TrusCont

Trusted Content Delivery

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

TrusCont™

Virtual Disk 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 using virtual disks.

This manual focuses on the TrusCont Virtual Disk Protection (VPD) Toolkit software which is used to copy protect software and data for distribution on virtual disks.

1.1 Key Features

- Powerful diskless copy protection
- One virtual disk file can be licensed to numerous recipients using activation codes. Each of which can be assigned a different expiration date.
- Ability to revoke, suspend, renew each activation code individually.
- 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.
- Password protection.

1.2 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.

2. How does it Work?

Using the VDP Toolkit you create a virtual disk file that contains the files you wish to publish. You can then deliver it to your customers using any file sharing service. The virtual disk is protected and cannot be used by anyone without getting an activation code from you. Therefore, it is safe to make it publicly available for download.

End users need to download and install the TrusCont Virtual Drive Manager (if they haven't previously done it) from this link: https://www.truscont.com/vdm

Then end users can download the virtual disk file, and double click it to mount it on their PC. When accessing the protected files on the virtual disk for the first time each end user will be required to enter his activation code.

By default each activation code can be used to access the virtual disk on a single PC. Following activation end users can use the files on the virtual disk but cannot make any copies of it.

To issue and manage activation codes login to your account on the TrusCont License Management System (https://www.truscont.com/license). You control for how long each end user is allowed to use your files by setting a term in days, months and years for each code you create. You can suspend, revoke, renew/reset, activations of each code and also add additional activations for allowing access to the virtual disk from additional PCs using the same code.

3. 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.

3.1 Software Protection

A program file protected by TrusCont will run and function normally exactly as its unprotected origin as long as the virtual disk on which it was originally delivered is mounted to the local PC.

If the virtual disk is not mounted then the protected program file will not run. Instead, a message requesting the end user to mount the virtual disk will be displayed. This message can be customized (*5.3.2 Program Files Protection Settings*).

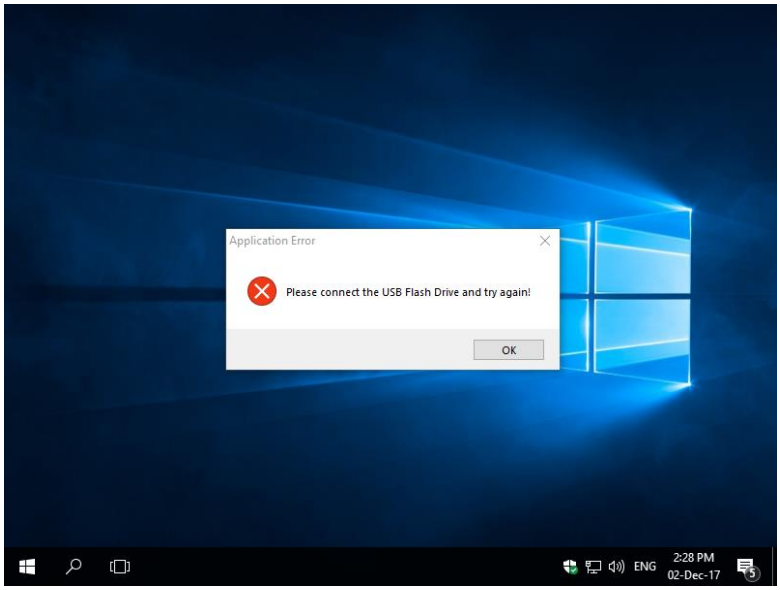

Figure 1: Running a Protected Application While the Virtual Disk is Unmounted

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 Virtual disk can contain multiple protected files. Each file may be protected with a different password.

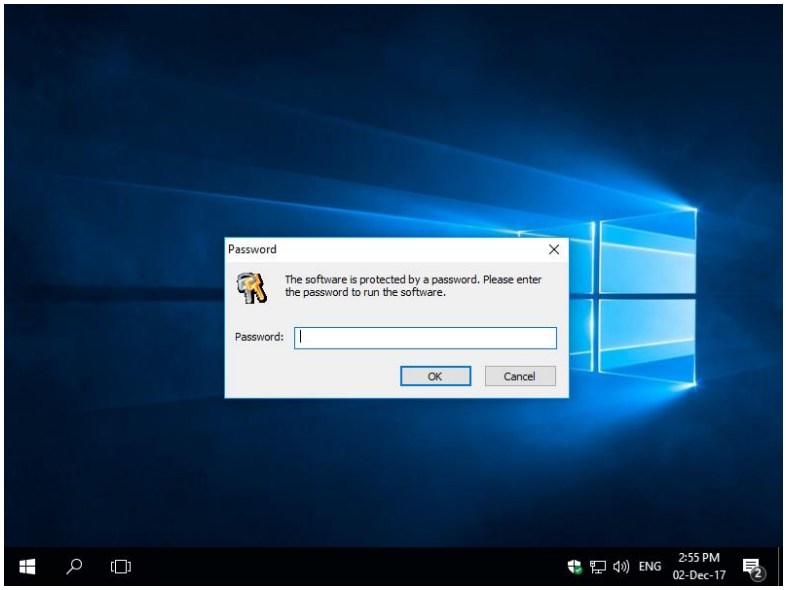

Figure 2: Protecting Program Files with a Password

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 Virtual disk may contain multiple protected files. Each file may have a different expiration date and time limit settings.

3.2 Data Files Protection

3.2.1 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 VDP Toolkit automatically adds a small Autorun file to your virtual disk. 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.

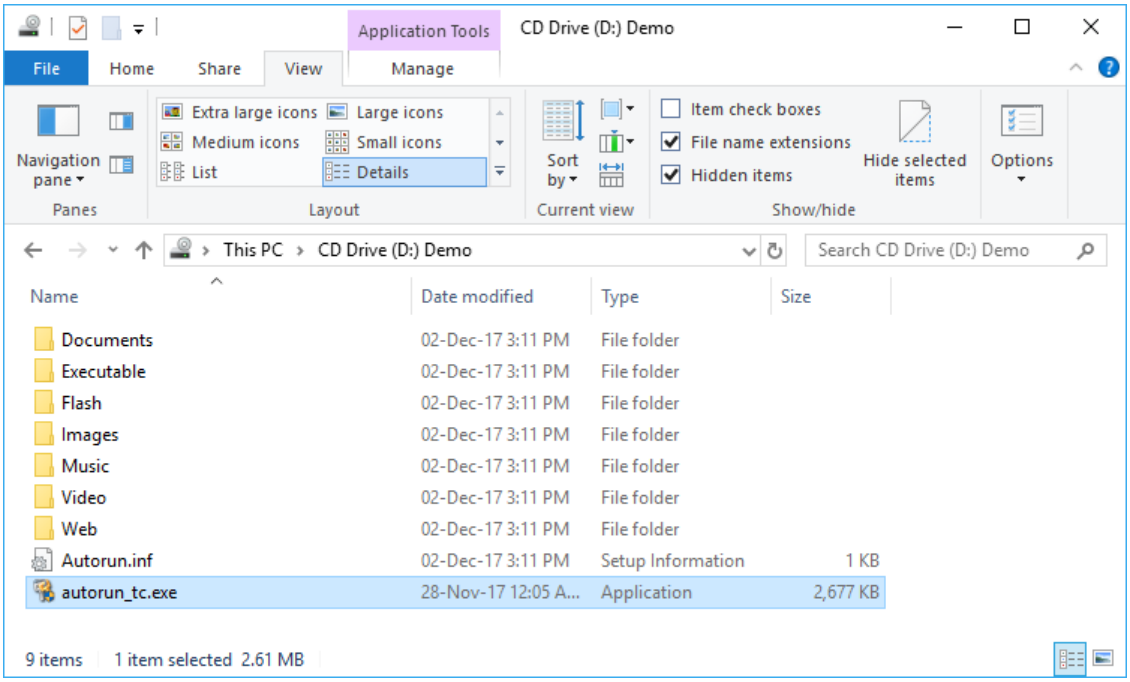

Figure 3: The TrusCont Autorun File

When the TrusCont Autorun file loads it looks for the virtual disk on which your protected data files are stored. If the virtual disk is mounted on 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 virtual disk. 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 virtual disk is not affected.

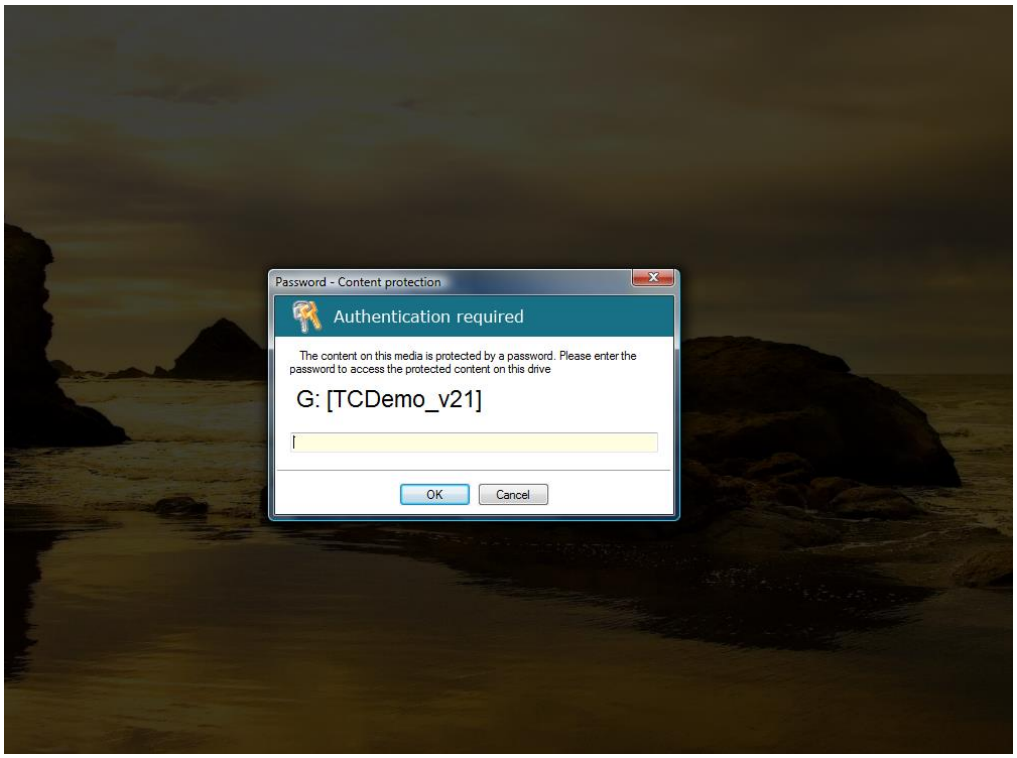

Figure 4: Global Password Dialog

3.2.2 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 (*5.4.6.2 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 virtual disks*.

*** Warning: Publishers that customize the list of allowed applications (whether explicitly or by storing the applications on the same virtual disk) 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.
- 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.

Figure 5: Tray icon notification on prohibited operation

3.3 Local Administrator Rights

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

Important note: by default all home users have local administrator rights. In some corporate environments users may have restricted accounts. TrusCont requires the end users to have only local administrator rights, administrator rights for the network is not required.

4. Using TrusCont VDP Toolkit

Make sure you always use the latest version of the VDP Toolkit. The latest version of the VDP 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 VDP 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.

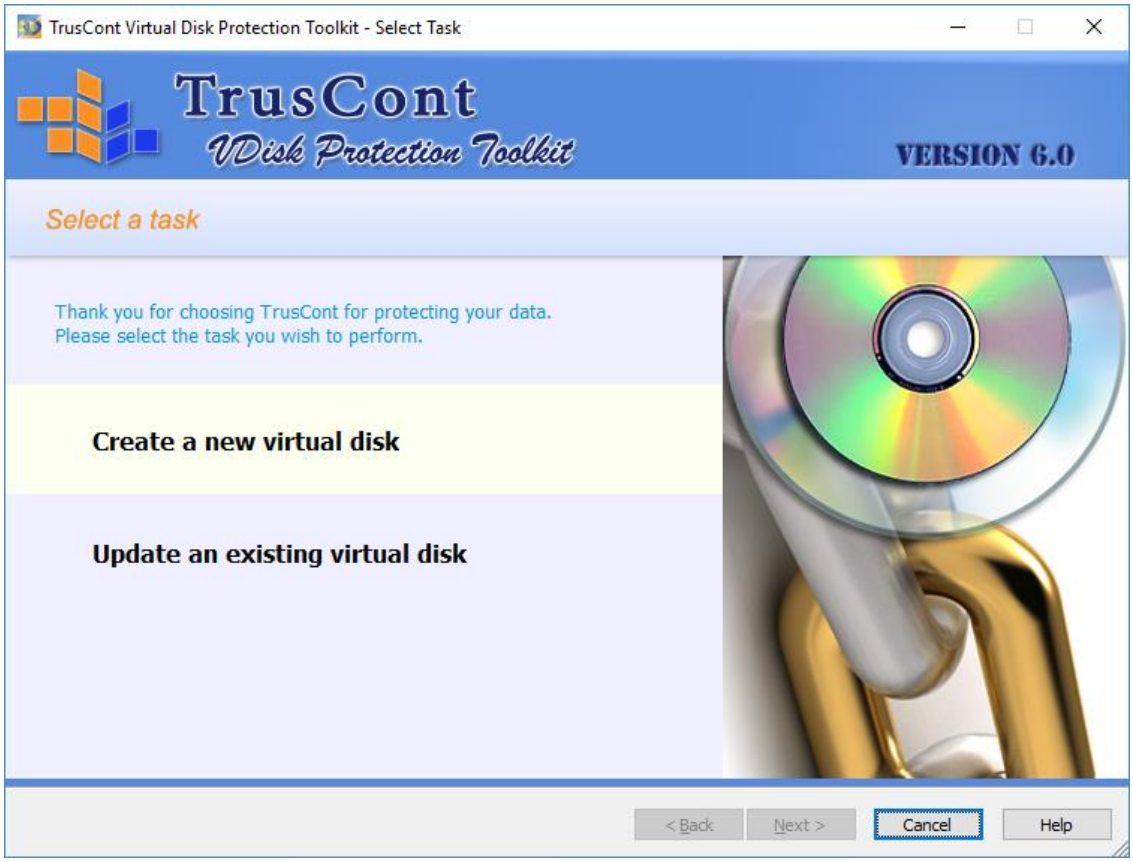

Figure 6: The main page of the VDP Toolkit

The VDP 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.

5. Creating a New Virtual Disk

5.1 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 virtual disk.

- ☑ Do not use files that are already protected – Protected files from a previously protected virtual disk cannot be stored on new virtual disks. Using protected files in virtual disks will result in virtual disks containing unreadable or corrupted files.

- ☑ Verify the functionality of your title – The virtual disk protection process doesn't change the functionality of your files in any way. Verify that your title works as planned before using the VDP Toolkit. Protected virtual disks are write protected. 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 virtual disk 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.

5.2 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 are adding to your virtual disk. The right panel contains a check list of the files on your virtual disk that can be protected, allowing you to choose which files you wish to protect and set the desired protection options.

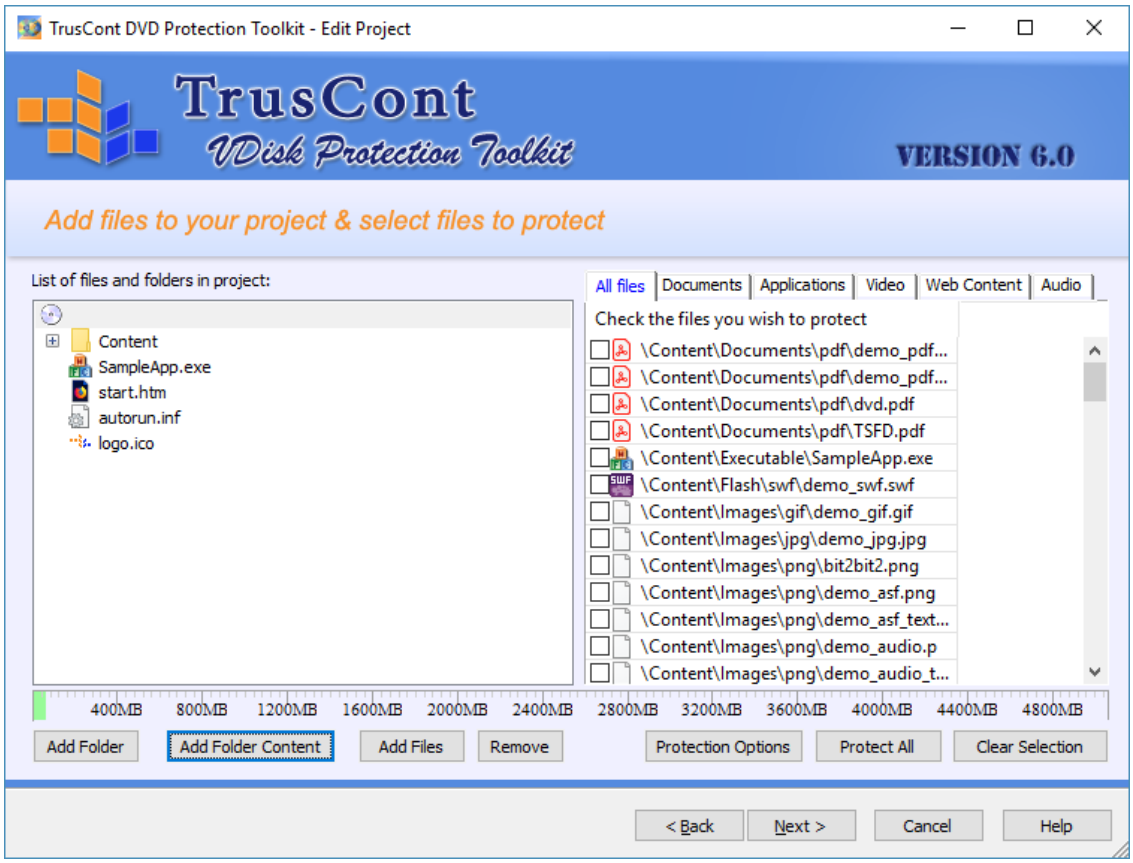

Figure 7: The Edit Project Page

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.

5.2.1 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.

5.2.2 Adding Folder Content

To add to the virtual disk 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 *5.1 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.

5.2.3 Adding Files

To add individual files to your virtual disk 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'.

5.2.4 Removing Files and Folders

To remove files or folders from the virtual disk, 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.

5.3 Setting Copy Protection Options

5.3.1 Select the files you wish to protect

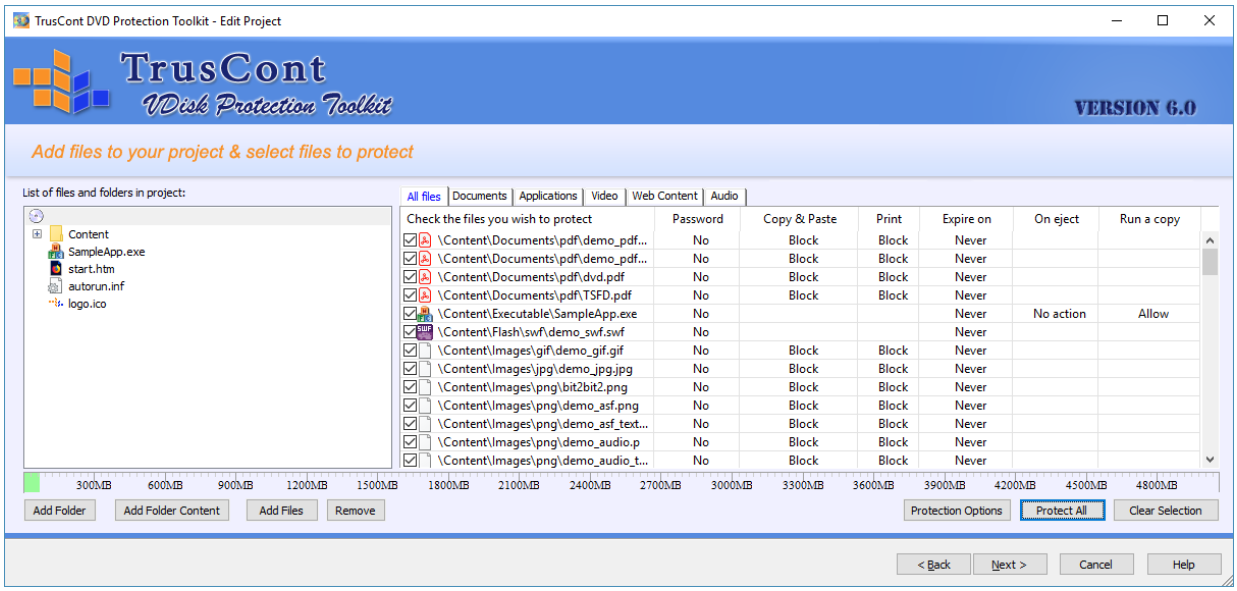

Figure 8: Setting copy protection options

Files added to the virtual disk 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 creating your virtual disk:

☑ 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 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 B – 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.

5.3.2 Program Files Protection Settings

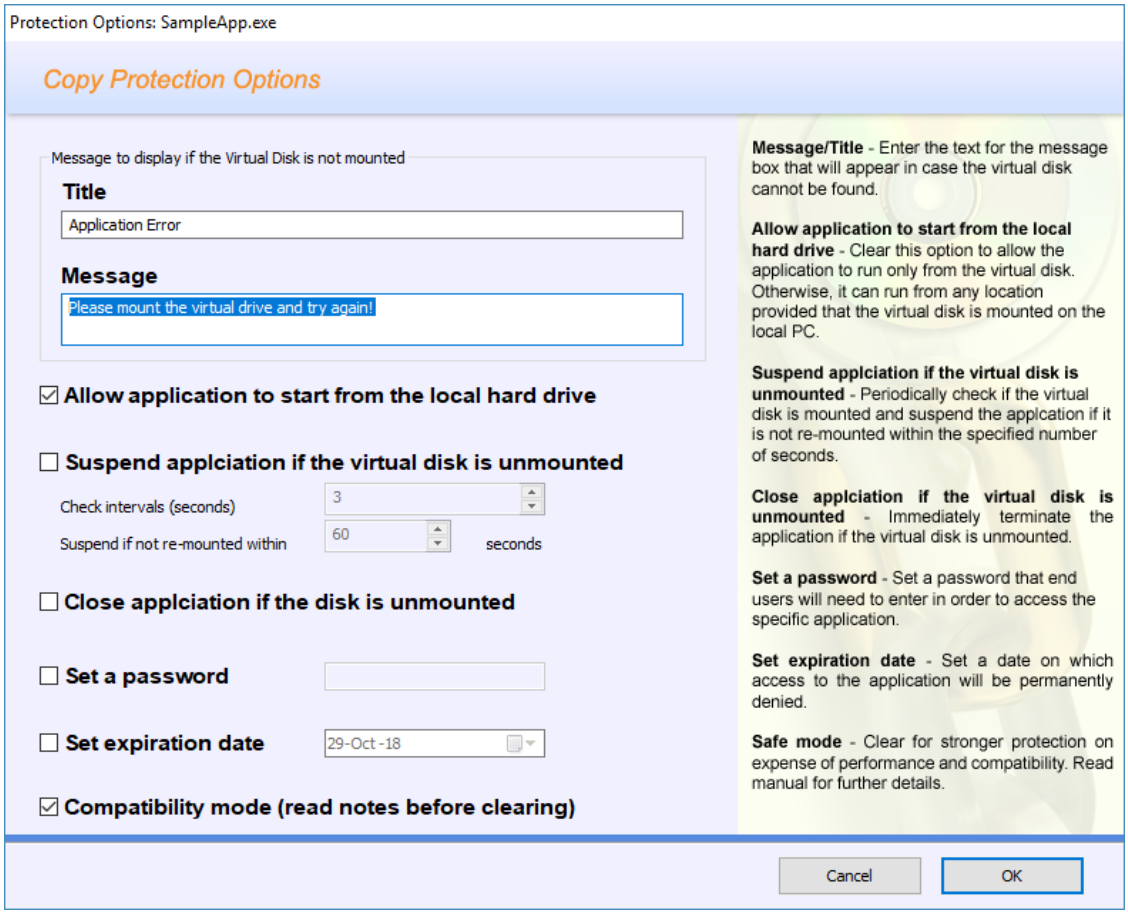

Figure 9: Copy protection options for program files

> **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 while the virtual disk in unmounted
Default	Title: Application Error Message: Please mount the virtual disk 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 virtual disk must be mounted on 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 virtual disk itself.
Default	Enabled (allowed)

Setting	**Suspend application if the virtual disk is unmounted**
Description	Periodically checks if the virtual disk is unmounted while the protected application is running. If the virtual disk is not re-mounted within the specified number of seconds the application is suspended and a message asking the end user to mount the virtual disk is displayed
Default	Disabled

Setting	**Close application if the virtual disk is unmounted**
Description	Immediately close the protected application if the virtual disk is unmounted.
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	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 processes 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 is 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 *5.4 Project options* for further instructions on enabling this option.

5.3.3 Data Files Protection Settings

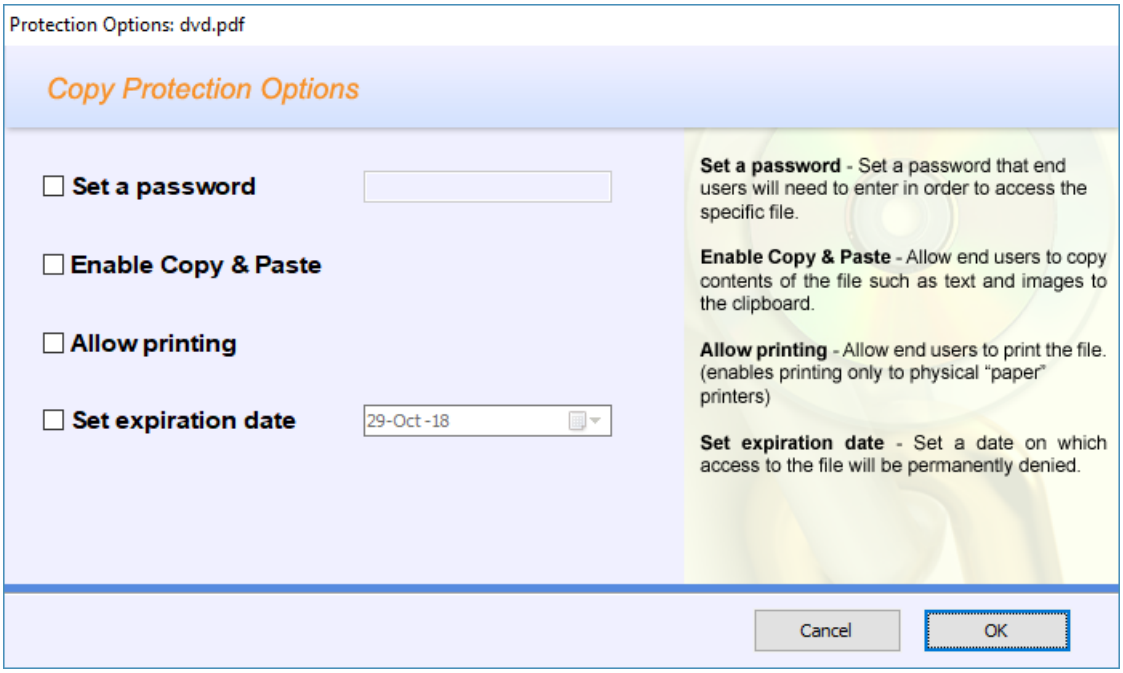

Figure 10: Data files protection options

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

Note: By default the expiration date is 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 *5.4 Project options* for further instructions on enabling this option.

5.4 Project options

Figure 11: The Project Options Page

5.4.1 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 virtual disk among other drives that exist on their local PC. The volume label may contain only English characters and numbers.

5.4.2 Use External Time Source Only

Expiration dates 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 retrieves 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 was not applied to at least one file of your virtual disk then this option will be disabled and grayed out.

5.4.3 Rename TrusCont Autorun File

When protecting data files that are not EXE program files the software automatically adds to your virtual disk the TrusCont Autorun file (refer to section *3.2.1 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 virtual disk then this option is disabled and grayed out.

5.4.4 Set a Global Password

Enable this option to provision access to all protected data files on your virtual disk 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 virtual disk then this option is disabled and grayed out.

5.4.5 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 Virtual disk, and the performance of 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 virtual disk. 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 virtual disk then this option is disabled and grayed out.

5.4.6 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 virtual disk options page.

5.4.6.1 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 *3.2.2 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).

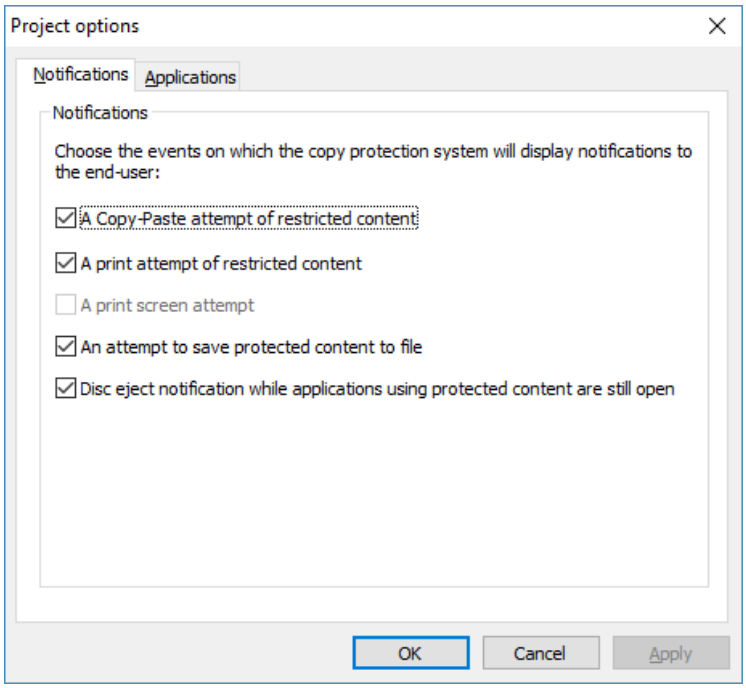

Figure 12: Enabling and Disabling Content Protection Notifications

5.4.6.2 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 stored on the specific virtual disk.

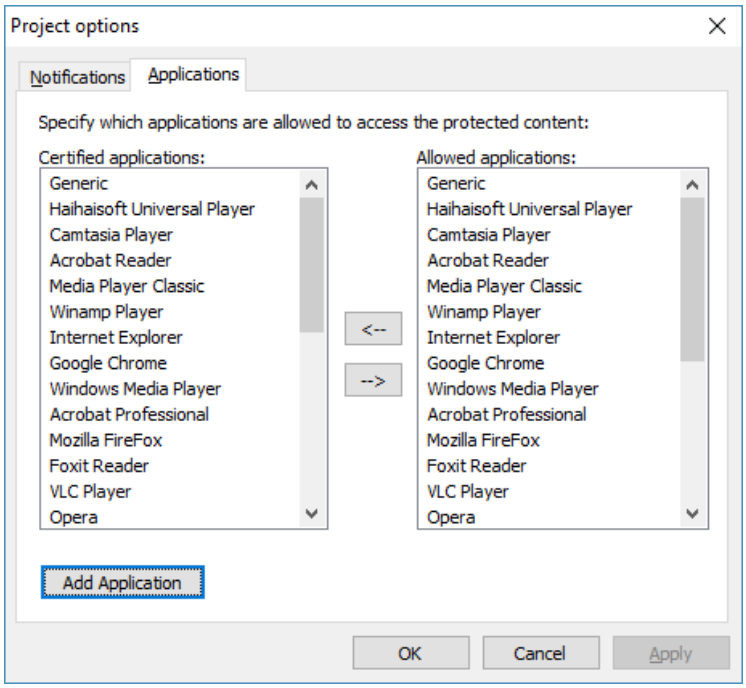

Figure 13: The default list of allowed applications

To deny access of a specific application 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 product (for further instructions please refer to *Appendix A – Customizing 3rd Party Applications Support for Content Protection*).

5.5 Saving the Virtual Disk

Click next on the project settings page to proceed to the login page.

Figure 14: The Login Page

The software requires you to login in order to proceed. The next button on this page is grayed out until you successfully login. You may check the 'Remember me' option before clicking the Login button if you want the software to remember your login credentials.

Enter the email and password of your TrusCont account and click the Login button. Then click next to proceed.

Click the Browse button and specify the location and filename for saving the virtual disk file. Finally, click next to complete the process and wait for the software to finish saving the virtual disk file.

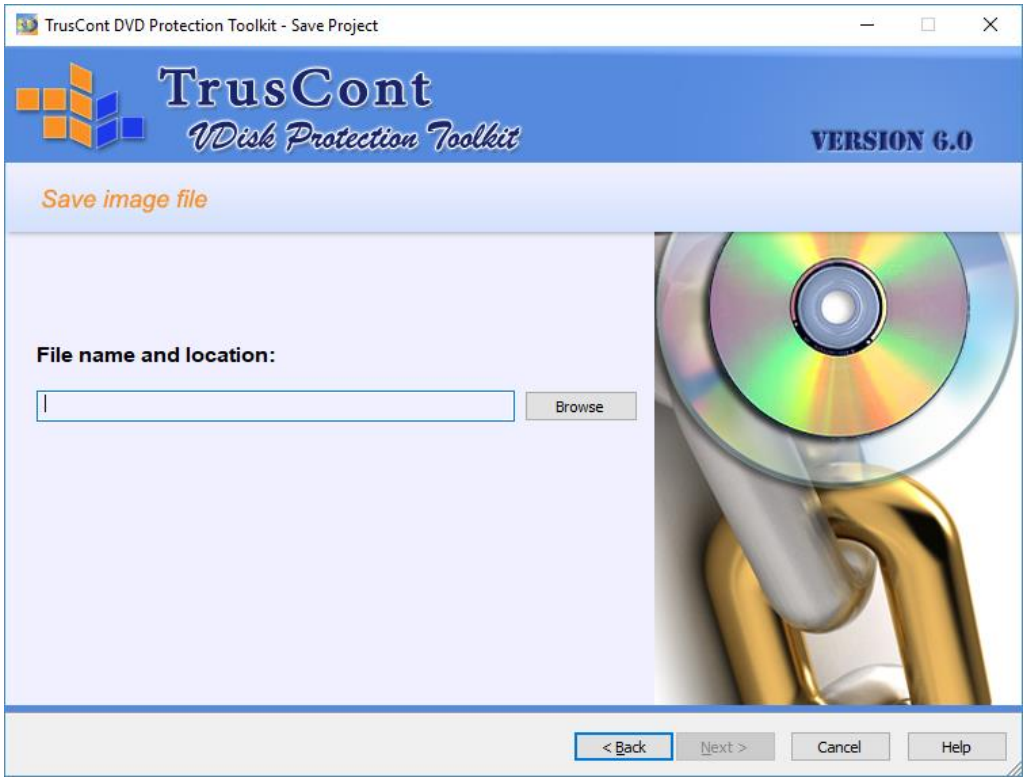

Figure 15: Specifying Filename and Location for Saving the Virtual Disk

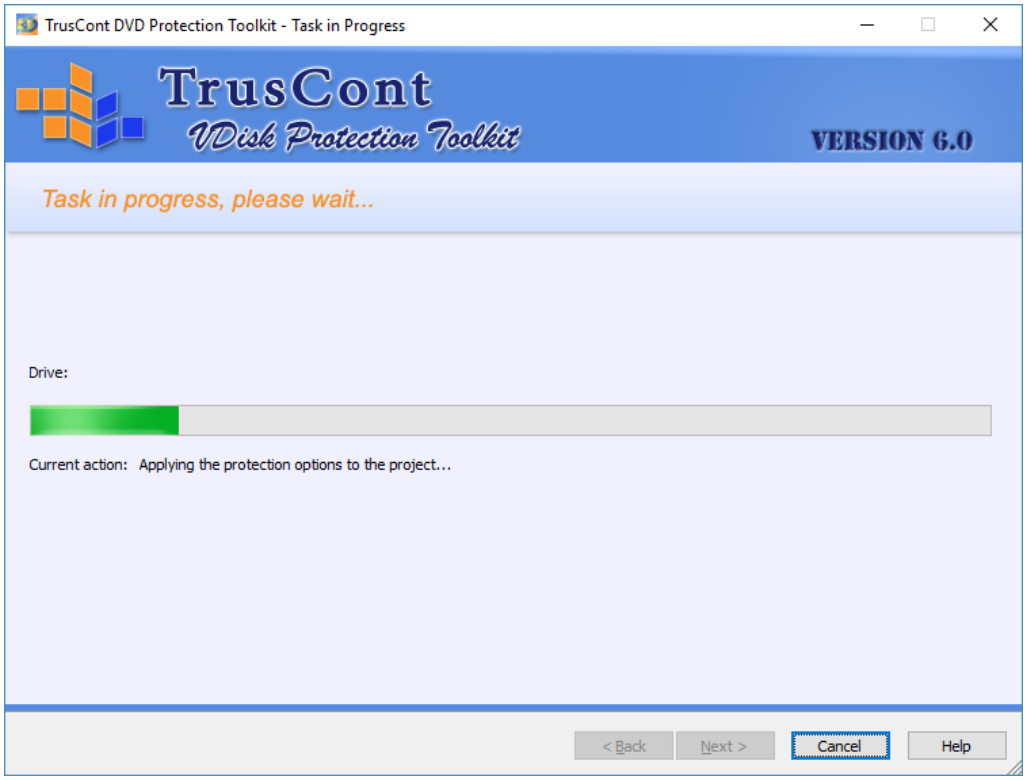

Figure 16: The Virtual Disk Saving Process

6. Delivering the Virtual Disk to End Users

You may deliver the virtual disk file to your customers any way you want. It can be delivered on offline media such as USB flash drives, or online by making it available for download via the Internet or a private network.

6.1 Uploading the Virtual Disk

In order to deliver the virtual disk to customers online you will need to make it available for download. You can upload it to your own website, or use any online / cloud file sharing service such DropBox, OneDrive, Google Drive, Amazon S3, WeTransfer, etc.

There is no problem making the virtual disk file publicly available for download since it is protected and cannot be used by anyone without getting an activation code.

6.2 Issuing Activation Codes for End Users

A. Open your favorite Internet browser and navigate to https://www.truscont.com/license

B. Login and then click the 'Virtual Disk Publishing' link on the top menu

C. A list of the virtual disks you have created will appear. The default name of each virtual disk is its volume label followed by the date and time on which it was created (UTC).

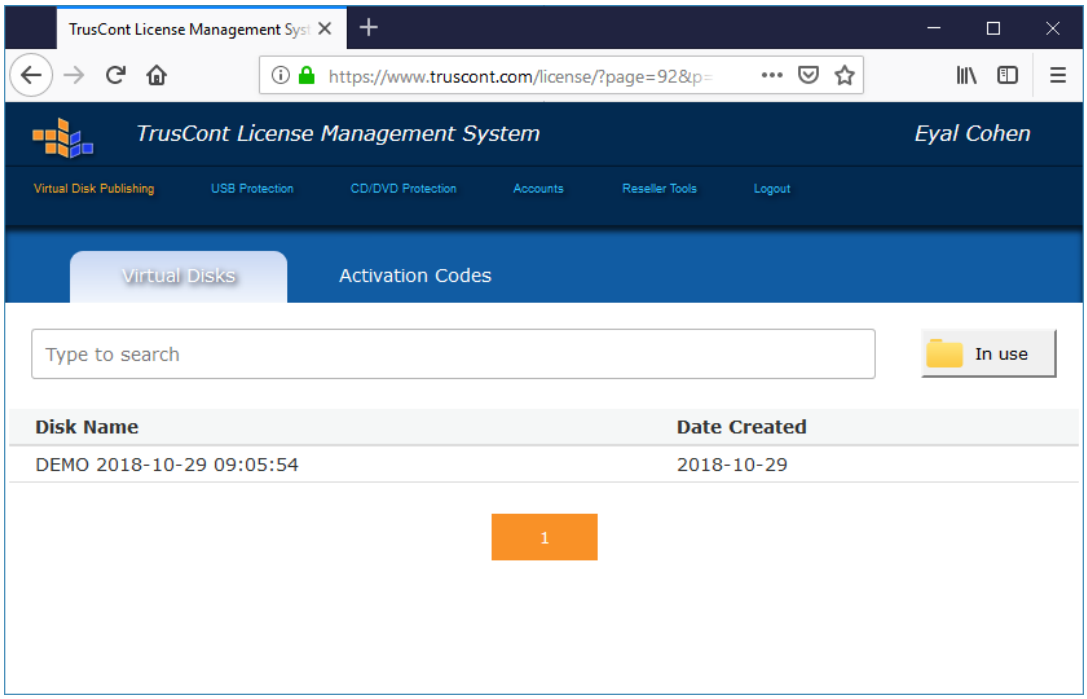

Figure 17: The Virtual Disks List

D. Click the virtual disk for which you wish to create activation codes. The following window will appear

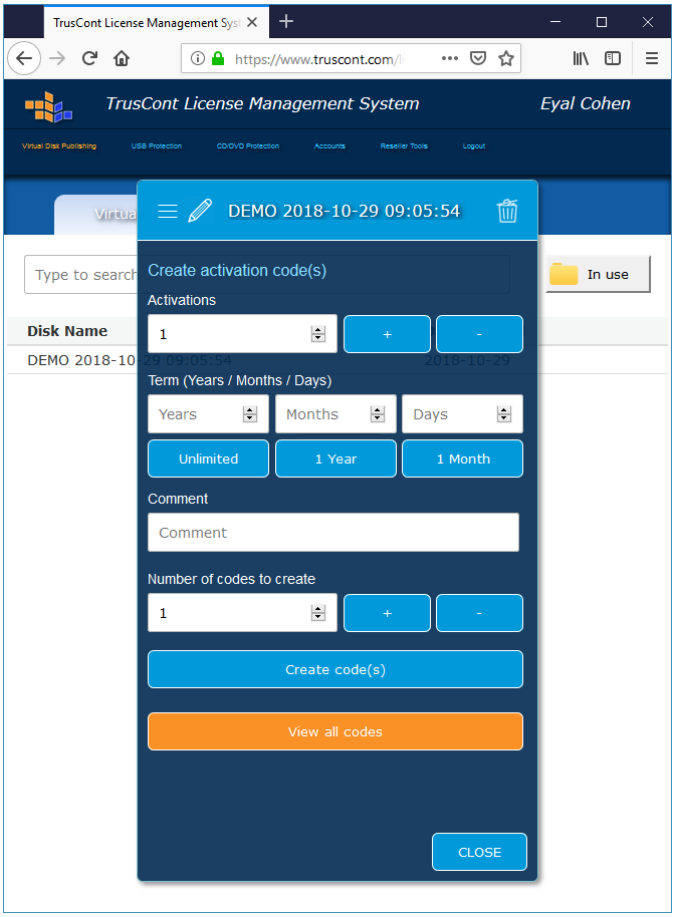

Figure 18: Create Activation Codes Form

E. Enter the number of activations you wish to assign to the activation code. Each activation enables the end user to use the virtual disk on one PC. The default is 1.

F. Enter the license term in days, months, and years. At the end of the term the specific activation code will expire and the specific end user will no longer be able to access the protected files on your virtual disk. You may also use the preset buttons to set the term to 1 month, or 1 year, or unlimited (99 years).

G. Optionally enter a comment such as customer name, order number or any other reference that will help you identify the specific user / code in the future.

H. If you wish to create multiple codes with identical comment, term, and number of activations then set the 'Number of codes to create' value to the required number of codes.

I. Finally, click 'Create code(s)'. The new code will appear on the screen. If you wish to view all codes you have previously created for the specific virtual disk then click the virtual disk and then click the orange 'View all codes' button.

6.3 Accessing the Virtual Disk – Instructions for End Users

A. Download and install TrusCont Virtual Drive Manager. This is required only once – there is no need to install it before accessing additional virtual disks. The latest version can be downloaded via the following link:

   https://www.truscont.com/vdm

B. Download and open the virtual disk file. If you have received the file on offline media then double click it to open.

C. Enter your activation code when prompted.

D. A new virtual drive will appear on your PC containing the protected files.

6.4 Managing Activation Codes

TrusCont Virtual Disk Publishing allows you to control each of the activation codes you issue independently. You can temporarily suspend activations, permanently revoke an activation, add additional activation to existing codes, and change the activation term.

6.4.1 Browsing and Searching for Activation Codes

A. Open your favorite Internet browser and navigate to https://www.truscont.com/license

B. Login and then click the 'Virtual Disk Publishing' link on the top menu

C. To view all activation code you issued for a specific virtual disk, click the virtual disk from the list and then click the orange 'View all codes' button.

D. To view all issued activation codes for all the virtual disks you have created click the 'Activation Codes' tab.

E. You can search for a specific activation code or comment by typing it in the search bar.

F. You can further filter search results by activation status by clicking the button next to the search bar.

6.4.2 Suspending and Resuming Activations

Suspending an activation code temporarily blocks access to the protected files stored on the virtual disk from all the PCs on which the disk was activated using the specific code. Access is blocked only the next time the user tries to access the virtual disk while being online and remains blocked until the activation is resumed.

To suspend / resume an activation code click the specific code from the activation codes list and then click the 'Suspend / resume' button.

6.4.3 Permanently Revoking Activations

Revoking an activation code permanently revokes entitlement to the protected files stored on the virtual disk for all the PCs on which the disk was activated using the specific code. Revoking an activation code is irreversible. If a PC/user needs to be re-entitled a new activation code needs to be issued. Access to the virtual disk is actually blocked only the next time the user tries to access the virtual disk while being online.

To permanently revoke an activation code click the specific code from the activation codes list and then click the trash bin icon on the title bar.

6.4.4 Adding Activations to Existing Codes

Adding activations to an existing code allows the code owner to activate the virtual disk on additional PCs. To add activations to an existing activation code click the specific code from the activation codes list, then specify the number of activations you wish to add and click the 'Add' button.

6.4.5 Resetting the Activation Term

To renew an expired activation code or resetting the term of an active code click the specific code from the activation codes list, then click the pencil icon on the title bar. Specify the new term in days, months, and years, then click the 'Reset term' button.

The new activation term is relative to the moment of setting it.

7. Updating Protected Virtual disks

TrusCont allows you to deliver updates to your customers without requiring them to re-activate the product.

A. Open the VDP Toolkit and select 'Update an existing virtual disk'.

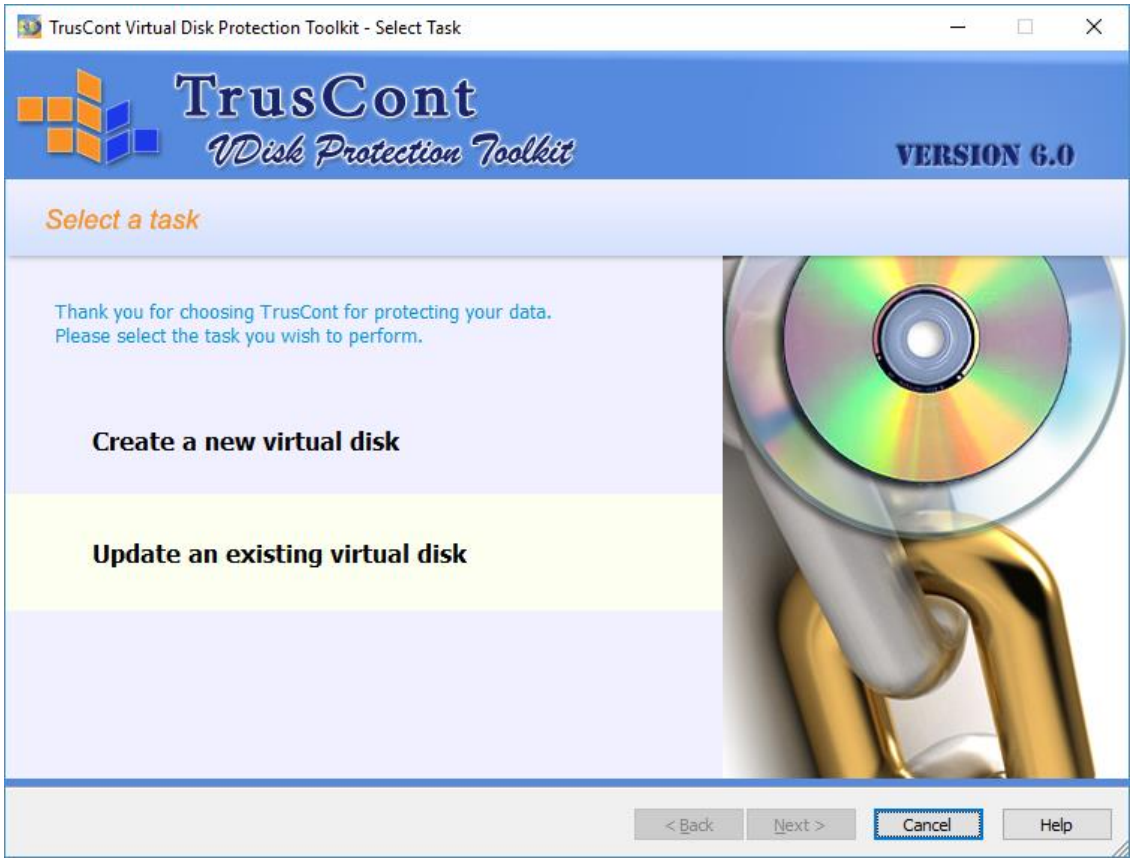

Figure 19: Updating an Existing Virtual Disk

B. Click 'Browse' and select the virtual disk file that you wish to update.

C. Follow the instructions in sections *5.2 Adding Files and Folders – 5.5 Saving the Virtual Disk*

D. This procedure doesn't change the original virtual disk file. It creates a new virtual disk file that you can deliver to your existing customer. Customers that have already activated the previous virtual disk will be able to access the updated virtual disk without the need to re-enter any activation codes.

E. Creating an updated virtual disk doesn't create a new record on your virtual disks list. To create new activation codes for it use the existing record of the original virtual disk (see section *6.2 - Issuing Activation Codes for End Users*).

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 the VDP Toolkit and create a new virtual disk.
2. Open the default list of allowed applications (see section *5.4.6.2 Default List of Allowed Applications*).

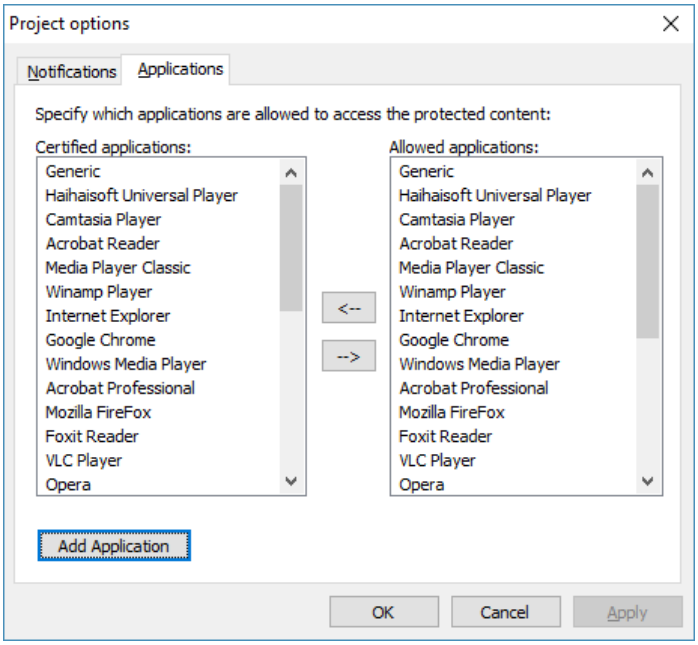

Figure 20: Certified Application List

3. Click 'Add Application'

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

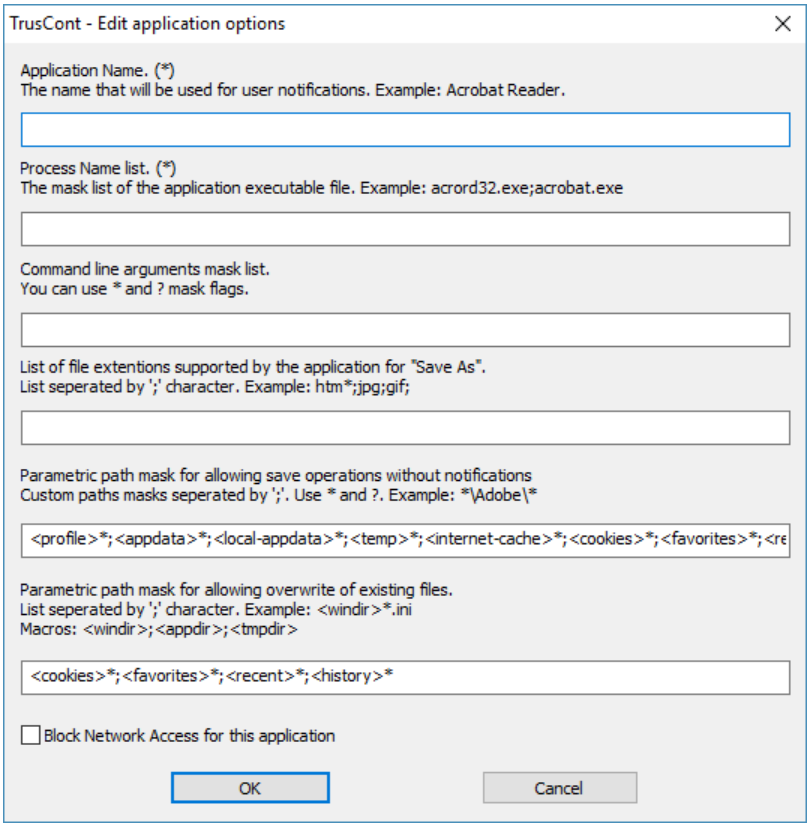

Figure 21: The Application Setup Form

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 mountion.

Appendix B – 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 VDP Toolkit is installed. The default folder in 64 Bit Windows is: "C:\Program Files (x86)\TrusCont\VDP Toolkit". The default folder for 32 Bit Windows is "C:\Program Files\TrusCont\VDP 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.

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