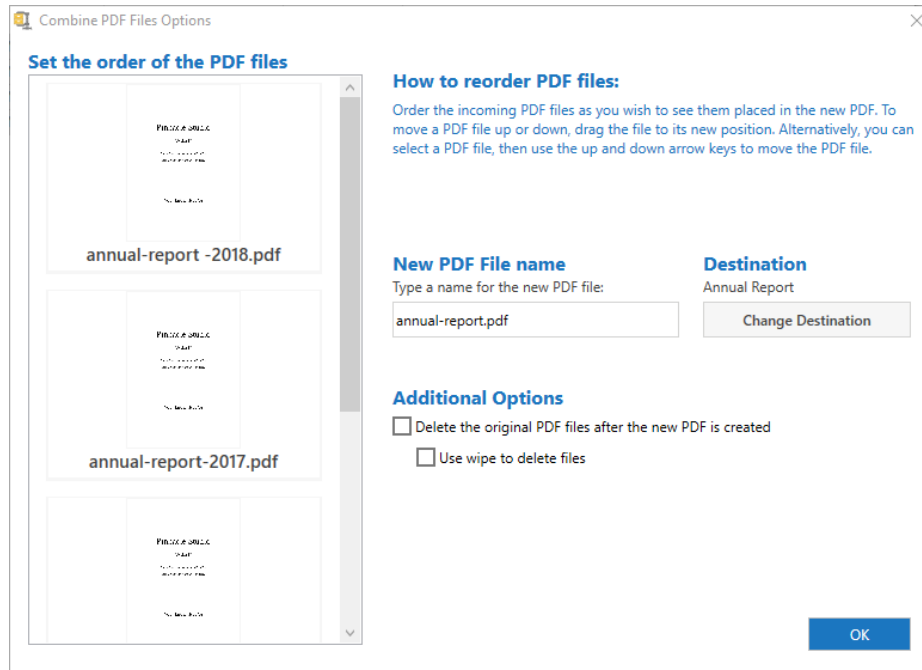
Sign PDF Files

This conversion option lets you sign PDFs created inside or outside WinZip. When you enable this feature, a dialog box opens with the following options:
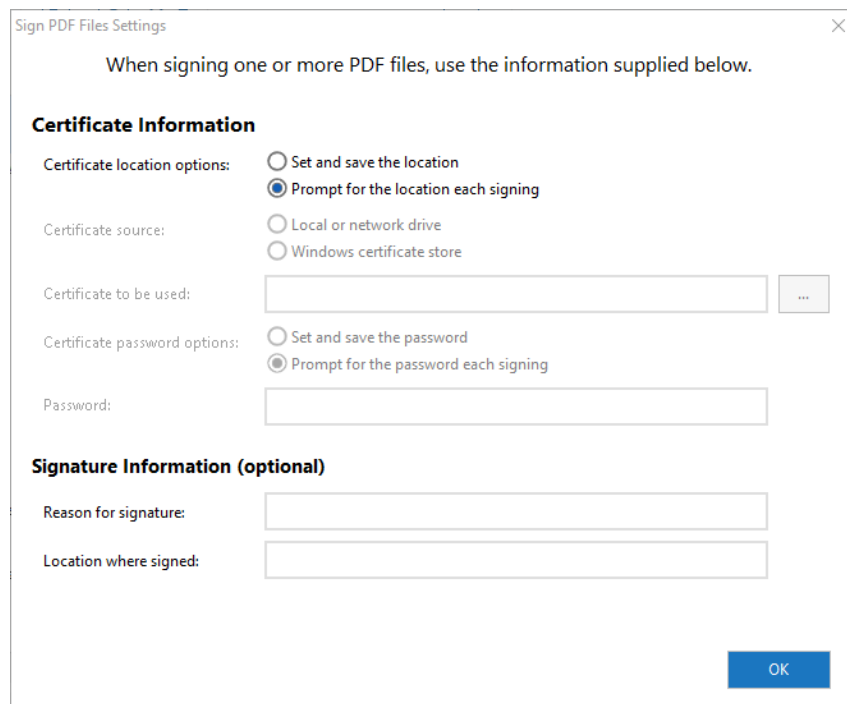
- **Certificate location options:** Choose a set location or prompt for a location each time.
- **Certificate source:** Choose a local certificate or get one from the Windows certificate store.
- **Certificate password options:** Choose a set password or prompt for a password each time a PDF is signed. If you set the password, it displays in the password box the next time you open the settings. Note that some certificates do not require a password—the **Certificate password options** are hidden if this is the case.
- **Signature information:** This section is optional and allows you to add helpful details.

Cloud Services

Many cloud services are available and are increasingly popular for personal and professional use. WinZip Enterprise helps your organization optimize the use of a variety of cloud services, while also providing controls to govern their availability to users. WinZip Enterprise supports the following cloud services:

- Alibaba Cloud
- Microsoft Azure Cloud
- Box
- CenturyLink
- CloudMe
- Dropbox
- FTP
- Google Cloud

- Google Drive
- IBM Cloud
- 1&1 IONOS
- MediaFire
- Microsoft Office 365
- NAS Cloud
- OneDrive
- OpenStack
- OVH

- Rackspace
- S3 Compatible
- SharePoint
- SugarSync
- SwiftStack
- Teams SharePoint
- Wasabi
- WebDAV
- ZipShare

Users can work more quickly with Zip files stored to a cloud service by using On-demand Downloading. When this feature is enabled (DISABLEVIRTUALZIP property), users download a virtual version of a selected Zip file from the cloud service. The virtual Zip file lets users see what the Zip file contains, but only the specific file or files that the user chooses to open are then downloaded. If other editing is initiated, such as adding new files, the entire Zip file is downloaded.

Please note: If you want any of the "Share" features that generate and send a download link to be available, there must also be at least one cloud service enabled. WinZip can then be used to upload what is being shared, place it in a folder specific to the upload date, generate a download link, and insert the link as specified. If a specific "root" folder is desired or needed (common for enterprise-specific cloud services), the admin property **WRITABLE_FOLDER_[service]** can be set during the install.

In addition to cloud storage services, cloud sharing services, such as **ZipShare™**, can be used to share files. Users can login to any service that has been enabled using the Cloud Services drop down menu on the **Settings** tab of the ribbon interface. A Default Cloud Service can also be set here or, if desired, a default cloud service can be configured by the software administrator as WinZip Enterprise is installed by using the DEFAULTCLOUDSERVICE property. Along with this, the administrator can set the NOUSERCLOUDDEFAULT property to TRUE and users will not be able to change the default cloud service.

With enabled cloud services, WinZip Enterprise can be used to:

- Create Zip files from files that are saved on a cloud service
- Save Zip files to a cloud service
- Unzip files to a cloud service
- Generate a link to files saved on a cloud service that will be placed in an email message
- Share files in a Zip file to an enabled social media feature

Cloud configuration notes

- **Amazon S3** storage and sharing is compatible with services that support Signature Version 4. In addition, at least one bucket must exist in your S3 storage area. Configure your Amazon credentials using environment variables or config/credential files as specified in the Amazon S3 specs. If you need to use the Amazon GovCloud FIPS 140-2 endpoint, then you must configure WinZip for FIPS 140-2 compliance, and it will then display in the selection list.
- **Google Cloud**: This service requires creation of a service account for users to log into and a JSON or P12 configuration file. The service account log ins must provide cloudplatformprojects.readonly and devstorage.full_control or devstorage.read_only scope access.
- **IBM Cloud**: To create "Share file links" in IBM Cloud, the administrator needs to set the WRITABLE_FOLDER_IBMCLOUD MSI property to a folder that permits sharing.
- **OpenStack** authentication values can be set using only environment variables as described in the "Environment Variables" section of the OpenStack documentation: https://docs.openstack.org/python-openstackclient/pike/cli/man/openstack.html
- **OpenStack**: To create "Share file links" for OpenStack (for providers that support it), the administrator needs to set the WRITABLE_FOLDER_OPENSTACK MSI property to a folder that permits sharing. Sharing is on by default for OpenStack providers, but not all providers implement this feature. To disable sharing in OpenStack, set the following registry value in the MSI's registry table to **1**: "SOFTWARE\Nico Mak Computing\WinZip\WXF\WzWXFopenstack\Default" Name: "DisableShare" Value: 1
- **S3 Compatible**: This service is limited to services that support V4 signatures. Not all services are 100% compatible. Many services, for example, do not provide a method for obtaining URLs for file sharing.
- **SwiftStack** authentication values can be set using environment variables or a credential file as described in the "Configuring S3 Clients" section of the SwiftStack documentation: https://www.swiftstack.com/docs/admin/middleware/s3_middleware.html. Note that "region" can only be set using a credential file.
- **Teams Sharepoint:** Add the registry key in the WinZip MSI (HKEY_LOCAL_MACHINE\SOFTWARE\Nico Mak Computing\WinZip\WXF\WzWXFteamsspt\Default\WritableRootFolder) to indicate the default share folder path for users, and the WinZip MSI also contains a related property (WRITABLE_FOLDER_TEAMSSHAREPOINT) for the WritableRootFolder value. The administrator can

set the value by modifying the related property (WRITABLE_FOLDER_TEAMSSHAREPOINT) in Orca. The default value of WRITABLE_FOLDER_TEAMSSHAREPOINT is "\".

Social Media

As with other WinZip Enterprise features, Social Media features are turned off by default. Companies might restrict some or all social media usage to many or most users or offer access only to certain departments. By creating multiple MST files and assigning them to the appropriate Organizational Units in Active Directory, these features can be made available to the appropriate groups in WinZip as well.

As mentioned in the previous section, users will need at least one cloud service to be available within WinZip if **Share** features are to be used. Social Media usage is one example of a Share feature.

With WinZip, users can login to or logout of enabled social media features using the Social Media drop down menu on the **Settings** tab. After opening a Zip file with WinZip, users can click **Social Media** on the **Unzip** tab, change the message to be posted if desired, and select one or more enabled social media features. Then, when the **OK** button is clicked, the file will be uploaded to the default share service and the message, along with a link to that file, will be posted. Social Media features are also available when using WinZip Express.

Registry settings for WinZip: Policies and more

When installing a WinZip upgrade, please keep in mind that some policies you may try to set may be negated by individual user settings from the previous version saved in **HKEY_CURRENT_USER\SOFTWARE\Nico Mak Computing\WinZip\[subkey].**

To avoid this issue, you can delete the WinZip subkey and String Values from all HKEY_USERS keys. They will then be recreated when WinZip is run by the user and values you have set will be propagated.

When the WinZip MSI file has been customized; either directly, by use of a transform, or through the use of a command line install; registry String Values will be created in **HKEY_LOCAL_MACHINE** during installation. Administrator level policies will be written only to **HKEY_LOCAL_MACHINE**, while others will be default settings that users can change. These latter ones will be written to **HKEY_CURRENT_USER** as well.

Properties that do not create registry settings

Some of the MSI properties prevent certain files and features from installing. These properties begin with either **ADD** or **INSTALL**. No registry entries are created for these items. You can choose to add or install these components during the WinZip installation process.

Default policies

By default, string values concerning WinZip policies will be created in the registry subkey **HKEY_LOCAL_MACHINE\SOFTWARE\Nico Mak Computing\WinZip\Policies**. Users that do not have permissions to edit HKLM will not be able to change these settings.

String Value	Description
DisableCloudServices	Default=ALL, all cloud services disabled; other options are NONE; ALIBABACLOUD, AMAZONS3, AZUREBLOB, BOX, CENTURYLINK, CLOUDME, DROPBOX, FTP, GOOGLECLOUD, GOOGLEDRIVE, IBMCLOUD, IONOS, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, OVH, RACKSPACE, S3COMPATIBLE, SHAREPOINT, SUGARSYNC, SWIFTSTACK, TEAMSSHAREPOINT, WASABI, WebDAV, and/or ZIPSHARE
DisableConversions	Default=ALL, disables all conversion features; other options are NONE; IMAGERESIZE, CONVPHOTOS, REMOVEPERSDATA, DOCTOPDF, WATERMARK, ENLARGEREDUCEIMAGE (File Management tool only), COMBINEPDFFILES and/or SIGNPDFFILES
DisableFileExpiration	Default=0, Schedule for Deletion option (file expiration) is available, off=1
DisableFIPSPolicyWarning	Default=0; Warning that displays when FIPSComplianceMode is set to RELAXED is not disabled; on=1
DisableNotificationServices	Default=ALL, all Social Media and Instant Messaging options enabled; other options are NONE; FACEBOOK, LINKEDIN, SLACK, TWITTER, YOUTUBE, GTALK, FACEBOOKCHAT, JABBER, YAHOOMESSENGER, OFFICE365GROUPS, TEAMS, and TWITTERMESSAGE
DisablePersonalContacts	Default=1, personal email addresses cannot be used in the WinZip emailer; off=0
DisableRecentArchives	Default=1, recently used archives are not recorded; off=0, they are recorded
DisableRecentJobs	Default=1, recently used jobs are not recorded; off=0, they are recorded
DisableRecipientServices	Default=ALL, no email address recipient services will be available; other options are NONE, EXCHANGECONTACTS, GOOGLECONTACTS, LDAPCONTACTS, OUTLOOKCONTACTS, OUTLOOKPOCONTACTS, SLACKCONTACTS, and YAHOOCONTACTS
DisableSettingsFromCloud	Default=1, WinZip settings cannot be saved to or retrieved from a cloud service; off=0
DisableShortLinks	Default=1, Link shortening options are disabled; on=0
DisableVirtualZip	Default=1, Zip virtualization for On-demand Downloading is disabled; on=0
DisableVirtualZipMetrics	Default=1, Zip virtualization metrics is disabled (default); on=0. The metrics save and retrieve Zip file directory size and location information to optimize the speed of loading cloud-based Zip files.
DisableZipAndShare	Default=1, No Zip and Share (WinZip Express) context menu entry and a disabled Zip and Share button on the Tools tab; both available=0
EncWipeDelete	Default=0, A caution message will display when certain files cannot be wiped, they are then deleted normally; on=1 (the caution message is suppressed, files of this type will be deleted only)
EncryptReplacements	Default=0, Unlocked: User can set preference to enable or disable the requirement to use a password when updating or deleting encrypted files (WinZip Options > Advanced). 1=Locked by admin to on (password always

	required; option hidden from user). 2=Locked by admin to off (password not required; option hidden from user).
EntX509Certificate	Default=0. For more information, see Enterprise-wide password management.
FIPSComplianceMode	Default=DISABLED (disables FIPS mode use in WinZip); other options are DEFAULT (WinZip follows the compliance setting of the computer), STRICT (allows only approved FIPS operations), RELAXED (shows warnings before executing unapproved FIPS operations)
HideRegInfo	Default=1, the link in the About WinZip dialog is hidden; off=0 (visible link).
WzBGTddtf	Default=0, *Create a custom cleaner* function in *Tools* is hidden; 1=custom cleaner function is displayed (function is available).

Password policies

WinZip Password Policy registry string values will be created in the same subkey as the default policies; **HKEY_LOCAL_MACHINE\SOFTWARE\Nico Mak Computing\WinZip\Policies**. These string values are only created if the default value has been changed. To prevent users from changing your password policies, you should consider including the **passwordrestrict** String Value set to **1** as this will remove access to the **Passwords** tab in WinZip Options.

String Value	Description
alwaysencrypt	Default=0 (FALSE); TRUE=1
encryptionrestrict	Default=No string value and no restrictions; ZIP20, AES128, AES256 (use any combination, separated by a comma to remove particular encryption strengths)
passwordlength	Default=8; any number from 1 to 99 can be used
passwordreqlower	Default=0 (FALSE); TRUE=1 (at least one lower case letter required)
passwordreqnumber	Default=0 (FALSE); TRUE=1 (at least one number required)
passwordreqsymbol	Default=0 (FALSE); TRUE=1 (at least one symbol required)
passwordrequpper	Default=0 (FALSE); TRUE=1 (at least one upper case letter required)
passwordrestrict	Default=0 (FALSE); TRUE=1 (Password tab removed from WinZip Options eliminating user access to changing policies)

Other settings

Additional settings are controlled by string values created in other subkeys. If no WinZip settings currently exist in each user hive, these will be propagated. Otherwise, the WinZip subkey in each user hive should be deleted or these settings should be specifically created in the corresponding subkey for each user hive.

The following table displays string values that are created in **HKEY_LOCAL_MACHINE\SOFTWARE\Nico Mak Computing\WinZip\WinZip**.

String Value	Description
AutoOpenDocs	Default=1, Zip files containing a single Microsoft Office file will automatically cause the file to open in that application; off=0
DefaultCloudService	Default=DEFAULT, no cloud service set to be the default; specify the name of a supported cloud service to be the default
DefaultShareService	Default=DEFAULT, no cloud service set to be the default; specify the name of a supported share service to be the default
DisableAOD	Default=0, users have access to the auto-open for Office files check box in WinZip Options; on=1
JobPromptOnRun	Default=1, WinZip backup files (.wjf) will display a prompt before running; off=0
NoEditMailAccts	Default=0, users can edit email accounts; on=1
NoInternalEmailer	Default=0, the WinZip emailer is available for use with email features of WinZip; on=1
NoUserCloudDefault	Default=DEFAULT (off), users can specify a default cloud service; TRUE=users cannot specify a default cloud service
ShowShared2MeFolders	Default=1 (on). For OneDrive and Google Drive, the user can see if files originate from another user's shared folder.
ShowTips	Default=1, Tip of the Day displays when WinZip opens empty; off=0

Alternate Association

A string value named **AltAssoc1** can be created in the subkey **HKEY_LOCAL_MACHINE\SOFTWARE\Nico Mak Computing\WinZip\AltAssoc**. The value of this string will set an alternate extension to be used for Zip files when needed.

When creating an alternate extension, you must also inform WinZip that it needs to use that extension. To do that, create a string value named **UseAltExten** with a value of 1 in the subkey **HKEY_LOCAL_MACHINE\SOFTWARE\Nico Mak Computing\WinZip\AltAssoc**.

Check for Updates

If desired, the **Check for Updates** feature in WinZip can be completely disabled. To do so, the NoUpdateChecking string in the subkey **HKEY_CURRENT_USER\Software\Nico Mak Computing\WinZip\UpdateCheck** must have a value of **1**. As explained above with other values, if steps are taken to insure values will be propagated from the HKEY_LOCAL_MACHINE hive, you can and should make this change to the same string in the subkey **HKEY_LOCAL_MACHINE\Software\Nico Mak Computing\WinZip\UpdateCheck**.

WinZip Command Line Support Add-On 6.0

The WinZip Command Line Support Add-On lets you access the power of WinZip through a command line for scripting, batch files, macros, enterprise-wide passwords, and other tasks where you prefer to bypass the WinZip user interface.

The add-on supports FIPS 140-2 Relaxed mode (not Strict mode) and is WIP-aware (Windows Information Protection).

For full instructions on using the Command Line Support Add-On, see the Help file. You can access the Help from your Windows application list (**WinZip** folder > **WinZip Command Line Add-On Help**) or you can access it directly from the programs folder (**Program Files\WinZip** folder: **WZCLINE.CHM**). The Help includes a list of the latest features (in the **Contents** area, open the **Overview** section, and click **What's New in Version 6.0**).

Installing WinZip Command Line Support Add-On 6.0

1. After WinZip Enterprise is installed, double-click **wzcline60-64.msi** (64-bit) or **wzcline60-32.msi** (32-bit).
2. Follow the instructions in the installation wizard.

WinZip Courier 12

WinZip Enterprise includes the full-featured WinZip Courier application, rather than WinZip Express for Outlook.

General Considerations

Email attachments can be compressed into a .zip file before sending. By default, attachments are zipped, but you can disable automatic zipping or set conditions for prompted zipping. You can further reduce the size of email by having WinZip Courier upload the .zip file to a cloud service so that the email need only include a download link. This keeps the size of Outlook data files to a minimum. You can also configure an expiration for the files that you upload to cloud locations. WinZip Courier can be used with the same Cloud Services available in WinZip. The services that are made available to users is completely within the control of the software administrator. Email attachment security can be maintained with encryption and password policies.

Also, with WinZip Courier conversion features you can convert Microsoft Office documents to PDF files and further protect appropriate image attachments by adding a watermark to them.

For those situations where one set of users can and should have different features available to them, different Organizational Units can be defined in Active Directory. Then, by also creating multiple .mst files and Group Policy installs, each user set would have only the appropriate features.

Installation

As with WinZip Enterprise, the WinZip Courier install file for Enterprise lets you select the desired features to install, rather than requiring you to disable unwanted ones. The following information concerns entries in the MSI file **Property** table. These entries can be configured to add features or change the behavior of WinZip Courier.

Property	Description
ADMINSENDITEM	Default=0, normal default (zipping on), no Admin setting; 1=attachment zipping on, user can change default; 2=attachment zipping off, user can change default; 3=attachment zipping on, user cannot change default; 4=attachment zipping off, user cannot change default
DEFAULTCLOUDSERVICE	Default=DEFAULT, no cloud service selected; specify a supported service to be the default
DISABLECLOUDSERVICES	Default=ALL, all cloud services disabled; other options are NONE; AMAZONS3, BOX, CLOUDME, DROPBOX, FTP, GOOGLEDRIVE, IBMCLOUD, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, RACKSPACE, SHAREPOINT, SUGARSYNC, SWIFTSTACK, and/or ZIPSHARE
DISABLECONVERSIONS	Default=ALL, disables all conversion features; other options are NONE; IMAGERESIZE, CONVPHOTOS, REMOVEPERSDATA, DOCTOPDF, WATERMARK, ENLARGEREDUCEIMAGE (File Management tool only)
DISABLEMSGEDITZIPOPTION	Default=0, user can change zip setting in messages; On=1, user cannot change zip setting in messages (DISABLEMSGEDITZIPOPTION applies to both Outlook and the Web Courier dialog)
DISABLEWEBCOURIER	Default=0, allows installation of the Web Courier component; on=1, do not install the Web Courier component
NOENCRYPTION	Default=0, allows encryption to be used while zipping; on=1
NOUPDATECHECKING	Default=1, Courier will not check for available updates; off=0

Zipping Options

You can choose from the following zipping options in WinZip Courier:

- **Zipx**: Latest compression method applied for a smaller file size.

- **Zip**: Legacy compression (Zip 2.0)
- **Optimize Zipx by saving identical files as references**: Analyzes the fileset for duplicate files and includes only the one version during compression. References are used to ensure that any duplicate versions are repopulated when the compressed file is unzipped.

Attachment Options

The Zip Attachments defaults and options available to users depend on the permissions (properties) set at installation.
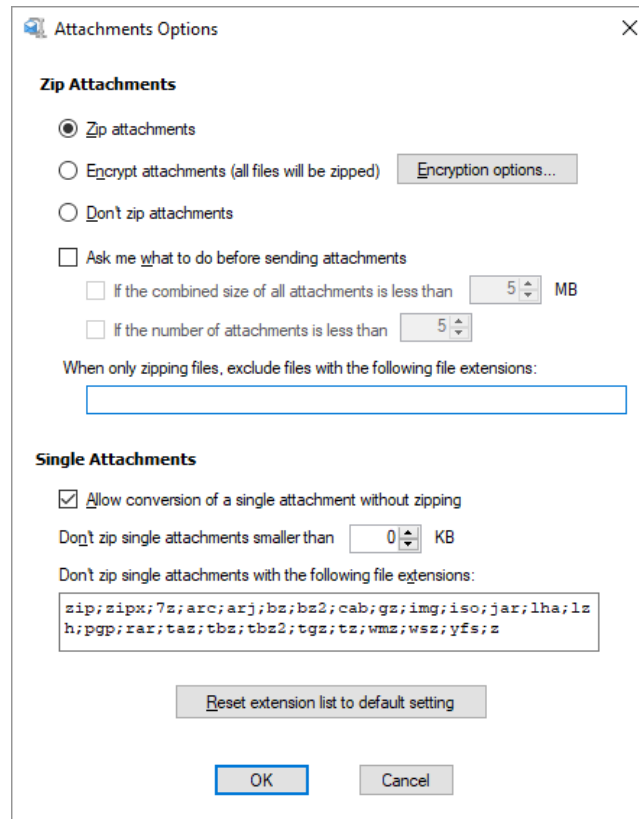

Attachment options include:

Zip Attachments

- **Zip attachments:** When this option is selected, attachments are zipped automatically unless the attachment matches certain conditions.
- **Encrypt attachments (all files will be zipped)**: If the WinZip password policy "always encrypt" is turned on, this option will be enabled and all other options will be grayed out. If the Courier **NOENCRYPTION** property has been set to **1**, this option, and the corresponding **Encryption options** button will be grayed out. Otherwise, if this option is enabled, Courier will always zip your attachments and you will be prompted to type a password to encrypt the attachments.
  - o **Encryption options** button: If no encryption restrictions have been configured for WinZip, you can choose from three encryption methods in the **Encryption Options** dialog. Courier will use

the method you select when zipping and encrypting attachments. Note that WinZip password policies also affect Courier's encryption.
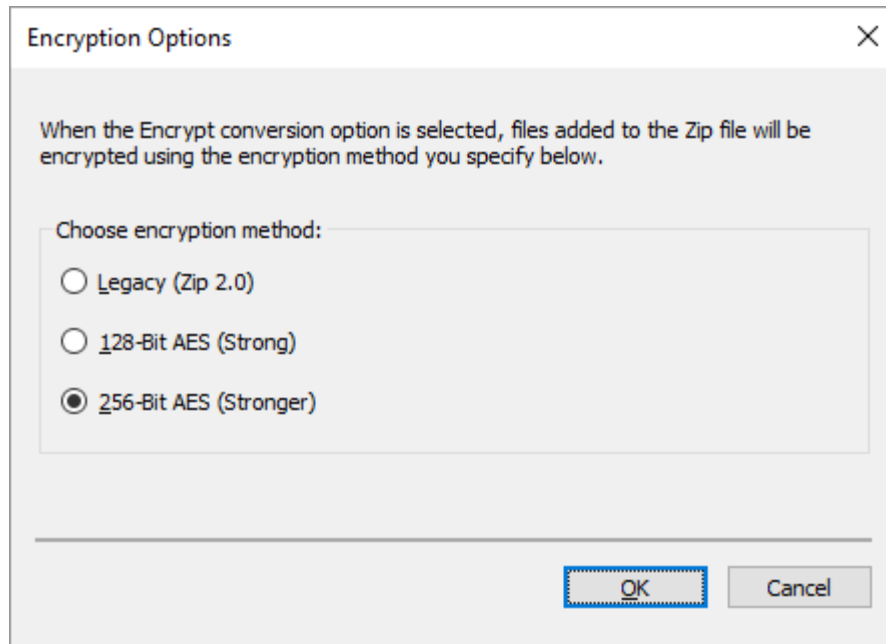
- **Don't zip attachments:** When this option is enabled, WinZip will not zip attachments by default.
- **Ask me what to do before sending attachments**: When this check box is marked and no conditions are set, the user is always prompted before zipping. If size or number conditions are set, the user is prompted only when the attachments meet the conditions.
  Conditions include:
  - **The combined attachment size is less than** [x] **MB**, where x is a size set by the user
  - **The number of attachments is less than** [x], where x is the number of attachments set by the user
  - **When only zipping files, exclude files with the following file extensions:** This box lets you type file formats that you want to exempt from zipping.

Single Attachments

- **Allow conversion of a single attachment without zipping**: When this check box is marked, conversion settings can be applied to a single attachment without requiring zipping.
- **Don't zip single attachments smaller than** [x] **KB**: Lets the user determine the minimum size for zipping single attachments.
- **Don't zip single attachments with the following file extensions:** This box lets you type file formats that you want to exempt from zipping. If you want to reset the extension list, click **Reset extension list to the default setting**.

Note: Encryption uses Zip files to provide a standard format that allows for proper decryption.

Configuring Customizations

After you select the desired features, customizing the installation is necessary to make those changes. An MSI file editor, such as Microsoft Orca, can be used either to edit the Property table directly or to create one or more transform files (.mst). Properties described in the tables above can be added to a Windows Installer command line as install options. The basic syntax for such a command is:

msiexec /Option <Required Parameter> [Optional Parameter]

For more on this, see Command line usage for installing with the WinZip MSI file.

Password policies

WinZip Courier does not create or maintain its own set of password policies. It has one property that allows you to completely disable encryption as an option. Otherwise, Courier is governed by the password policies you set in WinZip. For instance, if you have disabled two of the encryption methods in WinZip, leaving AES-256 as the only option, the same will be true for Courier. By default, the only password policy governing Courier will be that the password must be 8 characters in length. When encryption is turned on in WinZip Courier, it will zip your email attachments. Be careful, as this supersedes other settings. If **AlwaysEncrypt** is turned on in WinZip, Courier will always zip and encrypt email attachments.

Note: If you've set up WinZip for FIPS 140-2 compliance, WinZip Courier will also be compliant. Likewise, if the Enterprise Wide Password feature has been configured for WinZip, it will also apply to Courier.

Cloud Services

WinZip Courier provides the option to use cloud services and links when sending large files. It also provides an easy method for sending links to files previously stored in the cloud. In earlier versions, the ZipSend service was provided to enable the sending of larger file attachments. Now, all of the cloud services that WinZip Enterprise offers are also available in Courier, giving users many new options, including ZipShare.

Cloud Options

The **WinZip Courier Options** dialog, shown with the Cloud Service section outlined, can be opened using the Courier drop down menu that displays in Outlook. When users click the Cloud options button, a **Configure Cloud Service** dialog, similar to the one below will open.
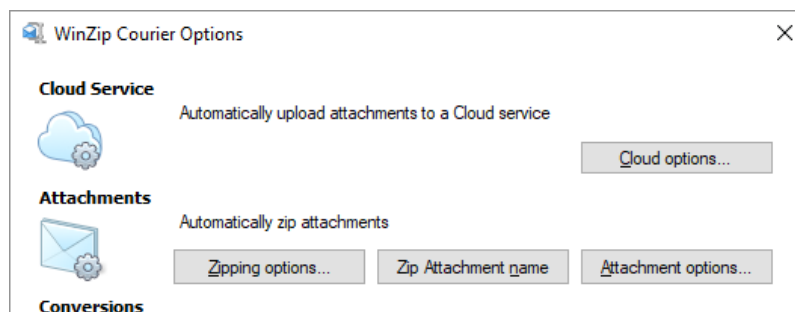
The **Configure Cloud Service** dialog displays only those cloud services that are not disabled. This dialog relates to the sending of file attachments.

Automatically sent attachments through a cloud service

In the top section, a default threshold size can be set or changed. This determines when attachments will be sent through a cloud service. Always and never are the other two options.

Select the cloud service to configure

In the middle section of the dialog, users can:

- Select a cloud service from the list and login to that service
- Logout of any logged in service
- Set a service to be the default.
- Add an additional cloud service of the same type (such as a second ZipShare account)
- Edit the nickname that was given to an account

## Schedule when uploaded file will expire

In the bottom section of the dialog, users can choose to mark the **Expire uploaded file after [x] days** check box and set the number of days before the file expires.
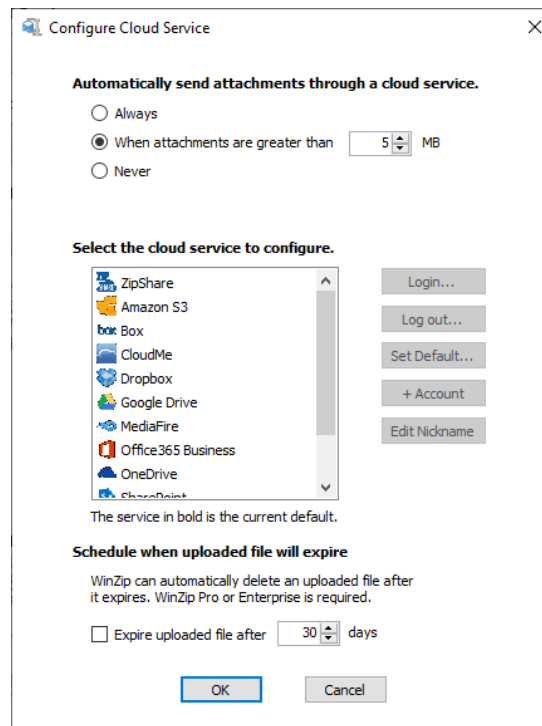
> **Note:** If the **DisableFileExpiration** property in WinZip has been turned on (set to **1**), Courier users will not be able to schedule files to expire.

Email from Cloud

Additionally, Courier lets users find and select a file that was previously uploaded to a cloud service. As mentioned, the configuration dialog above governs how Courier will treat files that are attached to email messages.The **Email from Cloud** button, which is located in the WinZip Courier section of the Message tab in an email message. If this button is clicked, a **Select Files to Share** dialog will display with the default cloud service automatically selected. In the left pane of this dialog, other enabled services will also be displayed for use. Unlike selecting a file from a drive connected to the computer, a file selected from a cloud service will cause Courier to insert a standard text box saying, "Please click the link below to access files from my *cloud service*" followed by a link to the file. When sharing this way, users can select any available file (it does not
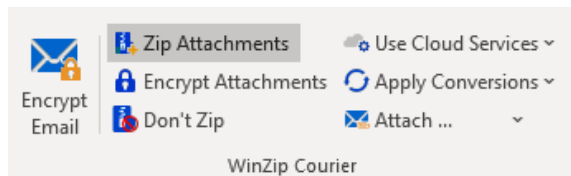
need to be a Zip file), Courier will insert a link to the file, and the recipient will then be able to download it. See the WinZip Courier section of the WinZip Knowledge Base for more concerning cloud services.
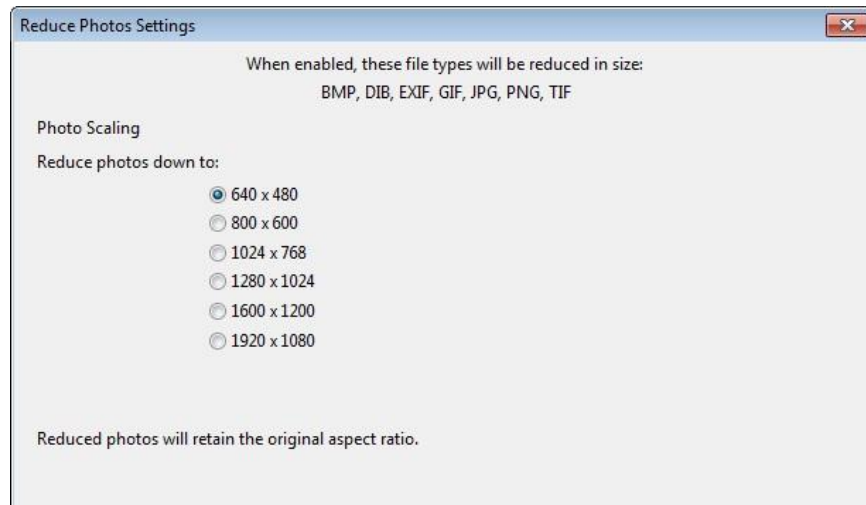
Conversions

Additional WinZip Courier features are listed under the heading of Conversions. Some of these features must be enabled by the administrator. Conversion options can be set as a Courier default by checking the appropriate box in the options dialog. Each of the features can also be configured by clicking its **options** button.
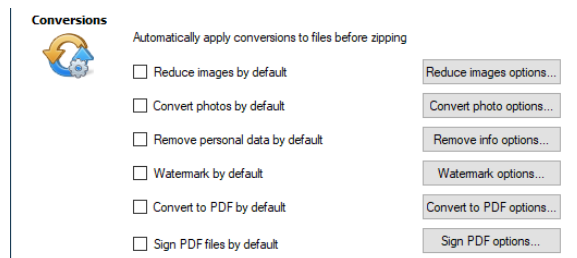

Reduce images options

Read-only PDF files include options for PDF **Resolution** and for **JPG Quality**. If a document is converted to a read-only PDF, the file size after conversion will likely be significantly larger. However, it will be more difficult to copy the contents, relieving a security concern.

This conversion option can be used with the following supported picture/image files: BMP, DIB, EXIF, GIF, JPG, PNG, and/or TIF. Reducing the size of an image affects its file size and resolution. This is usually fine for sharing, but not when quality is of major importance, such as when images are going to a printer.


Convert photo options

This conversion option is used to convert image files, such as photos, from one file type to another. In some cases, converting to another file type can result in smaller file sizes. It is also useful in converting images to a common file format for sharing. Supported file types are: BMP, GIF, JPG, JP2, PNG, PSD, TIF, WEBP, and SVG.
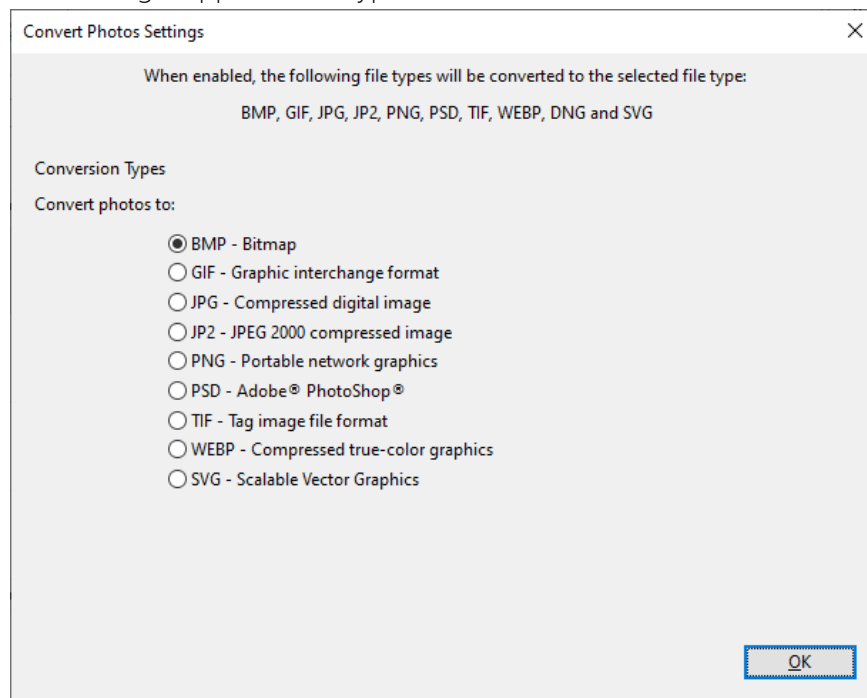
Remove info options

This conversion option (also referred to as **Remove personal data**) is used to remove EXIF metadata from files. Supported file types are: DOC, DOCX, GIF, JPG, PDF, PNG, PSD, PPT, PPTX, XLS, and XLSX. Different file types include different types of metadata. When this option is enabled, all metadata is removed from files, with the following exceptions:

- Copyright
- Rights
- Producer
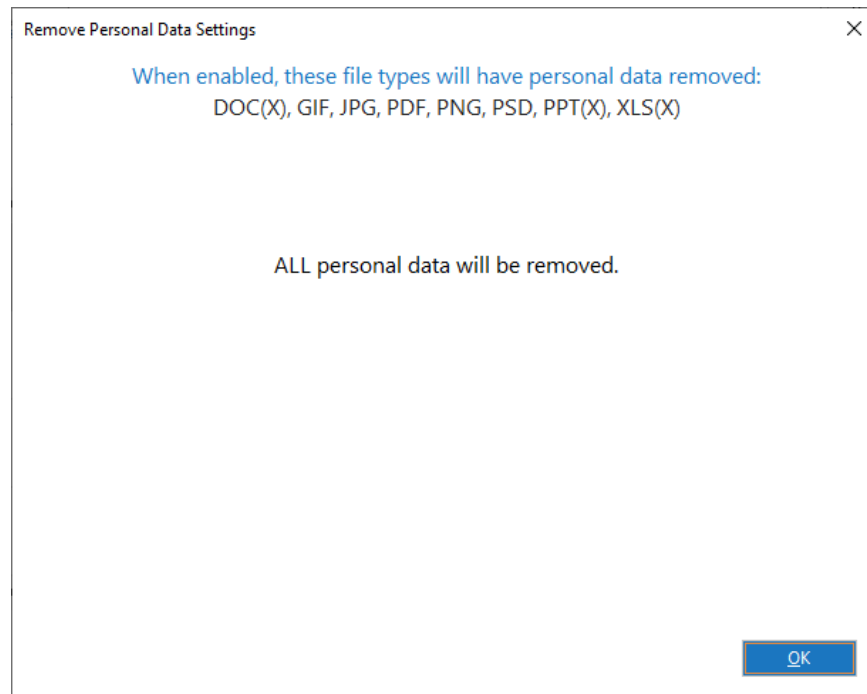
Convert to PDF options

This conversion option can be used with Microsoft Word files, Microsoft Excel files, Microsoft PowerPoint files, and a range of common image and metadata file formats. Specifically, those file types are DOC, DOCX, XLS, XLSX, PPT, PPTX, CCITT, GIF, JPG, PNG, TIFF, BMP, EMF, EXIF, ICON, WMF. When the **Convert to PDF by default** box is checked, the **PDF Conversion Settings** dialog will display. It can also be opened by clicking the button when editing settings is desired.

Default settings will create PDF files that can be edited and from which text can be copied. Options include **Removing Word Comments**, **Make PDF read-only**, and **Remove Word Markup**.
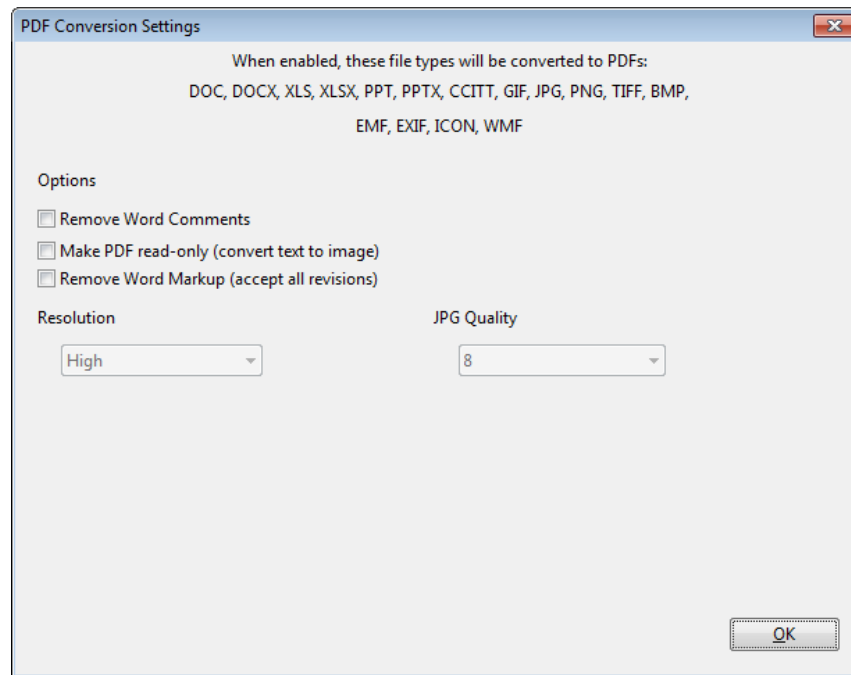

Watermark options

This conversion option protects pictures and PDF by stamping them with a sentence or text phrase, such as **Confidential, do not copy**. Supported file types are: BMP, GIF, JPG, PDF, PNG, and TIF.

The **Watermark Settings** dialog opens when this option is first selected and can be edited in the user interface. The following options are available:

- **Placement** – Choose where the watermark appears; this is shown graphically
- **Direction** – Choose from four directions in which your text will appear
- **Transparency** – Determine how solid or transparent the text will be
- **Text** – Use default text of change as desired
- **Font** – Choose the type and size of the font to be used. **Note:** When a "shrink to fit" view is used with a very large picture that has a watermark applied, that watermark might seem quite small.
- **Include a date stamp**
- **Include a time stamp**
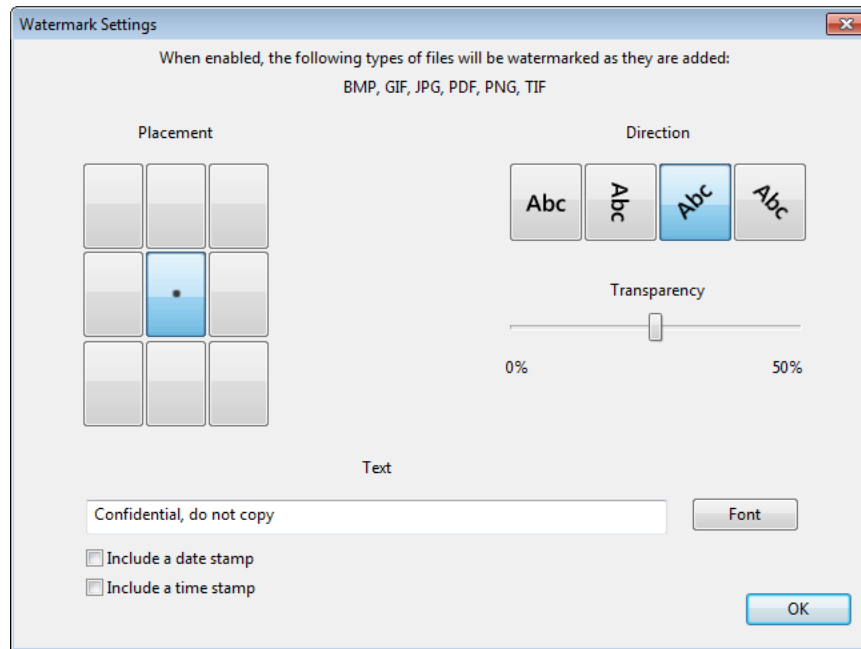
Sign PDF options

Signing a PDF is a way of approving or authenticating your digital document. You can set certificate location options, as well as the certificate source and password options. You can also set optional signature information, such as reason for signature and where the document was signed.
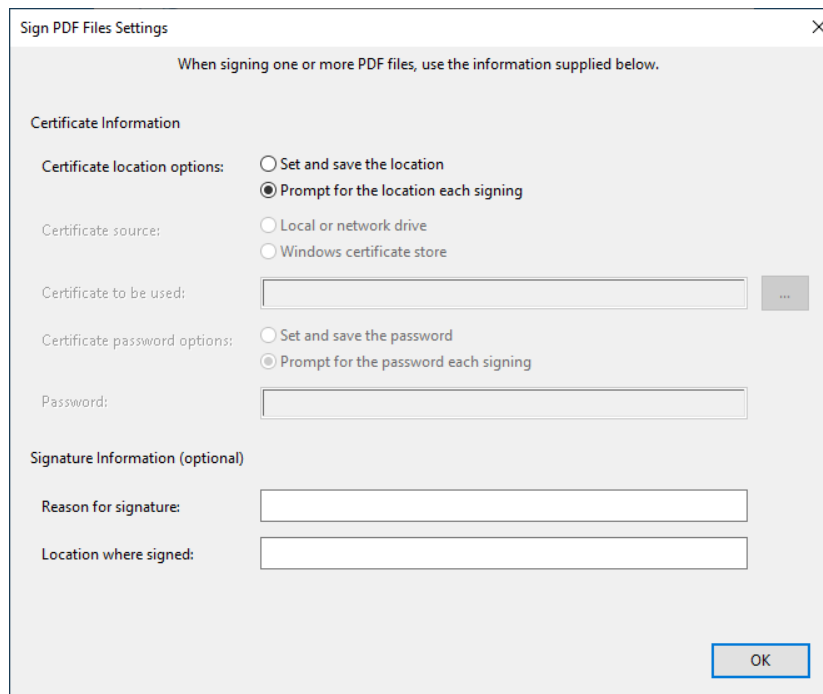
FIPS 140-2 Compliance – Configuration Considerations

There are a number of considerations when setting up FIPS compliance for an organization. In addition to the list of considerations below, please refer to the following sources:

- For Information about setting up FIPS 140-2 compliance, please use the following Technet article: https://technet.microsoft.com/en-us/library/security/cc750357.aspx
- For an example usage scenario, please see *Scenario 3 – Prepare for FIPS 140-2 Compliance*.

FIPS tips and considerations

- The machine or Windows operating system FIPS policy is the Local Security Policy. The registry setting for this is **HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled=1**.
- You can set FIPS mode for WinZip when you install WinZip or you can edit the **FIPSComplianceMode** registry string with one of the following values: **DEFAULT**, **STRICT**, or **RELAXED**. For more information about the **FIPSComplianceMode** property and its values, see *Choosing WinZip features*.
- The FIPS mode in WinZip operates in conjunction with the Windows operating system FIPS policy. In other words, to ensure a FIPS-compliant environment, the machine policy and the WinZip policy should both be **ON**.
- Some WinZip customers have indicated that they would like to operate WinZip in a FIPS mode that is independent from the Windows operating system policy without producing warnings about non-compliance. WinZip can accommodate this type of setting with an additional deployment policy for disabling the warnings. For example, with the WinZip **FIPSComplianceMode** set to **RELAXED**, WinZip will use the Windows FIPS 140-2 validated cryptographic modules and only the FIPS 140-2 approved AES-256 method will be allowed for Zip encryption. Other operations that would normally be blocked when FIPS is enabled in the Windows operating system are still allowed. An example would be decryption operations that use non-AES-256 methods and/or strengths. If the FIPS policy is **OFF** at the machine level but **ON** in WinZip, all we can really say is that WinZip will use the compliant modules and approved methods for encryption. We cannot be sure of the compliancy of transmission by email, or upload, etc. Full compliance ought to be environment-wide, not application specific. But the reality for some organizations is that some applications might not be FIPS 140-2 aware and might break when operated on a machine with FIPS mode **ON**. Ideally, to ensure full and comprehensive FIPS 140-2 compliance, a dedicated machine with FIPS mode **ON**, should be used to communicate with government organizations that require compliance.

Example Usage Scenarios

This section presents a number of scenarios to demonstrate proper setup steps. Each includes a description, installation preparation, installation steps, and additional information when applicable. The titles give the main description, but other features are also included. The scenarios are meant as a guide and are not an exclusive or required method. In most cases, a scenario can be combined with other scenarios depending on the desired result.

To start, download the necessary installation file package, the WinZip registration file (WinZip.wzmul), and the WinZip Courier registration file (WinZipEC.ecmul). The installation file package includes all of the Enterprise installation files. This EXE file can be run to unzip the files to a folder. Registration files must be downloaded using the particular link given at the time of purchase. If, at a future time, files are needed again but have been misplaced, customers can email help@winzip.com and download links will be provided.

Scenario 1 – SharePoint Environment

Description

Installing and using WinZip Enterprise in a domain where SharePoint is the only cloud service made available. This scenario also includes:

1. A desktop shortcut for WinZip
2. The PDF conversion and the watermark conversion
3. Zip and Share (WinZip Express) for the SharePoint web interface
4. No other cloud services installed
5. 256-bit AES encryption availability
6. A maximum upload size for SharePoint of 30 MB
7. Password length of 12 characters
8. Passwords require at least one lower case letter, one number, one symbol, and one upper case letter
9. Group Policy installation
10. Automatic copying of the registration file (USER_WZMUL_LOCATION property)
11. WinZip Courier

Installation preparation

Files needed: The installation files for WinZip Enterprise, WinZip Courier, and WinZip Express for SharePoint Server plus the WinZip.wzmul file and the WinZipEC.ecmul file.

WinZip

Using Orca or some other MSI file editing software, create one or more transform files (.mst) for WinZip, setting the following items in the Property table to these values:

Property	Value
ADDDESKTOPICON	1
DISABLECLOUDSERVICES	ALIBABACLOUD, AMAZONS3, AZUREBLOB, BOX, CENTURYLINK, CLOUDME, DROPBOX, FTP, GOOGLECLOUD, GOOGLEDRIVE, IBMCLOUD, IONOS, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, OVH, RACKSPACE, S3COMPATIBLE, SUGARSYNC, SWIFTSTACK, TEAMSSHAREPOINT, WASABI, WebDAV, ZIPSHARE
DISABLECONVERSIONS	IMAGERESIZE,ENLARGEREDUCEIMAGE
DISABLEZIPANDSHARE	0
ENCRYPTDISABLEMETHODS	ZIP20,AES128
INSTALL[*cloud service]	0 (Separate properties for each cloud service; the names are ALIBABACLOUD, AMAZONS3, AZUREBLOB, BOX, CENTURYLINK, CLOUDME, DROPBOX, FTP, GOOGLECLOUD, GOOGLEDRIVE, IBMCLOUD, IONOS, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, OVH, RACKSPACE, S3COMPATIBLE, SUGARSYNC, SWIFTSTACK, TEAMSSHAREPOINT, WASABI, WebDAV, ZIPSHARE; example: INSTALLZIPSHARE)
MAXUPSZ_SHAREPOINT	30
PASSWORDLENGTH	12
PASSWORDREQLOWER	TRUE
PASSWORDREQNUMBER	TRUE
PASSWORDREQSYMBOL	TRUE
PASSWORDREQUPPER	TRUE

Add a row to the Property table. Property name = USER_WZMUL_LOCATION; value = the path to a shared network folder where WinZip.wzmul has been saved - enter as \\server\share\subfolder.

Courier

Create a transform file setting the following items in the Property table to these values:

Property	Description
DEFAULTCLOUDSERVICE	SHAREPOINT
DISABLECLOUDSERVICES	AMAZONS3, BOX, CLOUDME, DROPBOX, FTP, GOOGLEDRIVE, IBMCLOUD, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, RACKSPACE, SUGARSYNC, SWIFTSTACK, ZIPSHARE
DISABLECONVERSIONS	IMAGERESIZE,

Installing

1. Plan for and install WinZip Express for SharePoint Server. SharePoint services will temporarily stop and then restart in order to allow the **Zip and Share** menu entry to be added.
2. Create a WinZip software installation Computer Configuration Group Policy for the desired Organizational Unit. Add the transform (.mst file) to the Modifications tab of the policy.
3. Create a Courier software installation Computer Configuration Group Policy for the desired Organizational Unit. Add the transform (.mst file) to the Modifications tab of the policy.
4. Create a script to copy the WinZipEC.ecmul file to each computer in the OU. The destination folder should be C:\ProgramData\WinZipEC.

WinZip and WinZip Courier should be found on each target computer, they should open as registered applications, and SharePoint will be available after entering the user name and password.

Scenario 2 – Amazon S3 Environment

Description

Installing and using WinZip Enterprise in a domain where Amazon S3 and Office 365 (OneDrive for Business) are the only cloud services being made available. This scenario also includes:

1. The WinZip program menu group
2. Sharing on Facebook (for use with a company page)
3. Reduce photos when zipping and Resize photos when managing files
4. Maximum uploading size for Amazon S3 of 70 MB
5. WinZip Express features (Zip and Share, Snap and Share, Scan and Share)
6. Command Line install
7. Automatic copying of the registration file (USER_WZMUL_LOCATION property)
8. WinZip Courier configured to always zip file attachments

Installation preparation

Files needed: The installation files for WinZip Enterprise and WinZip Courier plus the WinZip.wzmul file and the WinZipEC.ecmul file.

<u>WinZip</u>

Using Orca or some other MSI files editing software create one or more transform files (.mst) for WinZip setting the following items in the Property table to these values:

Property	Value
ADDMENUGROUP	1
DEFAULTSHARESERVICE	AMAZONS3 (Note: another service could be used if desired)
DISABLECLOUDSERVICES	ALIBABACLOUD, AZUREBLOB, BOX, CENTURYLINK, CLOUDME, DROPBOX, FTP, GOOGLECLOUD, GOOGLEDRIVE, IBMCLOUD, IONOS, MEDIAFIRE, ONEDRIVE, OPENSTACK, OVH, RACKSPACE, S3COMPATIBLE, SHAREPOINT, SUGARSYNC, SWIFTSTACK, TEAMSSHAREPOINT, WASABI, WebDAV, and/or ZIPSHARE
DISABLECONVERSIONS	CONVPHOTOS, DOCTOPDF, REMOVEPERSDATA, WATERMARK
DISABLENOTIFICATIONSERVICES	LINKEDIN,TWITTER
DISABLEZIPANDSHARE	0
ENABLEEXPRESSFEATURES	1
MAXUPSZ_AMAZON	70

Add a row to the Property table. Property name = USER_WZMUL_LOCATION; value = the path to a shared network folder where WinZip.wzmul has been saved - enter as \\server\share\subfolder.

<u>Courier</u>

Create a transform file setting the following items in the Property table to these values:

Property	Description
ALWAYSZIPATTACHMENTS	1
DEFAULTCLOUDSERVICE	AMAZONS3
DISABLECLOUDSERVICES	BOX, CLOUDME, DROPBOX, FTP, GOOGLEDRIVE, IBMCLOUD, MEDIAFIRE, OFFICE365, ONEDRIVE, OPENSTACK, RACKSPACE, SHAREPOINT, SUGARSYNC, SWIFTSTACK, ZIPSHARE
DISABLECONVERSIONS	CONVPHOTOS, DOCTOPDF, REMOVEPERSDATA, WATERMARK

Installing

1. Create and run a WinZip command line script for installing similar to:
   msiexec /i file.msi /qn TRANSFORMS=file.mst

2. Create and run similar command line for Courier
3. Create a script to copy the WinZipEC.ecmul file to each computer in the OU. The destination folder should be C:\ProgramData\WinZipEC.

WinZip with WinZip Express features and WinZip Courier should be found on each target computer, they should open as registered applications, and the Amazon S3 cloud will be available after entering the access key and secret access key, and OneDrive for Business will be available. When sharing to the company Facebook page for the first time, a login will be required.

Scenario 3 – Prepare for FIPS 140-2 Compliance

Description

Installing and using WinZip Enterprise as part of a FIPS 140-2 compliant Windows solution. When choosing to encrypt, each Zip file being created will have AES 256-bit encrypted data and certified Windows components will be used for all encrypting of data. This scenario has no cloud services, and no social media usage. Converting to PDF and placing a watermark on files also protects files that you zip. This scenario also includes:

1. A start menu shortcut
2. Preconfigured job files for zipping and encrypting personal file backups
3. A somewhat long password length requirement (20 characters)
4. Password policies to require at least one lower case letter, one number, one symbol, and one upper case letter
5. Command line install with property changes made as part of the command line
6. Automatic copying of the registration file (USER_WZMUL_LOCATION property)

Installation preparation

The Local Security Policy for each computer must be configured so that FIPS 140-2 policy setting is enabled. This setting relates to the following Registry key and value:

HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\Enabled=1

Files needed: The installation files for WinZip Enterprise and the WinZip.wzmul file.

Installing

1. Create a WinZip command line script for installing similar to:
   msiexec /i file1.msi /qn ADDSTARTMENU=1 FIPSComplianceMode=DEFAULT
   DISABLECONVERSIONS=IMAGERESIZE,ENLARGEREDUCEIMAGE INSTALLJOBFILES=1
   PASSWORDLENGTH=20 PASSWORDREQLOWER=TRUE PASSWORDREQNUMBER=TRUE
   PASSWORDREQSYMBOL=TRUE PASSWORDREQUPPER=TRUE
   USER_WZMUL_LOCATION=\\server\share\subfolder

WinZip should be found on each target computer, it should open as a registered application, AES 256-bit encryption will always be used when creating Zip files (no other encryption will be available), and viewing contents of files in Zip files or extracting from Zip files that use encryption weaker than AES 256-bit will be stopped programmatically.

Scenario 4 – Multiple Cloud Access Environment

Description

Installing and using WinZip Enterprise in a domain where multiple cloud services are made available, SharePoint being the default. This scenario will also include:

1. A desktop shortcut for WinZip
2. All conversions available
3. Zip and Share (WinZip Express)
4. Most recently used list for files will be turned on
5. Zip20 encryption disabled
6. SharePoint, Amazon S3, Office 365 (OneDrive for Business), Google Drive, and OneDrive allowed as cloud services
7. A maximum upload size of 50 MB for each cloud service
8. WinZip Express features (Zip and Share, Snap and Share, Scan and Share)
9. Group Policy installation
10. Automatic copying of the registration file (USER_WZMUL_LOCATION property)
11. WinZip Courier

Installation preparation

Files needed: The installation files for WinZip Enterprise, WinZip Courier, and WinZip Express for SharePoint Server plus the WinZip.wzmul file and the WinZipEC.ecmul file.

WinZip
Using Orca or some other MSI files editing software create one or more transform files (.mst) for WinZip setting the following items in the Property table to these values:

Property	Value
ADDDESKTOPICON	1
DISABLECLOUDSERVICES	ALIBABACLOUD, AZUREBLOB, BOX, CENTURYLINK, CLOUDME, DROPBOX, FTP, GOOGLECLOUD, IBMCLOUD, IONOS, MEDIAFIRE, OPENSTACK, OVH, RACKSPACE, S3COMPATIBLE, SUGARSYNC, SWIFTSTACK, WASABI, WEBDAV, ZIPSHARE
DISABLECONVERSIONS	NONE

DISABLERECENTARCHIVES	0
DISABLEZIPANDSHARE	0
ENABLEEXPRESSFEATURES	1
ENCRYPTDISABLEMETHODS	ZIP20
MAXUPSZ_AMAZON	50
MAXUPSZ_GDRIVE	50
MAXUPSZ_SHAREPOINT	50
MAXUPSZ_ ONEDRIVE	50

Add a row to the Property table. Property name = USER_WZMUL_LOCATION; value = the path to a shared network folder where WinZip.wzmul has been saved - enter as \\server\share\subfolder.

Courier
Create a transform file setting the following items in the Property table to these values:

Property	Description
DEFAULTCLOUDSERVICE	SHAREPOINT
DISABLECLOUDSERVICES	BOX, CLOUDME, DROPBOX, FTP, IBMCLOUD, MEDIAFIRE, OPENSTACK, RACKSPACE, SUGARSYNC, SWIFTSTACK, ZIPSHARE
DISABLECONVERSIONS	NONE

Installing

1. Plan for and install WinZip Express for SharePoint Server. SharePoint services will temporarily stop and then restart in order to allow the **Zip and Share** menu entry to be added.
2. Create a WinZip software installation Computer Configuration Group Policy for the desired Organizational Unit. Add the transform (.mst file) to the Modifications tab of the policy.
3. Create a Courier software installation Computer Configuration Group Policy for the desired Organizational Unit. Add the transform (.mst file) to the Modifications tab of the policy.
4. Create a script to copy the WinZipEC.ecmul file to each computer in the OU. The destination folder should be C:\ProgramData\WinZipEC.

WinZip with WinZip Express features and WinZip Courier should be found on each target computer; they should open as registered applications; and SharePoint, Amazon S3, Google Drive, and OneDrive will be available after entering the appropriate user names and passwords.

Scenario 5 – "The Works", Minus Social Media for Some

Description

Install WinZip Enterprise by Group Policy and give the maximum feature set to the "Marketing OU", but remove Social Media options for those not in the Marketing OU. No default cloud service or share service will be defined. When available, users will be able to set those on their own. The password policy will be the

WinZip default, which is a length of 8 characters and the Password Policy tab in WinZip Options will be available.

Installation preparation

Files needed: The installation files for WinZip Enterprise, WinZip Courier, and WinZip Express for SharePoint Server, plus the WinZip.wzmul file and the WinZipEC.ecmul file.

WinZip
Using Orca or some other MSI files editing software create the Marketing OU transform file(s) for WinZip setting the following items in the Property table to these values:

Property	Value
ADDDESKTOPICON	1
ADDMENUGROUP	1
ADDSTARTMENU	1
DISABLECLOUDSERVICES	NONE
DISABLECONVERSIONS	NONE
DISABLENOTIFICATIONSERVICES	NONE
DISABLEZIPANDSHARE	0
ENABLEEXPRESSFEATURES	1
INSTALLEXPRESSOFFICE	1
INSTALLJOBFILES	1
INSTALLPREVIEWER	1
NOINTERNALEMAILER	0
PASSWORDRESTRICT	DEFAULT
USAGECOLLECTLOCK	0

Add a row to the Property table. Property name = USER_WZMUL_LOCATION; value = the path to a shared network folder where WinZip.wzmul has been saved - enter as \\server\share\subfolder.

Create a second WinZip transform file for all target computers that are not in the Marketing OU setting the value of **DISABLENOTIFICATIONSERVICES** to **ALL**, which is the default value, listed below to demonstrate the difference in properties between this table and the configuration above.

Property	Value
ADDDESKTOPICON	1
ADDMENUGROUP	1
ADDSTARTMENU	1
DISABLECLOUDSERVICES	NONE
DISABLECONVERSIONS	NONE
DISABLENOTIFICATIONSERVICES	ALL
DISABLEZIPANDSHARE	0

ENABLEEXPRESSFEATURES	1
INSTALLEXPRESSOFFICE	1
INSTALLJOBFILES	1
INSTALLPREVIEWER	1
NOINTERNALEMAILER	0
PASSWORDRESTRICT	DEFAULT
USAGECOLLECTLOCK	0

Add a row to the Property table. Property name = USER_WZMUL_LOCATION; value = the path to a shared network folder where WinZip.wzmul has been saved - enter as \\server\share\subfolder.

<u>Courier</u>
Create a transform file setting the following items in the Property table to these values:

Property	Description
DISABLECLOUDSERVICES	NONE
DISABLECONVERSIONS	NONE

Note: Only one transform will be needed for Courier, as it does not include Social Media features.

Installing

1. Plan for and install WinZip Express for SharePoint Server. SharePoint services will temporarily stop and then restart in order to allow the **Zip and Share** menu entry to be added.
2. Create a WinZip software installation Computer Configuration Group Policy for the Marketing Organizational Unit. Add the first transform (.mst file) to the Modifications tab of the policy.
3. Create a second WinZip software installation Computer Configuration Group Policy for the other targeted Organizational Unit. Add the second transform to the Modifications tab of the policy.
4. Create a Courier software installation Computer Configuration Group Policy for the desired Organizational Unit. Add the transform (.mst file) to the Modifications tab of the policy.
5. Create a script to copy the WinZipEC.ecmul file to each computer in the OU. The destination folder should be C:\ProgramData\WinZipEC.

WinZip Express features, WinZip Express for Office, and WinZip Courier should be found on each target computer and they should open as registered applications. Marketing OU users will find all WinZip and Courier features available and will be able to configure password policies and other features as they desire. Users in the other targeted OU will have the same features minus the use of Social Media.

WinZip Computing	Corel Corporation
P.O. Box 540	1600 Carling Ave.
Mansfield, CT	Ottawa, ON
06268 USA	Canada, K1Z 8R7