



# Blanco File Eraser

Administrator Manual for Version 8.3 (ref: 04062019)

# Definitions

Item	Explanation
<b>Batch file</b>	A batch file is a text file consisting of a sequence of commands to be implemented by the command interpreter (computer program).
<b>Command line</b>	The line on the display screen where a command is expected. Generally, the command line is the line that contains the most recently displayed command prompt.
<b>GUI</b>	Graphical user interface.
<b>HTML</b>	HTML, which stands for Hyper Text Markup Language, is the predominant markup language for web pages. It provides a possibility to create structured documents by denoting structural semantics for text such as headings, paragraphs, lists etc as well as for links, quotes, and other items.
<b>Parameters</b>	A parameter is the same as a command line argument. The argument essentially communicates how the program should perform and execute the commands.
<b>Scheduled Task Wizard</b>	Scheduled Task Wizard is a program included with the operating system. The name is self-explanatory considering its main feature is to schedule programs to run automatically.
<b>Shred</b>	A legacy term for erasing data securely. Means the same thing than “erase”.
<b>String</b>	String is a data type consisting of a sequence of characters. A string is often carried out as a word (byte).
<b>Wild-card</b>	A “wild-card” or a wild-card character can be used as a substitute for any other character in a string (see “string”).
<b>Windows Event log</b>	Windows Event log tracks every specific and noteworthy event that occurs on your computer, e.g. when it encounters an error. These logs can be viewed via the Windows Event Viewer.
<b>Windows Event Viewer</b>	Event Viewer is a component of Microsoft's Windows NT line of operating systems that lets administrators and users view the event logs on a local or remote machine.
<b>Windows registry</b>	Windows registry is a database used within Windows operating systems that stores configurations and option settings.
<b>XML</b>	eXtensible Markup Language is a markup language that defines a set of rules for interpreting documents.

# Table of Content

1	About the Solution.....	4
1.1	Installation .....	4
1.2	System requirements.....	4
2	Command line.....	5
2.1	Basic commands.....	5
2.2	Advanced commands.....	7
2.3	Erasure algorithms .....	9
2.4	Examples .....	9
3	Scheduling .....	11
4	Event Logging.....	14
4.1	Windows Event Viewer .....	14
5	Reporting .....	15
5.1	Different Report Formats.....	15
6	Configuration.....	16
6.1	License management .....	17
6.2	Connecting to Management Console automatically .....	19
6.3	Import Existing Report to Blancco Management Console via the Command Line .....	19
6.4	Importing reports manually into Blancco Management Console.....	20
6.5	Reporting settings .....	20
6.5.1	Changing the location of local erasure reports .....	20
6.5.2	Disabling reporting .....	21
6.5.3	Generating Reports in PDF Format.....	21
6.5.4	Disabling erasure on network drives.....	21
6.6	Handling Erasure of Previous Versions .....	21
6.6.1	Disabling Erasure of Previous Versions .....	21
6.7	Disabling Report Erasure.....	22
7	Activation Troubleshooting .....	23
8	Contact Information .....	24

# 1 About the Solution

This solution is optimized for secure erasure of selected files and folders in a corporate network. It can be used to erase specified paths or commanded with automated tasks using various rules. Detailed information of each erasure is stored into an erasure report. The report provides the unique proof that the erasure has been performed successfully.

The software includes graphical user interface (GUI) with full functionality, but the suggested solution is to use the command line option to schedule operations. This means the software will perform the erasure of files and folders in the background on selected machines.

The software is designed to work with Windows scheduling, and this document describes a concrete example of how to set up Windows scheduling.

Note: The user must at all times follow the guidance, procedures and practices described in the provided documentation and all guidance given by Blancco. Failing to do so might result in incorrect handling or configuration of the software, which in turn can result non-secure erasure result or incorrect configuration of the software.

## 1.1 Installation

The delivery contains an .exe installer. To start the installation process, run the executable. The license is a site license according to your contract. The license is activated using the GUI on the machine it is installed on. MSI installer can be requested as an option in your contract.

## 1.2 System requirements

Windows Server: 2012 R2, 2012 and 2008 all versions.

Windows 10, 8.1, 8 and 7 all versions.

Supported file systems are NTFS, FAT32 and exFAT.

Both 32 and 64 bit systems are supported.

The Blancco File Eraser software works on single machines or in a network. It is a Windows based solution and can erase selected files on both clients and servers.

Display resolution of 1024\*768 or greater.

Note that Management Console version 4.8 or newer is required, if report validation is required.

Certified and approved for Windows 8.1, Windows 8 and Windows 7.



## 2 Command line

### 2.1 Basic commands

The command line program is called **BlanccoFileEraserCmd.exe**.

Use the following parameters to achieve the desired operation. The parameters should be passed on to the operation according to the example above. Some operations require you to enter an algorithm – the available numerical representations are listed in section 0. Parameters listed in brackets “[ ]” are optional and not required for the operation.

Silent Shred files or folders (without the GUI). No report will be generated.	
Command	/ss algorithm [/force] [/leave] file [file...]
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
/leave	[optional] Indicates that the file should be erased but not deleted.
/force	[optional] Indicated that the file should be removed even a program is currently having it open. The file handles will be forcefully closed before erasure.
File	Specifies the file or folder to erase. Folders are erased recursively. More files can be specified, separated by space. The whole path should be specified, i.e. c:\temp.txt

**Note:** Force command requires administrator rights. When using the force command some stability issues may occur if you remove a file that another program is currently using.

**Note:** By beginning the command with **/ssbatch** a file will be called by the Blancco software instead of the direct erasure path. This file may contain multiple paths for erasing various files in different locations and is useful in more complex environments. Each erasure file path is listed as one row in this file.

Silent Shred files or folders (without the GUI). Report will be generated.	
Command	/ssl algorithm [/force] [/leave] [/log:logfilepath] [/loglevel:target] file [file...]
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
/leave	[optional] Indicates that the file should be erased but not deleted.
/force	[optional] Indicated that the file should be removed even a program is currently having it open. The file handles will be forcefully closed before erasure.
/log	[optional] Report file path can be specified as an optional parameter.
/loglevel	[optional] If set to <i>target</i> only the target of the operation will be reported and not each file in the operation.
File	Specifies the file or folder to erase. Folders are erased recursively. More files can be specified, separated by space. The whole path should be specified, i.e. c:\temp.txt

**Note:** Force command requires administrator rights. When using the force command some stability issues may occur if you remove a file that another program is currently using.

**Note:** By starting the command with **/sslbatch**, a file will be called by the Blancco software instead of the direct erasure path. This file may contain multiple paths for erasing various files in different locations and is useful in more complex environments. Each erasure file path is listed as one row in this file. One report will be created for all erasure operations regardless of the amount of file paths listed in this file.

Silent Shred files or folders from target file (without the GUI). No report will be generated.	
<b>Command</b>	/ssbatch algorithm batch_file [/force] [/leave]
<b>Flags</b>	
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
<b>/leave</b>	[optional] Indicates that the file should be erased but not deleted.
<b>/force</b>	[optional] Indicated that the file should be removed even a program is currently having it open. The file handles will be forcefully closed before erasure.
<b>batch_file</b>	A file containing the files to erase. The file should contain whole paths. One path per line. The whole path to the batch file should be specified, i.e. c:\batch.txt

Silent Shred files or folders from target file (without the GUI). Report will be generated.	
<b>Command</b>	/sslbatch algorithm batch_file [/force] [/leave] [/log:logfilepath] [/loglevel:target]
<b>Flags</b>	
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
<b>/leave</b>	[optional] Indicates that the file should be erased but not deleted.
<b>/force</b>	[optional] Indicated that the file should be removed even a program is currently having it open. The file handles will be forcefully closed before erasure.
<b>/log</b>	[optional] Report file path can be specified as an optional parameter.
<b>/loglevel</b>	[optional] If set to <i>target</i> only the target of the operation will be reported and not each file in the operation.
<b>batch_file</b>	A file containing the files to erase. The file should contain whole paths. One path per line. The whole path to the batch file should be specified, i.e. c:\batch.txt

Silent Shred files older than date (without the GUI). Creates report file.	
<b>Command</b>	/ssotd algorithm yyyy-mm-dd file [file...]
<b>Flags</b>	
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
<b>yyyy-mm-dd (Date)</b>	Specifies the date for erasing files older than the date in the chosen path.
<b>File</b>	Specifies the target file or folder. One or more paths can be given, separated by space. The whole path should be specified, i.e. c:\temp.txt. If a folder is given, the old files inside the folder are erased recursively. Folders themselves are not removed.

Silent Shred files older than number of days (without the GUI). Creates a report file.	
<b>Command</b>	/ssotnd algorithm days file [file...]
<b>Flags</b>	
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
<b>Days</b>	Files not modified within this many days will be erased (for example 90 days: "90"). Days must be a value larger than 0.
<b>File</b>	Specifies the target file or folder. One or more paths can be given, separated by space. The whole path should be specified, i.e. c:\temp.txt. If a folder is given, the old files inside the folder are erased recursively. Folders themselves are not removed.

## 2.2 Advanced commands

Silent Shred Temporary Internet Files (without the GUI).	
Command	/stifs algorithm [stifs]
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
stifs	[optional] Run “Silent Shred Temporary Files” operation after completing “Silent Shred Temporary Internet Files” operation.

Silent Shred Temporary Internet Files for all users on the computer (without the GUI). report is not created.	
Command	/satif algorithm
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.

Silent Shred Temporary Internet Files for all users on the computer (without the GUI). Report is created.	
Command	/satifl algorithm
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.

Silent Shred Temporary Files (without the GUI).	
Command	/stfs algorithm [stifs]
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
stifs	[optional] Run “Shred Temporary Internet Files” after completing “Shred Temporary Files” operation.

Silent Shred Temporary Files for all users on the computer (without the GUI). Report is not created.	
Command	/satf algorithm
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.

Silent Shred Temporary Files for all users on the computer (without the GUI). Report is created.	
Command	/satfl algorithm
Flags	
Algorithm	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.

Silent Shred Recycle Bin (without the GUI). Report is created.	
Command	/rs

Silent Shred Recycle Bin for all users on the computer (without the GUI). Report is not created.	
--	--

<b>Command</b>	/ras algorithm
<b>Flags</b>	
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.

#### Silent Shred Recycle Bin for all users on the computer (without the GUI). Report is created.

<b>Command</b>	/rasl algorithm
<b>Flags</b>	
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.

#### Silent Shred Free Disk Space (without the GUI).

<b>Command</b>	/ws drive algorithm [wfs]
<b>Flags</b>	
<b>Drive</b>	Defines one or more drives to run the operation on. I.e. "iok" should perform the operation on drive I: then O: and last K:.
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
<b>wfs</b>	[optional] Run "Silent Shred File Slack" operation with the same parameters after completion of "Silent Shred Free Disk Space".

#### Silent Shred File Slack (without the GUI).

<b>Command</b>	/wfs drive algorithm [ws]
<b>Flags</b>	
<b>Drive</b>	Defines one or more drives to run the operation on. I.e. "iok" should perform the operation on drive I: then O: and last K:.
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.
<b>ws</b>	[optional] Run "Silent Shred Free Disk Space" operation with the same parameters after completion of "Silent Shred File Slack".

#### Silent Shred Previous Versions of all files on the drive (without the GUI). Report is not created

<b>Command</b>	/pv algorithm drive
<b>Flags</b>	
<b>Drive</b>	Defines one or more drives to run the operation on. Multiple drive letters can be given without space in between. For example, "C" erases from drive C, while "CD" erases from drives C and D.
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.

#### Silent Shred Previous Versions of all files on the drive (without the GUI). Report is created.

<b>Command</b>	/pvl algorithm drive
<b>Flags</b>	
<b>Drive</b>	Defines one or more drives to run the operation on. Multiple drive letters can be given without space in between. For example, "C" erases from drive C, while "CD" erases from drives C and D.
<b>Algorithm</b>	Specifies the algorithm used (for example 0). See all available algorithms in chapter 2.3.



## 2.3 Erasure algorithms

The following erasure algorithms can be used when erasing files and folders.

Identifier	Algorithm name	Number of overwriting rounds
0	HMG Infosec, Lower Standard (DEFAULT ALGORITHM)	1
1	HMG Infosec, Higher Standard	3
2	Peter Gutmann's Algorithm	35
3	DoD 5220.22-M	3
4	Bruce Schneier's Algorithm	7
5	Navy Staff Office Publication (NAVSO P-5239-26)	3
6	National Computer Security Center (NCSC-TG-025)	4
7	Air Force System Security Instruction 5020	4
8	US Army AR380-19	3
10	OPNAVINST 5239.1A	3
11	NSA 130-1	3
12	DoD 5220.22-M ECE	7
13	BSI-2011-VS (similar)	3
14	BSI-GS (similar)	2
15	BSI-GSE (similar)	3
16	NIST 800-88 Clear*	1
50	Aperiodic random overwrite**	1

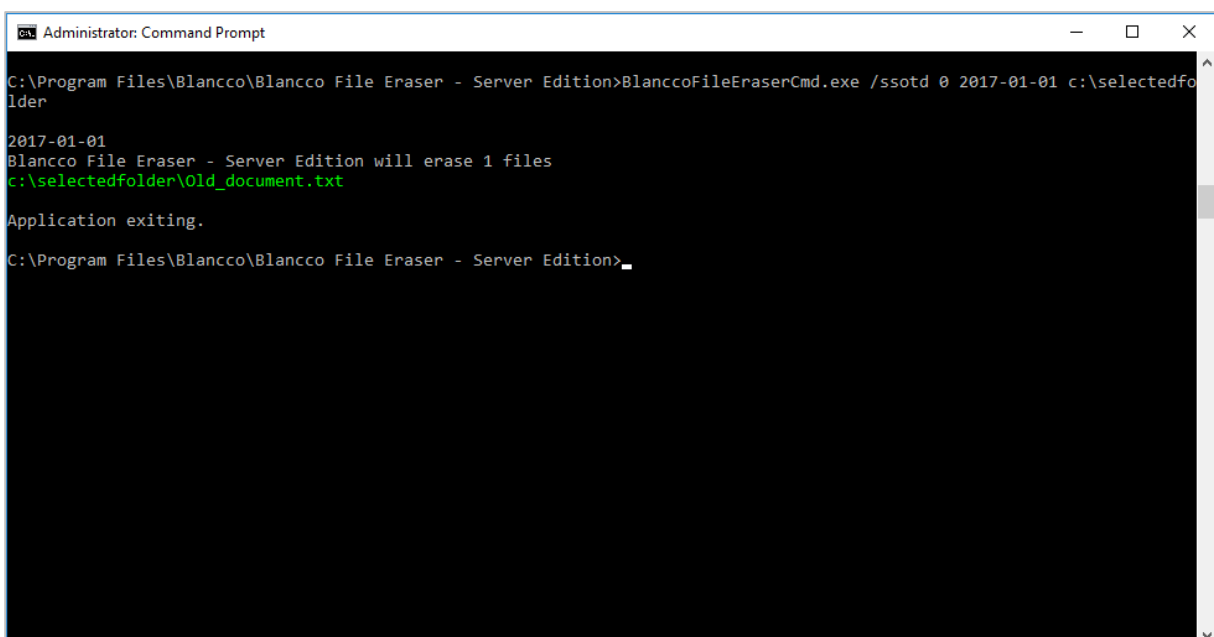
\* Includes 100% verification of the erasure for files smaller than 64MB. Files larger than 64MB, will include at least 10% verification.

\*\* One round of overwriting with aperiodic pseudo random data

## 2.4 Examples

This example will erase the files that are older than the fixed date given as argument. The operation is done for the specified folder, and *HMG Infosec, Lower Standard* algorithm is used:

```
BlanccoFileEraserCmd.exe /ssotd 0 2017-01-01 c:\selectedfolder
```

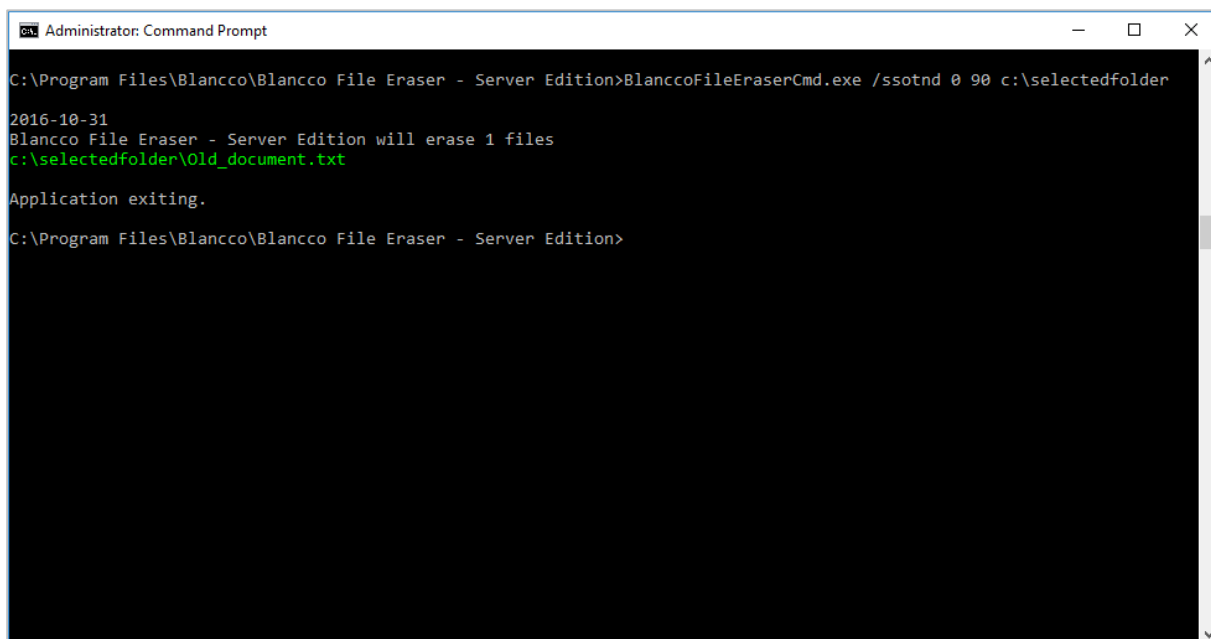


```
Administrator: Command Prompt
C:\Program Files\Blancco\Blancco File Eraser - Server Edition>BlanccoFileEraserCmd.exe /ssotd 0 2017-01-01 c:\selectedfo
lder
2017-01-01
Blancco File Eraser - Server Edition will erase 1 files
c:\selectedfolder\Old_document.txt
Application exiting.
C:\Program Files\Blancco\Blancco File Eraser - Server Edition>
```

The next example will erase the files older than 3 months at any day you run the operation. That is, the three months will be defined by the number of days (90) from the current date and not a fixed date.

The folder specified will be erased with *HMG Infosec, Lower Standard* algorithm:

```
BlanccoFileEraserCmd.exe /ssotnd 0 90 c:\selectedfolder
```



```
Administrator: Command Prompt
C:\Program Files\Blancco\Blancco File Eraser - Server Edition>BlanccoFileEraserCmd.exe /ssotnd 0 90 c:\selectedfolder
2016-10-31
Blancco File Eraser - Server Edition will erase 1 files
c:\selectedfolder\Old_document.txt
Application exiting.
C:\Program Files\Blancco\Blancco File Eraser - Server Edition>
```

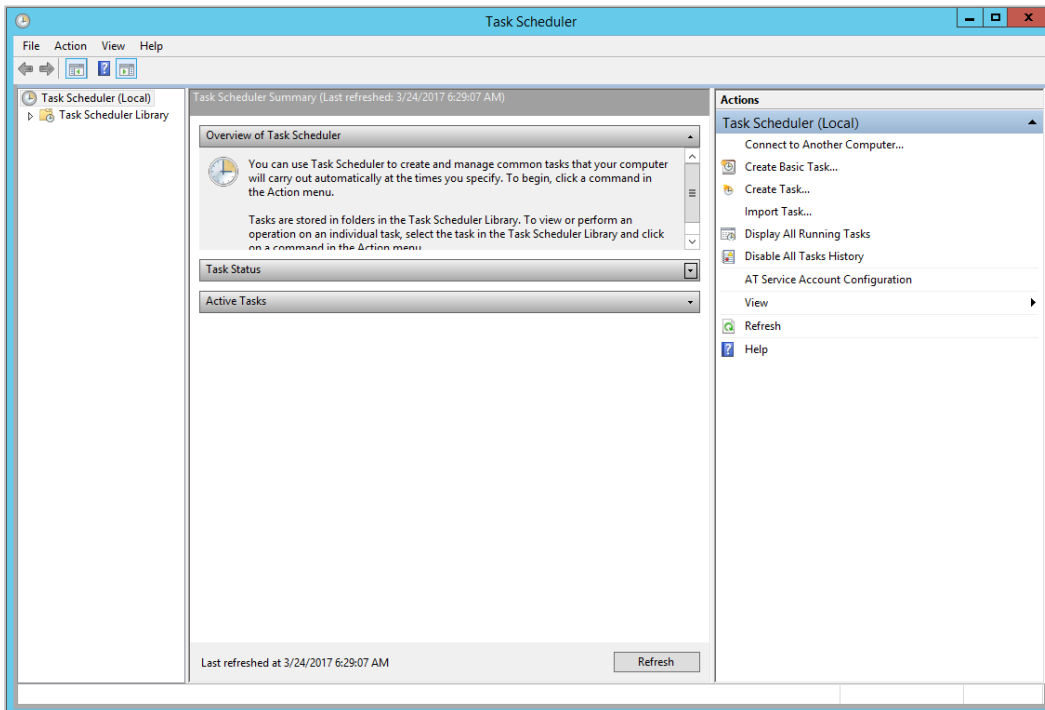
**Note:** When you choose the location of the file or files that should be erased you can also use “wild-cards”, i.e., if you write **C:\temp\\*.\*** all files in the temp folder will be selected for erasure.

**Tip:** When creating many erasure operations to run, the most common practice is to create a batch file (.bat) that can be used when setting up the Windows scheduling for example.

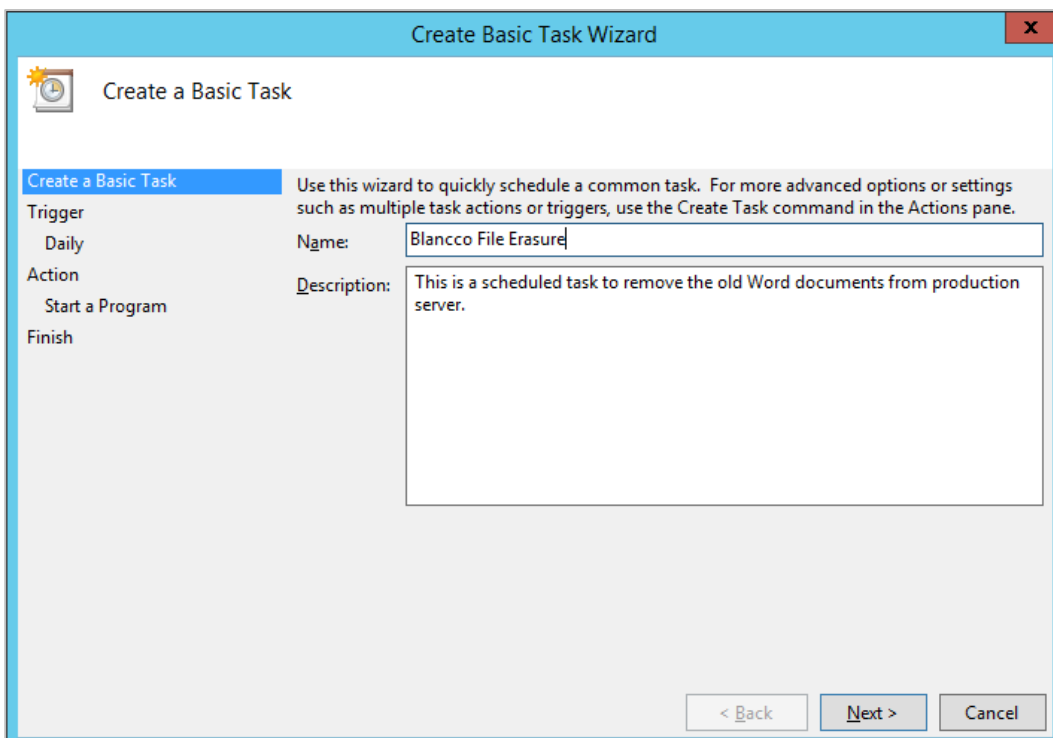
### 3 Scheduling

This chapter offers an example on how to schedule erasure operations with Blancco File Eraser.

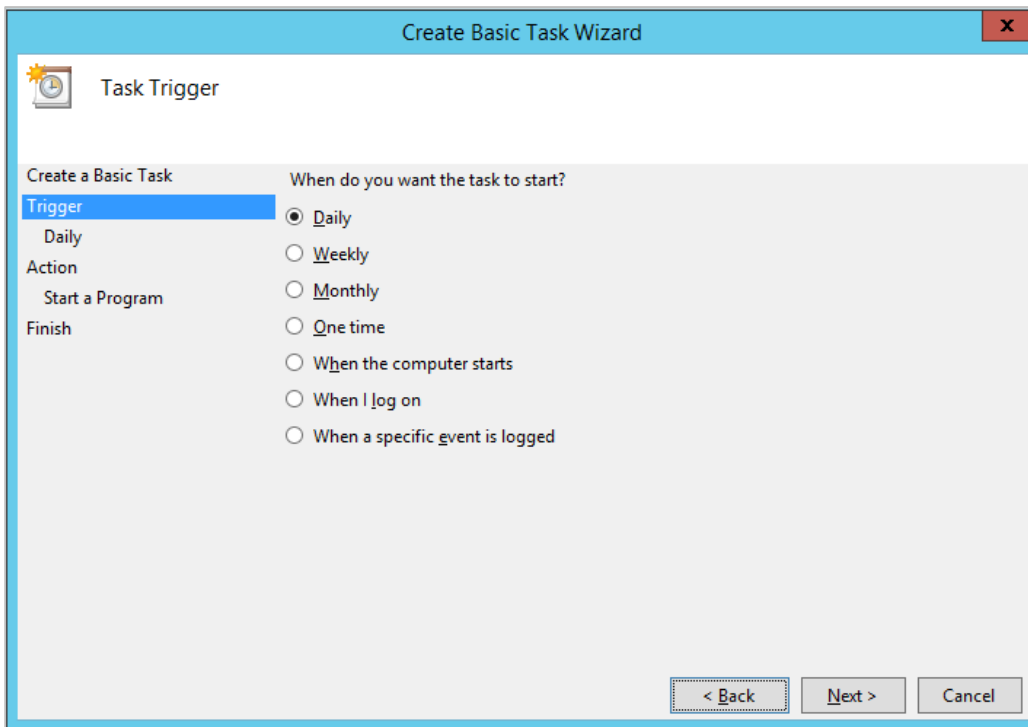
You can add a scheduled task in Microsoft Windows 7 by opening the *Control Panel -> System and Security -> Administrative Tools* and selecting *Task Scheduler*.



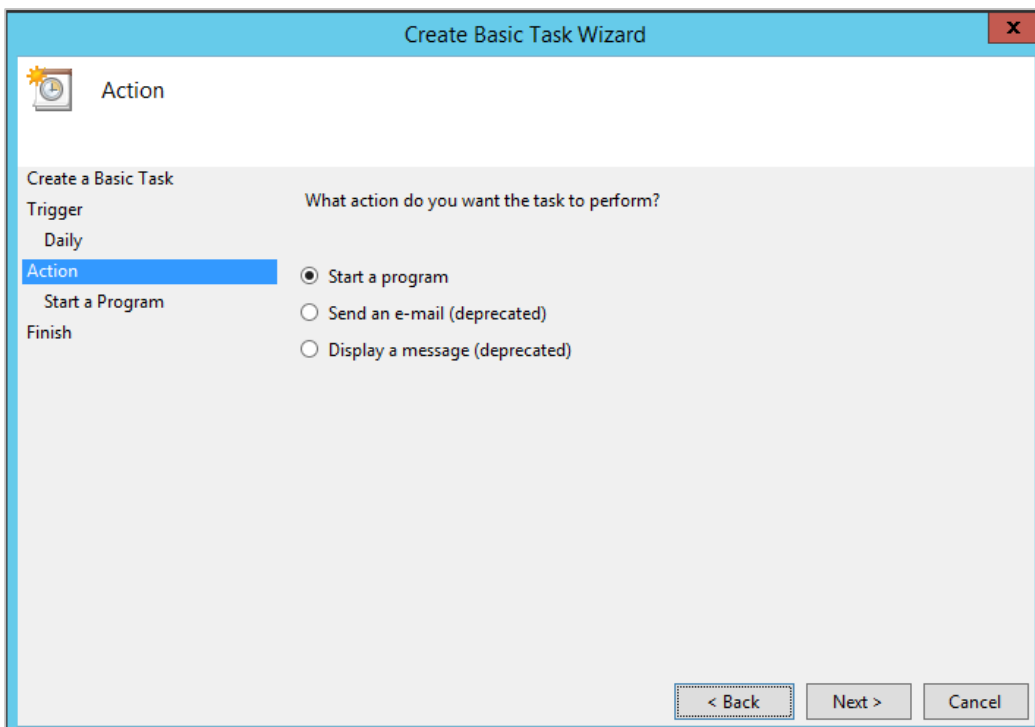
Select *Create Basic Task...*. A guide will open and you can supply a name and a description of the operation that you now is creating.



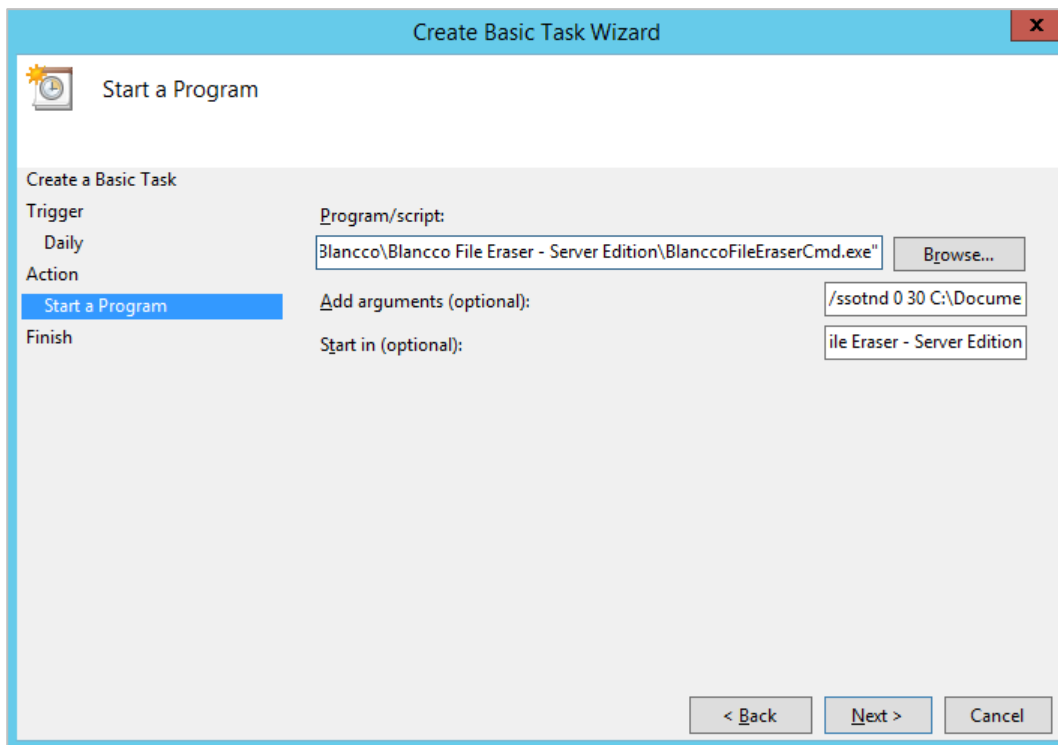
Specify the trigger for the scheduled task to begin. The most common is to do it by time, for instance weekly, but you can also do it at each login and when a specific event has been logged.



Select that you want to start a program as an action.



Specify the path to the exe in the installation folder. As argument you specify according to the parameters below. In this case we specify `/ssotnd 0 30 C:\Documents\*.doc` to remove all Word files older than 30 days in a specific folder. Select the installation folder as *Start in* folder.



**Create Basic Task Wizard**

**Start a Program**

Create a Basic Task

Trigger: Daily

Action: **Start a Program**

Finish

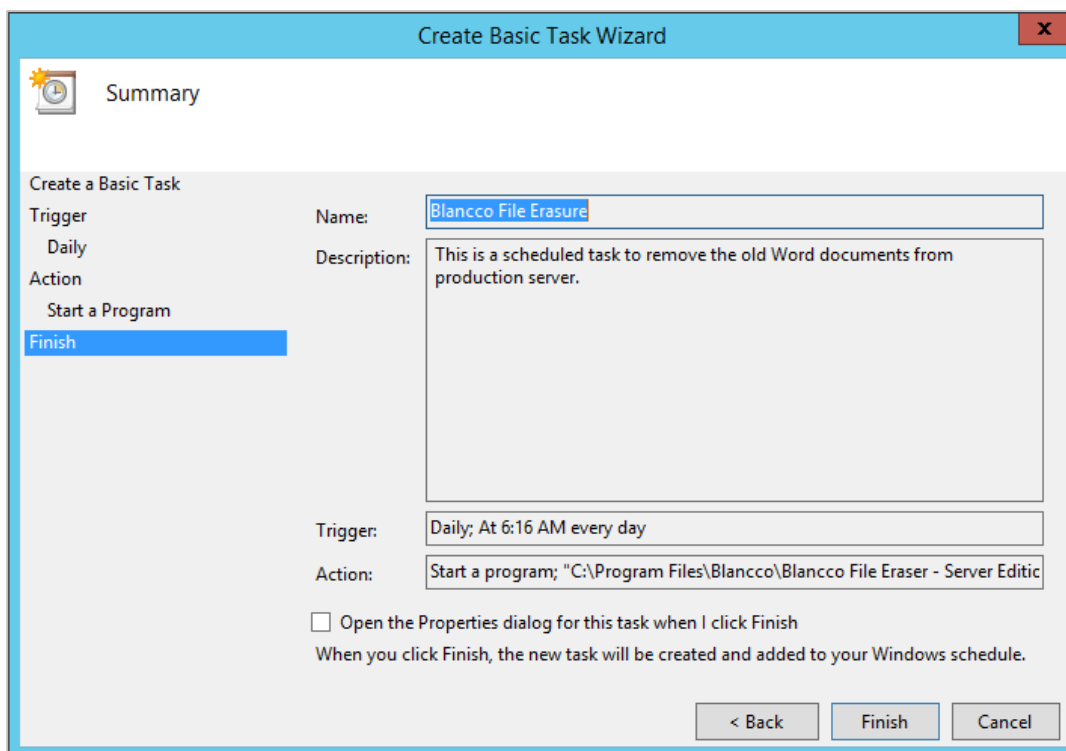
Program/script:

Add arguments (optional):

Start in (optional):

< Back   Next >   Cancel

The guide will show you a summary of the settings you have made and you can finish the guide.



**Create Basic Task Wizard**

**Summary**

Create a Basic Task

Trigger: Daily

Action: **Start a Program**

Finish

Name:

Description:

Trigger:

Action:

☐ Open the Properties dialog for this task when I click Finish

When you click Finish, the new task will be created and added to your Windows schedule.

< Back   Finish   Cancel

**Note:** When you use the Windows scheduling and run as a user it is important that you either choose or create a user account that has full user rights to the files that will be selected for erasure.

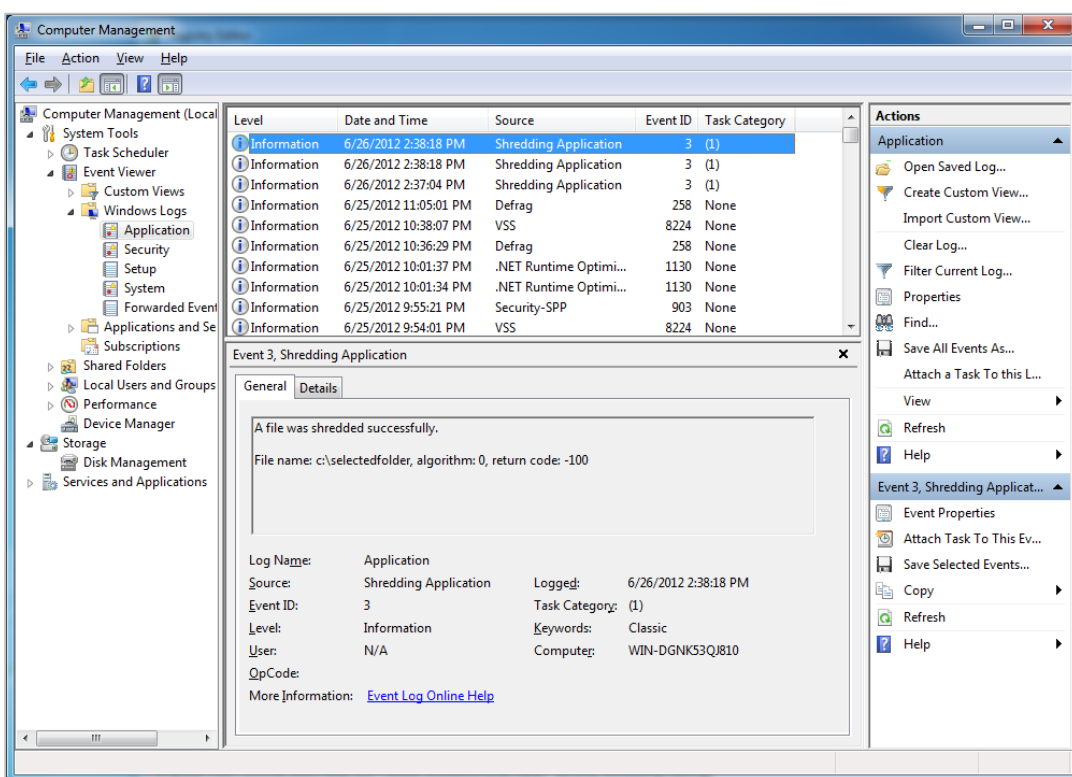
## 4 Event Logging

There is a log module built in to the application that can be easily activated or requested as a default feature. The standard module uses the Windows Event log.

### 4.1 Windows Event Viewer

The result of the event logging can be viewed in the Windows Event Viewer. The information contains the following information:

- If the job was successful (otherwise a warning will be shown)
- File that was erased
- Time when erasure operation was completed
- Erasure algorithm used
- Computer name where the job was performed.



*The result of the event logging can be viewed in the Windows Event Viewer.*

Please use the following registry setting to activate or deactivate this feature:

HKEY_LOCAL_MACHINE\SOFTWARE\Blancco\Shredding\Settings			
DWORD	EventLog	Possible values are 0, 1 and 2.  0 = Inactive 1 = The logging is set to normal mode. If you select a single this will be added as a log event. If you select a folder this will be added as a log event. 2 = Extensive logging is activated. If you select a single file this will be added as a log event. If you select a folder a log event will be created for each of the files in the folder. If you use wildcards all files included in the erasure will be logged.	Defines whether logging to the Windows Event Log should be active or not.

## 5 Reporting

The solution stores information about the erasure to report files. Erasure reports can be handled by an administrator. A report contains for example erasure duration, date and information about the user and the erasure algorithm. Also, optional custom fields can be included to the report.

Erasure reports provide an audit trail of the erasure process and comply with data protection regulations and guidelines.

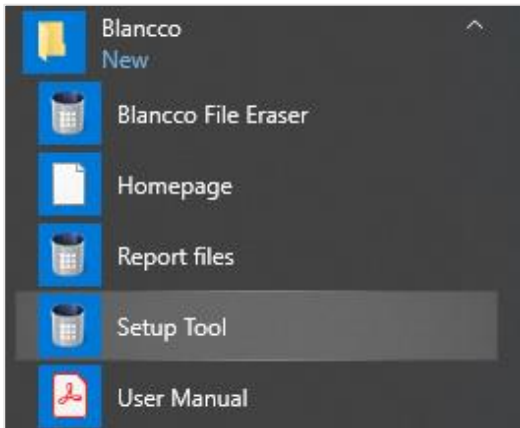
### 5.1 Different Report Formats

The software can generate erasure reports in the following formats:

- PDF – Human-readable erasure report that can be viewed using a generic PDF-viewer.
- XML – This format is required for uploading the report to Blancco Management Console.

## 6 Configuration

All the settings are stored in registry values. The settings can be modified using Blancco Setup Tool that can be opened by selecting “Setup Tool” from the Windows start menu:



The tool can also be launched through the command line (CMD), by entering the following command:

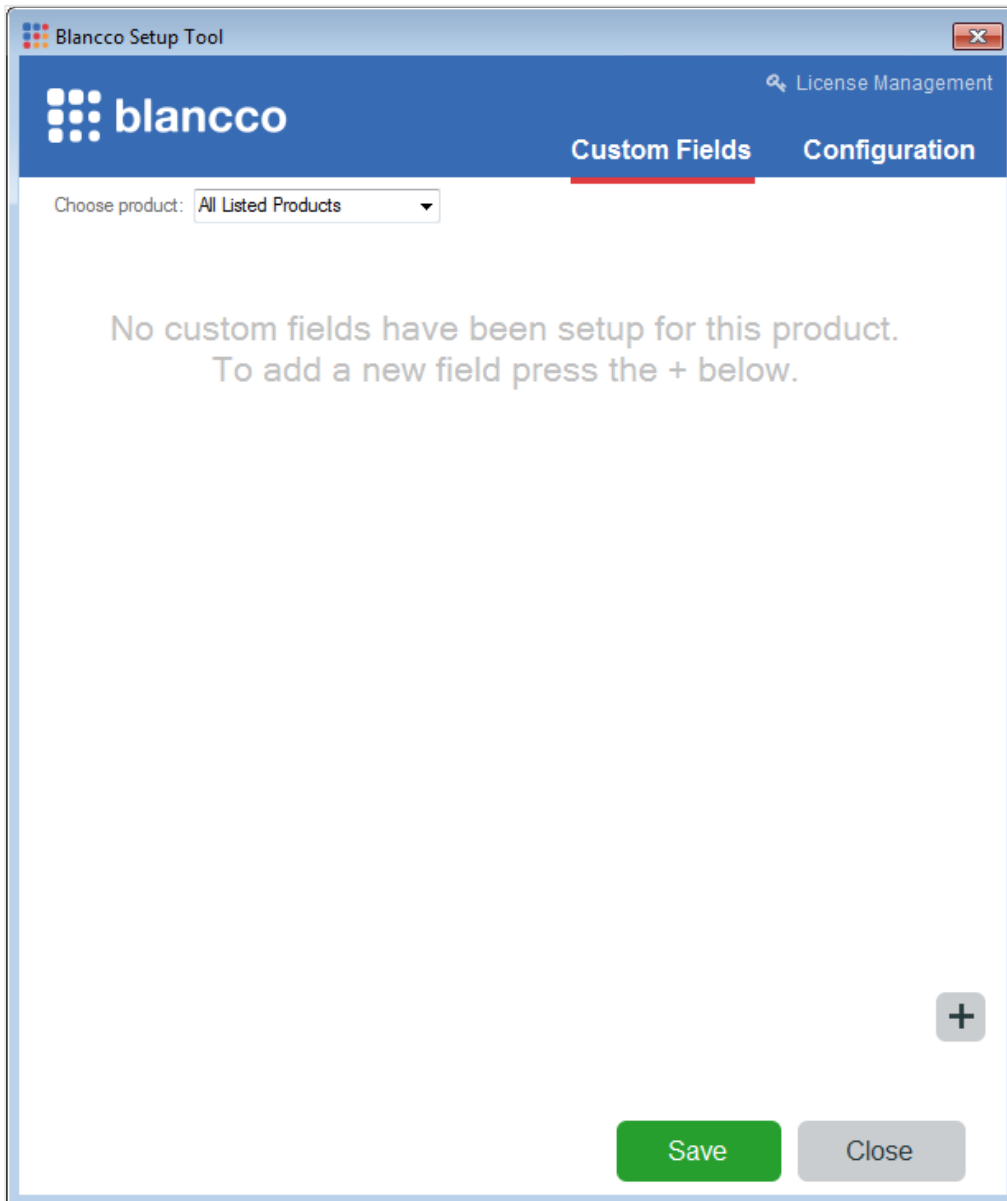
```
BlanccoFileEraserCmd.exe /setup
```

The Blancco Setup Tool allows you to configure license management, include custom fields in the report process, connect to an SMTP server as well as enable automatic connection to Blancco Management Console.



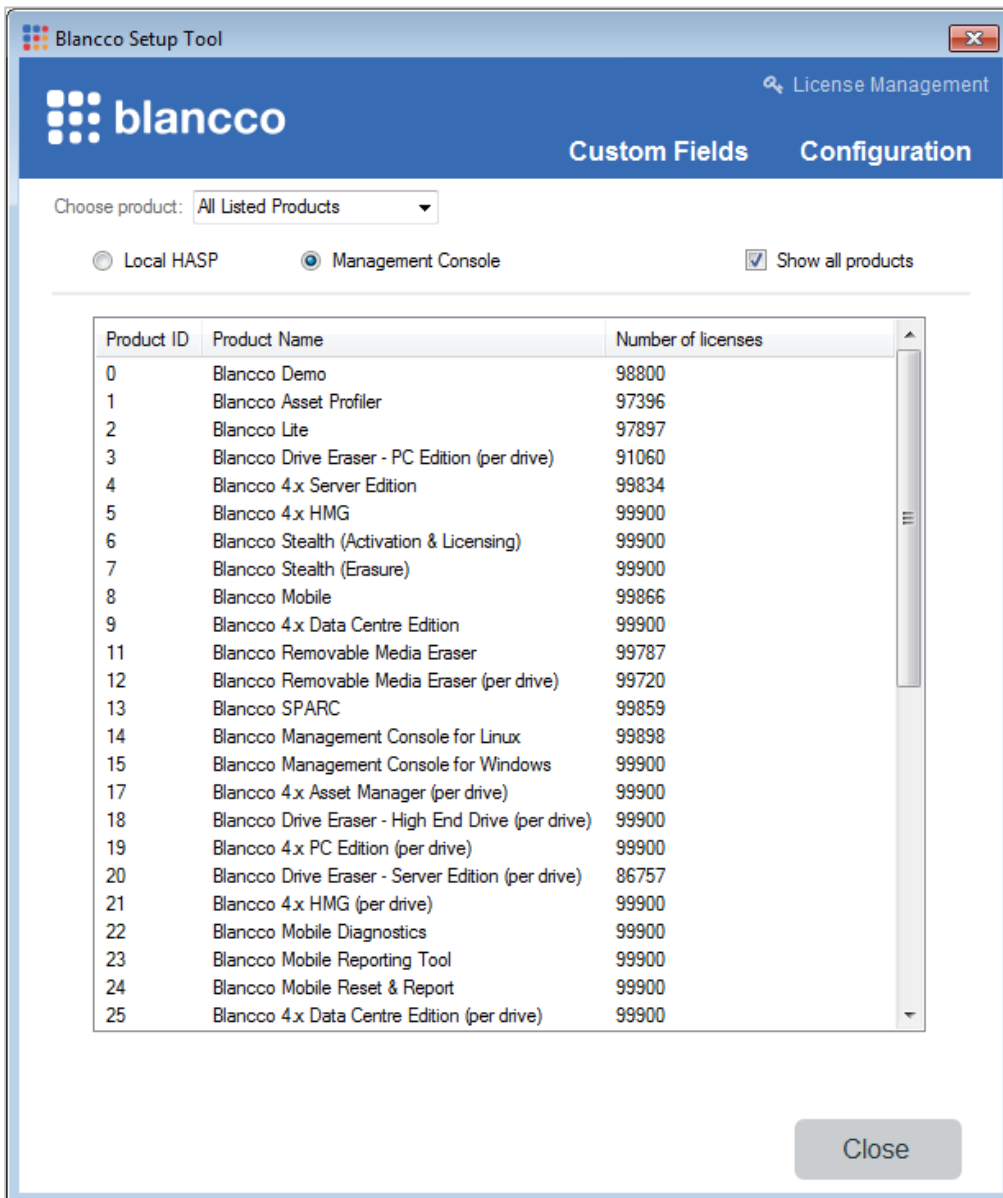
## 6.1 License management

To manage the licenses, click the “License management” text at the top right corner of Blancco Setup Tool window:



In the license management view, you can choose which product to set up in the drop down list. You can also select if you want to use licenses from a local Blancco HASP key or from Blancco Management Console.

If you check the box “Show all products”, you will see a list of all Blancco products and the current number of available licenses.



*Example of product list shown with number of licenses available.*

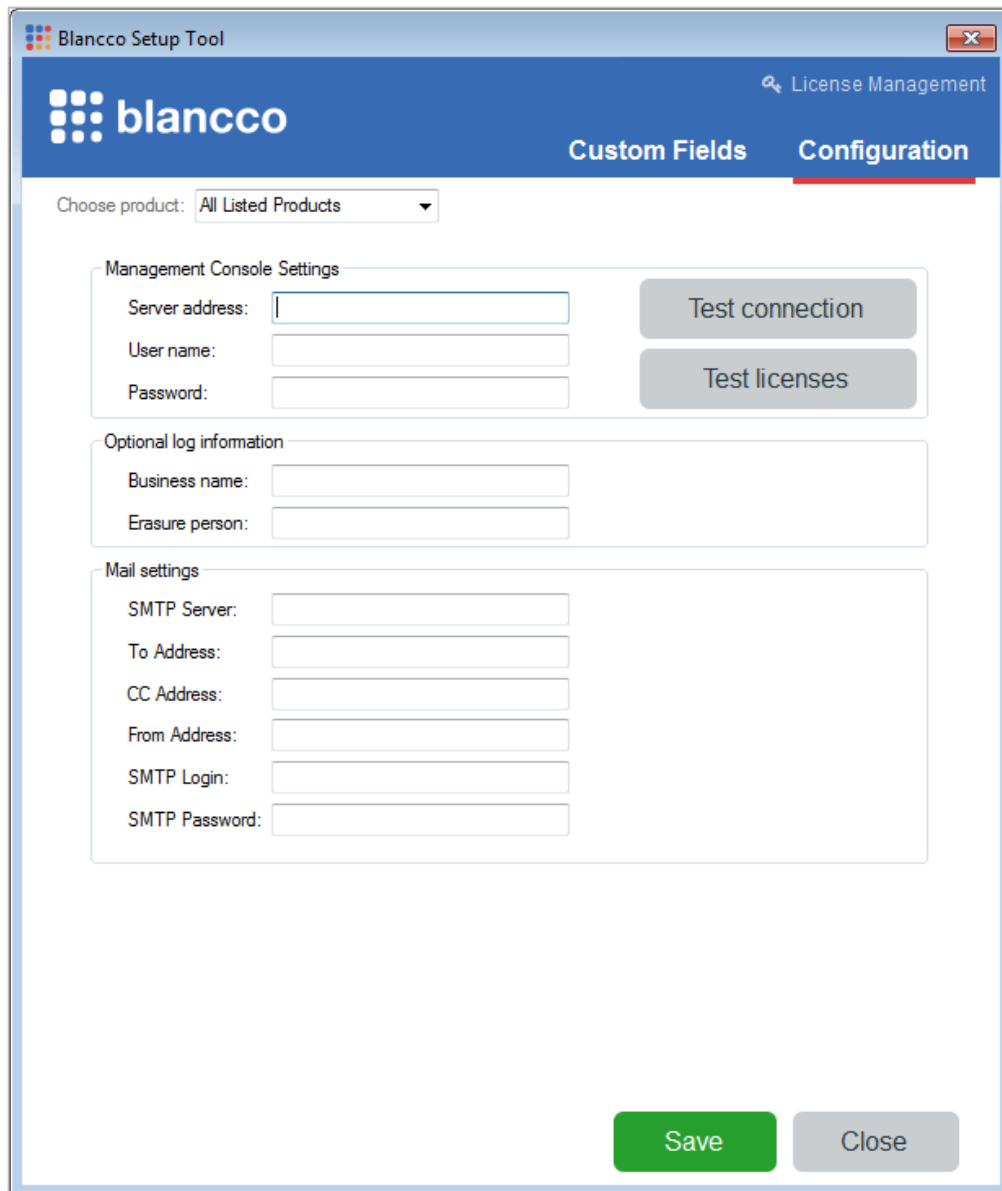
## 6.2 Connecting to Management Console automatically

To automatically send reports into Blancco Management Console, you need to specify the “Server address”, “User name” and “Password” fields in the “Management Console Settings” section. The User name and Password should correspond to the account on the Blancco Management Console specified by the Server address field.

Reports can also be uploaded to the Blancco Cloud automatically or manually by using the server address: <https://cloud.blancco.com:443>

To add “Business name” and “Erasure person” information into the erasure report, fill in the fields in “Optional log information” section.

To send the reports by email from the erasure client, fill in the fields in “Mail settings” section.



The screenshot shows the 'Blancco Setup Tool' window with the 'Configuration' tab selected. The window has a blue header with the 'blancco' logo and a search icon labeled 'License Management'. Below the header, there are two tabs: 'Custom Fields' and 'Configuration'. A dropdown menu labeled 'Choose product:' is set to 'All Listed Products'. The main content area is divided into three sections: 'Management Console Settings', 'Optional log information', and 'Mail settings'. The 'Management Console Settings' section contains three input fields: 'Server address:', 'User name:', and 'Password:'. To the right of these fields are two buttons: 'Test connection' and 'Test licenses'. The 'Optional log information' section contains two input fields: 'Business name:' and 'Erasure person:'. The 'Mail settings' section contains six input fields: 'SMTP Server:', 'To Address:', 'CC Address:', 'From Address:', 'SMTP Login:', and 'SMTP Password:'. At the bottom of the window are two buttons: 'Save' (green) and 'Close' (gray).

*Connect to Blancco Management Console, add report information and send reports via email.*

## 6.3 Import Existing Report to Blancco Management Console via the Command Line

To send an existing report file to BMC, use the following command:

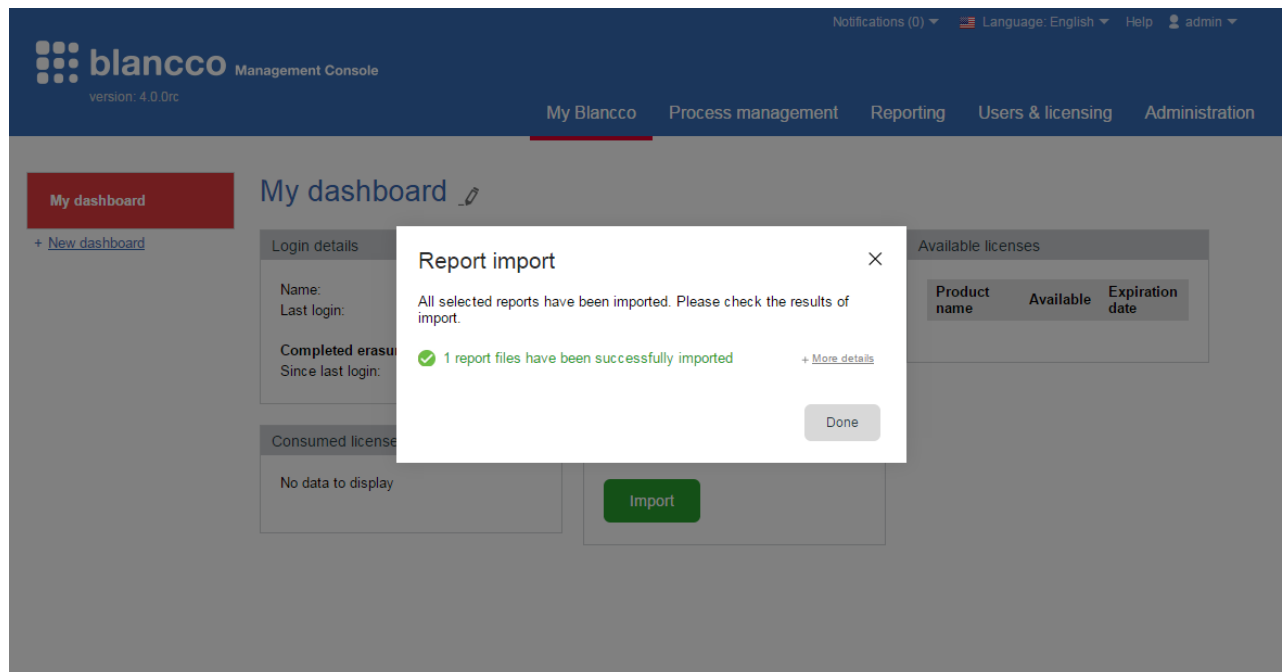
```
*.exe /send <xml report full path>
```

This command takes one XML file as parameter and sends it to the configured BMC.

Note that the \*.exe can BlanccoFileEraser.exe or BlanccoFileEraserCmd.exe

## 6.4 Importing reports manually into Blancco Management Console

XML reports can also be manually imported into Blancco Management Console. The reports are available one by one, and in addition all in one file. The single files are named after date and operation start time. The file with all the reports is called **all.xml**.



*Example of view after successful import.*

If all the reports have been imported successfully, it is recommended to remove the local **all.xml** file. That way a new file will be created, and it will include only the new reports that have not yet been imported into the database.

## 6.5 Reporting settings

### 6.5.1 Changing the location of local erasure reports

The default report location is under the application data directory of the local user. To change this to another local path or to a central storage point other than Blancco Management Console, please create the following registry value:

HKEY_LOCAL_MACHINE\SOFTWARE\Blancco\Blancco File Eraser\Settings			
String	ReportDirectory	Z:\logs	The value identifies the folder in which the report file will be saved.

You can also check the local report path directly from the command line with the following command:

```
BlanccoFileEraserCmd.exe /checkxmlsettings
```

```

Administrator: Command Prompt
C:\Program Files\Blancco\Blancco File Eraser - Server Edition>BlanccoFileEraserCmd.exe /checkxmlsettings
Log files will be created in:
C:\Users\Blancco\AppData\Roaming\Blancco\Blancco File Eraser\Logs\
Application exiting.
C:\Program Files\Blancco\Blancco File Eraser - Server Edition>

```

If you receive an error when running this command, please install the latest version of .NET Framework.

## 6.5.2 Disabling reporting

This registry value can be used to disable erasure report generation (XML, PDF formats).

HKEY_LOCAL_MACHINE\SOFTWARE\Blancco\Blancco File Eraser\Settings			
DWORD	DisableReporting	Possible values are 0 and 1. 0 = Reporting is active 1 = Reporting is disabled	Defines if erasure reports are created or not.

## 6.5.3 Generating Reports in PDF Format

By default, an erasure report is generated in XML and PDF format. To disable the PDF report generation, change the registry setting described below:

HKEY_LOCAL_MACHINE\SOFTWARE\Blancco\Blancco XML Reports			
DWORD	MakeReportIntoPdf	Possible values are 0 and 1. 0 = Do not create PDF report 1 = Create PDF report	Defines if a PDF report should be generated. If emailing of the report is activated, the PDF file is sent.

## 6.5.4 Disabling erasure on network drives

Normally user can erase files on network drives. To prevent this, change the registry settings as described below.

HKEY_LOCAL_MACHINE\SOFTWARE\Blancco\Blancco File Eraser\Settings			
DWORD	DisableErasureOnMappedDrive	Possible values are 0 and 1. 0 = Files on network drives can be erased 1 = Erasure of files on network drives is disabled	Defines if files on network drives can be erased. If activated (1), files on network drives cannot be erased.

## 6.6 Handling Erasure of Previous Versions

Note: Previous version erasure erases all previous versions from specific drives for all users. It cannot be used to erase history for single file or single user's history.

From GUI, all the Previous Versions from all the drives included in the target files are erased. For example, if the erasure operation erases files in C drive, then after the file erasure, Previous Versions are erased from C drive.

### 6.6.1 Disabling Erasure of Previous Versions

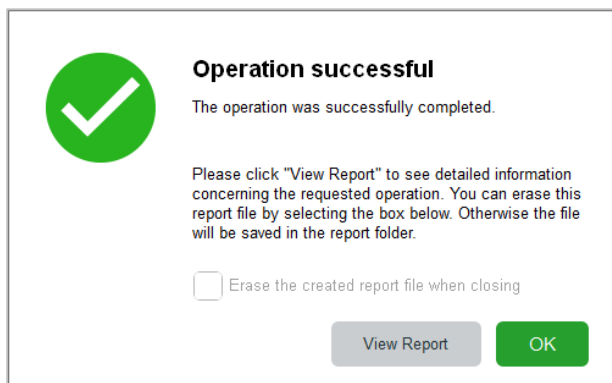
Normally user can erase Previous Versions of the file. To prevent this, change the registry settings as described below:

HKEY_LOCAL_MACHINE\SOFTWARE\Blancco\Blancco File Eraser\Settings			
DWORD	LeavePV	Possible values are 0 and 1.  0 = Previous versions can be erased by the user. 1 = Previous versions cannot be erased by the user.	Defines if Previous Versions of the files can be erased by the user. If activated (1), the Previous Versions of the files cannot be erased by the user.

## 6.7 Disabling Report Erasure

Normally, if there were exceptions during the erasure, the erasure summary window shows an option to delete the report.

This option can be disabled, and the user won't be able to select the option after that:



HKEY_LOCAL_MACHINE\SOFTWARE\Blancco\Blancco File Eraser\Settings			
DWORD	EraseReport	Possible values are 0 and 1.  0 = Erasure summary window allows the user to erase the report. 1 = Erasure summary window doesn't allow the user to erase the report.	Defines if the user can erase the report through the erasure summary window. The erasure option is only shown if the erasure had exceptions.

## 7 Activation Troubleshooting

1. **The license is not accepted.**
  - The license code must be entered exactly as it appears in the license info.
  - Including upper and lowercase letters, periods, etc...
2. **The program seems to hang when the code is activated.**
  - The program tries for five minutes and during this period there will be no progress.
  - If it takes longer than 30 seconds it is most likely that a firewall or a similar program blocks access to our activation server.
3. **The activation went well, but at the next start-up, the program has forgotten the registration information.**
  - There is possibly an anti-virus protection that blocks access to the program. Start the application as the administrator by right-clicking the program icon and selecting "Run as Administrator". Then you can continue activating the program as usual.

## 8 Contact Information

Visit the technical knowledgebase (FAQ) and contact Blancco Technical Support by submitting a technical support ticket at:

<https://support.blancco.com/>

See the instructional videos for Blancco products at:

<https://www.blancco.com/en/videos>

For contact information and the latest information about secure data erasure solutions, visit the Blancco website at:

<https://www.blancco.com/>

We are always looking for ways to improve our products. Please let us know if you have any suggestions!