

Roxio Secure Burn Enterprise Deployment Guide

Welcome to the system administrator's deployment guide.

This guide is designed to help system administrators deploy Roxio® Secure Burn™ Enterprise in their organization.

Prior to installing Roxio Secure Burn Enterprise, please ensure that all previous versions of the software have been uninstalled and that all other applications are closed.

The default installation location for Roxio Secure Burn Enterprise is **C:\Program Files(x86)\Roxio\Roxio Burn**.

This guide presents the following topics:

- Installing Roxio Secure Burn Enterprise from the command prompt
- Using the registry
- Using the Permissions Manager
- System requirements
- Contact information



This guide is intended only for the deployment of a multiple-user license of Roxio Secure Burn Enterprise 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 Roxio Secure Burn Enterprise, or to tailor the product to fit their organization's needs.



Individuals can simply install Roxio Secure Burn Enterprise by running the setup.exe installer program included on their installation disc or in the installation files. Setup.exe is an installer designed with a graphical user interface, and it provides all instructions necessary for normal installation. To learn how to use Roxio Secure Burn, please open the application, click the Help menu, and select from one of the available options.

Installing Roxio Secure Burn Enterprise from the command prompt

Roxio Secure Burn Enterprise can be installed by calling the setup.exe file from the commands prompt (Windows 7, Windows 8, Windows 8.1, and Windows 10).

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

You can install Roxio Secure Burn Enterprise from a shared network location, or uninstall the application from the command prompt.

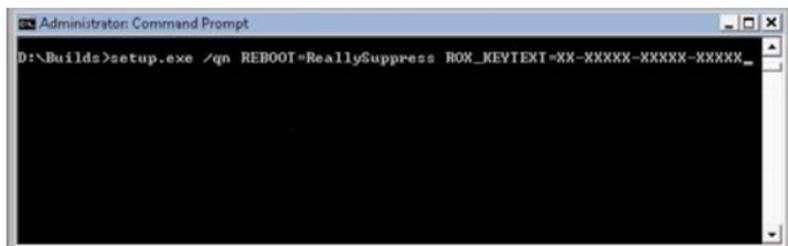
Command line parameters

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 a log file in case you should run into a problem that requires assistance from Roxio's Global Customer Care team.

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. 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 Roxio Secure Burn Enterprise install files are located.



The following tables list the available parameters:

Required parameters

Parameter	Description
Add CD Key	ROX_KEYTEXT=XX-XXXXX-XXXXX-XXXXX

Install options

Parameter	Description
/qn	Silent install (no dialogs)
Reboot=ReallySuppress	Suppress reboot

Optional parameters

Parameter	Description
{lang}=XXX	XXX is a three-letter language code (ENU, FRA, ITA, ESN, JPN, DEU, NLD etc.). It applies only to the use of setup.exe.
MPI_EULA_ACCEPTED=1	Switch to automatically accept the End-User License Agreement.

SMS and SCCM

Roxio Secure Burn Enterprise is compatible with Microsoft's Desktop Deployment tools, including SMS and System Center Configuration Manager.

Active Directory Group Policy

Roxio Secure Burn Enterprise 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 Roxio Secure Burn Enterprise 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**, and include the desired command line parameters.



You must have system administrator privileges to install Roxio Secure Burn Enterprise from the command prompt.

To install from a shared network location

- 1 Copy the contents of the Roxio Secure Burn Enterprise installation disc to a network location.
- 2 From a remote computer, go to the Start search box (Windows Vista, Windows 7, Windows 8, Windows 8.1, and Windows 10), or the **Start ► Run** menu.
- 3 Browse to the shared copy of the disc and enter the **setup.exe** command with the desired parameters.

For a list of parameters that can be added to the command line, see “Command line parameters” on page 2.



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 Roxio Secure Burn Enterprise

- Type the following command:
`"C:\ProgramData\Uninstall\{D593D658-FF81-4069-9A69-D9F6B17BD6A2}\setup.exe" /X {D593D658-FF81-4069-9A69-D9F6B17BD6A2} /qn REBOOT=ReallySuppress`

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 ROX_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 = "Roxio Secure Burn Enterprise"

; 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 /ROX_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 = Roxio

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.



Roxio Secure Burn Enterprise 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\Roxio\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 **Options** dialog box.
- **1** (default value) — By default discs are finalized, and the user cannot change this setting in the **Options** dialog box.



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

Enabling logging

Depending on your version of Roxio Secure Burn Enterprise, 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\Roxio\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 Permissions Manager.

Changing the log file location

You can change where the log is stored with the “LogPath” registry key in `HKEY_CURRENT_USER\SOFTWARE\Roxio\Basic Burn\Preference`

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

Setting password strength

Depending on your version of Roxio Secure Burn Enterprise, you may have the ability to configure the password strength in the registry.

There are five configuration parameters available:

Parameter	Description	Location
PasswordLength	Password length must be greater than or equal to the value you set (256 max.). The default value is 8.	<code>HKEY_CURRENT_USER\SOFTWARE\Roxio\Basic Burn\Preference\Password Length</code>
LowerCaseNum	Password must contain lower case letters. The default value is 1.	<code>HKEY_CURRENT_USER\SOFTWARE\Roxio\Basic Burn\Preference\LowerCaseNum</code>
UpperCaseNum	Password must contain upper case letters. The default value is 1.	<code>HKEY_CURRENT_USER\SOFTWARE\Roxio\Basic Burn\Preference\UpperCaseNum</code>

Parameter	Description	Location
NumeralCharNum	Password must contain numbers (digits). The default value is 1.	HKEY_CURRENT_USER\SOFTWARE\Roxio\Basic Burn\Preference\Numeral CharNum
SpecialCharNum	Password must contain symbols or punctuation. The default value is 1.	HKEY_CURRENT_USER\SOFTWARE\Roxio\Basic Burn\Preference\SpecialCharNum



The password condition is met when the user meets (=) or exceeds (>) the value set for the relevant parameter.

Setting default password

Depending on your version of Roxio Secure Burn Enterprise, 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\Roxio\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 **Roxio Secure Burn Enterprise**.
- 2 Click the **Options** button to display the **Options** dialog box.
- 3 In the **Options** 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 Roxio Secure Burn Enterprise.

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

Using the Permissions Manager

In Roxio Secure Burn Enterprise, the Permissions Manager enables the system administrator to create and modify user groups. By choosing settings in the Permissions Manager, the system administrator can limit disc and USB reading and writing capabilities both within and outside those groups.

Creating and managing group keys

Each user account with Roxio Secure Burn Enterprise is 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 Permissions 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, Roxio Secure Burn Enterprise features will be disabled, and passwords will be required for reading and writing encrypted discs.

Setting passwords

Depending on your version of Roxio Secure Burn Enterprise, you may have the ability to allow users to add a personal password to the discs they burn. Discs with passwords can be read by anyone who knows the password.

You can also set a default password.

Enabling logging

Depending on your version of Roxio Secure Burn Enterprise, you may have the ability to allow the application to report the event logs. When logging is enabled, Roxio Secure Burn Enterprise will report the disc operation events to the system event log. Logging is enabled by default.

Set up a group and master password

Group members can use the master password to access encrypted data.

Device access control setting

The following device control settings can be applied:

- **Read permission:** Marked (check mark in box) by default. When unmarked (no check mark), Roxio Secure Burn Enterprise and other third-party software can't read the disc or USB.
- **Write permission:** When unmarked (no check mark), Roxio Secure Burn Enterprise and other third-party software can't write to the disc or USB.
- **Write with Roxio Secure Burn only:** Unmarked (no check mark) by default. When marked (check mark in box), Roxio Secure Burn can read and write to disc or USB; third-party software can read only.

- **Access only the data encrypted with Roxio Secure Burn:** When marked, only the disc or USB data encrypted with Roxio Secure Burn can be read.

Burning non-encrypted discs

Depending on your version of Roxio Secure Burn Enterprise, you may have the ability to enable and disable burning of non-encrypted discs. This allows the user to burn the disc without encryption, so that the disc can be read outside of the groups. This setting is disabled by default.

Exporting and importing settings

The **Permissions Manager** allows you to import and export settings from one machine to another. 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 could then export those settings to a .grp file and import them into another computer or another user account.

Deploying permissions configurations

- Use **Export grp** or **Export Reg** to export the settings. Use **Import** to import the .grp file and enter the **WorkGroupID** of the original user. You can then apply the settings to another user account. For the .reg file, simply run the file with another user account on the same machine or a different machine to apply the settings.
- Copy the Permissions Manager application file. It is not necessary to install Permissions Manager on each computer. The Permissions Manager application file is password-protected. It is stored in the following directory: **C:\Users\{User}\AppData\Roaming\Roxio\Roxio Burn\PermissionManager\RBPermission.grp**.
- Set the GRP decoder key. The GRP file is encoded with a string (WorkGroupID) in **HKEY_CURRENT_USER\SOFTWARE\Roxio\Basic Burn\Preference\WorkGroupID**

You can copy the value from the original WorkGroupID on the machine that generated the GRP file, then run the following command on the target machine:

```
GenWorkGroupID.exe <original WorkGroupID> <path of  
RBPermission.grp>
```

This command generates a new WorkGroupID on the target machine based on the original WorkGroupID and the user information on the target machine. The new WorkGroupID is only valid for the current user of the target machine. This means that even if someone copied the GRP file to another machine or even if other users share the same machine, they can't read Roxio Secure Burn data.



GenWorkGroupID.exe is a standalone executable file can be found in **C:\Program Files(x86)\Roxio\Roxio Burn Administration** or **C:\Program Files(x86)\Roxio\Roxio Burn**.

More useful information about the Permissions Manager

- 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.
- Remember to run the **Permissions Manager** as the system administrator.

To launch the Permissions Manager

- Do one of the following:
 - Double-click the **Roxio Permission Manager** shortcut on the desktop.
 - Double-click **Permissions Manager.exe** in **C:\Program Files(x86)\Roxio\Roxio Burn Administration**.

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 Click **Apply** to confirm the change and leave the **Permissions Manager** open, or click **OK** to confirm the change and close the **Permissions 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.

To set read and write permissions by machine

- 1 In the **By machine** area, choose from the following settings:
 - Enable the **Read permission** check box to make discs or USBs readable (including by third-party software). To limit the read permission to data encrypted by Roxio Secure Burn, enable the **Access only the data encrypted with Roxio Secure Burn**.
 - Enable the **Write permission** check box to permit disc and USB authoring/writing and reading (including by third-party software). To limit permission to Roxio Secure Burn only (no third-party software), enable the **Write with Roxio Secure Burn only**.
- 2 Click **Apply** to confirm the change and leave the **Permissions Manager** open, or click **OK** to confirm the change, close the

Permissions Manager, and restart the computer to apply the settings.



Permission settings can be set at the **By machine** and **By user account** level.

Permission settings can be exported as an REG file and imported to other machines.

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. Roxio Secure Burn Enterprise 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**.

To enable a personal password

- In the **Permissions Manager**, enable the **Force Password Protection** check box.

To set a default password

- 1 Open the **Permissions Manager** on the computer where you wish to set a default password.

- 2 Click **Always use this password**.
- 3 If the button is disabled, the application may not support the use of a default password.
- 4 The password input dialog box appears.
- 5 Enter a password.
- 6 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.
- 7 Click **Apply**. The changes are applied the next time you restart Roxio Secure Burn Enterprise.



Be sure to write down your password and store it in a safe place. Roxio Secure Burn Enterprise is not able to retrieve lost passwords.

To enable logging

- In the **Permissions Manager**, enable the **Enable logging** check box.

To enable burning of non-encrypted discs

In the **Permissions Manager**, enable the **Burn non-encrypted discs** check box.

To export settings

- 1 Open the **Permissions Manager** on the computer with the settings that you wish to export.
- 2 Choose one of the following:
 - In the **By user account** area, click the **Export grp** or **Export Reg** button to export the settings for the user account

- In the **By machine** area, click the **Export REG** button to export the settings for the device.

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.



You can export group settings by clicking **Export GRP** or **Export REG**, but the membership settings between groups will not be exported to the reg file. 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

- 1 Open the **Permissions Manager** on the target computer.
- 2 Click **Import**.
- 3 In the **Open** dialog box, navigate to the settings file.
- 4 Click **Open**.

The settings are imported and displayed in the **Permissions Manager**.

- 5 Make any necessary adjustments.
- 6 Click **Apply** to confirm the change and leave the **Permissions Manager** open, or click **OK** to confirm the change and close the **Permissions Manager**.

System requirements

Roxio Secure Burn Enterprise has the following minimum system requirements:

- Microsoft® Windows® 7, 8, 8.1, 10 Ultimate, Professional, or Enterprise; 32-bit or 64-bit with latest service pack
Important: For Windows 7, security update 3033929 must be installed to avoid an operating system boot issue. For more information, visit <https://support.microsoft.com/en-us/kb/3033929>.
- Hard drive with at least 150 MB free space for the installation process
- Windows Media Player version 10, 11, or 12
- Internet Explorer 7, 8, 9, 10, or 11



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 Roxio, please use the following contact information.

North America

- E-mail address: vlp@roxio.com
- Web: <http://www.roxio.com/enz/company/vlp>

Europe / Middle East / Africa

- E-mail address: vlp.emea@roxio.com

- Phone Number: +44 1628 677 620
- Hours of operation: 8 a.m. to 6 p.m. GMT

Japan

- E-mail address: vlpsales@roxio.jp

Oceania

- E-mail address: vlp.oceania@roxio.com

Copyright © 2016 Corel Corporation. All rights reserved.
Roxio® Secure Burn™ Enterprise Deployment Guide

INFORMATION IS PROVIDED BY COREL ON AN “AS IS” BASIS, WITHOUT ANY OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THOSE ARISING BY LAW, STATUTE, USAGE OF TRADE, COURSE OF DEALING OR OTHERWISE. THE ENTIRE RISK AS TO THE RESULTS OF THE INFORMATION PROVIDED OR ITS USE IS ASSUMED BY YOU. COREL SHALL HAVE NO LIABILITY TO YOU OR ANY OTHER PERSON OR ENTITY FOR ANY INDIRECT, INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, BUT NOT LIMITED TO, LOSS OF REVENUE OR PROFIT, LOST OR DAMAGED DATA OR OTHER COMMERCIAL OR ECONOMIC LOSS, EVEN IF COREL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR THEY ARE FORESEEABLE. COREL IS ALSO NOT LIABLE FOR ANY CLAIMS MADE BY ANY THIRD PARTY. COREL’S MAXIMUM AGGREGATE LIABILITY TO YOU SHALL NOT EXCEED THE COSTS PAID BY YOU TO PURCHASE THE MATERIALS. SOME STATES/COUNTRIES DO NOT ALLOW EXCLUSIONS OR LIMITATIONS OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Corel, the Corel logo, Roxio and Secure Burn are trademarks or registered trademarks of Corel Corporation and/or its subsidiaries in Canada, the United States and elsewhere. WinZip is a registered trademark of VAPC (Lux) S.a.r.l. All other product names and any registered or unregistered trademarks mentioned are used for identification purposes only and remain the exclusive property of their respective owners.

Product specifications, pricing, packaging, technical support and information (“specifications”) refer to the retail English version only. The specifications for all other versions (including other language versions) may vary.