TrusCont
Trusted Content Delivery

TrusCont Ltd | 31 Weizman Street, Qiriat Bialik 2701212, Israel | Tel: +972 4 832 0555 Fax: +972 4 832 0550

TrusCont™

TSFD Protection Toolkit

Version 6.0

User's Manual

October 2018

Table of Contents

Table of Figures

1. Introduction

Thank you for choosing TrusCont security solutions.

TrusCont offers the most comprehensive and versatile copy protection solutions for both software and data files. Our products can protect more than 300 different file types by default and also include advanced features for protecting almost anything else including proprietary file formats and applications. The copy protection can be applied to optical discs (CD/DVD/BD), USB flash drives, and also downloadable content.

This manual focuses on the TrusCont TSFD Protection Toolkit software which is used to copy protect software and data on USB Flash Drives.

1.1 Key Features

- Powerful hardware based copy protection
- Copy protection for Windows applications, including both native code (win32) and Managed code applications.
- Copy protection for data files such documents, pictures, music files, and video clips.
- Copy protection for proprietary file formats and applications
- Protect files of any size
- Doesn't degrade performance or quality of the protected data allowing publishers to protect even the highest HD quality video without compromising performance and quality.
- Generically blocks screen capture / grabbing / streaming.
- Protected files open naturally in common applications such as Adobe Reader, Windows Media Player, VLC, Firefox, Chrome, Internet Explorer, and others.
- Preserves the original functionality of the protected data, including interlinks among protected files.
- Printing and Copy & paste control.
- Time limits – make your files expire at a specific date, and/or after a specific number of days since it is first used.
- Limit use of the protected files to specific number of computers, or users.
- Limit use of the protected files to a specific network domain.
- Password protection.

- Write protect the flash drive to prevent accidental deletion, modification, and even infection by viruses and malware.
- Easy to use duplication software – TrusCont TSFD Protection Toolkit.
- Mass production solutions available.

1.2 Applicable USB Flash Drives

TrusCont USB Copy Protection requires compatible USB Flash Drives. The TSFD Protection Toolkit enables publishers to apply the copy protection on 3rd party USB flash drives. However, it is highly recommended to use TrusCont Secure Flash Drives which offer the highest compatibility, copy protection level, and stability.

Publishers that prefer to use 3rd party USB Flash Drives should consider the following:

- Most 3rd Party USB Flash Drives may not be compatible with TrusCont USB Copy Protection. TrusCont doesn't provide a list of compatible brands / models since manufacturers of branded products change components very often sometimes even between 2 production runs of the same model.
- TrusCont TSFD Protection Toolkit includes an option to test a flash drive for compatibility. This test checks whether the software can recognize the components used in the USB Flash Drive. This feature is provided as a mean for testing potential compatibility. There is no guaranty that a flash drive reported as compatible will be usable with the software without actually trying to apply the copy protection on it. If you intend to use 3rd party flash drives then please refer to *Appendix B – Testing a Flash Drive for Compatibility* for further details.

1.3 What's New in Version 6.0

Version 6.0 includes many enhancements and fixes. This is a shortlist of the main changes:

- **Anti-Screen capture:** TrusCont is the only protection system that generically blocks screen grabbing, recording, and streaming attempts while the secured data is displayed. TrusCont doesn't use blacklisting approach and therefore is not limited to blocking only known applications. TrusCont effectively and generically blocks screen recording programs, remote desktop applications, and even Trojan horses!
- **Support for more than 300 different file types:** TrusCont continuously expand support for additional file formats. In V6.0 we added support for additional Microsoft Office file formats such as PowerPoint Show (PPSX) and many other file formats. TrusCont products can protect more than 300 different file formats and also include features for protecting almost anything else.
- **Enhanced software protection level:** Added an option for protecting program files using 'Enhanced' protection level. The Enhanced protection level applies extra anti-hacking features in order to aggressively resist anti-reverse engineering.
- **Re-plug after format:** An option to instruct the TSFD Protection Toolkit to request a re-plug of the USB flash drive after formatting. Increases compatibility to USB flash drives that cannot be reset via software.
- **Improved compatibility to 3rd party USB Flash Drives:** Added support for additional UFD technologies used in some retail USB Flash Drives. It is still highly recommended to use TrusCont Secure Flash Drives whenever possible.

2. End User Experience

TrusCont copy protection is incredibly transparent and friendly to the end user. As long as the end user uses a legitimate and valid copy of the protected data, your data will function exactly the same as its unprotected origin.

TrusCont may affect the functionality of your content in the following cases:

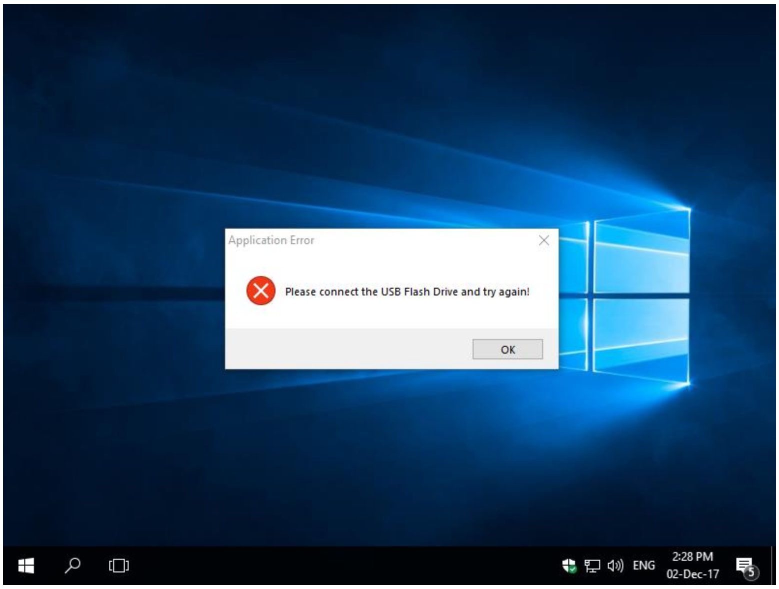
- An end user attempt to access an illegal copy of your files
- An end user attempt to access expired content
- An attempt to perform a restricted operation (e.g. printing, copy & paste)
- An attempt to access a resource requiring a password or an activation key

The affect on functionality depends on your content type and the copy protection settings that you apply to it.

2.1 Software Protection

A program file protected by TrusCont will run and function normally exactly as its unprotected origin as long as the USB Flash Drive on which it was originally recorded is connected to the local PC.

If the original USB Flash Drive is not connected then the protected program file will not run. Instead, a message requesting the end user to connect the original USB disk will be displayed. This message can be customized (*4.3.2 Program Files Protection Settings*).



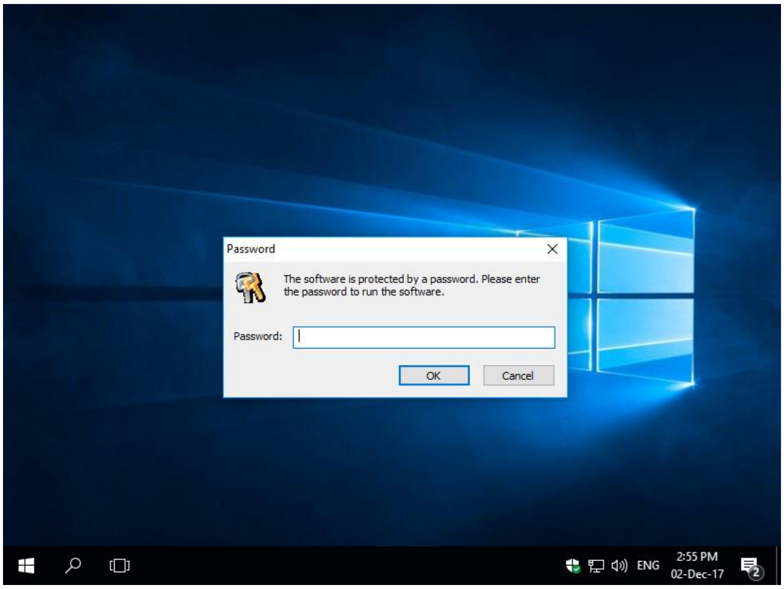
Application Error

Please connect the USB Flash Drive and try again!

Figure 1: Running a Protected Application without the Original USB Flash Drive

Password protection

Optionally, program files can be protected with a password. If a password is set, the copy protection system will also ask the end user for a password before allowing the protected file to run. If the password is correct the application will run. Otherwise an error message will appear. A USB Flash Drive can contain multiple protected files. Each file may be protected with a different password.



The software is protected by a password. Please enter the password to run the software.

Figure 2: Protecting Program Files with a Password

Expiration Dates & Time Limits

Use of protected files can also be limited by setting expiration dates and/or time limits. Trying to run a protected file after the expiration date will display an error message indicating the file has expired. A USB Flash Drive may contain multiple protected files. Each file may have a different expiration date and time limit settings.

Limit use to specific number of computers, users, or a domain

You can restrict the use of the USB Flash Drive to a predetermined number of computers / users, or a network domain. The copy protection automatically allows the computers / users / network domain on which the protected files are first used (refer to section *4.4.6 Restricted Use Mode* for further details). If the predetermined number of computers / users / domain has exceeded then the protected software will not run. Instead, a message will be displayed indicating the software cannot run under the current environment.

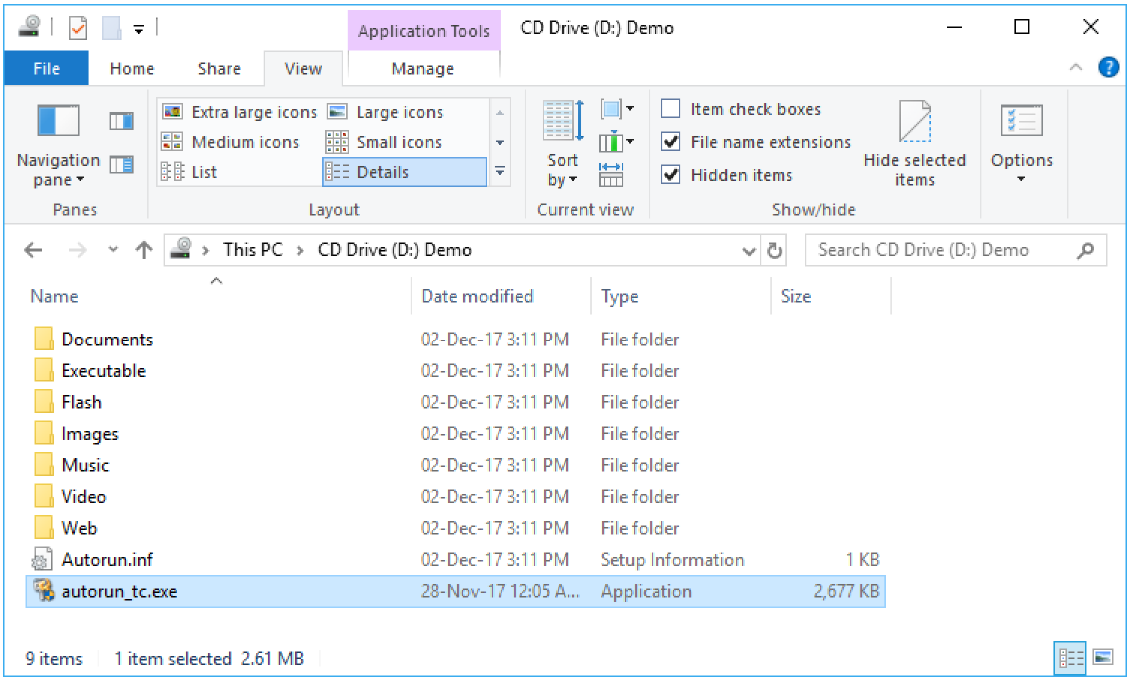
2.2 Data Files Protection

2.2.1 The TrusCont Autorun File

TrusCont data protection is one of a kind. It doesn't degrade your product's performance or quality and it allows protected files to be opened normally in common applications such as media players and internet browsers. With TrusCont you can protect almost any data file of any size. TrusCont fully preserves the functionality of your files, including interlinks among files.

When protecting data files, the TSFD Protection Toolkit automatically adds a small Autorun file to your USB Flash Drive. The default name of the TrusCont Autorun file is "autorun_tc.exe" (customizable). This file loads the TrusCont security software modules that allow 3rd party applications to read the protected data files transparently, and at the same time prevents the data from being saved, copied, printed, or otherwise exported to another medium unless specifically allowed in advance.

The TrusCont Autorun file doesn't affect the original Autorun functionality of your product. If your product already contains an autorun.inf file, then the TrusCont Autorun will automatically run your original Autorun file after it loads.



Name	Date modified	Type	Size
Documents	02-Dec-17 3:11 PM	File folder	
Executable	02-Dec-17 3:11 PM	File folder	
Flash	02-Dec-17 3:11 PM	File folder	
Images	02-Dec-17 3:11 PM	File folder	
Music	02-Dec-17 3:11 PM	File folder	
Video	02-Dec-17 3:11 PM	File folder	
Web	02-Dec-17 3:11 PM	File folder	
Autorun.inf	02-Dec-17 3:11 PM	Setup Information	1 KB
autorun_tc.exe	28-Nov-17 12:05 A...	Application	2,677 KB

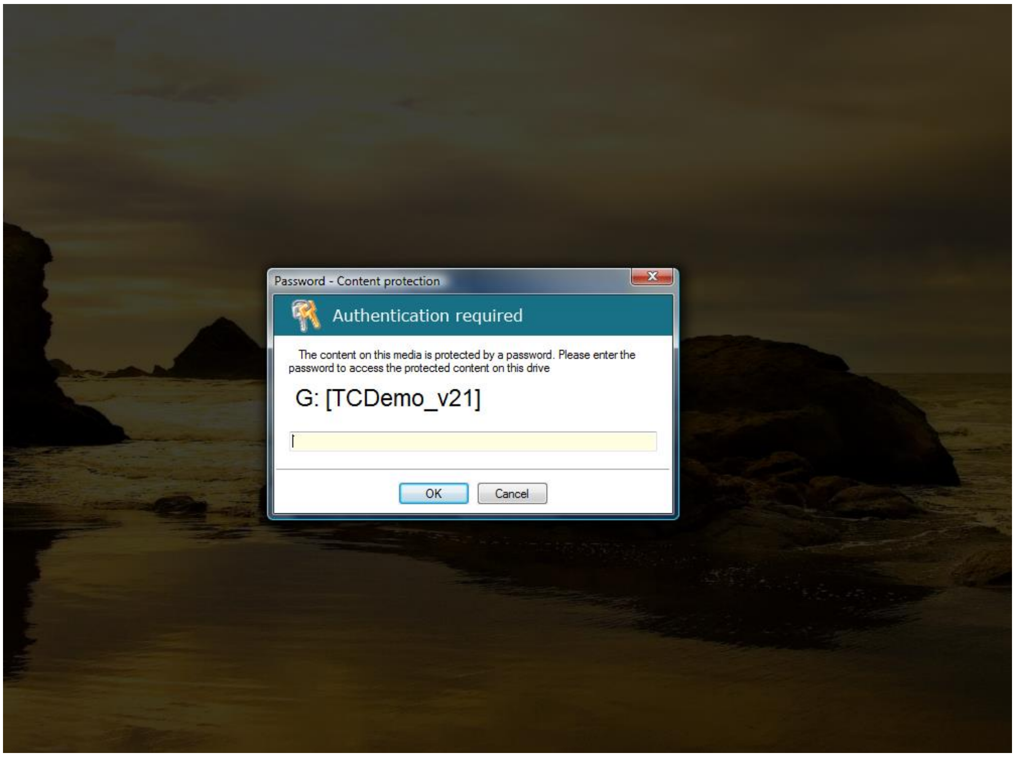
9 items 1 item selected 2.61 MB

Figure 3: The TrusCont Autorun File

When the TrusCont Autorun file loads it looks for the original USB Flash Drive on which your protected data files were recorded. If the original USB Flash Drive is connected to the computer it grants access to the protected files. Otherwise, it displays an error message and access to the protected files is denied.

TrusCont also enables you to protect your files with a Global Password. If such a password is set the TrusCont Autorun will ask the end user to enter the password every time it loads before grating access to the protected files and running the original Autorun file you may have on your product.

Global passwords secure only protected data files. If the end user enters the correct password, access is granted to all the files stored on the USB Flash Drive. Otherwise, access to the protected data files is denied. However, access to protected program files, and other unprotected files that may be stored on the same USB Flash Drive is not affected.



The content on this media is protected by a password. Please enter the password to access the protected content on this drive

G: [TCDemo_v21]

Figure 4: Global Password Dialog

2.2.2 Accessing Protected Data Files

Once the TrusCont Autorun is loaded, the protected data files can be viewed / played normally exactly the same as their unprotected versions. TrusCont allows the protected files to be accessed by the following applications:

- Applications included in the default list of applications certified by TrusCont (*4.4.7.2 Default List of Allowed Applications*)
- Other applications, including proprietary applications that are specifically added to the list of allowed applications* (*Appendix A – Customizing 3rd Party Applications Support for Content Protection*).
- Any other applications (EXE files) stored on the same USB Flash Drives*.

*** Warning: Publishers that customize the list of allowed applications (whether explicitly or by storing the applications on the same USB Flash Drive) should test their publications in order to make sure that the additional applications can properly read the protected files and function as expected. TrusCont cannot guaranty that applications not included in the default application list will be able to properly read protected files.**

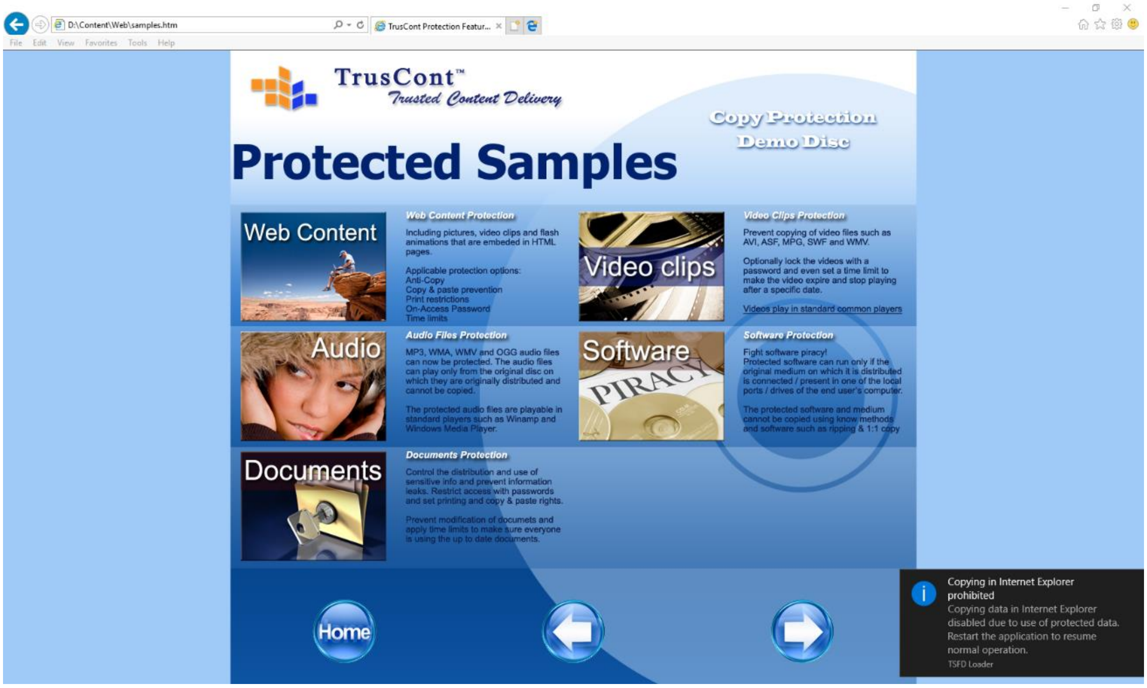
Whenever a user or an application tries to access a protected data file, TrusCont performs several additional checks before finally granting access to the specific file:

- Check that the file hasn't expired – in case an expiration date and/or a time limit were set on the specific file.
- Check if the specific file is protected by a password and if so prompt the user to enter the password.
- Check that the current logged in user can access the file, and that the file is allowed to be opened on the specific PC and/or network domain (in case user/computer/domain restrictions were set on the USB Flash Drive).
- Check that the application in which the file is being opened is allowed to access the file.

TrusCont guards the content of protected files by restricting the functionality of the reading applications. For example, an application that accesses a protected file on which a print restriction is set, will not be allowed to perform any print operations. Restrictions on an application are set only when it actually accesses a protected file and remain in effect until the application is closed.

TrusCont applies the restrictions to the entire application. For example, if an application accesses a file on which a print restriction is set, and at the same time the application accesses a second file on which printing is allowed, then the application will not be allowed to print also the second file, even if the second file is not protected at all.

When an end user tries to perform an operation that an application is restricted from performing (e.g. printing, or copy & paste), a tray icon notification appears that notifies the end user the operation he tries to perform is prohibited.



Web Content Protection

Including pictures, video clips and flash animations that are embeded in HTML pages.

Applicable protection options:
Anti-Copy
Copy & paste prevention
Print restrictions
On-Access Password
Time limits

Video Clips Protection

Prevent copying of video files such as AVI, ASF, MPG, SWF and WMV.

Optionally lock the videos with a password and even set a time limit to make the video expire and stop playing after a specific date.

Videos play in standard common players

Audio Files Protection

MP3, WMA, WMV and OGG audio files can now be protected. The audio files can play only from the original disc on which they are originally distributed and cannot be copied.

The protected audio files are playable in standard players such as Winamp and Windows Media Player.

Software Protection

Fight software piracy!
Protected software can run only if the original medium on which it is distributed is connected / present in one of the local ports / drives of the end user's computer.

The protected software and medium cannot be copied using know methods and software such as ripping & 1:1 copy

Documents Protection

Control the distribution and use of sensitive info and prevent information leaks. Restrict access with passwords and set printing and copy & paste rights.

Prevent modification of documets and apply time limits to make sure everyone is using the up to date documents.

Copying in Internet Explorer prohibited
Copying data in Internet Explorer disabled due to use of protected data. Restart the application to resume normal operation.
TSFD Loader

Figure 5: Tray icon notification on prohibited operation

2.3 <u>Local Administrator Rights</u>

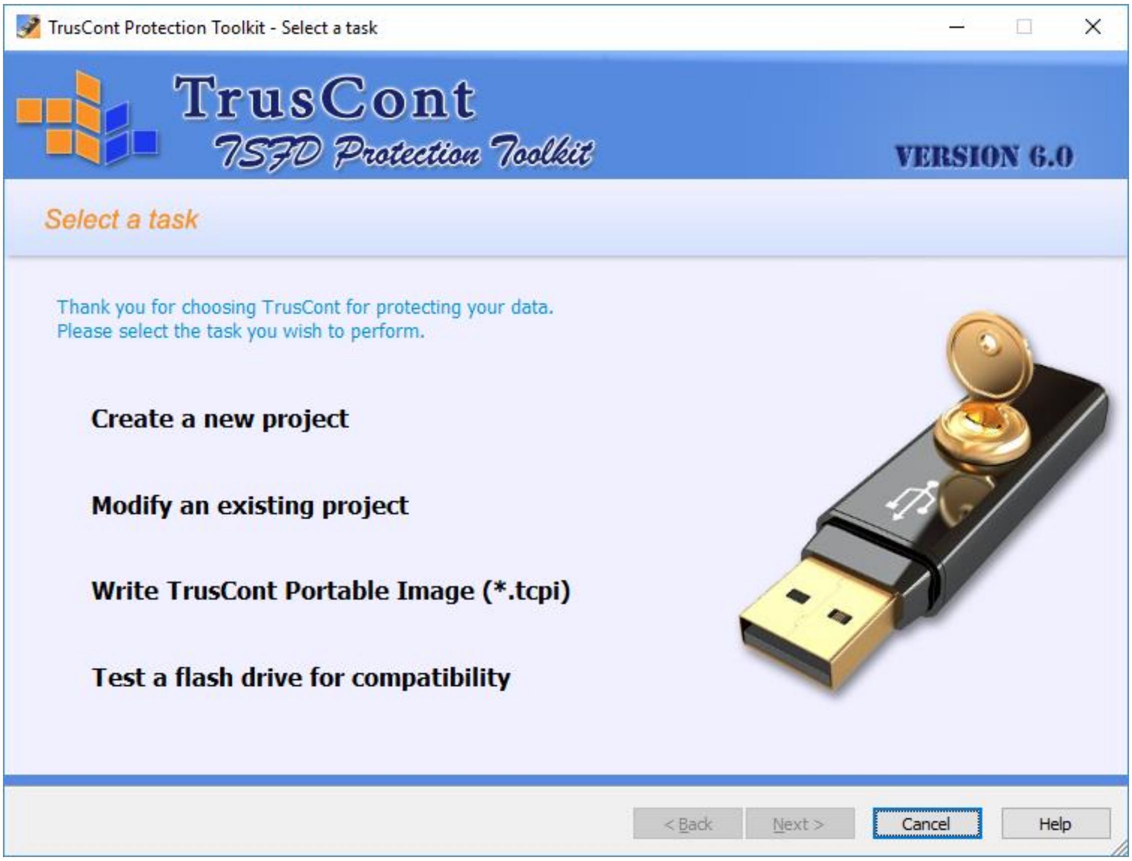
Running protected files requires local administrator rights. It is currently not possible to run files protected on TSFDs under restricted accounts.

<u>**Important note:**</u> by default all home users have local administrator rights. In some corporate environments users may have restricted accounts. TSFDs require the end users to have only local administrator rights, administrator rights for the network is not required.

3. Using TrusCont TSFD Protection Toolkit

Make sure you always use the latest version of the TSFD Protection Toolkit. The latest version of the TSFD Protection Toolkit is available for download as a single setup file on the TrusCont website (https://www.truscont.com). TrusCont website is the only official source for TrusCont software downloads.

To Install the TSFD Protection Toolkit on your PC double click the setup file and follow the instructions on the screen. Once installed, you may run the software by double clicking the shortcut on the desktop.



TrusCont Protection Toolkit - Select a task

Select a task

Thank you for choosing TrusCont for protecting your data.
Please select the task you wish to perform.

Create a new project

Modify an existing project

Write TrusCont Portable Image (*.tcpi)

Test a flash drive for compatibility

Figure 6: The main page of the TSFD Protection Toolkit

The TSFD Protection Toolkit is a wizard like software. The software tasks and settings are organized in a few consecutive pages that form a single path forward. To perform a task, select the desired task on the main page of the software, then complete the settings on each page and click next to move to the following page.

Description of the options on the main page of the software:

- Crate a new project – If this is the first time you use the TSFD Protection Toolkit then this is the place to start. Use this option to select which files you wish to include on your publication, set the required copy protection options, and finally save your project or duplicate it to your USB Flash Drives.
- Modify an existing project – open a project you saved earlier in order to modify it, or duplicate it on additional USB Flash Drives.
- Write s TrusCont Portable Image (*.tcpi) – a TrusCont Portable Image is a single file containing the entire files and settings of your project similar to an archive file. It cannot be changed after it is created and it is used for quickly mass producing your publications. Use this option to quickly write an image to a USB Flash Drive.
- Test a flash drive for compatibility – use this option to check if a USB Flash Drive is compatible with TrusCont USB Copy Protection (refer to *Appendix B – Testing a Flash Drive for Compatibility* for further instructions and important notes).

4. Creating a New Project

4.1 Content preparation checklist

To ensure proper creation of your project, please organize your content using the following guidelines:

☑ Organize files and folders collection – Create a new folder on your local PC and store all the files and folders you wish to publish in this folder (the 'Container' folder). Organize the files and folders structure exactly as you wish it will be stored on the USB Flash Drive.

☑ Do not use files that are already protected – Protected files from a previously protected USB Flash Drive cannot be used in new projects. Using protected files in new projects will result in USB Flash Drives containing unreadable or corrupted files.

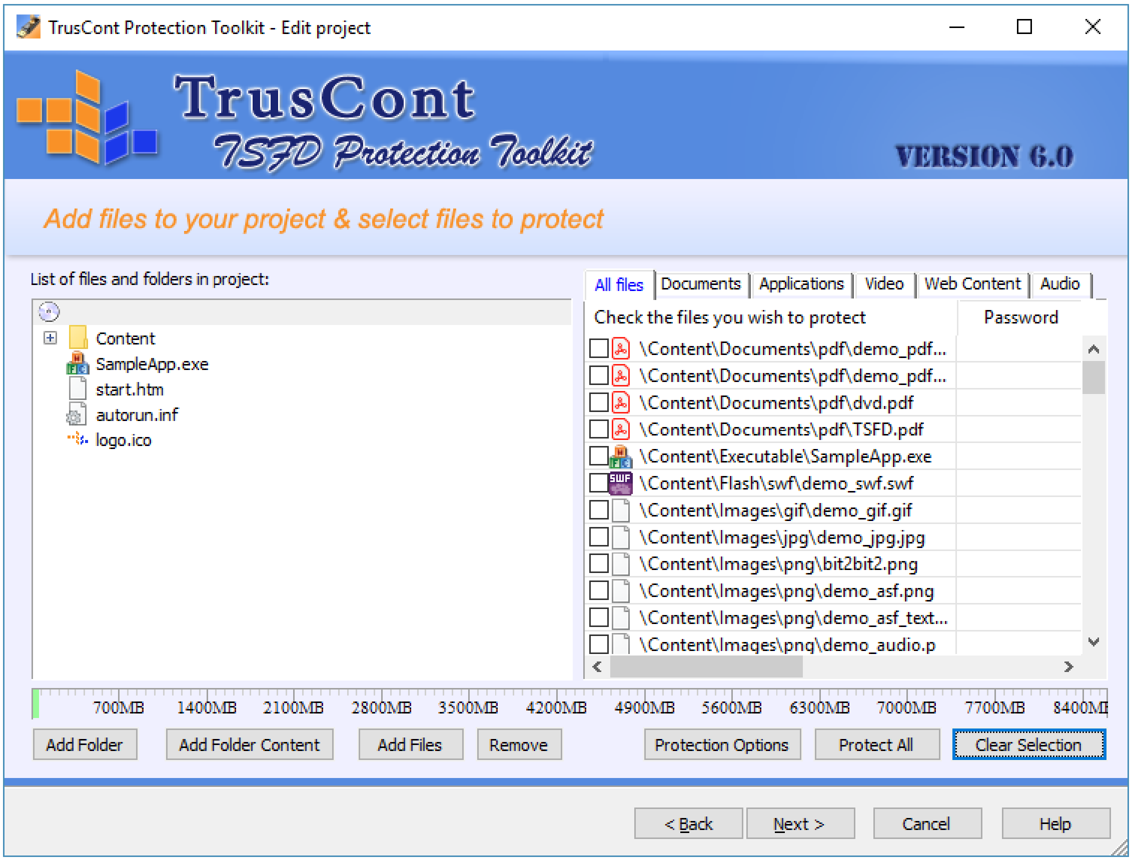
☑ Verify the functionality of your title – The TSFD protection process doesn't change the functionality of your files in any way. Verify that your title works as planned before using the Toolkit. If you plan to write protect your flash drives then make sure your data functions properly when stored on a read-only medium.

☑ Make sure your files are not being used – Make sure your project files are not open in any other software and remain unchanged through the project creation process.

☑ Archive your original files – TrusCont doesn't change your original source files. However, it is strongly recommended to archive the original unprotected files of all publications. TrusCont doesn't provide any tools for reversing the copy protection in case your original unprotected source files are lost.

4.2 Adding Files and Folders

The 'Edit Project' page has two main panels. The left panel is a tree view of all the files and folders that you add to your project. These are the files and folders that will eventually be recorded on your USB Flash Drives. The right panel contains a check list of the files on your project that can be protected, allowing you to choose which files you wish to protect and set the desired protection options.



Content
SampleApp.exe
start.htm
autorun.inf
logo.ico

□ \Content\Documents\pdf\demo_pdf...
□ \Content\Documents\pdf\demo_pdf...
□ \Content\Documents\pdf\dvd.pdf
□ \Content\Documents\pdf\TSFD.pdf
□ \Content\Executable\SampleApp.exe
□ \Content\Flash\swf\demo_swf.swf
□ \Content\Images\gif\demo_gif.gif
□ \Content\Images\jpg\demo_jpg.jpg
□ \Content\Images\png\bit2bit2.png
□ \Content\Images\png\demo_asf.png
□ \Content\Images\png\demo_asf_text...
□ \Content\Images\png\demo_audio.p

Figure 7: The Edit Project Page

The right panel allows you to filter the list of files by file type and location. For example, clicking the 'Video' tab will refresh the list and display only the video files on your project. To display only files located in a specific folder of your project, select the desired folder on the left panel.

4.2.1 Adding a Folder

First specify the location in which you wish to add the folder. To add a top level folder first select the disk icon on the left panel. Otherwise, select the existing folder to which you wish to add your new folder. Then click the 'Add Folder' button to open the folder selection window and select the folder you wish to add.

Note: Adding a folder also adds all the files and sub-folders included within it.

4.2.2 Adding Folder Content

To add to the project only the files and sub folders contained in a single folder without adding the containing folder itself use the 'Add Folder Content' button instead of the 'Add Folder' button. If you have followed the content preparation checklist on section *4.1 Content preparation checklist* then you can add all your files to the project at once by selecting the disk icon on the left panel, clicking the 'Add Folder Content' button, and then selecting your Container folder.

4.2.3 Adding Files

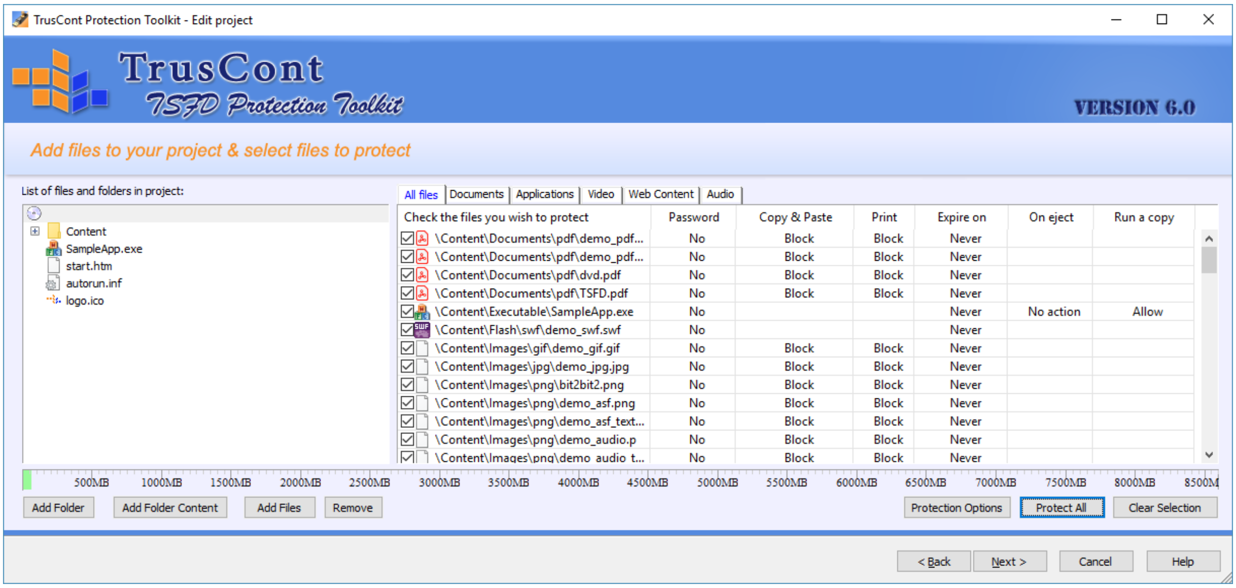
To add individual files to your project first select on the left panel the folder to which you wish to add the files, and then click the 'Add Files' button to open the files selection window. Select the files you wish to add and then click 'Open'.

4.2.4 Removing Files and Folders

To remove files or folders from the project, right click the item you wish to remove and then click 'Remove'. Alternatively, select the item on the left panel and click the 'Remove' button. Removing a folder removes also all the items within it.

4.3 Setting Copy Protection Options

4.3.1 Select the files you wish to protect



Check the files you wish to protect	Password	Copy & Paste	Print	Expire on	On eject	Run a copy
☑ \Content\Documents\pdf\demo_pdf...	No	Block	Block	Never		
☑ \Content\Documents\pdf\demo_pdf...	No	Block	Block	Never		
☑ \Content\Documents\pdf\dvd.pdf	No	Block	Block	Never		
☑ \Content\Documents\pdf\TSFD.pdf	No	Block	Block	Never		
☑ \Content\Executable\SampleApp.exe	No			Never	No action	Allow
☑ \Content\Flash\swf\demo_swf.swf	No			Never		
☑ \Content\Images\gif\demo_gif.gif	No	Block	Block	Never		
☑ \Content\Images\jpg\demo_jpg.jpg	No	Block	Block	Never		
☑ \Content\Images\png\bit2bit2.png	No	Block	Block	Never		
☑ \Content\Images\png\demo_asf.png	No	Block	Block	Never		
☑ \Content\Images\png\demo_asf_text...	No	Block	Block	Never		
☑ \Content\Images\png\demo_audio.p	No	Block	Block	Never		
☑ \Content\Images\png\demo_audio_t...	No	Block	Block	Never		

Figure 8: Setting copy protection options

Files added to the project are not protected by default. To protect a file you have to specifically check it on the right panel. You can check the files one by one, or click the 'Protect All' button in order to check all the files currently listed in the right panel.

Give some thought to your copy protection strategy before recording your content:

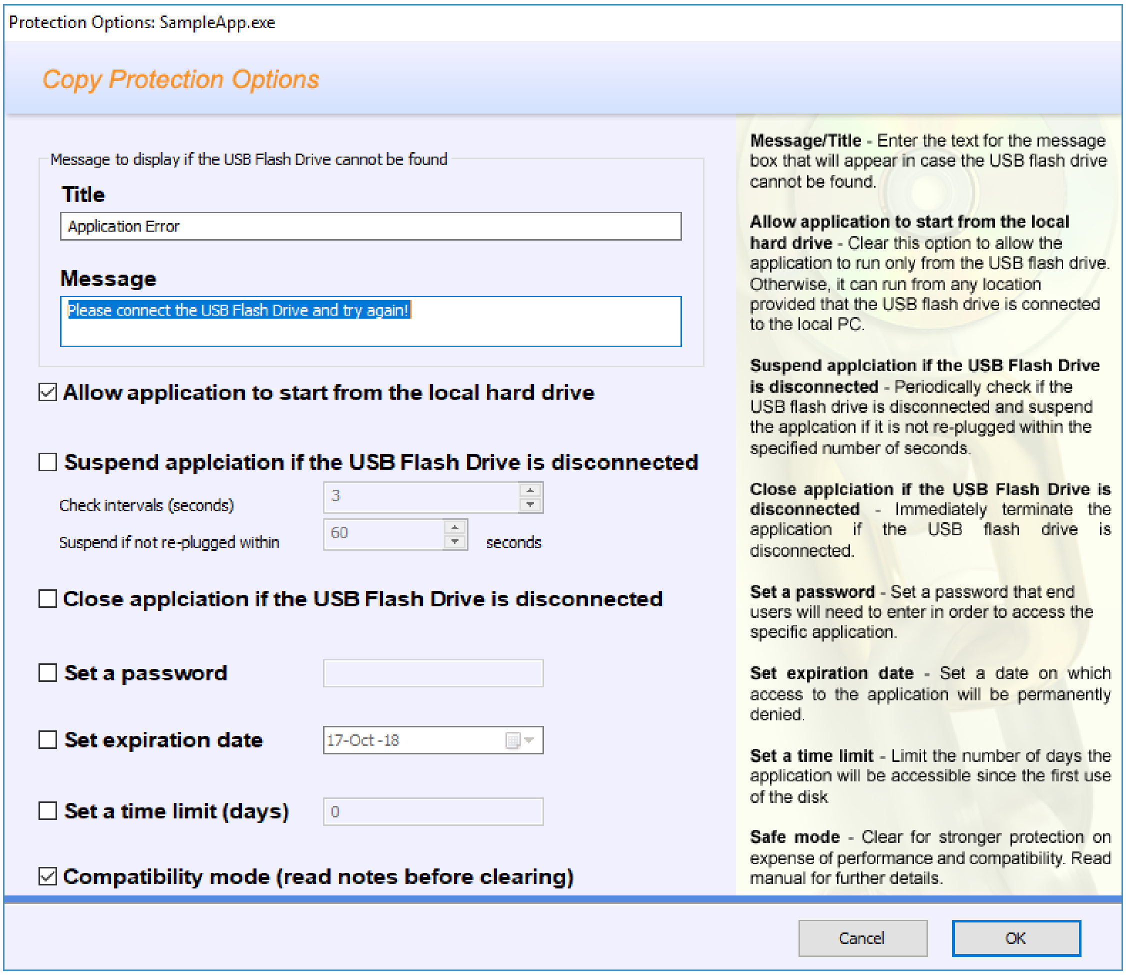
☑ Identify the most valuable files that require protection – When publishing software this may be the main program executable of your software. In training materials, service manuals, etc. this may be video files or documents.

☑ Protect only the valuable files that require protection – service files such as 3rd party applications, files without commercial value or files without sensitive content shall be left unprotected.

TrusCont USB Copy Protection can protect more than 300 different common file types. By default, only files of types included the default list of supported file types will be listed on the right panel. If you wish to protect other files that are not included in the default list, please refer to *Appendix C – Adding support for custom file types*

When checking a file on the right panel, TrusCont automatically applies to it the default copy protection settings based on its type. To change the default protection settings of a file double click its name on the table. To change the settings for multiple files click the 'Protection Options' button.

4.3.2 Program Files Protection Settings



Protection Options: SampleApp.exe

Copy Protection Options

Message to display if the USB Flash Drive cannot be found

Title: Application Error

Message: Please connect the USB Flash Drive and try again!

☑ Allow application to start from the local hard drive

☐ Suspend applciation if the USB Flash Drive is disconnected

Check intervals (seconds): 3

Suspend if not re-plugged within: 60 seconds

☐ Close applciation if the USB Flash Drive is disconnected

☐ Set a password

☐ Set expiration date: 17-Oct-18

☐ Set a time limit (days): 0

☑ Compatibility mode (read notes before clearing)

Message/Title - Enter the text for the message box that will appear in case the USB flash drive cannot be found.

Allow application to start from the local hard drive - Clear this option to allow the application to run only from the USB flash drive. Otherwise, it can run from any location provided that the USB flash drive is connected to the local PC.

Suspend applciation if the USB Flash Drive is disconnected - Periodically check if the USB flash drive is disconnected and suspend the applcation if it is not re-plugged within the specified number of seconds.

Close applciation if the USB Flash Drive is disconnected - Immediately terminate the application if the USB flash drive is disconnected.

Set a password - Set a password that end users will need to enter in order to access the specific application.

Set expiration date - Set a date on which access to the application will be permanently denied.

Set a time limit - Limit the number of days the application will be accessible since the first use of the disk

Safe mode - Clear for stronger protection on expense of performance and compatibility. Read manual for further details.

Figure 9: Copy protection options for program files

> **Note:** Some program files may be digitally signed. In order to protect the files TrusCont needs to change their data, which invalidates the digital signature. Current version of this software doesn't provide the means to digitally sign a file after it is protected. For further assistance on digitally signing files after protecting it please contact TrusCont technical support.

Setting	**Title / Message**
Description	Title and message text for the error message that will be displayed to the end user when attempting to run the protected program file without the USB Flash Drive
Default	Title: Application Error Message: Please connect the USB Flash Drive and try again!

Setting	**Allow application to start from the local hard drive**
Description	Allows the application to be installed/copied to the local hard drive (or any other medium). The original USB Flash Drive must be connected to the local PC in order to run the file. If this option is turned off, the end user can run the protected file only from the USB Flash Drive itself.
Default	Enabled (allowed)

Setting	**Suspend application if the USB Flash Drive is disconnected**
Description	Periodically checks if the USB Flash Drive is disconnected while the protected application is running. If the USB Flash Drive is not re-plugged within the specified number of seconds the application is suspended and a message asking the end user to connect the USB Flash Drive is displayed
Default	Disabled

Setting	**Close application if the USB Flash Drive is disconnected**
Description	Immediately close the protected application if the USB Flash Drive is disconnected.
Default	Disabled

Setting	**Set a password**
Description	Set a password that the end user will have to enter every time he runs the protected application. **Note:** The password cannot start or end with spaces. Spaces at the beginning and end of the password are automatically truncated.
Default	No password

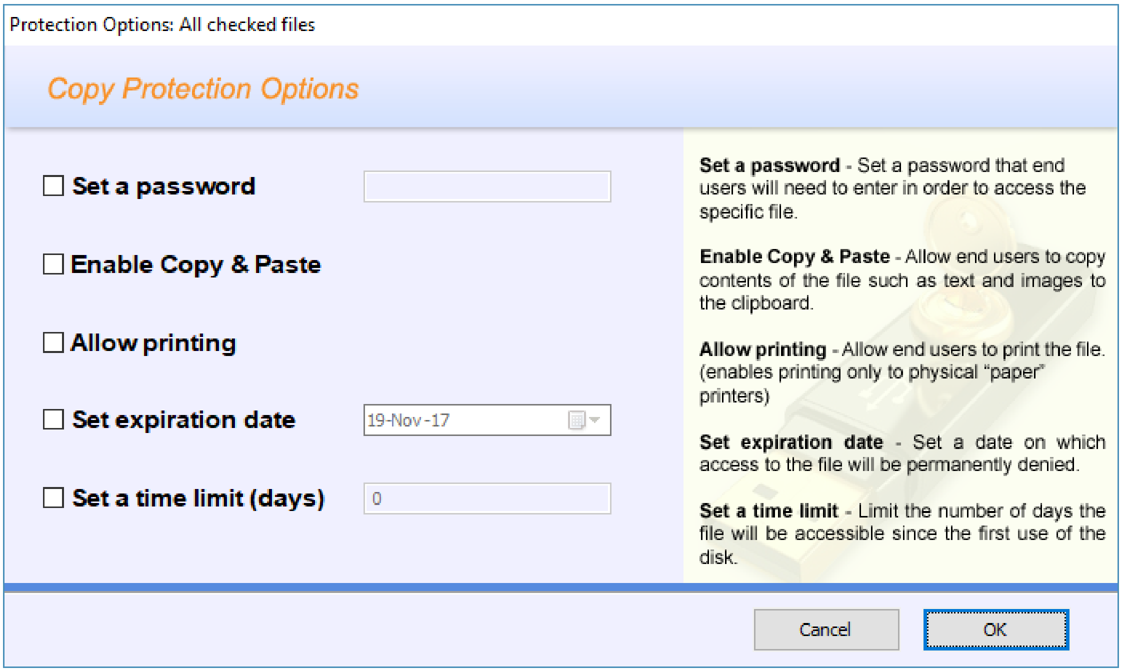
Setting	**Set expiration date**
Description	Make the protected application automatically expire at a specific date. Trying to run the application at a later date will display an error message indicating the file has expired.
Default	Never expire

Setting	**Set a time limit (days)**
Description	Set the number of days for which the protected application will be useable. The number of days are counted from the date in which any one of the protected files on the USB Flash Drive was first used. If the specified number of days have passed the application will not run and an error message will be displayed indicating the file has expired
Default	Unlimited

Setting	**Compatibility mode**
Description	Clear this option to apply enhanced and aggressive reverse engineering countermeasures on expense of performance. The enhanced protection level may not be compatible with program files that are used as child process and/or utilize inter-process communication techniques. The compatibility protection level is suitable for most publishers. It is the recommended protection level and therefore is enabled by default.
Default	Enabled

Note: By default the expiration date and time limit are tested against the end user's system clock and also an external time server if an internet connection is available. It is also possible to force the copy protection to use only an external time server. This results in a much stronger time limit but requires the end user to have an internet connection in order to run the protected file. Please refer to section *4.4 Project options* for further instructions on enabling this option.

4.3.3 Data Files Protection Settings



Protection Options: All checked files

Copy Protection Options

□ Set a password

□ Enable Copy & Paste

□ Allow printing

□ Set expiration date 19-Nov-17

□ Set a time limit (days) 0

Set a password - Set a password that end users will need to enter in order to access the specific file.

Enable Copy & Paste - Allow end users to copy contents of the file such as text and images to the clipboard.

Allow printing - Allow end users to print the file. (enables printing only to physical "paper" printers)

Set expiration date - Set a date on which access to the file will be permanently denied.

Set a time limit - Limit the number of days the file will be accessible since the first use of the disk.

Figure 10: Data files protection options

Note: Enable 'Copy & Paste', and 'Allow Printing' options are valid only for images and textual file formats. For all other file formats such as video and audio files these options are hidden.

Setting	**Set a password**
Description	Set a password that the end user will have to enter every time he opens the protected file. **Note:** The password cannot start or end with spaces. Spaces at the beginning and end of the password are automatically truncated.
Default	No password

Setting	**Enable Copy & Paste**
Description	Allow end users to copy contents of the protected file such as text and images to the clipboard.
Default	Disabled (Copying prohibited)

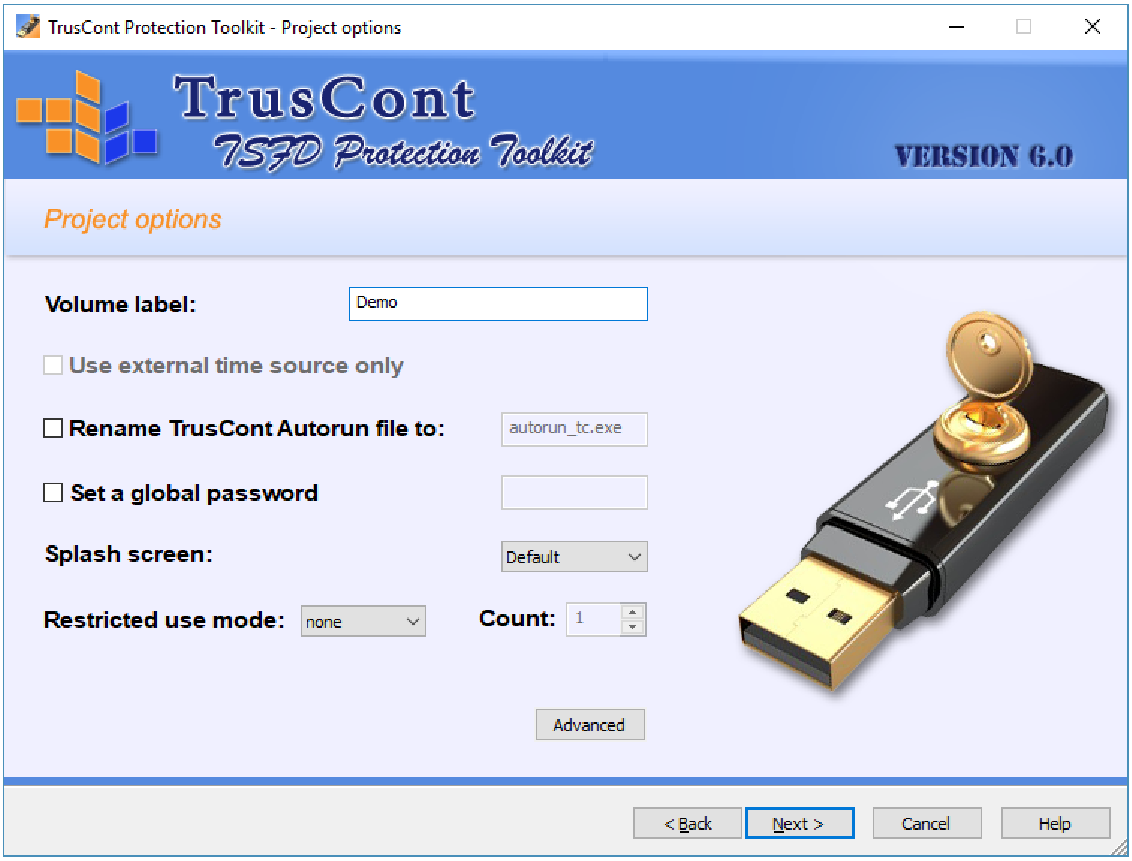
Setting	**Allow printing**
Description	Allow end users to print the protected file. Printing to virtual printers (print to file) is always disabled.
Default	Disabled (Printing prohibited)

Setting	**Set expiration date**
Description	Make the protected file automatically expire at a specific date. Trying to open the file at a later date will display an error message indicating the file has expired.
Default	Never expire

Setting	**Set a time limit (days)**
Description	Set the number of days for which the protected file will be valid. The number of days are counted from the date in which any one of the protected files on the USB Flash Drive was first used. If the specified number of days have passed the file will not open and an error message will be displayed indicating the file has expired
Default	Unlimited

Note: By default the expiration date and time limit are tested against the end user's system clock and also an external time server if an internet connection is available. It is also possible to force the copy protection to use only an external time server. This results in a much stronger time limit but requires the end user to have an internet connection in order to open the protected file. Please refer to section *4.4 Project options* for further instructions on enabling this option.

4.4 Project options



Volume label: Demo

□ Use external time source only

□ Rename TrusCont Autorun file to: autorun_tc.exe

□ Set a global password

Splash screen: Default

Restricted use mode: none

Count: 1

Figure 11: The Project Options Page

4.4.1 Volume Label

The volume label is the caption that is usually displayed next to the drive letter in windows file explorer. It helps end users to locate and identify your published USB Flash Drive among other drives that exist on their local PC. The volume label may contain only English characters and numbers.

4.4.2 Use External Time Source Only

Expiration dates and time limits applied to files are checked whenever the files are accessed. The copy protection first tries to validate the current date and time using known time servers via the Internet. If an Internet connection is not available the copy protection retrieve the current date and time using local resources such as the local system clock.

Enabling this option forces the copy protection to validate the current date and time using only external time servers. This results in a much stronger time limit protection but requires the end users to have an internet connection in order to open the protected files. If this option is enabled and an internet connection is not available then access to protected files is denied.

If an expiration date or a time limit was not applied to at least one file of your project then this option will be disabled and grayed out.

4.4.3 Rename TrusCont Autorun File

When protecting data files that are not EXE program files the software automatically adds to your project the TrusCont Autorun file (refer to section *2.2.1 The TrusCont Autorun File* for further details). The default TrusCont Autorun file name is "autorun_tc.exe". To change the default name check this option and enter the desired file name. The custom filename can include only English characters, numbers and underscores ('_') without any spaces, followed by a single dot ('.') and the extension 'exe'. If there are no protected data files on your project then this option is disabled and grayed out.

4.4.4 Set a Global Password

Enable this option to provision access to all protected data files on your project using a single global password. The TrusCont Autorun file requests the end user to enter the global password when it loads before granting access to the files. A global password can coexist with passwords applied to specific files. If there are no protected data files on your project then this option is disabled and grayed out.

4.4.5 Splash Screen

The TrusCont Autorun file may take a few seconds to load depending on the number of protected data files you have on your USB Flash Drive, and the performance of both your USB Flash Drive and the end user's PC.

While loading the TrusCont Autorun displays a default splash screen. You can change the default setting to 'Disabled' in case you don't want a splash screen to appear while the TrusCont Autorun loads. If you wish that the TrusCont Autorun will display your custom splash screen then set this option to 'custom' and include your splash screen image file in the top level (root) folder of your project. The splash filename must be 'tc_splash.bmp'. The image format must be BMP and the optimal size is 300 x 200 pixels.

If there are no protected data files on your project then this option is disabled and grayed out.

4.4.6 Restricted Use Mode

Protected USB Flash Drives can be used on only one PC at a time since it has to be connected to the local PC in order to access the protected files. You can further limit the environments in which the protected files can be used:

None	Disabled (Default). Any user can use the protected files on any PC provided that the USB Flash Drive is connected to the local PC.
Computer	Set a limit to the number of computers on which the end user can use the USB Flash Drive. The USB Flash Drive will automatically enable itself on the first computers on which it is used until the total number of computers exceeds the limit.
User	Set a limit to the number of users that are allowed to use the USB Flash Drive. The USB Flash Drive will automatically enable itself for the first users that access protected files until the total number of users exceeds the limit. User means the currently signed in user. This may be a local user or a domain user.
Domain	Limits the use of the protected files to users and PCs of a single network domain. The USB Flash Drive will automatically enable itself on the first network domain it is used.

Note:

1. Restricted use modes are not included in the basic USB Copy Protection license and require a purchase additional Activation Credits per USB Flash Drive according to the computers/users/domain count you set.
2. Restricted use modes require end users to have Internet connection in order to access protected files for the first time on each PC.

An attempt to access protected files in an environment (on a PC, or under a user account/domain) that exceeds the limit of allowed environments will display an error message indicating the files cannot be used in the current environment.

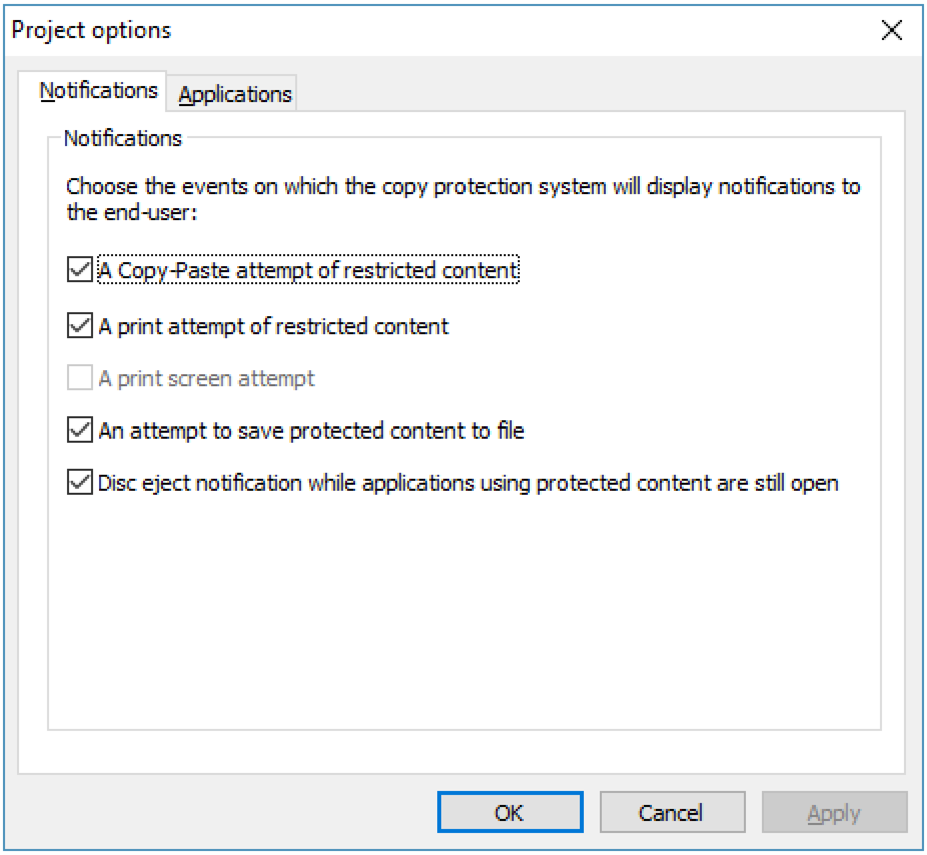
4.4.7 Advanced Project Options

Note: Changing the advanced project options may affect the copy protection functionality and/or user experience and is not recommended unless absolutely necessary.

To access the advanced project options click the 'Advanced' button on the project options page.

4.4.7.1 Toggling Data Protection Notifications

The copy protection system may display notifications to the end users that are triggered by attempts to perform a restricted operation (See section *2.2.2 Accessing Protected Data Files* for detailed description of the notifications). By default all notifications are turned on (except for the print screen attempt notification which is permanently disabled in this version).



Choose the events on which the copy protection system will display notifications to the end-user:

☑ A Copy-Paste attempt of restricted content

☑ A print attempt of restricted content

□ A print screen attempt

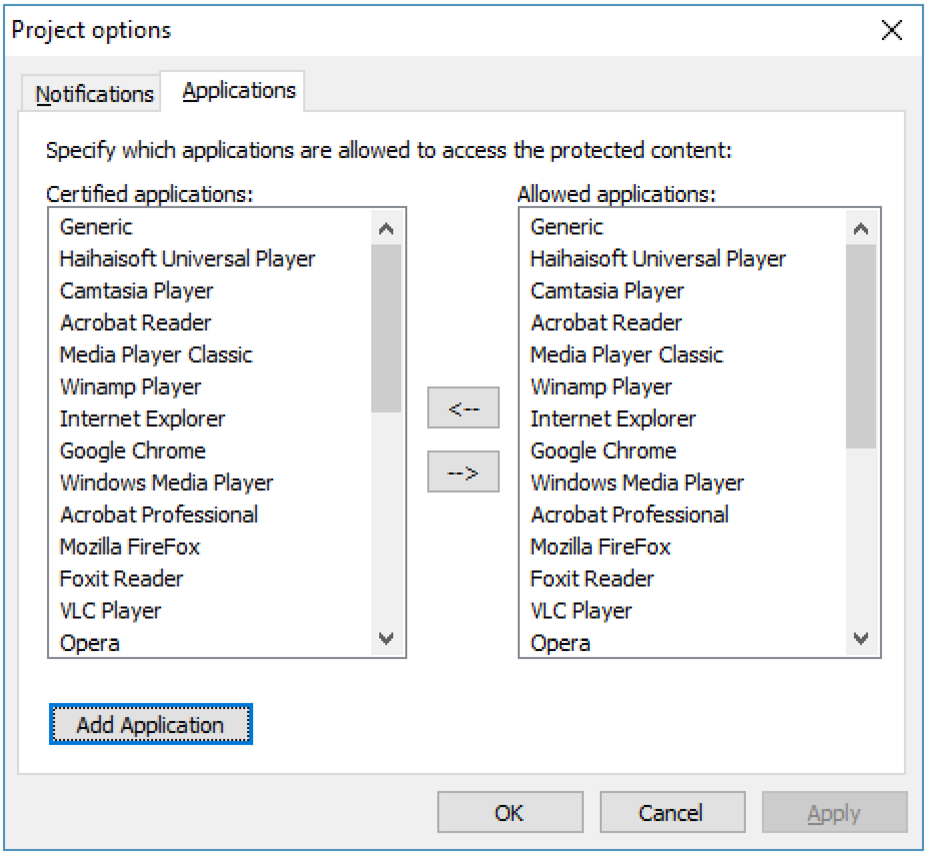
☑ An attempt to save protected content to file

☑ Disc eject notification while applications using protected content are still open

Figure 12: Enabling and Disabling Content Protection Notifications

4.4.7.2 Default List of Allowed Applications

The 'Applications' tab includes 2 lists of applications. The left one (Certified applications list) is a list of common applications that were tested by TrusCont in order to ensure they function properly when reading protected files. The second list includes the applications that will be allowed to access protected files of the specific project.



Specify which applications are allowed to access the protected content:

Certified applications:

Generic
Haihaisoft Universal Player
Camtasia Player
Acrobat Reader
Media Player Classic
Winamp Player
Internet Explorer
Google Chrome
Windows Media Player
Acrobat Professional
Mozilla FireFox
Foxit Reader
VLC Player
Opera

Allowed applications:

Generic
Haihaisoft Universal Player
Camtasia Player
Acrobat Reader
Media Player Classic
Winamp Player
Internet Explorer
Google Chrome
Windows Media Player
Acrobat Professional
Mozilla FireFox
Foxit Reader
VLC Player
Opera

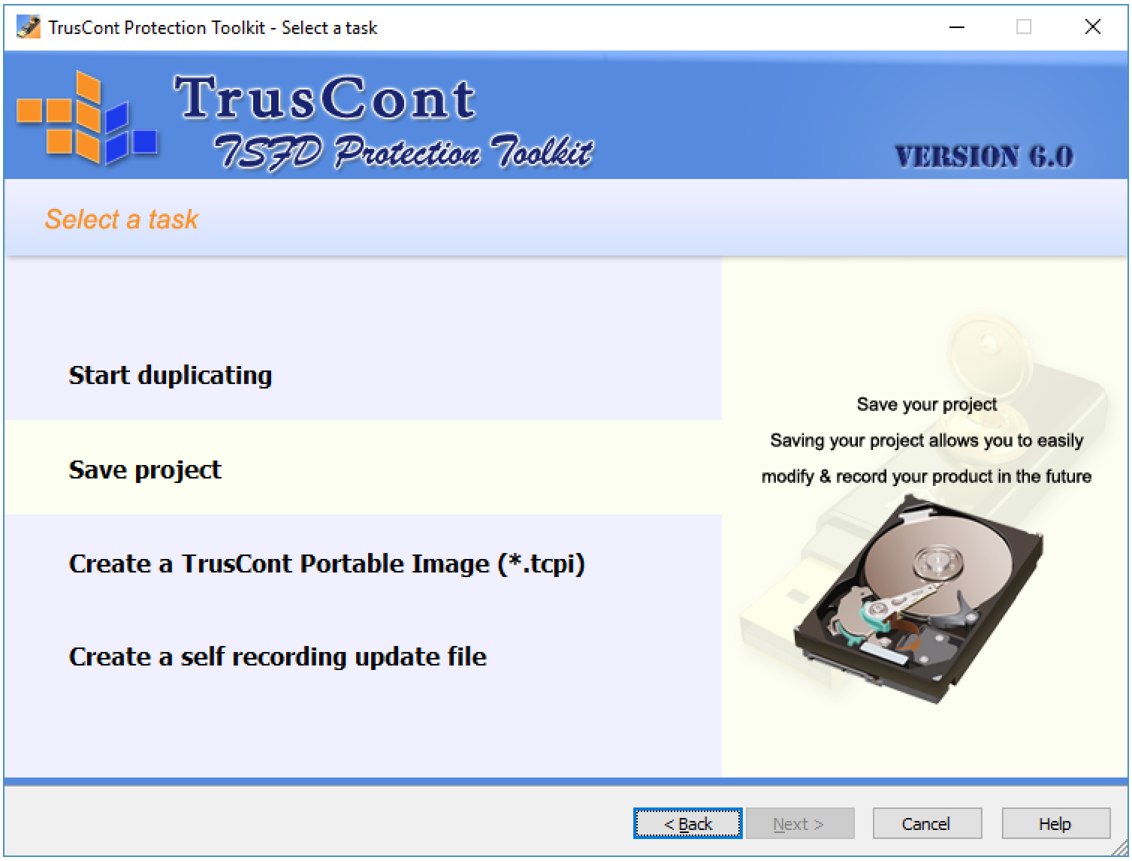
Figure 13: The default list of allowed applications

To deny a specific application access to protected files remove it from the right list by selecting it and clicking the left arrow. It is also possible to grant access to other 3rd applications including proprietary applications. Granting access to applications not included in the default list is not recommended unless absolutely necessary for your project (for further instructions please refer to *Appendix A – Customizing 3rd Party Applications Support for Content Protection*).

5. Saving a Project

Saving a project eliminates the need to remember the various settings used, and the need to repeat the project creation process in case you need to duplicate additional USB Flash Drives, or make changes to the existing project in the future.

Clicking 'Next' on the project options page brings up the following page prompting you to select the task you wish to perform on the project you have just created.



TrusCont Protection Toolkit - Select a task
TrusCont
TSFD Protection Toolkit
VERSION 6.0
Select a task
Start duplicating
Save project
Create a TrusCont Portable Image (*.tcpi)
Create a self recording update file
Save your project
Saving your project allows you to easily
modify & record your product in the future
< Back
Next >
Cancel
Help

Figure 14: Saving a project

To save your project select the 'Save project' task. Then click 'Browse' on the following page in order to specify a file name and location for saving the file.

> **Note:** The saved project file includes references to the files you added to your project. Changing, deleting, or moving the files from their original location may invalidate the project file and render it useless.

5.1 Opening a Saved Project

In order to open an existing project run the TSFD Protection Toolkit and select the 'Modify an existing project'. Then click the 'Browse' button and select the project file you wish to open. Alternatively, you can double click the saved project file in Windows File Explorer and it will automatically open within the TSFD Protection Toolkit.

The TSFD Protection Toolkit will then redirect to the 'Project Edit' page allowing you to modify the various project settings. The remainder of the process from this point is identical to creating a new project.

Note: The saved project file includes references to the files you added to your project. Changing, deleting, or moving the files from their original location may invalidate the project file and render it useless.

6. Duplicating a Project to USB Flash Drives

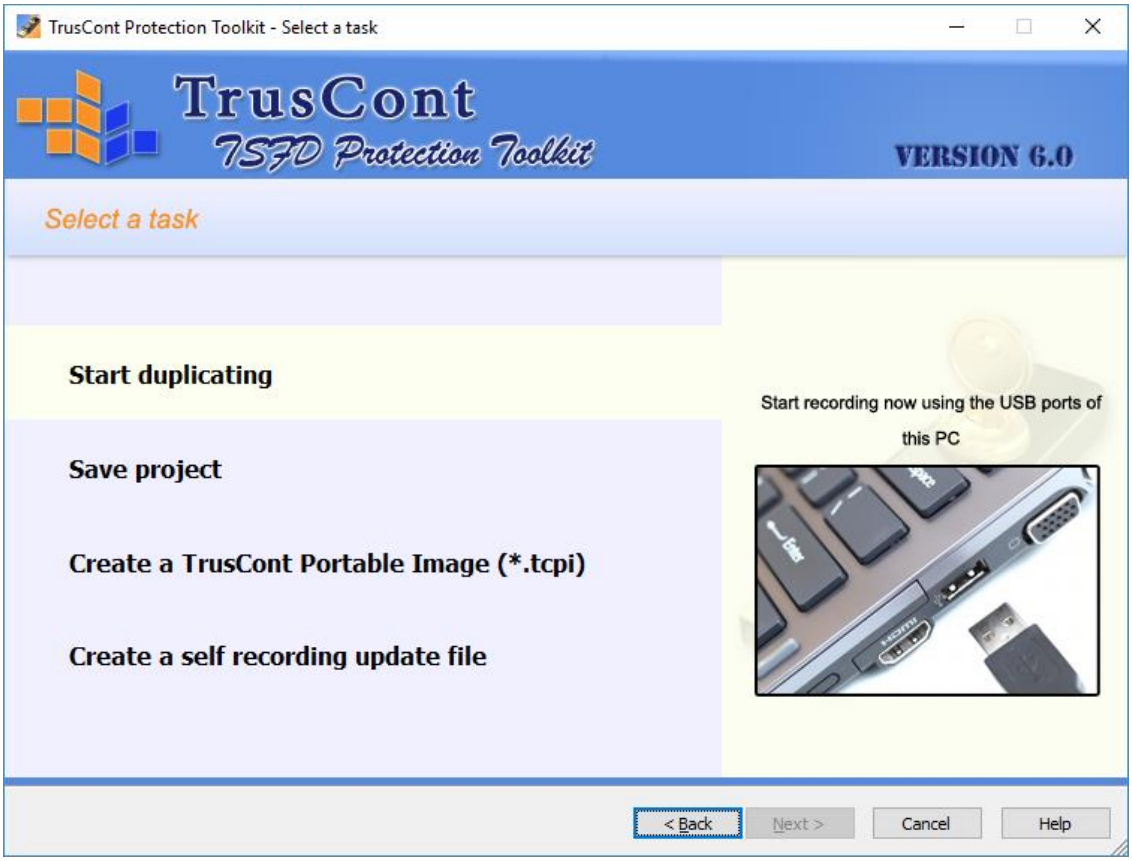
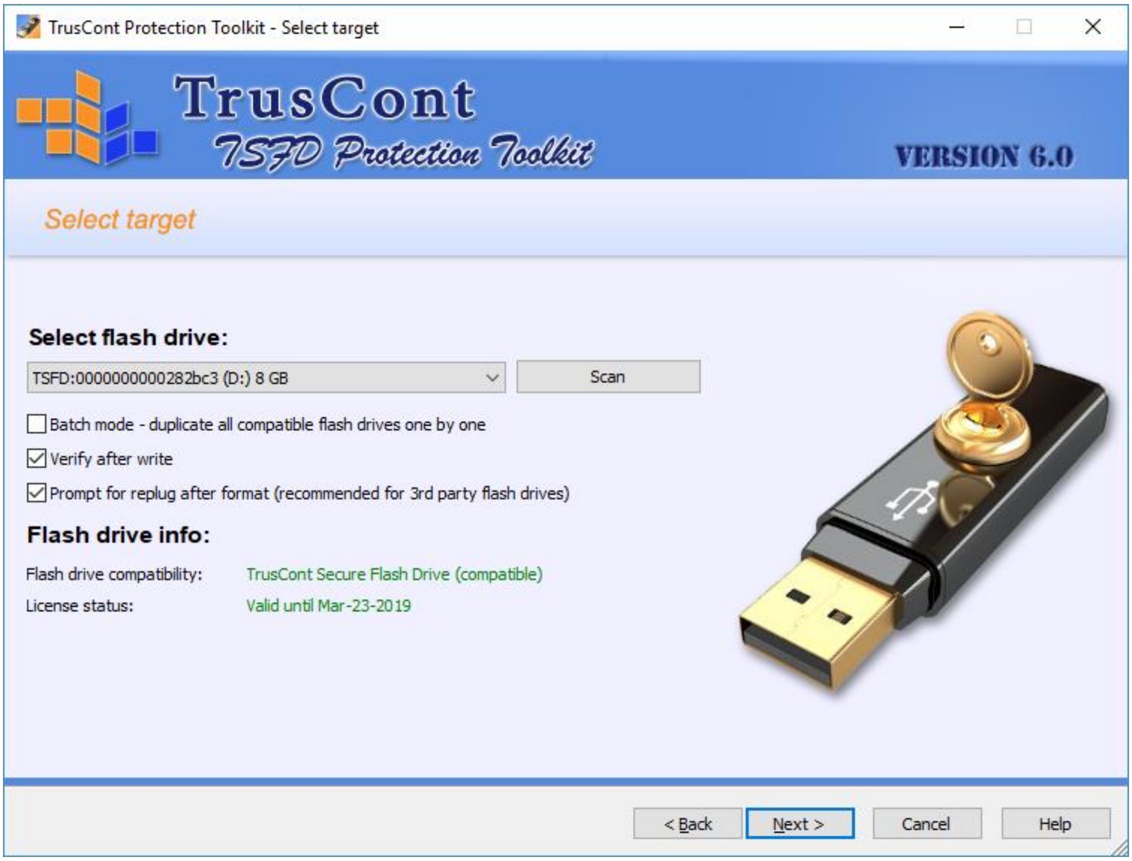

TrusCont Protection Toolkit - Select a task
TrusCont
TSFD Protection Toolkit
VERSION 6.0
Select a task
Start duplicating
Save project
Create a TrusCont Portable Image (*.tcpi)
Create a self recording update file
Start recording now using the USB ports of this PC
< Back
Next >
Cancel
Help

Figure 15: Duplicating to USB Flash Drives

Note:

1. You may want to save your project before duplicating it to USB Flash Drives. Saving a project eliminates the need to remember the various settings used, and the need to repeat the project creation process in case you need to duplicate additional USB Flash Drives, or make changes to the existing project
2. If you plan to publish more than a few USB Flash Drives that contain the same product, consider creating and duplicating using a TCPI image. Refer to section *7. Creating a TCPI Image File* for further details.

Selecting the 'Start duplicating' task brings up the target selection page. The TSFD Protection Toolkit automatically lists the USB Flash Drives that are currently connected to your local PC. If your USB Flash Drive is not listed, or was not connected to the PC at the time this page appeared then plug-in your USB Flash Drive and click the 'Scan' button.



TrusCont Protection Toolkit - Select target

Select target

Select flash drive:

TSFD:0000000000282bc3 (D:) 8 GB

□ Batch mode - duplicate all compatible flash drives one by one

☑ Verify after write

☑ Prompt for replug after format (recommended for 3rd party flash drives)

Flash drive info:

Flash drive compatibility: TrusCont Secure Flash Drive (compatible)

License status: Valid until Mar-23-2019

Figure 16: Select a target USB Flash Drive for duplication

TrusCont Secure Flash Drives offer the highest compatibility, copy protection level, and stability but you may also use USB Flash Drives sourced from 3rd parties. When selecting a target USB Flash Drive the software displays its compatibility level to TrusCont USB Copy Protection and its license status. Please refer to *Appendix B – Testing a Flash Drive for Compatibility* for further details on USB Flash Drive compatibility and licensing.

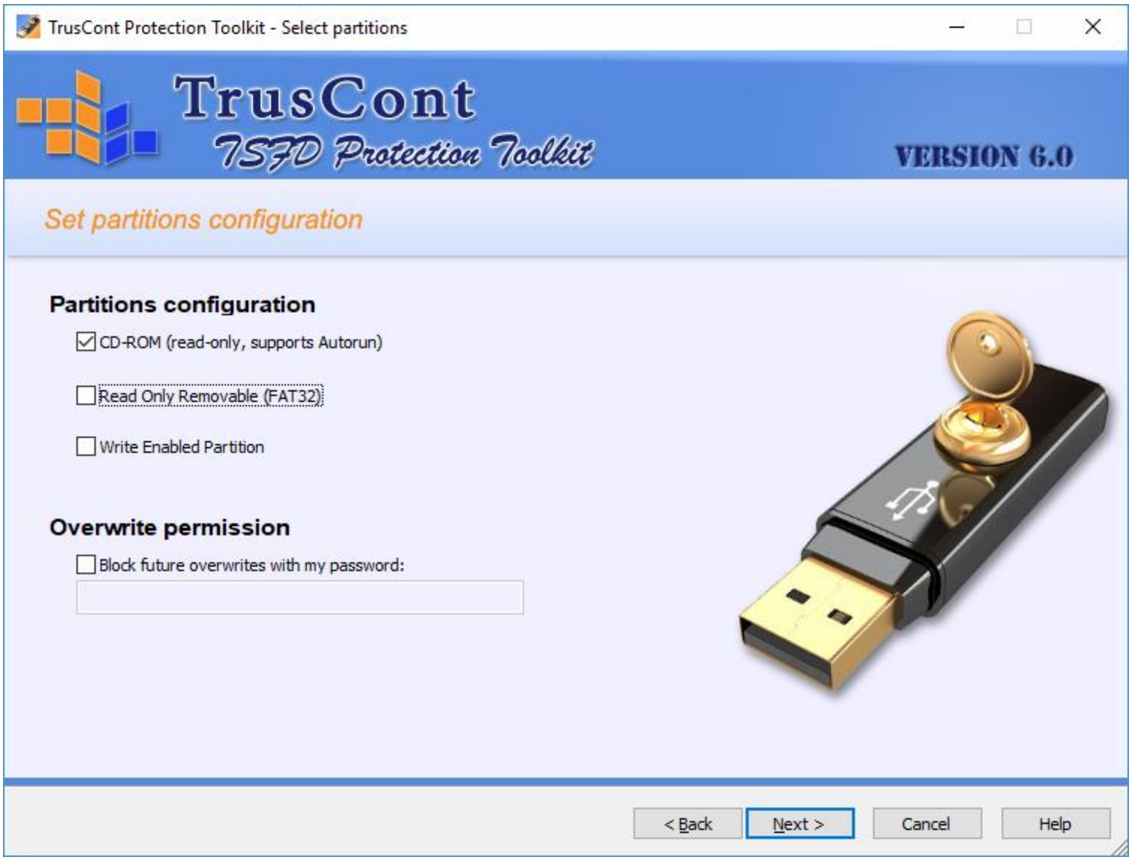
Check the 'Batch mode' option if you wish to duplicate multiple USB Flash Drive. The TSFD Protection Toolkit is an entry level software for duplicating USB Flash Drives one at a time (for mass duplication solutions please refer to this web page: https://www.truscont.com/solutions/duplication-solutions). When checking the batch mode option instead of selecting a specific target, the software duplicates the project to all the compatible USB Flash Drives that it detects. It will still duplicate the detected USB Flash Drives one at a time but will not require user intervention after each one unless an error is encountered.

Verify after write is enabled by default. When enabled the software will read back the data from the USB Flash Drive after writing in order to make sure it was written properly (bit to bit verification). Low quality USB

Flash Drive may contain bad blocks, or poor data retention capacities. If you trust the quality of your USB Flash Drives you may disable this options in order to speed up production.

Prompt for replug after format is checked by default and instructs the software to ask for re-plugging the USB flash drive after repartitioning it. Setting this option may increase compatibility to USB flash drives that cannot be reset by software means. In case the TSFD Protection Toolkit detects that the USB flash drive can be reset safely it will not ask for a re-plug even if this option is turned on.

6.1 Setting Partitions Configuration


TrusCont Protection Toolkit - Select partitions
TrusCont
TSFD Protection Toolkit
VERSION 6.0
Set partitions configuration

Partitions configuration

☑ CD-ROM (read-only, supports Autorun)

□ Read Only Removable (FAT32)

□ Write Enabled Partition

Overwrite permission

□ Block future overwrites with my password:

< Back
Next >
Cancel
Help

Figure 17: Setting partitions configuration

There is no need to format the target USB Flash Drives. The TSFD Protection Toolkit automatically partitions and formats the USB Flash Drives for you before duplicating. The valid partition configurations are:

Partition	File system	Max file size	Read-only	Autoplay support
CD-ROM	ISO / UDF	Unlimited	Yes	Yes
Read-only removable	FAT32	2 GB	Yes	No
Write enabled	FAT32	2 GB	No	No

The CD-ROM partition is the default and the recommended partition type. It is a read-only partition type that supports storage and protection of files at any size. It also supports the Windows autoplay feature, making it the ideal partition type for software and data publishing.

It is also possible to partition the USB Flash Drive into 2 separate partitions: CD-ROM + Write enabled partitions, or Read-only removable + Write enabled partitions. On 2 partition configurations the project files are recorded on the first (CD-ROM, or the read-only removable) partition. The unused space of the USB Flash Drive is allocated to the second write enabled partition which is left blank.

6.2 Overwrite Permission

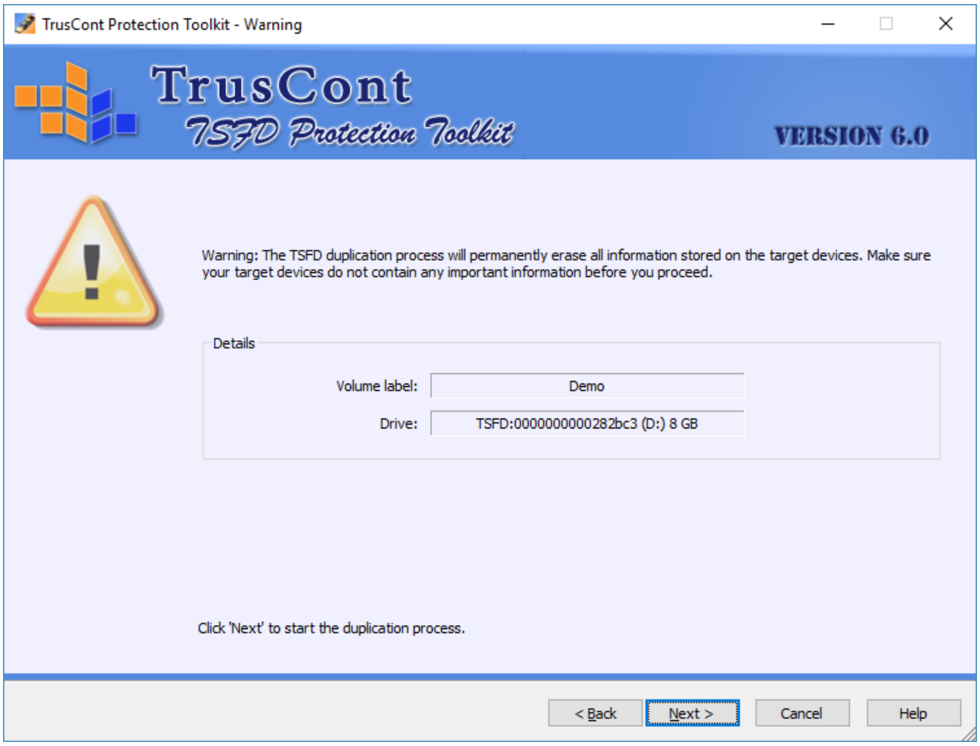
The TSFD Protection Toolkit can be used to overwrite protected USB Flash Drives with new data even if the protected USB Flash Drives include read-only partitions. Overwriting a protected USB Flash Drive is possible unlimited number of times for as long as its copy protection license is valid. For additional info on the USB Copy Protection license terms please refer to section *8 Updating Protected USB Flash Drives*.

To prevent 3rd parties from overwriting your USB Flash Drives, the TSFD Protection Toolkit allows you to block future overwrite with a password. To set the password check the option 'Block future overwrite with my password' and enter your desired password. This password can be set only once and cannot be changed. If a password is already set, then you must enter it at this field, otherwise any write attempt will fail.

6.3 Starting the Duplication Process

Click 'Next' on the partitions configuration page to start the duplication process. The software will display a warning page indicating the USB Flash Drive is about to be overwritten. Click 'Next' to confirm and start the duplication.

During the duplication process, the software may ask you for your TrusCont credentials in order to pool the required copy protection credits from your account.



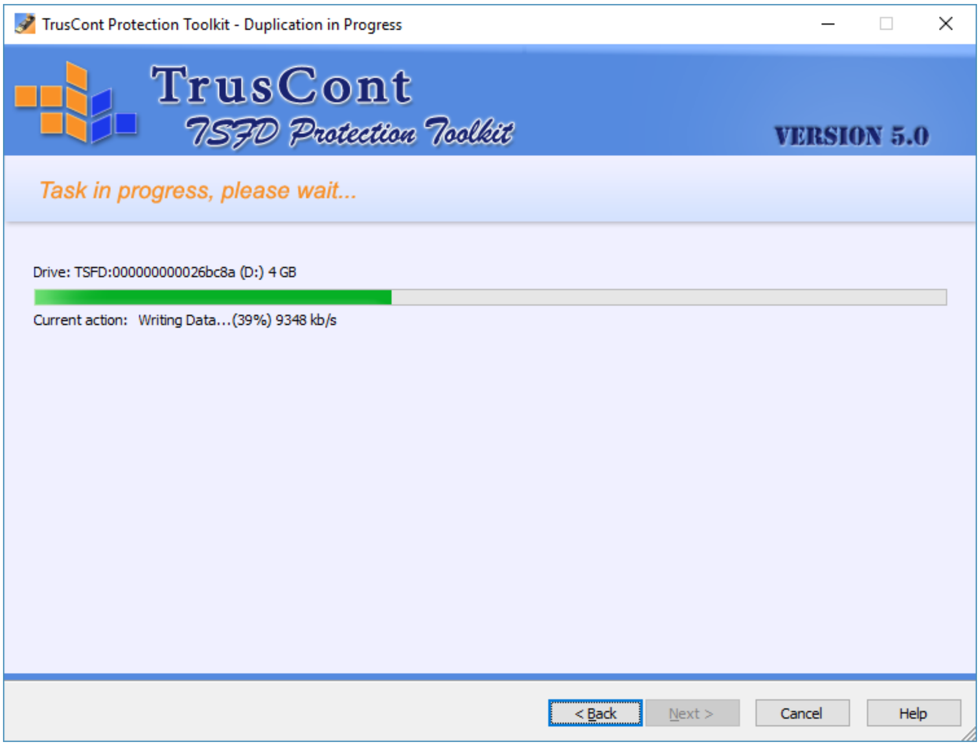
Warning: The TSFD duplication process will permanently erase all information stored on the target devices. Make sure your target devices do not contain any important information before you proceed.

Volume label: Demo

Drive: TSFD:0000000000282bc3 (D:) 8 GB

Click 'Next' to start the duplication process.

Figure 18: Overwrite warning page



Task in progress, please wait...

Drive: TSFD:000000000026bc8a (D:) 4 GB

Current action: Writing Data...(39%) 9348 kb/s

Figure 19: The duplication process

7. Creating a TCPI Image File

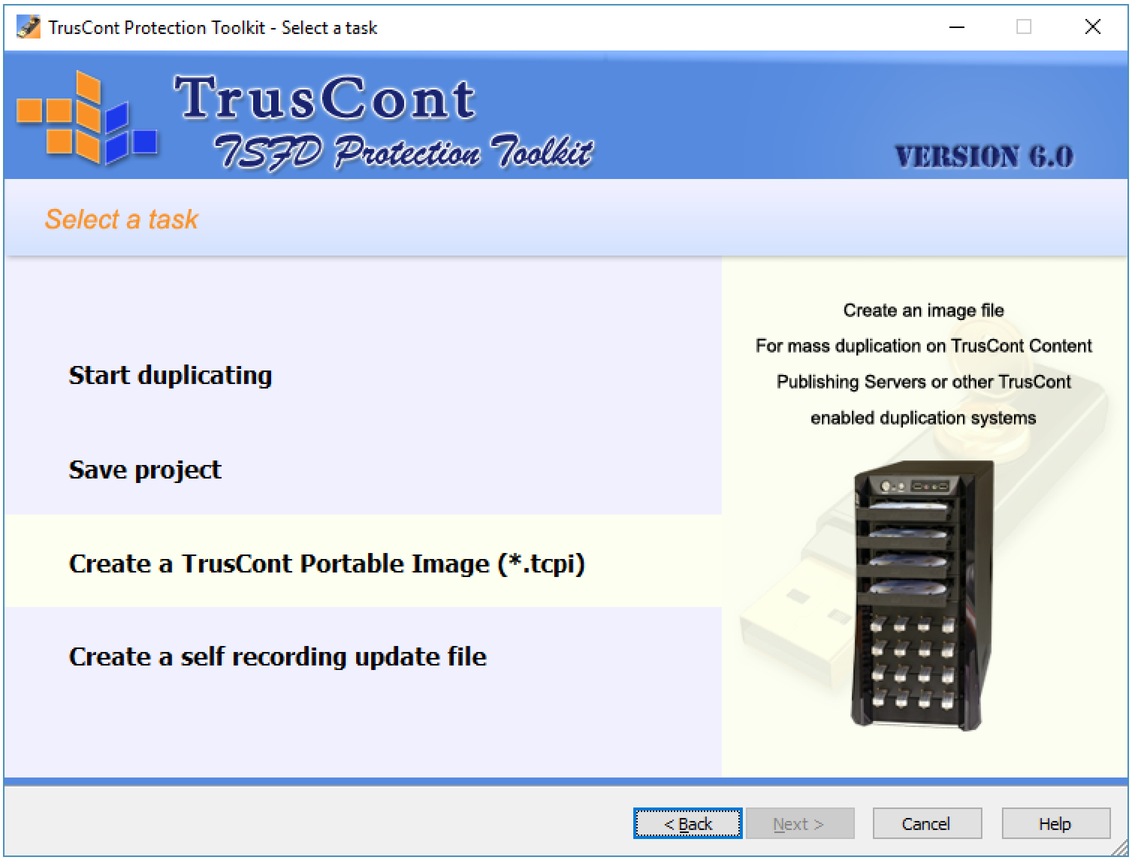

TrusCont Protection Toolkit - Select a task
TrusCont
TSFD Protection Toolkit
VERSION 6.0
Select a task
Start duplicating
Save project
Create a TrusCont Portable Image (*.tcpi)
Create a self recording update file
Create an image file
For mass duplication on TrusCont Content Publishing Servers or other TrusCont enabled duplication systems
< Back
Next >
Cancel
Help

Figure 20: Creating a TCPI image

A TCPI image is a single file that contains a sealed compilation of all your protected files and settings. It makes it easy to archive your compiled project and have it ready for quickly duplicating on USB Flash Drives. If you plan to publish more than a few USB Flash Drives that contain the same product, you should create a TCPI image of your project and use it for duplicating all your USB Flash Drives. A TCPI image is a sealed compilation of the project – once created it cannot be changed.

Duplicating from a TCPI image provides the following benefits:

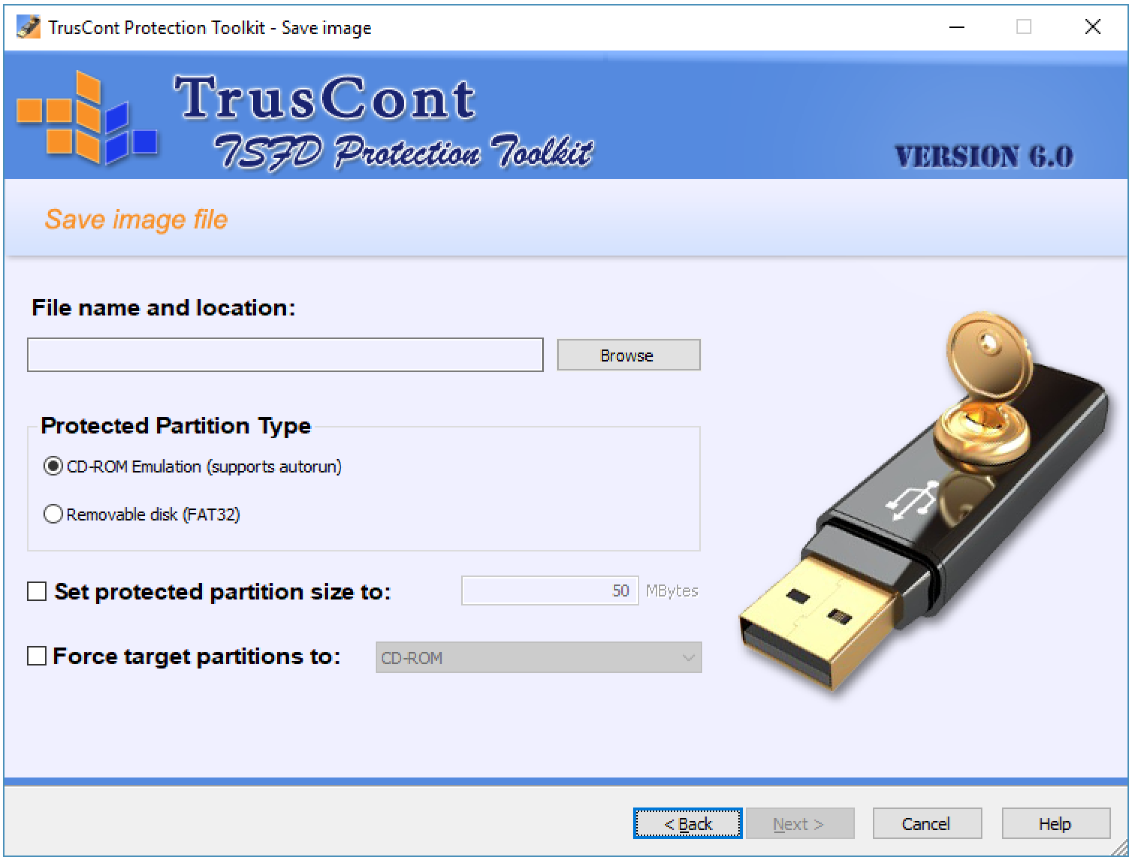
1. **Mass production** – A TCPI image can be used to mass duplicate USB Flash Drives using TrusCont professional duplication solutions (https://www.truscont.com/solutions/duplication-solutions). It also provides much faster one offs duplication using the TSFD Protection Toolkit and simplifies the production process.

2. **Updates** – the TSFD Protection Toolkit also allows you to create updates for Protected USB Flash Drives that were already sent to customers. One of the update options is to create an update file that updates

only USB Flash Drives that contain a specific product. This option requires the original TCPI image in order to identify the original product it contains.

3. **Interchangeability** – makes your USB Flash Drives interchangeable. This means that a protected program file from one USB Flash Drive can be ran using another USB Flash Drive duplicated from the same image. All USB Flash Drives duplicated from the same image are interchangeable. USB Flash Drives duplicated from different images, directly from source files, or from a saved project are not interchangeable.

To save your project as a TCPI image, select the 'Create a TrusCont Potable Image (*.tcpi)' task. Then click the 'Browse' button on the 'Save Image File' page in order to specify a file name and location for saving the image.



TrusCont Protection Toolkit - Save image

Save image file

File name and location:

Protected Partition Type

● CD-ROM Emulation (supports autorun)

○ Removable disk (FAT32)

□ Set protected partition size to: 50 MBytes

□ Force target partitions to: CD-ROM

Figure 21: Creating a TCPI image

Select the target partition type for all target USB Flash Drives that will be duplicated from the image you create. The default, and recommended partition type is CD-ROM, which is a read-only partition type that supports files bigger than 2 GB and Windows autoplay.

The TSFD Protection Toolkit automatically allocates the minimum required capacity for storing your files. If you plan to publish updates to USB Flash Drives that will be duplicated from this image then you may want to set the partition size manually to a larger size in order to allow your product to grow. This is only required if you plan to have a second write enabled partition on your USB Flash Drives, which prevents resizing of the first partition.

The 'Force target partitions to' option allows you to force a specific partitions configuration on all USB Flash Drives duplicated from this image file.

8. Updating Protected USB Flash Drives

TrusCont USB Copy Protection includes a versatile update mechanism. You can update flash drives at hand, and also remotely update flash drives that were already sent to customers. The updates can be generic, or selective to specific products or customers.

8.1 The License Term

The license term of a protected USB Flash Drive is 12 months starting from the first write of protected files. During the license term it is possible to overwrite the flash drive and protect other files unlimited number of times. This allows publishers to test, remaster and update the content freely as needed. After the license expires the existing content remains protected and usable of course. Renewing the license is possible and is required only if the existing content needs to be updated.

In order to renew expired licenses of USB Flash Drives at hand simply use the TSFD Protection Toolkit to record your new files. The TSFD Protection Toolkit will ask you for your account credentials in order to pool 1 credit from your account and renew the license for an additional term of 1 year.

Renewing the license of flash drives that were already sent to customers is done by providing a license code along with the update file (refer to section *8.4.1.1 Managing update entitlement* for further details).

8.2 Planning Ahead for Future Updates

Planning for future updates before duplicating your USB Flash Drives is very important especially if you plan to publish updates for USB Flash Drives after shipping it to end users.

☑ **Keep the original image of your product**

You will need it in the future in order to remotely update USB Flash Drives that contain the specific product (image).

- ✓ Save your project
- ✓ Create a TCPI image file
- ✓ Archive the image in a safe place
- ✓ Duplicate all USB Flash Drives you plan to publish from the same TCPI image.

☑ **Provision overwrites using a password**

Overwrite permission passwords (refer to section *6.2 Overwrite Permission* for further details) can be useful for remotely updating USB Flash Drives regardless of the product originally recorded on it. It also guaranties that your USB Flash Drives cannot be overwritten by a 3rd party's generic update, or even using the TSFD Protection Toolkit itself.

- ✓ Save your passwords in a safe place – it cannot be restored or changed
- ✓ Maintain a list detailing which password you use for each product
- ✓ Avoid using multiple passwords for the same product, unless you wish to differ update paths for various user groups of the same product.
- ✓ Do not disclose your passwords. End users don't need to know the passwords in order to apply updates. The passwords are the only key to overwriting your USB Flash Drives.

8.3 Updating flash drives at hand

Updating flash drives at hand is possible by simply overwriting it with the updated data:

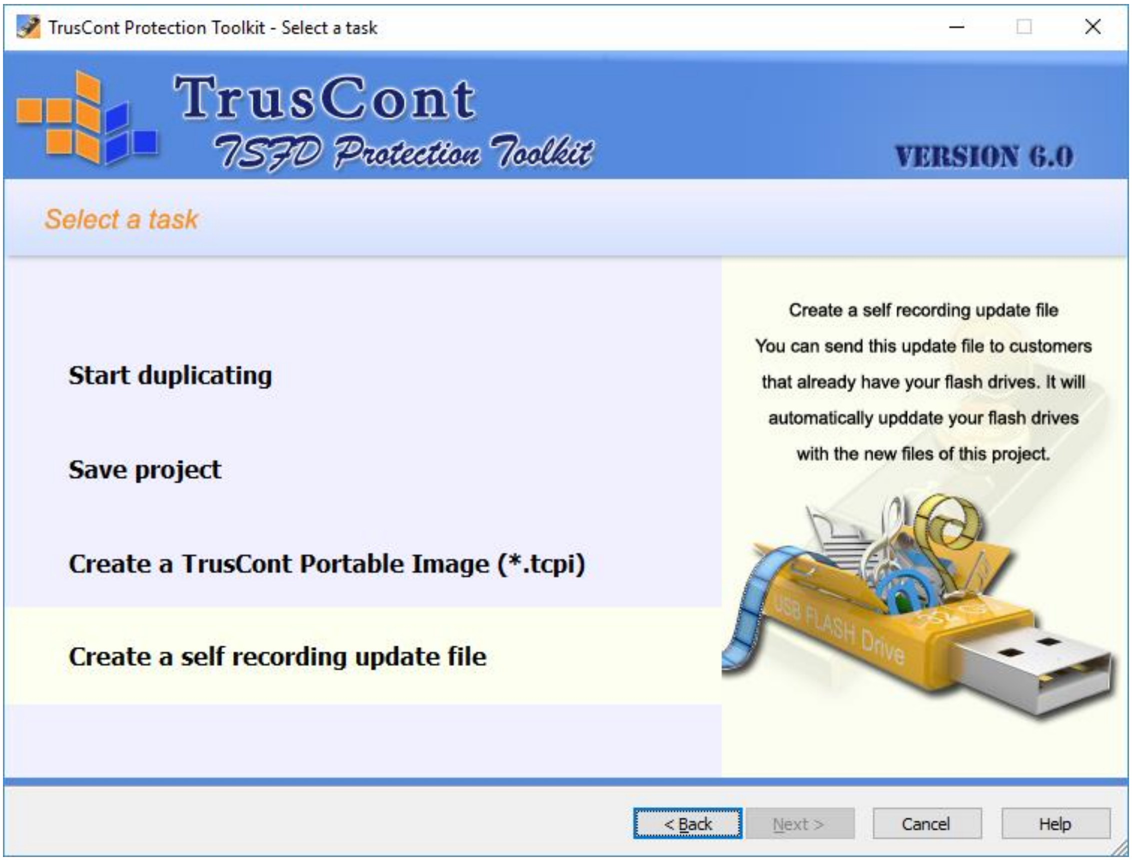
1. Create a new project using the updated files, or modify the project you saved previously.
2. Optionally save the project as a new project file and create a TCPI image file
3. Duplicate the new project on the USB Flash Drives that need to be updated.

8.4 Updating flash drives remotely

It is also possible to update the content of protected USB Flash Drives that were already sent out to customers. This is achieved by creating a self-recording update file using the TSFD Protection Toolkit and delivering it to eligible customers.

8.4.1 Creating a Self Recording Update File

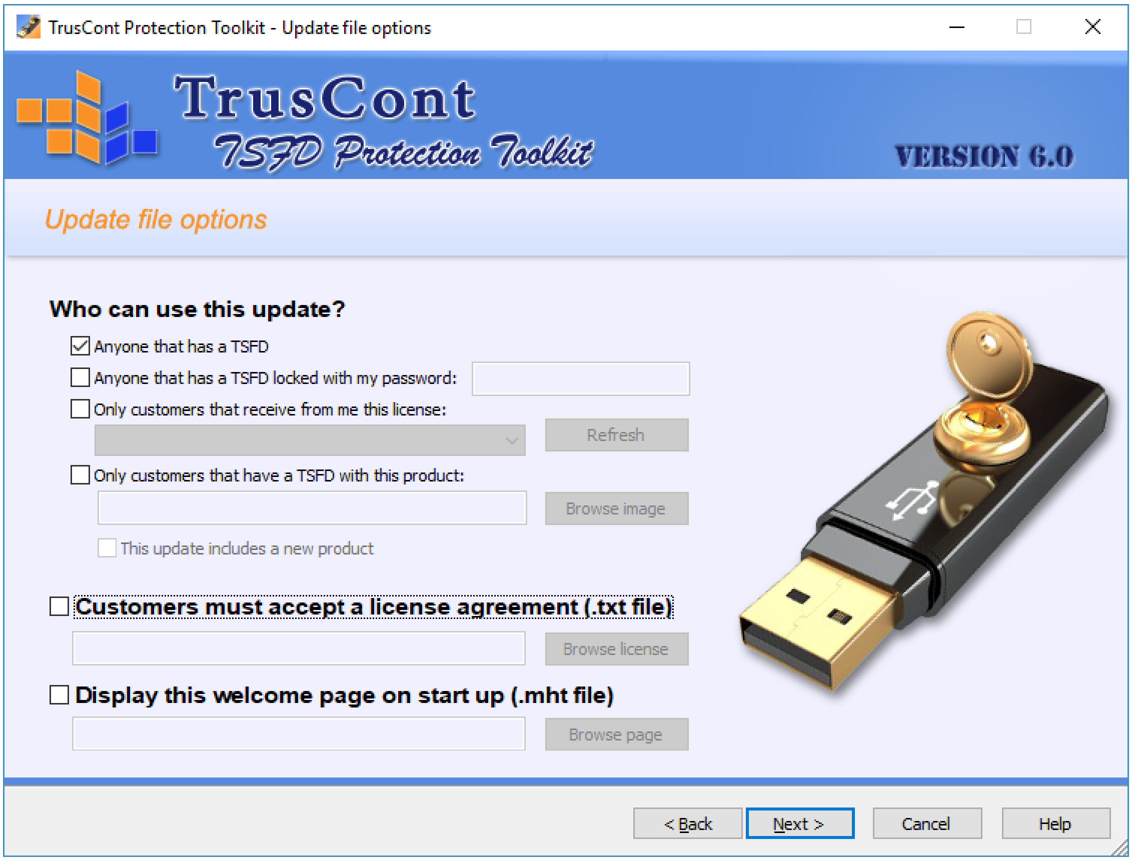
A self-recording update file is actually a TCPI image in EXE format that contains the new files and copy protection settings. End users in possession of USB Flash Drives eligible for the update can simply double click the update file in order to overwrite the target USB Flash Drive with the new files and settings.



Create a self recording update file
You can send this update file to customers that already have your flash drives. It will automatically upddate your flash drives with the new files of this project.

Figure 22: Creating a self recording update file

To create a self recording update file open the TSFD Protection Toolkit and create a new project. Follow the instructions on section *4 Creating a New Project* in order to add the updated files to the project, apply the desired copy protection settings, and set the project options. Then select the task 'Create a self recording update file'.



TrusCont Protection Toolkit - Update file options

Update file options

Who can use this update?

☑ Anyone that has a TSFD

☐ Anyone that has a TSFD locked with my password:

☐ Only customers that receive from me this license:

☐ Only customers that have a TSFD with this product:

☐ This update includes a new product

☐ **Customers must accept a license agreement (.txt file)**

☐ **Display this welcome page on start up (.mht file)**

Figure 23: Managing update entitlement

8.4.1.1 Managing update entitlement

When creating the update file, the Toolkit allows you to choose which customers are entitled to use it:

Anyone that has a TSFD – This option creates a generic, unrestricted update file that can be used by anyone to update any USB Flash Drive previously protected by TrusCont, which is not blocked by an overwrite permission password.

Anyone that has a TSFD locked with my password – The update will be applicable only to USB Flash Drives protected by TrusCont that are already blocked from being overwritten using the specified password.

Only customers that receive from me this license – The update file will require end users to input a license code. Publishers can login to their account on the TrusCont website in order to issue the codes. By default each code can be used only once to update a single USB Flash Drives. This option allows publishers to control the update entitlement of each individual customer.

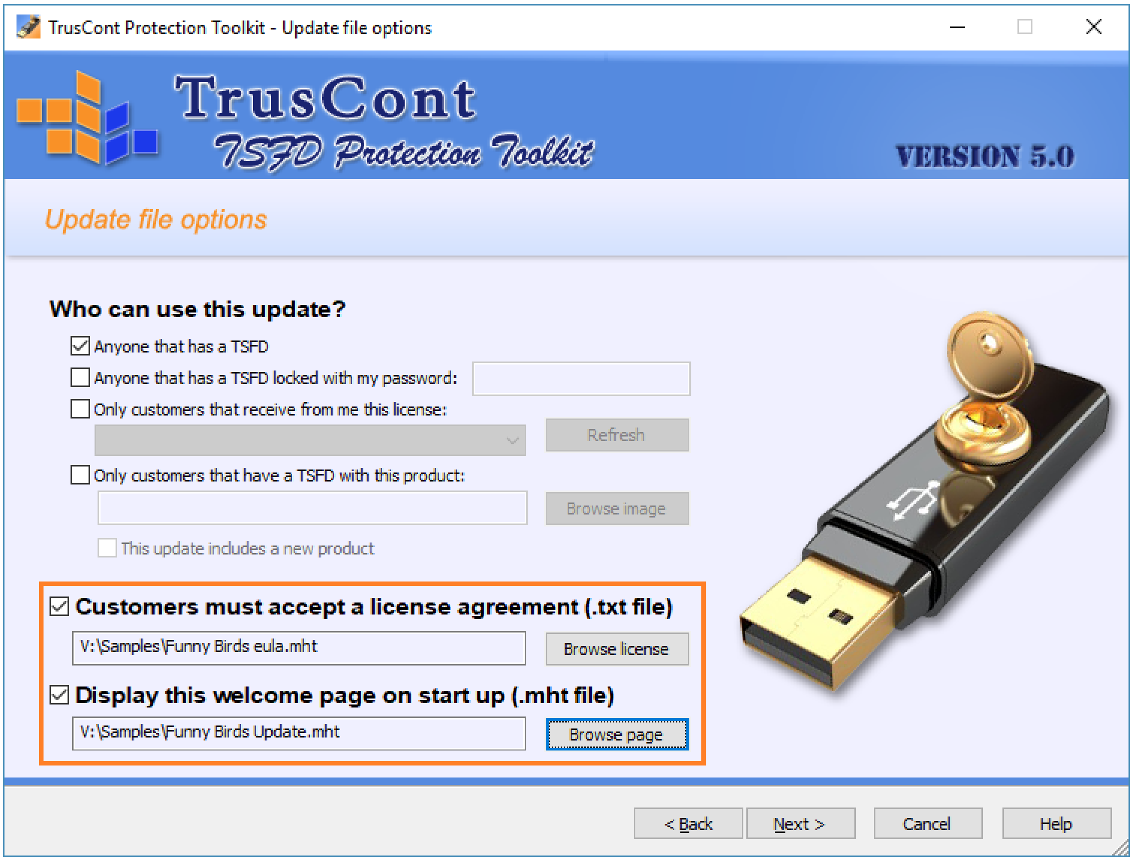
Issuing license codes requires 1 Activation Credit per code (purchased separately). In addition, the code can be coupled with a USB Copy Protection Credit in case the license of the USB Flash Drive that needs to be updated has already expired (refer to section *8.1 The License Term* for further details).

Only customers that have a TSFD with this product – The update will be applicable only to USB Flash Drives that contain a specific product. This option requires you to specify the TCPI image file used for recording the product being updated.

This option also allows you to specify that the update contains a new product. This means that USB Flash Drives updated with this update file will not be applicable for future updates generated for the previous product stored on it prior to this update. In other words, USB Flash Drives that previously contained product X, which was replaced by product Y, can now receive only updates for product Y and are no longer eligible for updates generated for product X.

8.4.1.2 Adding a Welcome Page and a License Agreement

The update file can include a custom welcome page that will be displayed when customers run it. In addition you can add a license agreement that will be displayed after the welcome page and will require end users to accept it in order to apply the update.



TrusCont Protection Toolkit - Update file options

Update file options

Who can use this update?

☑ Anyone that has a TSFD

□ Anyone that has a TSFD locked with my password:

□ Only customers that receive from me this license:

□ Only customers that have a TSFD with this product:

□ This update includes a new product

☑ **Customers must accept a license agreement (.txt file)**

V:\Samples\Funny Birds eula.mht

☑ **Display this welcome page on start up (.mht file)**

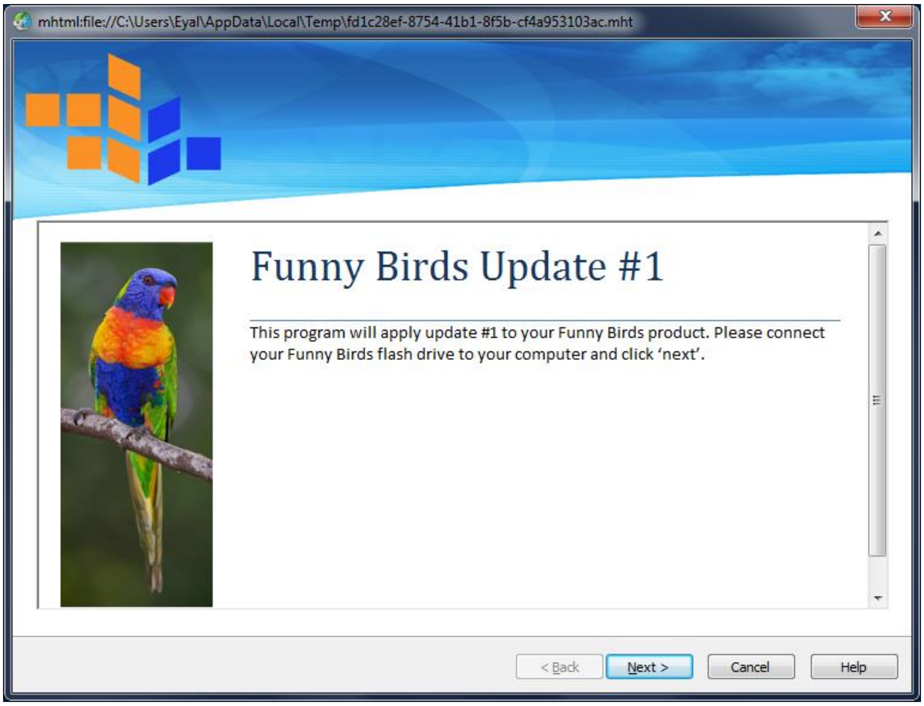
V:\Samples\Funny Birds Update.mht

Figure 24: Adding a Welcome Page and a License Agreement

The welcome page needs to be in a single web page format (MHT file). MHT files can be created using Microsoft Word. Create your documents then select 'Save As' and choose 'Save as type: Single web page (*.mht; *.mhtl)'. The license agreement can be a plain text file or an MHT file.

8.4.2 Using a Self Recording Update File

The update file is actually an EXE program file that records the update to the end users' USB Flash Drives. To start the update process the end user simply double clicks the update file. If you have included a welcome page in your update file, it will be the first page that the end user sees. This is a sample welcome page that includes a title, picture and some text:

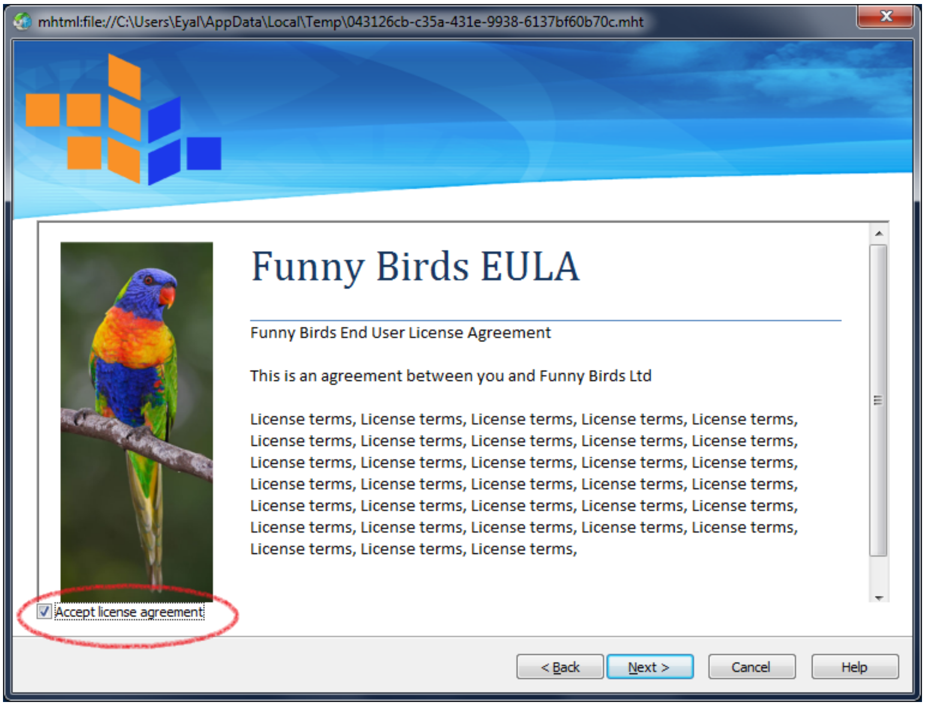

mhtml:file://C:\Users\Eyal\AppData\Local\Temp\fd1c28ef-8754-41b1-8f5b-cf4a953103ac.mht
< Back
Next >
Cancel
Help

Funny Birds Update #1

This program will apply update #1 to your Funny Birds product. Please connect your Funny Birds flash drive to your computer and click 'next'.

Figure 25: Sample Welcome Page

If you have included an End User License Agreement in your update, it will be displayed immediately after the welcome page. The end user must accept the license agreement in order to proceed with the update process.


mhtml:file://C:\Users\Eyal\AppData\Local\Temp\043126cb-c35a-431e-9938-6137bf60b70c.mht
< Back
Next >
Cancel
Help

Funny Birds EULA

Funny Birds End User License Agreement

This is an agreement between you and Funny Birds Ltd

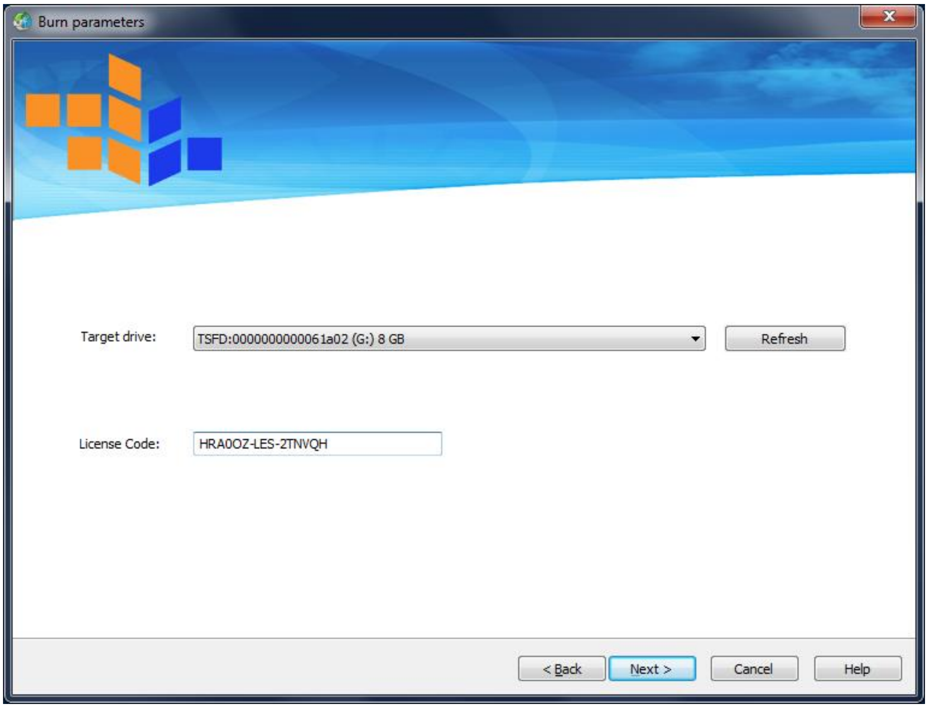
License terms, License terms,

☑ Accept license agreement

Figure 26: End User License Agreement Sample

After the user accepts the license agreement and clicks 'Next' the software looks for compatible USB Flash Drives. If more than one compatible device is detected the end user can select which one he wishes to update.

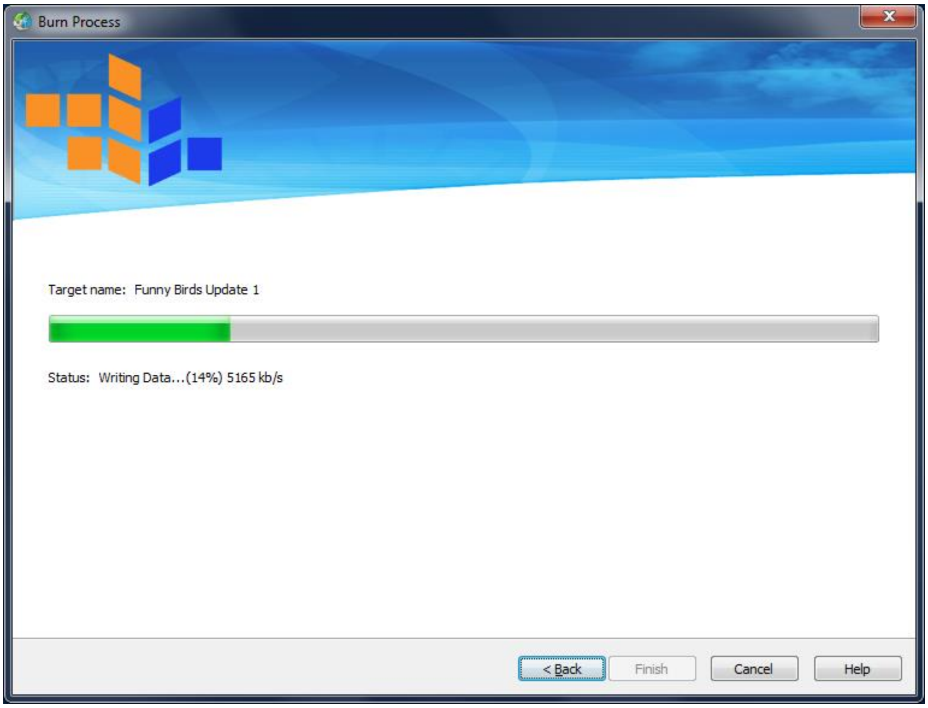
On this page the end user also has to enter his license code if the update requires it. Clicking next will automatically start the update recording process.



Target drive: TSFD:00000000000061a02 (G:) 8 GB

License Code: HRA0OZ-LES-2TNVQH

Figure 27: Target Drive and License Code



Target name: Funny Birds Update 1

Status: Writing Data...(14%) 5165 kb/s

Figure 28: The Update Recording Process

Appendix A – Customizing 3rd Party Applications Support for Content Protection

Introduction

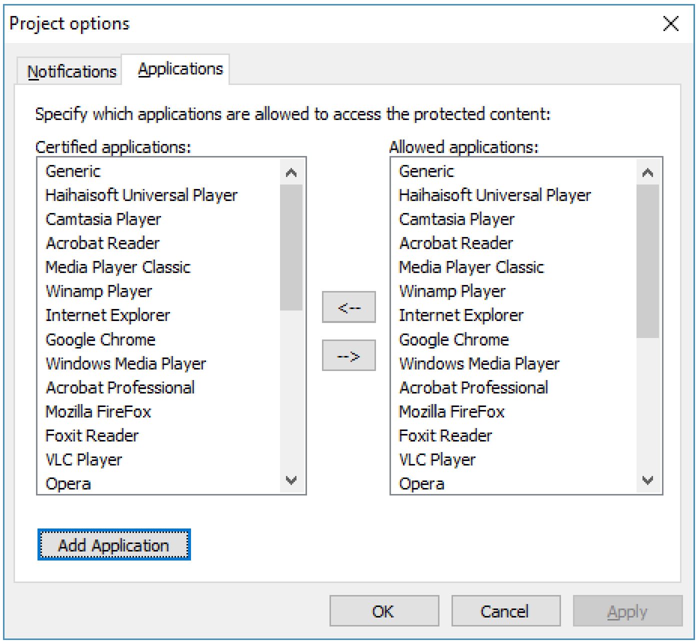
By default TrusCont software allows a list of certified 3rd party applications reading protected content files. Other 3rd party (standard or proprietary) applications that are not included in this list are either not tested or not compatible with TrusCont copy protection. This appendix describes how customers can add support for additional 3rd party applications

Warning

There is no guaranty that applications not specifically certified by TrusCont and included in the default list will be able to read protected files properly. TrusCont shall not be liable for any direct and/or indirect consequences of using this feature. It is highly recommended that customers test their products thoroughly before actual publication. Testing on multiple systems and configurations is recommended in order to ensure your proprietary application can read protected files properly.

Instructions

1. Open your project, or create a new one
2. Open the default list of allowed applications (see section *4.4.7.2 Default List of Allowed Applications*).



Specify which applications are allowed to access the protected content:

Certified applications:

Generic
Haihaisoft Universal Player
Camtasia Player
Acrobat Reader
Media Player Classic
Winamp Player
Internet Explorer
Google Chrome
Windows Media Player
Acrobat Professional
Mozilla FireFox
Foxit Reader
VLC Player
Opera

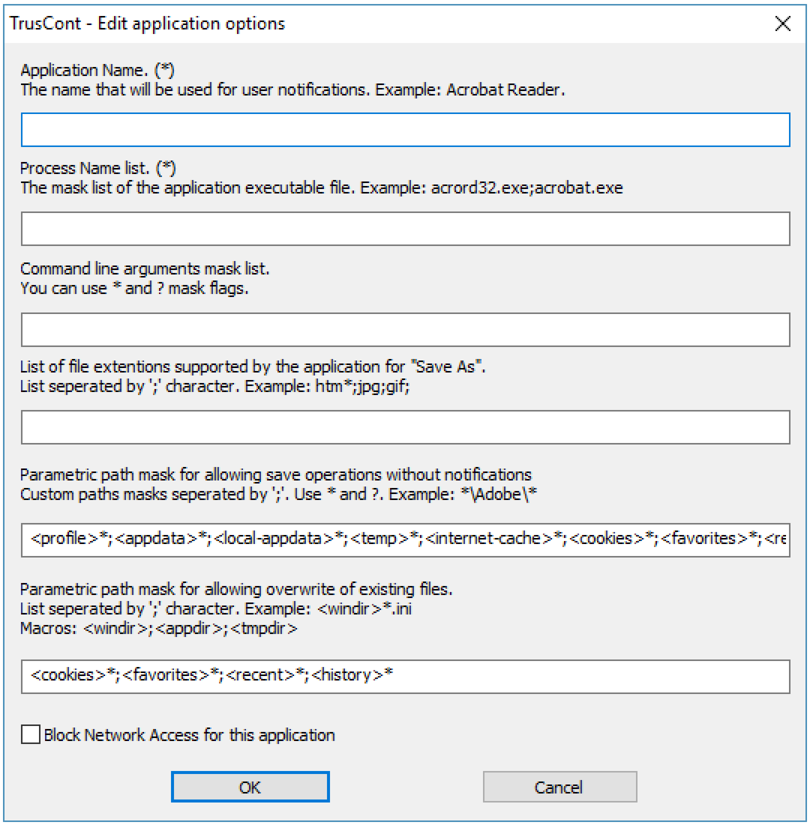
Allowed applications:

Generic
Haihaisoft Universal Player
Camtasia Player
Acrobat Reader
Media Player Classic
Winamp Player
Internet Explorer
Google Chrome
Windows Media Player
Acrobat Professional
Mozilla FireFox
Foxit Reader
VLC Player
Opera

Figure 29: Certified Application List

3. Click 'Add Application'

4. Complete the application setup form according to the following guidelines:



TrusCont - Edit application options

Application Name. (*)
The name that will be used for user notifications. Example: Acrobat Reader.

Process Name list. (*)
The mask list of the application executable file. Example: acrord32.exe;acrobat.exe

Command line arguments mask list.
You can use * and ? mask flags.

List of file extentions supported by the application for "Save As".
List seperated by ';' character. Example: htm*;jpg;gif;

Parametric path mask for allowing save operations without notifications
Custom paths masks seperated by ';'. Use * and ?. Example: *\Adobe*

<profile>*;<appdata>*;<local-appdata>*;<temp>*;<internet-cache>*;<cookies>*;<favorites>*;<re

Parametric path mask for allowing overwrite of existing files.
List seperated by ';' character. Example: <windir>*.ini
Macros: <windir>;<appdir>;<tmpdir>

<cookies>*;<favorites>*;<recent>*;<history>*

□ Block Network Access for this application

Figure 30: The Application Setup Form

a. **Application Name** – The name of your application.

b. **Process Name List** – List of all EXE file names of your application that should have access to protected content files. Multiple file names shall be separated by a semicolon (';').

c. **Command Line Arguments** – Enter command line arguments that may be required for your application.

d. **List of extensions supported by the application's "Save As" option** – List all the extension that your application typically allows to save. The Toolkit will not allow your application to save any files. However, if end users try to save files with the listed extensions from your application the Toolkit display a notification that the files cannot be saved. For all other extensions (e.g. temporary files) the Toolkit will not provide any notification.

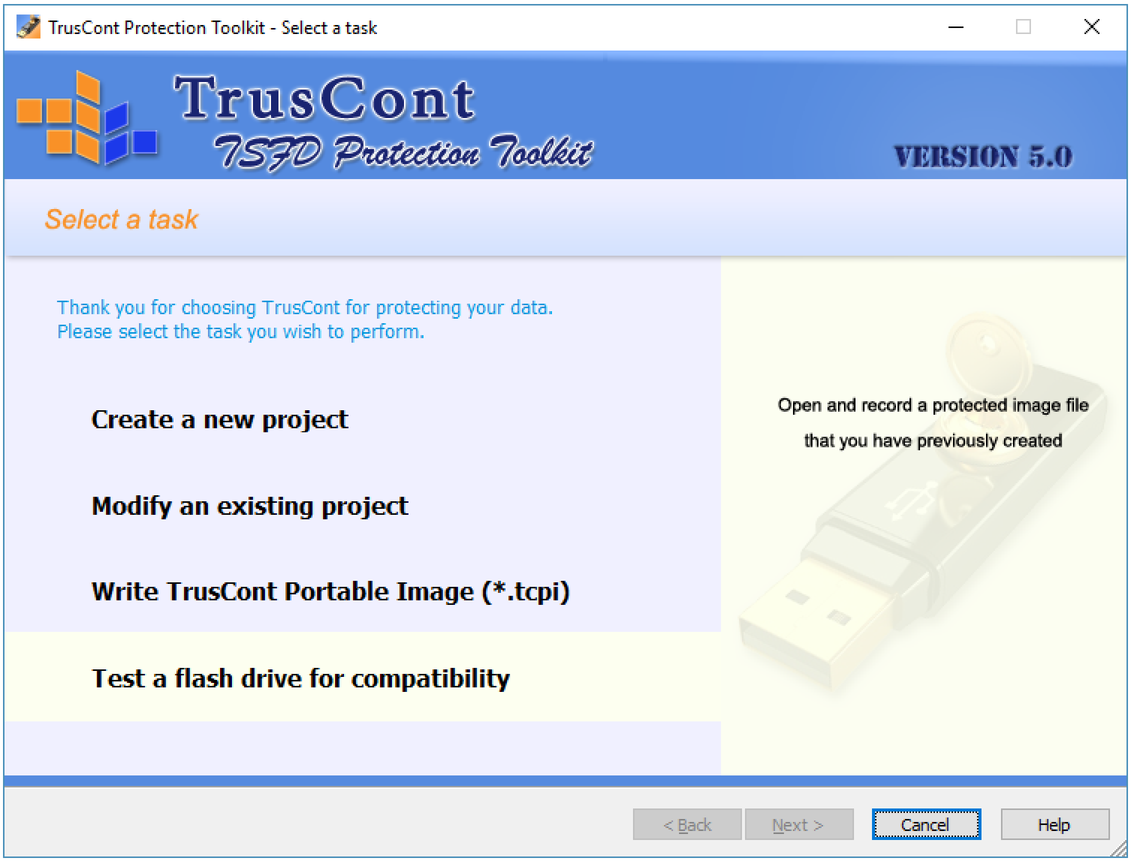
e. **Parametric path mask for allowing save operations without notifications** – List all paths for which the Toolkit will not display any notification even if the saved file has an extension included in the list of the previous section (d).

f. **Parametric path mask for allowing overwrite of existing files** – List all paths for which the Toolkit will allow overwriting of existing files. By default the copy protection doesn't allow overwriting of protected files because all writes are encrypted. Overwriting existing files with encrypted data makes the files invalid. You should include in this path list only locations that do not contain important files that your application may overwrite.

g. **Block network access for this application** – Specify whether or not you wish your application to have network access when reading protected files. Block network access if you suspect that your application may allow transmission of data read from protected files through a network connection.

Appendix B – Testing a Flash Drive for Compatibility

TrusCont USB Copy Protection requires compatible USB Flash Drives. The TSFD Protection Toolkit enables publishers to apply the copy protection on 3rd party USB flash drives. However, it is highly recommended to use TrusCont Secure Flash Drives which offer the highest compatibility, copy protection level, and stability.



Thank you for choosing TrusCont for protecting your data.
Please select the task you wish to perform.

Create a new project

Modify an existing project

Write TrusCont Portable Image (*.tcpi)

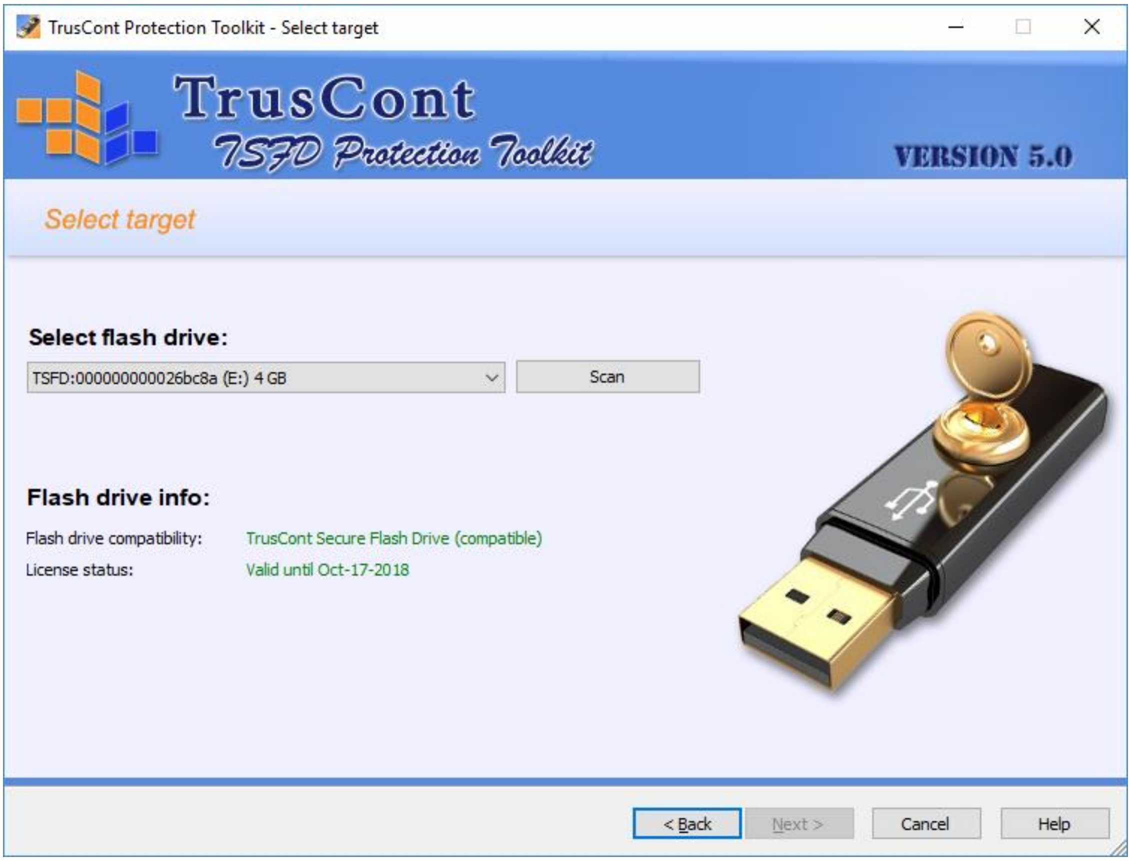
Test a flash drive for compatibility

Open and record a protected image file that you have previously created

Figure 31: Testing a flash drive for compatibility

To test a flash drive for compatibility:

1. Open the TSFD Protection Toolkit
2. Connect the USB Flash Drive(s) that you wish to test
3. Select the option 'Test a flash drive for compatibility'
4. All detected USB Flash Drive are listed on the drop down list box. Select a flash drive from the list in order to view its compatibility level and license status.
5. If your USB Flash Drive is not listed, make sure it is connected and the PC detects it, then click 'Scan' to refresh the list.



Select flash drive:

TSFD:000000000026bc8a (E:) 4 GB

Flash drive info:

Flash drive compatibility: TrusCont Secure Flash Drive (compatible)

License status: Valid until Oct-17-2018

Figure 32: Compatibility test report

Possible compatibility levels

Status	**Meaning**
TrusCont Secure Flash Drive	The selected USB Flash Drives is either a TrusCont Secure Flash Drive, or a compatible USB Flash Drive which was already programmed and has a valid USB Copy Protection license
Compatible	The Selected USB Flash Drive may be compatible. See remarks below.
Incompatible	The selected USB Flash Drive is incompatible and cannot be used with TrusCont USB Copy Protection.

Remarks

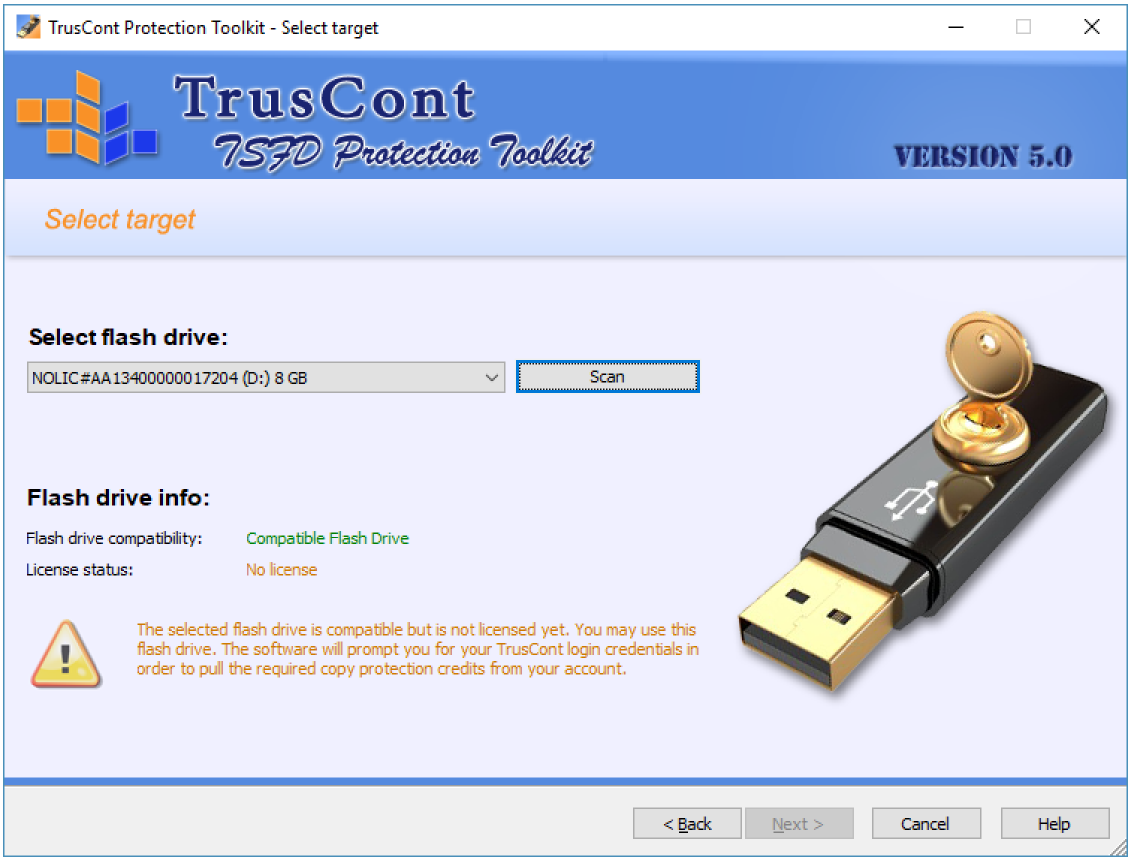
- This feature is provided as a mean for testing potential compatibility. There is no guaranty that a flash drive reported as compatible will be usable with the software without actually trying to apply the copy protection on it.

- It is likely that a 3rd party USB Flash Drive reported as compatible will be 100% functional and compatible with TrusCont USB Copy Protection. However, some 3rd party USB Flash Drives that are reported as compatible may still exhibit the following problems:
    - Limited functionality – incompatibility with specific partition configurations, the write protection, or the copy protection features of the software.
    - Failure to write to the USB Flash Drives
    - Missing or corrupted data even after a successful write
- A batch of USB Flash Drives can contain both compatible and incompatible flash drives, even if all the flash drives are of the same brand and model. USB Flash Drive manufacturers often change parts and firmware versions during a product lifetime without necessarily changing its model, part number, etc..

The license status

In addition to the compatibility level, the software also reports the license status of the USB Flash Drive:

Status	**Meaning**
Valid until [date]	The selected USB Flash Drive has a valid copy protection license and can be used to protect files. The reported date is the date in which the license will expire.
Expired	The Selected USB Flash Drive contains a license which has already expired. The license status doesn't affect end users in any way. The protected files it may contain are still protected and usable. The license has to be renewed only if there is a need to protect new data and update/overwrite the selected USB Flash Drive.
No license	The selected USB Flash Drive is potentially compatible with the software but doesn't contain a valid license yet. Using the selected USB Flash Drive with the software for the first time will require you to enter your TrusCont account credentials. The software will then pool 1 USB Copy Protection credit from your account and apply a new license to the flash drive.
N/A	The selected USB Flash Drive is incompatible with TrusCont USB Copy Protection.



Select flash drive:

NOLIC#AA13400000017204 (D:) 8 GB

Flash drive info:

Flash drive compatibility: Compatible Flash Drive

License status: No license

The selected flash drive is compatible but is not licensed yet. You may use this flash drive. The software will prompt you for your TrusCont login credentials in order to pull the required copy protection credits from your account.

Figure 33: The license status

Appendix C – Adding support for custom file types

By default TrusCont software allows you to protect common files types that were tested with TrusCont copy protection. The default list includes more than 300 different file types.

If you wish to protect proprietary, or other file formats that are not included in the default list please follow these instructions:

*** Warning: TrusCont cannot guaranty that files of types that are not included in the default list will be readable after protecting it. Carefully test that your files are readable by the applications in which they are intended to be used before publishing.**

1. Open Windows File Explorer and navigate to the folder in which the TSFD Protection Toolkit is installed. The default folder in 64 Bit Windows is: "C:\Program Files (x86)\TrusCont\TSFD Protection Toolkit". The default folder for 32 Bit Windows is "C:\Program Files\TrusCont\TSFD Protection Toolkit"

2. Copy the file tcpm_custom.ini to your desktop and open it for editing using Notepad or other text editor.

3. Replace all XXX occurrences with the extension of the file that you wish to protect. If you wish to add support for multiple file types then list all extensions separated by a semicolon. For example, in order to add support for the file types QQQ, WWW, and EEE, replace XXX with: .QQQ;.WWW;EEE

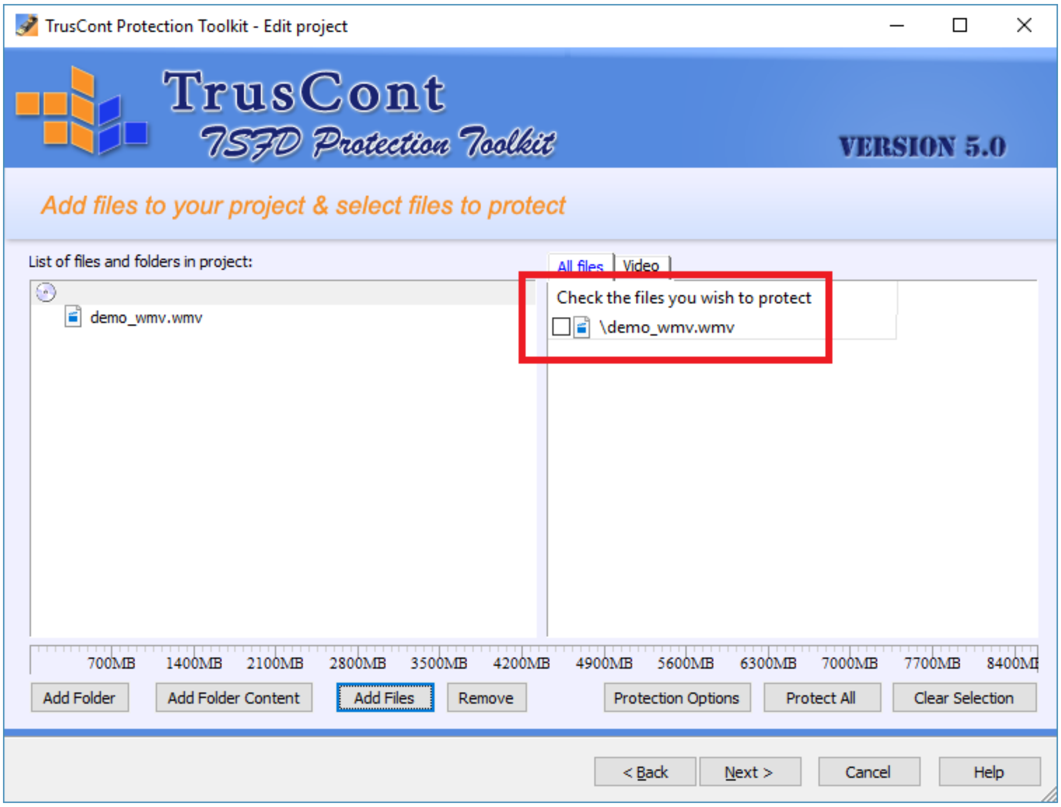
4. Save the file and copy it back to its original location and overwrite the original file.

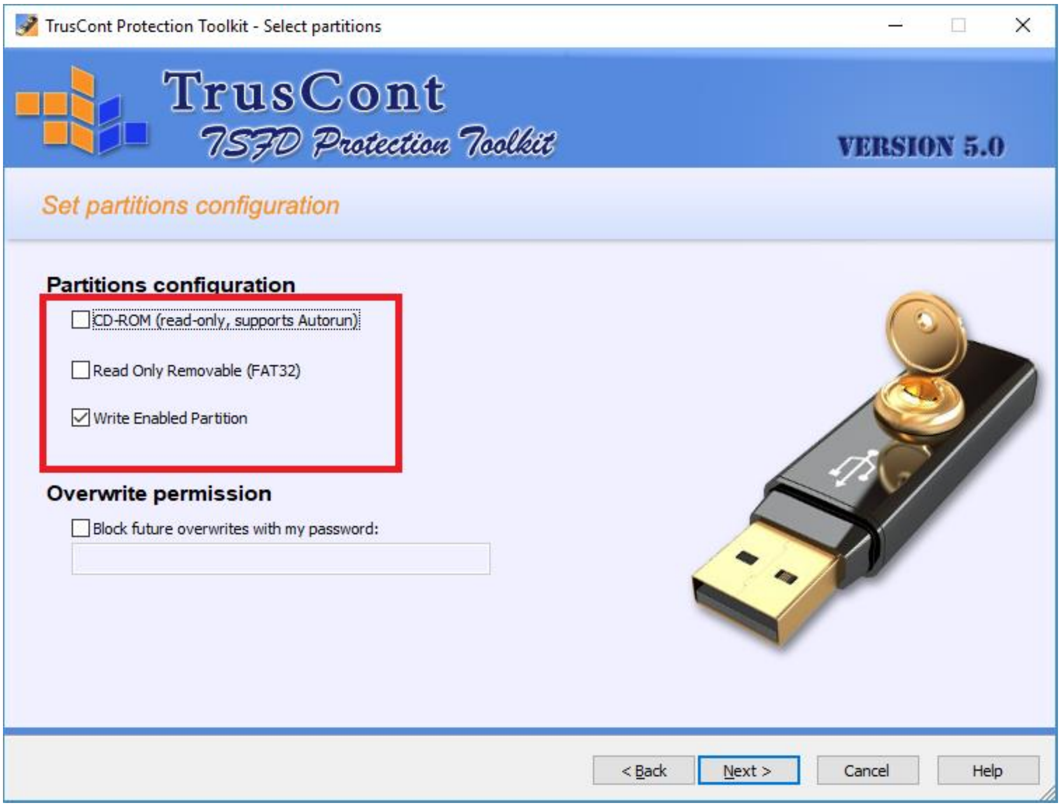
Appendix D – Formatting TrusCont Protected Flash Drives

The TSFD Protection Toolkit automatically repartition and formats the flash drive for you before recording new content. However, if you wish to remove the write protection of a previously protected flash drive you can use the TSFD Protection Toolkit to record something on a write enabled partition, then format it using Windows.

Important: If the flash drive was protected by an overwrite permission password you will need to have the password in order to perform this process.

1. Open the TSFD Protection Toolkit and create a new project.
2. Add a file to the project.
3. don't check any files to be protected (see 1st screenshot below), and record on a write enabled partition (see 2nd screenshot below – check 'Write Enabled partition' and only then uncheck 'CD-ROM')
4. When done – remove the flash drive from the PC, and then plug it back in
5. The flash drive should be unlocked now. You may Format it using Windows Explorer.





TrusCont Protection Toolkit - Select partitions

Set partitions configuration

Partitions configuration

□ CD-ROM (read-only, supports Autorun)

□ Read Only Removable (FAT32)

☑ Write Enabled Partition

Overwrite permission

□ Block future overwrites with my password:

Additional Support Information

TrusCont Ltd,
31 Weizman Street
Qiriat Bialik 2701212
Israel

Email: support@truscont.com

Tel: +1 720 477 6632 (US)
Tel: +44 2070482882 (UK)
Tel: +972 4 832 0555 (Israel)
Fax: +972 4 832 0550 (Israel)
https://www.truscont.com