

# WinZip SafeMedia Manager Administrator Guide

Welcome to the WinZip® SafeMedia™ Manager Administrator Guide.

This guide is designed to help system administrators configure and deploy WinZip SafeMedia in their organization.

This guide is intended only for a multiple-user license of WinZip SafeMedia and does not apply to other versions of the software. These instructions are designed for information technology professionals who may need to use advanced techniques to deploy WinZip SafeMedia, or to tailor the product to fit their organization's needs.

Topics include:

- Overview
- Preparing for WinZip SafeMedia deployment
- Installing and uninstalling WinZip SafeMedia from the command prompt
- Using the registry
- About the WinZip SafeMedia Manager
- Creating and managing groups in WinZip SafeMedia Manager
- Setting permissions
- Deploying WinZip SafeMedia Manager configurations
- About passwords
- System requirements
- Contact information

This guide also includes a reference section that expands upon some topics. For more information, see "Reference section" on page 19.

## Overview

The basic process of deploying WinZip SafeMedia involves the following steps:

- 1 The administrator installs WinZip SafeMedia to their system.
- 2 The administrator also installs the administrator-only companion application, WinZip SafeMedia Manager, to their system.

- 3 In WinZip SafeMedia Manager, the administrator sets the user and machine permissions, optionally creating groups so that different permissions can be assigned according to the user's role in the organization.
- 4 The administrator exports the permissions settings as a tool (.exe), group (.grp), or registry (.reg) file. The easiest deployment uses the tool (.exe file). If the tool isn't an option because of the environment or other factors, the group (.grp) or registry (.reg) files can be used.
- 5 The administrator deploys WinZip SafeMedia to users and deploys the permission settings for each user or machine.
- 6 The administrator tests the results to ensure the application and permissions are working as expected.

### Example deployment flow

- 1 As the administrator, open **WinZip SafeMedia Manager**.
- 2 In the **WinZip SafeMedia Manager** window, click **New** to add a new group, and name the group.
- 3 In the **By user account** area, choose the **Force password protection** option.
- 4 Click the **Apply** button.
- 5 Click **Export tool**, and choose a destination for the configuration tool file, choose the **Not password protected**, and click **OK**.
- 6 Install **WinZip SafeMedia** to the user machine.
- 7 Run the configuration tool (.exe) on the same user machine to configure the user account with the settings.

## Preparing for WinZip SafeMedia deployment

Before you install WinZip SafeMedia, we recommend that you do the following:

- Uninstall all previous versions of the software.
- Close all other applications.
- Reboot systems.

The default installation location for WinZip SafeMedia is **C:\Program Files(x86)\WinZip SafeMedia\WinZip SafeMedia**.

**Note:** At any point, if a disc drive is not recognized on a computer, try installing the latest drivers for the disc drive. If the issue persists, contact Support: [www.winzip.com/support](http://www.winzip.com/support).

## Installing and uninstalling WinZip SafeMedia from the command prompt

WinZip SafeMedia can be installed by calling the setup.exe file or the .msi file from the commands prompt (Windows 7, Windows 8, Windows 10, and Windows 11).

One or more parameters can be added to customize the installation.

You can install WinZip SafeMedia from a shared network location, or uninstall the application from the command prompt.

### Command line parameters

You can add parameters to your install instructions to control the installation experience and the amount of interaction required from the users. The command line syntax can be used with network management tools to perform a network-based deployment.

You can also include instructions that generate an installation log file in case you should run into a problem that requires assistance from the WinZip Support team.

Example installation command line for .msi, enables installation log:

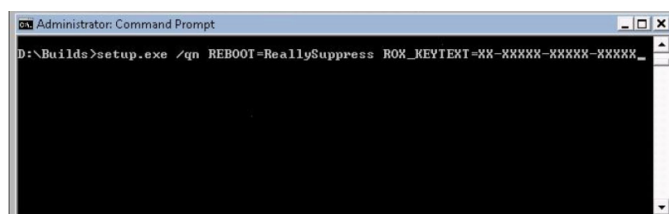
```
msiexec /i "WinZip SafeMedia.msi" /L*V "<log path>"
```

Example installation command line for .exe, enables installation log:

```
"WinZip SafeMedia.exe" /v"/L*V <log path>"
```

Setup.exe is the installer application, designed to provide a graphical user interface for the typical end-user installation. This application can also run silently, without the graphical user interface. You can also install from the .msi file.

Below is an example of the syntax used to perform a silent install from the setup.exe file. The location of the setup.exe file will depend on where on the system the WinZip SafeMedia install files are located.



The following tables list the available parameters:

### Required parameters

Description	Parameter	.msi	.exe
KEYTEXT=XX-XXXX-XXXX-XXXX-XXXX-XXXX	Add CD Key	Change to sn= XX-XXXX-XXXX-XXXX	Change to sn= XX-XXXX-XXXX-XXXX

## Install options

Description	Parameter	.msi	.exe
Silent install (no dialogs)	/qn	/qn	/qn
Suppress reboot		/VReboot=ReallySuppress	*Not supported

## Optional parameters

Description	Parameter	.msi	.exe
Switch to automatically accept the End-User License Agreement.	MPI_EULA_ACCEPTED=1	/VMPI_EULA_ACCEPTED=1	*Not supported
Enables and locks the "Enable password protection" check box (cannot be disabled by a user).	/ EnableForceSecureBurn	FORCESECUREBURN=1	/VFORCESECUREBURN=1
Enable installation log		/L*V "<log path>"	/v"/L*V <log path>"
Remove Cloud access	FORCENOCLOUD	FORCENOCLOUD=1	/VFORCENOCLOUD=1

## SMS and SCCM

WinZip SafeMedia is compatible with Microsoft's Desktop Deployment tools, including SMS and System Center Configuration Manager.

## Active Directory Group Policy

WinZip SafeMedia is compatible with Group Policy deployment and can be installed by using the script file.

There are two methods that can be used to deploy the application through Group Policy:

- Script File Deploy
- Zap Installer Deploy



When deploying through Group Policy, use the Group Policy options (**Computer Configuration** ▶ **Administrative Templates** ▶ **System** ▶ **Scripts**) to set the **Maximum wait time for Group Policy** scripts to 0.

## To install WinZip SafeMedia from the command prompt

- 1 Open the Windows System **Command Prompt** window. (you must run it as an Administrator).

For Windows 8 or higher, you can right-click the **Start** menu, and click **Command Prompt (Admin)** in the context menu.

If a **User Account Control** prompt appears, click **Yes** to continue installation.

- 2 Call the product **setup.exe** or **.msi** file, and include the desired command line parameters.



You must have system administrator privileges to install WinZip SafeMedia from the command prompt.

## To install from a shared network location

- 1 Copy the contents of the WinZip SafeMedia installation disc to a network location.
- 2 From a remote computer, go to the Start search box (Windows 7, Windows 8, and Windows 10), or the **Start ▶ Run** menu.
- 3 Browse to the shared copy of the disc and enter the **setup.exe** or **.msi** command with the desired parameters.

For a list of parameters that can be added to the command line, see “Command line parameters” on page 3.



When installing the software or when rebooting your system at the end of an installation, you must be logged into the system with administrator privileges.

## To uninstall WinZip SafeMedia

- Type the following command: **C:\ProgramData\Uninstall\{B2E47DE7-800B-40BB-BD1F-9F221C3AEE87}\setup.exe" /X {B2E47DE7-800B-40BB-BD1F-9F221C3AEE87} /qn REBOOT=ReallySuppress**



After you run the uninstall, you must reboot to remove any remaining files and before you install another version of the software.

## To use Script File Deploy

- 1 Create a shared path to the installer folder on the server.
- 2 Create a script file with the following command line parameter: **\\server\shared folder\setup.exe KEYTEXT=XX-XXXXX-XXXXX-XXXXX /qn REBOOT=ReallySuppress.**

## To create Group Policy

- 1 Launch the Group Policy Object Editor.
- 2 Under **Computer Configuration**, select **Windows Settings ▶ Scripts**, and double-click **Startup**.
- 3 Click **Add**.

- 4 Browse to your script file.
- 5 Click **OK**.
- 6 Restart the client machine and verify the installation during login.



To uninstall by editing the script file on Windows 7, Windows 8, Windows 8.1, and Windows 10, use the following command: **C:\ProgramData\Uninstall\{D593D658-FF81-4069-9A69-D9F6B17BD6A2}\setup.exe" /X {D593D658-FF81-4069-9A69-D9F6B17BD6A2} /qn REBOOT=ReallySuppress**

## To use Zap Installer Deploy

- Create a Zap file based on the following example:

*[Application]*

*; Only FriendlyName and SetupCommand are required, everything else is optional.*

*; FriendlyName is the name of the program that will appear in the software installation snap-in and the Add/Remove Programs tool.*

*; REQUIRED*

*FriendlyName = "WinZip SafeMedia"*

*; SetupCommand is the command line used to run the program's Setup. With Windows Server 2003 and later you must specify the fully qualified path containing the setup program.*

*; Long file name paths need to be quoted. For example: SetupCommand =*

*"\\server\share\long\_folder\setup.exe" /unattend REQUIRED*

*SetupCommand = "\\server\share\setup.exe /KEYTEXT-XX-XXXXX-XXXXX-XXXXX /qn REBOOT=ReallySuppress"*

*; Version of the program that will appear in the software installation snap-in and the Add/Remove Programs tool. OPTIONAL*

*DisplayVersion = 4.0*

*; Version of the program that will appear in the software installation snap-in and the Add/Remove Programs tool. OPTIONAL*

*Publisher = WinZip*

## To publish the program

- 1 In **User Configuration**, right-click **Software Installation**, and click **New**.
- 2 Click **Package**.
- 3 Type the path to the folder containing the .zap file.
- 4 Click **Open**.

- 5 In the **Files of Type** box, click **ZAW Down-level applications package (\*.zap)**.
- 6 Click the .zap file, and then click **Open**.
- 7 Click **Publish**, and then click **OK**.
- 8 The client computer can now add the program through the Control Panel.



WinZip SafeMedia cannot be uninstalled with a Zap file. Please see the script file for uninstall procedures, or remove the program through the Control Panel.

## Using the registry

You can use registry keys to control settings such as disc finalizing, write permissions, event logging, and passwords.

### Finalizing the disc

It is recommended that you always finalize the disc. There is a registry key to control the finalize disc function.

The registry key is named "ForceDiscClosed" in

**HKEY\_CURRENT\_USER\SOFTWARE\WinZip\Basic Burn\Preference.**

The value type is DWORD, and the value number should be 0 or 1.

- **0** — By default discs are not finalized. The user can change this setting by enabling the **Always close DVD disc (no longer append data)** check box in the **Settings** dialog box.
- **1** (default value) — By default discs are finalized, and the user cannot change this setting in the **Settings** dialog box.



This feature can be set by the WinZip SafeMedia Manager. The registry key setting will be ignored if permissions have been set in WinZip SafeMedia Manager.

### Enabling logging

Depending on your version of WinZip SafeMedia, you may have the ability to enable and disable event logging for the current user by using the registry.

The registry key is named "EnableLogging" in

**HKEY\_CURRENT\_USER\SOFTWARE\WinZip\Basic Burn\Preference.**

The value type is DWORD, and the value number should be 0 or 1.

- **1** (default value) — Logging is enabled for the current user.
- **0** — Logging is disabled for the current user.



The registry key will be ignored if logging is set in the WinZip SafeMedia Manager.

## Changing the log file location

You can change where the log is stored with the "LogPath" registry key in **HKEY\_CURRENT\_USER\SOFTWARE\WinZip\Basic Burn\Preference**

The registry is empty by default and writes to the default location: **C:\ProgramData\WinZip Log Files**.

## Setting default password

Depending on your version of WinZip SafeMedia, you may have the ability to set a default password for the current user by using the registry.

The registry key is named "DefaultPassword" in **HKEY\_CURRENT\_USER\SOFTWARE\WinZip\Basic Burn\Preference**.

The value type is REG\_SZ, and the default password string should be encrypted but not input into the registry directly.

## To set a default password

- 1 Launch WinZip SafeMedia.
- 2 Click the **Settings** button to display the **Settings** dialog box.
- 3 In the **Settings** dialog box, click **Always use this password**.  
The default password dialog box appears.
- 4 Type the password you wish to set, and click **Apply**.



You must restart the computer to apply the device access control settings for WinZip SafeMedia.

The registry key will be ignored if the password is set in the WinZip SafeMedia Manager.

## About the WinZip SafeMedia Manager

The WinZip SafeMedia Manager is standalone administrator-only software that is shipped with WinZip SafeMedia. The administrator installs WinZip SafeMedia Manager to their own system and uses it to create configuration files that can be used to control external media reading and writing capabilities and set encryption rules for users and user machines.

The WinZip SafeMedia Manager also enables the system administrator to create and modify user groups. Groups can be used to assign different read and write permissions according to role or department.

To install the WinZip SafeMedia Manager, run the setup.exe. By default the application is installed to **C:\Program Files (x86)\WinZip SafeMedia\WinZip SafeMedia Manager**.

**Note:** Remember to run the WinZip SafeMedia Manager as the system administrator.



## To launch the WinZip SafeMedia Manager

- Open the application as the system administrator from one of the following locations:
  - From the Windows **Start** menu, choose **WinZip SafeMedia > WinZip SafeMedia Manager**.
  - **WinZip SafeMedia Manager** shortcut on the desktop.
  - **SafeMedia Manager.exe** in C:\Program Files (x86)\WinZip SafeMedia\WinZip SafeMedia Manager.

## Creating and managing groups in WinZip SafeMedia Manager

You can create groups in the WinZip SafeMedia Manager that let you assign different permissions to users and machines. For example, you could create three groups, one for IT administrators, one for managers, and one for other employees. The encryption, read, and write permissions can be set differently for each group.

Each user account with WinZip SafeMedia can be associated with a specific group when you assign it a group key. Computers (devices) within a group are permitted to read discs created by other users within that group without the need to enter a password. A computer can belong only to one group, but the computer can be given permission to read discs written by members from other groups. System administrators can set, change, and delete those permissions by using the WinZip SafeMedia Manager. They can also change group memberships.

Deleting a group key prevents a computer from reading a disc encrypted with that specific key, unless the disc is also protected by a password that the user knows. If the deleted group key is the only one associated with a computer, WinZip SafeMedia group features will be disabled, and passwords will be required for reading and writing encrypted discs.

**Note:** It is not necessary to create groups if you want a single set of permissions to apply to all users and all machines.

## To enter a new group or change a group key


1 Do one of the following:


- To create a new group, click **New**. A new group and group key (a GUID) is created automatically.
- To change **Group Key** or **Group Name**, click an existing group name or group key and edit the highlighted information.

A group key can be any combination of letters and numbers up to 40 characters in length.

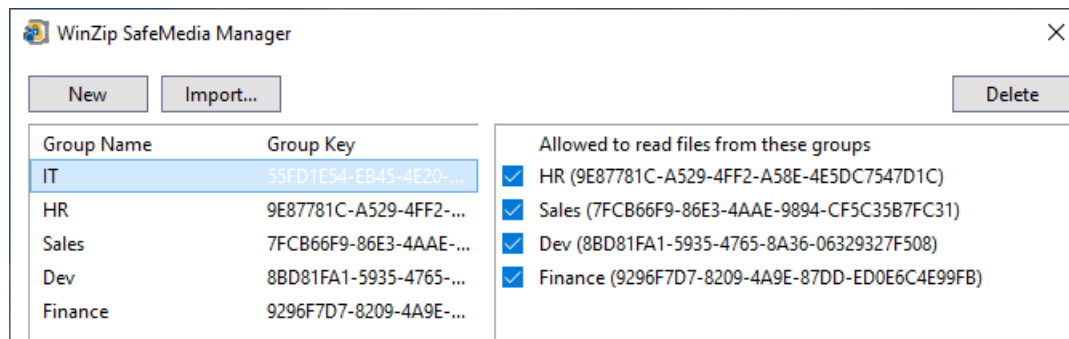
2 In the **Allowed to read files from these groups** column, specify the read access for files encrypted by other groups.

- 3 Click **Apply** to confirm the change and leave the WinZip SafeMedia Manager open, or click **OK** to confirm the change and close the WinZip SafeMedia Manager

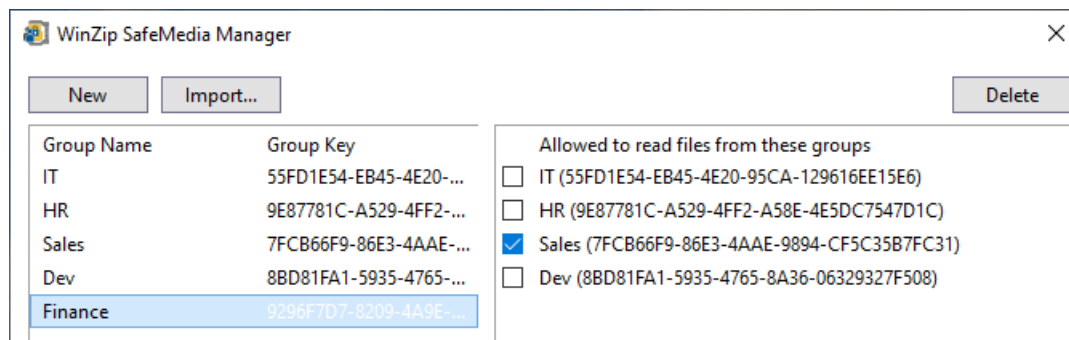
 The group name is a helpful way to keep track of groups if your group keys are intentionally set to prevent replication by end users. Follow the steps described above to create group names for each group key.

 Group information and permissions can be changed, but the changes must be exported and updated for affected users and machines. Changes affect access to previously encrypted files.

In the example below, there are five groups. Members of the first group (IT) can read files from any other group, without requiring a password.




The fifth group (Finance) can read files encrypted by Sales without a password, but need to know the password for files encrypted by any other group.




## To change group membership

- 1 If the new group key is not already listed, enter it in one of the group key fields.
- 2 Select the group from the **Group Name** list.
- 3 In the **Allowed to read files from these groups** list, enable the check boxes for the groups whose files can be read by the group that you selected in the **Group Name** list.

 Discs previously created on a computer may become unreadable after the original group key is changed or deleted. WinZip SafeMedia cannot retrieve the data.

### To delete a group key

- 1 From the **Group Key** list, select the key you want to delete.
- 2 Click **Delete**.

 Discs previously created on a computer may become unreadable after the original group key is changed or deleted. WinZip SafeMedia cannot retrieve the data.

## Setting permissions

The administrator can use the WinZip SafeMedia Manager to set the read, write, and encryption permissions for users in WinZip SafeMedia. If you created groups, permissions can be set for each group.

The WinZip SafeMedia Manager settings determine which options will be available to users in the WinZip SafeMedia **Settings** window.

Points to remember:

- Group settings are per user, so each user on the machine can have different permissions.
- By machine settings affect read/write permissions for third-party software.

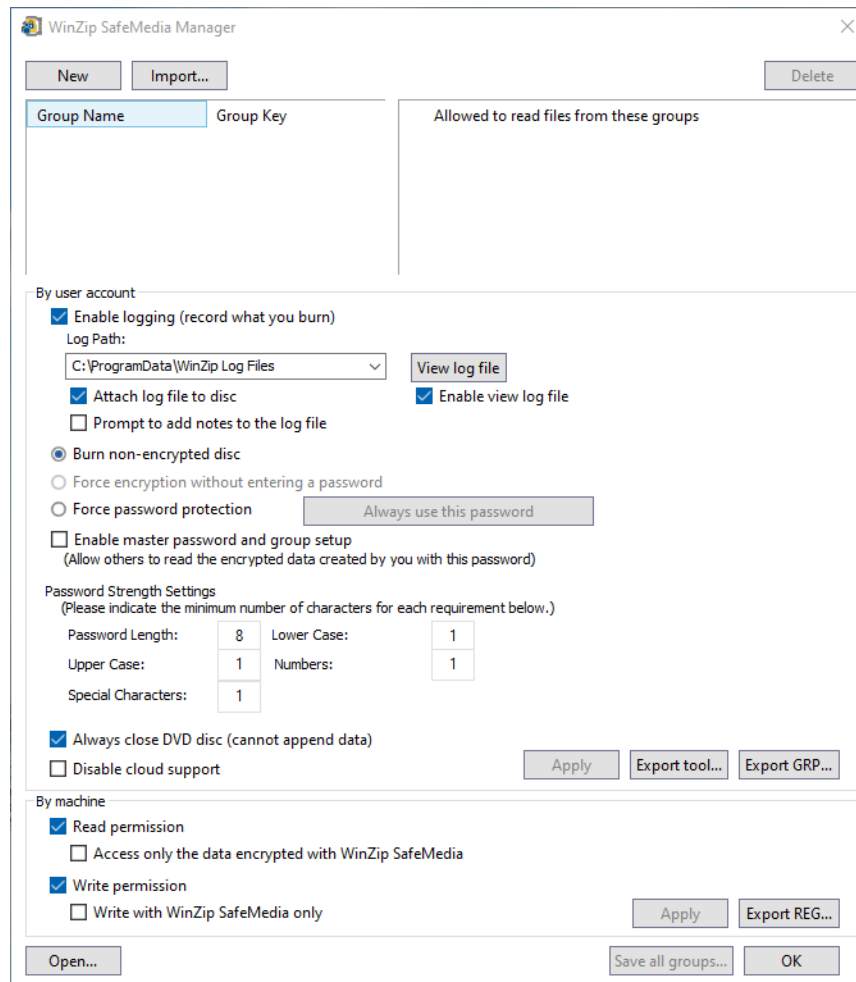
**Note:** Permissions settings in the WinZip SafeMedia Manager override permissions set in the registry.

The permissions available in the WinZip SafeMedia Manager are listed below. Permissions are organized **By user account** or **By machine**.

### To set permissions in WinZip SafeMedia Manager

- 1 Choose the permissions you want in the **By user account** or **By machine** area of the **WinZip SafeMedia Manager** window.
- 2 Click **Apply** to confirm the change and leave the **WinZip SafeMedia Manager** open, or click **OK** to confirm the change, close the **WinZip SafeMedia Manager**, and restart the computer to apply the settings.

You can now export the settings. You will export settings for each group you have created. For more information, see "Deploying WinZip SafeMedia Manager configurations" on page 15.



*WinZip SafeMedia Manager*

## Enable logging (record what you burn)

With this option enabled, the logging feature is turned on. This means all events related to saving or burning files to external media devices are logged in a .txt file for tracking and reference purposes.

Event logs are saved in two locations, the Windows Event Viewer and a fixed file. Depending on the location, the event log will contain different events. For details about event logs, see “Reference: Event logs” on page 19.

Settings for event logging include:

- **Log Path:** Specifies where the event log is saved.
- **Attach log file to disc:** Includes a copy of the event log with the encrypted file set.
- **Prompt to add notes to the log file:** Lets users add custom notes to the event log file.
- **Enable view log file:** Lets users view the log file.

## Burn non-encrypted disc

With this option enabled, users can choose to save or burn files to external media devices without encrypting the files. Users can choose between encrypting or not-encrypting by setting the option in their desktop copy of WinZip SafeMedia **Settings** dialog box.

## Force encryption without entering a password

With this option enabled, users are not prompted to enter a password when they save or burn to external media devices. This means that only the groups that have permission to view the encrypted files will be able to read the files. The files cannot be opened by other users (no password option available).

## Force password protection

With this option enabled, a password must be used when saving or burning to external media devices. This means that users outside the groups that have permission to read the encrypted files must enter the password if they want to read the encrypted files.

A default password can be entered in the WinZip SafeMedia Manager by clicking the **Always use this password** button and entering a password. The password must be at least eight characters and include one or more capital letters and at least one number, symbol, or punctuation character. Until your password has met these requirements, the password strength indicator is set to **Invalid**, and the **Save** button is disabled. Be sure to write down your password and store it in a safe place. WinZip SafeMedia is not able to retrieve lost passwords.

If the application finds a default password, WinZip SafeMedia will encrypt the data with the password without displaying a password dialog box.

If the application does not find a default password, WinZip SafeMedia will display a password dialog box before every burning action. The application cannot burn a disc without the user entering a password or choosing the default password option.

## Enable master password and group setup

With this option enabled, at the time of encryption, users have the option of choosing a specific group that can read the files by entering the designated password.

## Password strength settings

The administrator can set parameters for user passwords by setting a minimum value for any of the following parameters:

- **Password Length**
- **Lowercase**
- **Uppercase**

- **Numbers**
- **Special Characters**

## **Always close DVD disc (cannot append data)**

After burning to a disc, this option forces the disc closed so that no additional files can be appended. For information about alternative ways of setting this option, see Reference: Always close DVD disc (cannot append data).

## **Disable cloud support**

This option lets you disable WinZip SafeMedia cloud support. When the check box is enabled, the Cloud window is blocked, preventing users from adding cloud-based files and folders to the File List Editor.

## **By machine**

You can use the WinZip SafeMedia Manager to set the following permissions for individual computers. These computer-based permissions control drives that can be used for removable media.

- **Read permission** — With this option enabled (check mark in box, on by default), the machine can read data from removable media.
  - **Access only the data encrypted with WinZip SafeMedia** — With this option enabled, only media encrypted with WinZip SafeMedia can be read from removable media sources—third-party software can't read data from any removable media sources.
- **Write permission** — With this option enabled, the machine can write data to removable media.
  - **Write with WinZip SafeMedia only** — With this option enabled, the machine can write to removable media only when using WinZip SafeMedia.

Write permissions can also be controlled by setting the registry key, a DWORD 32-bit value **HKEY\_LOCAL\_MACHINE\SOFTWARE\WinZip\Basic Burn\Preference\WritePermission** in a 32-bit environment or

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\WinZip\Basic**

**Burn\Preference\WritePermission** in a 64-bit environment. If the value is set to 1 (default setting), the write permission is turned on and the application can burn the disc. If the value is set to 0, the write permission is turned off and the application cannot burn the disc. The key can be deployed only by the Administrator, since it is under HKLM under registry.

**Note:** Settings in the WinZip SafeMedia Manager override permissions set in the registry.

## Deploying WinZip SafeMedia Manager configurations

Deployment of configuration settings is accomplished by first exporting the settings and then importing them to other computers or user accounts where WinZip SafeMedia is installed.

For example, if you set one user to belong to Group A, with permission to read discs burned in Groups B, C, and D, you would export those settings and then import them using that user's account. There are different ways to export and import permissions settings.

### To export user permissions by using the configuration tool (.exe)

- 1 Open the **WinZip SafeMedia Manager** on the computer with the settings that you wish to export.
- 2 In the **By user account** area, click the **Export tool** button to export the settings for the user account.
- 3 In the **Save the tool to** box, enter a location for the file.
- 4 Choose one of the following options:
  - **Not password protected** — the configuration tool file (.exe) must be kept in a secure location.
  - **Password protected** — you must enter a password before you can run the configuration tool file (.exe). This option protects the file, but might cause issues if using any deployment automation.
- 5 Click **OK**.

You can now run the tool on user machines to configure user permissions.



When you export group settings by clicking **Export GRP**, only the selected group is exported.



If you are using your own computer to create export configurations, be sure to export your own settings first. When you are finished, use the import steps below to restore your settings to their original state.

### To export settings by using GRP files

- 1 Open the **WinZip SafeMedia Manager** on the computer with the settings that you wish to export.
- 2 In the **By user account** area, click the **Export GRP** button to export the settings for the user account.  
The **Save As** dialog box appears.
- 3 Give your settings configuration a name, and choose a destination where the file should be saved.

- 4 Click **Save**.
- 5 Place the settings file in a location that can be accessed from the target computer.



When you export group settings by clicking **Export GRP**, only the selected group is exported.



If you are using your own computer to create export configurations, be sure to export your own settings first. When you are finished, use the import steps below to restore your settings to their original state.

### To import settings by using the configuration tool (.exe)

- On the target computer, run the .exe file that you exported from the **WinZip SafeMedia Manager**.

If the tool was created using a password, then that password must be passed as an argument to the tool.

A new WorkGroupID based on the original and the user's account will be generated on the machine. WinZip SafeMedia will then honor the configured settings

### To import settings that were exported as a GRP file

**Note:** The group file is encrypted and cannot be used by WinZip SafeMedia directly. To decrypt and import the settings, a separate tool is required. This tool is called

**GenWorkGroupID.exe** and can be found in the following folder where WinZip SafeMedia Manager is installed: **C:\Program Files (x86)\WinZip SafeMedia\WinZip SafeMedia Manager\**

- 1 Copy the exported GRP file to the target environment (another machine and/or user) or make it available to that environment by using a share.
- 2 From the target environment, run the command: "**GenWorkGroupID.exe (XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX) <path of GRP file>**"

A new WorkGroupID based on the original and the user's account will be generated on the machine. WinZip SafeMedia will then honor the configured settings.

### To import settings that were exported as a REG file

- On the target computer, run the REG file that you exported from the WinZip SafeMedia Manager. It will then be imported into the Registry. As an alternative, you can run Regedit.exe with the appropriate arguments. WinZip SafeMedia will then honor the configured settings



## About passwords

When a password is set, WinZip SafeMedia will look for passwords in the following places, listed according to priority from high to low:

- A password set in the WinZip SafeMedia Manager.
- A registry string value **HKEY\_LOCAL\_MACHINE\SOFTWARE\WinZip\Basic Burn\Preference\DefaultPassword** in a 32-bit environment or **HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\WinZip\Basic Burn\Preference\DefaultPassword** in a 64-bit environment. The value of the string is encrypted, so the Administrator should set the password in the **Settings** dialog box (see next bullet) to get a valid encrypted password string value and set it back to the registry key.
- A password set by the user in the **Settings** dialog box. This password saves the value as an unreadable encrypted value in the registry string **HKEY\_CURRENT\_USER\Software\Winzip\WinZip Burn\DefaultPassword**.

If the application finds a set password, WinZip SafeMedia will encrypt the data with the password without displaying a password dialog box during the burning action.

If the application does not find a set password, WinZip SafeMedia will display a password dialog box before every burning action. The application cannot burn a disc without a password, except in the way mentioned below (see “Burn non-encrypted disc” on page 13).

## System requirements

WinZip SafeMedia has the following minimum system requirements:

- Microsoft® Windows® 7, 8, 8.1, 10, 11 Ultimate, Professional, or Enterprise; 32-bit or 64-bit with latest service pack. Windows Server 2008, 2012 R2 or 2016.
- 1 GHz or faster processor
- 1 GB RAM for 32-bit systems; 2 GB RAM for 64-bit systems
- Hard drive with at least 150 MB free space for the installation process
- .NET version 4 or later
- Graphics DirectX 9 or later with WDDM 1.0 driver
- Display minimum of 800 x 600 pixels
- Windows Media Player version 10 or higher
- Internet Explorer 9 or higher, with the latest updates

## Supported media

- USB drives and storage devices
- SD memory cards

- Discs: CD-R/RW, DVD-R/+R/-RW/+RW/+R DL/-R DL, DVD-RAM, BD-R/RE/-R DL, BD-R XL (100 and 128 GB), M-Disc DVD, M-Disc BD



Windows has a character limit for files and folder names; please ensure folder and folder path is less than 256 characters.

USB with FAT32 format can't support single files larger than 4 GB.

## Contact information

For additional information about Enterprise products from WinZip, please visit

[www.winzip.com](http://www.winzip.com).



## Reference section

The following section includes reference information for the WinZip SafeMedia Manager Administrator Guide.

**Note:** This section contains several topics related to setting permissions by using registry keys. It is important to note that settings in the WinZip SafeMedia Manager override permissions set in the registry.

Topics include:

- Reference: Event logs
- Reference: Always close DVD disc (cannot append data)

### Reference: Event logs

WinZip SafeMedia supports event logs which record disc-related actions in .txt file format. You can enable or disable event logs.

Event logs are saved in two locations, the Windows Event Viewer and a fixed file. Depending on the location, the event log will contain different events.

#### Event log locations

Event logs are created in two locations:

- Windows Event Viewer
- A fixed file: `C:\ProgramData\WinZip Log Files\Current User name_YYYYMMDDHHMMSS.txt`

#### Event logs in Windows Event Viewer

The following events will be logged in the Windows Event Viewer:

- Burn data disc initialized
- Burn data disc completed
- Burn data disc failed
- Burn data disc canceled
- Copy disc initialized
- Copy disc completed

- Copy disc failed
- Copy disc canceled
- Burn image initialized
- Burn image completed
- Burn image failed
- Burn image canceled
- Disc ejected
- Disc inserted
- Disc erased
- Quick verification of data disc initialized
- Verification of data disc initialized
- Unknown operation type

The following log format is used:

*Source: WinZipSafeMedia*

*User Name: PC-GV227GBGU\Corel*

*Log File: C:\ProgramData\WinZipSafeMedia Log Files\PC-GV227GBGU.Corel\_20150108133716.txt*

*Task with time: Writing is completed in drive (E) at 1/8/2015 1:37:16 PM*

## **Event logs in fixed files**

Date, Computer Name, User Name, and a list of files and folders are recorded in the following format when an external media event is initialized:

*Date: Thu Jan 08 11:31:40 2019*

*Computer Name: PC-GV227GBGU*

*User Name: PC-GV227GBGU.Corel*

*Project includes 0 folder(s) and 4 file(s)*

=====

*C:\Users\Corel\Pictures\IMG\_0659.JPG*

*C:\Users\Corel\Pictures\IMG\_0660.JPG*

*C:\Users\Corel\Pictures\IMG\_0662.JPG*

*C:\Users\Corel\Pictures\2010-03-22\Thumbs.db*

*END OF FILE*

## Enabling event logging

The main method of enabling event logging is to choose this option in the WinZip SafeMedia Manager.

Alternatively, you can set the registry key, a DWORD 32-bit value

**HKEY\_LOCAL\_MACHINE\SOFTWARE\WinZip\Basic Burn\Preference\EnableLogging** in a 32-bit environment or **HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\WinZip\Basic Burn\Preference\EnableLogging** in a 64-bit environment. If the value is set to 1 (default setting), the log is generated. If the value is set to 0, no log is generated.

## Complete list of event log IDs

The table below maps the **Event IDs** that are presented in the **Event Viewer** with their corresponding meaning and ID Names.

<b>ID Value</b>	<b>The meaning of the ID</b>	<b>ID Name</b>
1001	Disc inserted into the drive	EVENT_DISC_INSERTED
1002	Disc ejected from the drive	EVENT_DISC_EJECTED
1003	Writing is initiated for the drive	EVENT_BURN_DATA_INITIATED
1004	Writing is completed on the drive	EVENT_BURN_DATA_COMPLETED
1005	Started copy on the drive	EVENT_BURN_COPY_INITIATED
1006	Completed copy on the drive	EVENT_BURN_COPY_COMPLETED
1007	Started burn image on the drive	EVENT_BURN_IMAGE_INITIATED
1008	Completed burn image on the drive	EVENT_BURN_IMAGE_COMPLETED
1009	Writing is failed on the drive	EVENT_BURN_DATA_FAILED
1010	Writing is canceled on the drive	EVENT_BURN_DATA_CANCELED
1011	Failed to copy data on the drive	EVENT_BURN_COPY_FAILED
1012	Copying is canceled on the drive	EVENT_BURN_COPY_CANCELED
1013	Failed to burn image on the drive	EVENT_BURN_IMAGE_FAILED
1014	Burning image is canceled on the drive	EVENT_BURN_IMAGE_CANCELED
1015	Started erase disc on the drive	EVENT_ERASE_INITED
1016	Erase disc completed on the drive	EVENT_ERASE_COMPLETED
1017	Failed to erase disc on the drive	EVENT_ERASE_FAILED
1018	Quick verify the burn data on the drive	EVENT_DISC_QVERIFY
1019	Verify the burn data on the drive	EVENT_DISC_VERIFY
1020	Writing is initiated for the drive	EVENT_LOCAL_BURN_DATA_INITIATED
1021	Writing is completed on the drive	EVENT_LOCAL_BURN_DATA_COMPLETED
1022	Writing is failed on the drive	EVENT_LOCAL_BURN_DATA_FAILED

1023	Writing is canceled on the drive	EVENT_LOCAL_BURN_DATA_CANCELED
1024	Started copy on the drive	EVENT_LOCAL_BURN_COPY_INITIATED
1025	Completed copy on the drive	EVENT_LOCAL_BURN_COPY_COMPLETED
1026	Failed to copy data on the drive	EVENT_LOCAL_BURN_COPY_FAILED
1027	Copying is canceled on the drive	EVENT_LOCAL_BURN_COPY_CANCELED
1028	Started erase encrypted file on the drive	EVENT_LOCAL_ERASE_INITED
1029	Erase encrypted file completed on the drive	EVENT_LOCAL_ERASE_COMPLETED
1030	Failed to erase encrypted file on the drive	EVENT_LOCAL_ERASE_FAILED
1031	Erasing is canceled on the drive	EVENT_LOCAL_ERASE_CANCELED

## Event log terminology

The following table is a glossary of common event log terminology.

Term	Definition
Date	The date when the event occurred
Computer Name	The name of this computer
User Name	The name of the user of this computer
	Describe the status of WinZip SafeMedia, for example, Burning, Canceling, etc.
Volume Label	The name of the volume
Volume SN	The serial number of the volume
Volume ID	The ID value of the volume
Type	The type of disc, for example, DVD+RW
Status Of Media	The status of media, for example, Appendable, Closed session, etc.
Files	The files used in the event
File System	For example, UDF 1.5, FAT32, etc.
Disc Number	The number of the disc that is in this computer
Encryption	The encryption status of the drive
User Password	Does the user need to enter a password
Spanned Set	When the data is too large, we need to burn it separately on several discs. This key represents whether the current disc is one of the discs.

Data Size On Disc Set	The total data size for the disc set
Network Volume	The name of network

## Reference: Always close DVD disc (cannot append data)

After burning to a disc, this option forces the disc closed so that no additional files can be appended. In addition to setting this option in the WinZip SafeMedia Manager, you can enable this feature by setting a registry key, a DWORD 32-bit value

**HKEY\_LOCAL\_MACHINE\SOFTWARE\WinZip\Basic Burn\Preference\ForceDiscClosed** in a 32-bit environment or

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\WinZip\Basic Burn\Preference\ForceDiscClosed** in a 64-bit environment.

The key can be deployed only with Administrator permission, since it is under HKLM under registry.

- If the value is set to 1 (default setting), the **Always close DVD disc** check box in the **Settings** dialog box is enabled and grayed out to prevent change.
- If the value is set to 0, the **Always close DVD disc** check box is disabled and open to change.
- If the value is set to 2, the **Always close DVD disc** check box is enabled and open to change.

© 2021 Corel Corporation. All rights reserved.

## WinZip® SafeMedia Manager Administrator Guide

Corel, WinZip, SafeMedia, Roxio and Secure Burn are trademarks or registered trademarks of Corel Corporation in Canada, the U.S., and/or elsewhere.

All other company, product and service names, logos, brands and any registered or unregistered trademarks mentioned are used for identification purposes only and remain the exclusive property of their respective owners. Use of any brands, names, logos or any other information, imagery or materials pertaining to a third party does not imply endorsement. We disclaim any proprietary interest in such third-party information, imagery, materials, marks and names of others. For all notices and information about patents please visit <https://www.corel.com/patents>.