

# 1. TOC

---

English (United States) .....	2
Español (España) .....	55



# Drive Eraser Configuration Tool

User Manual for version 3.8.0

2023-08-02

# Table of Contents

---

<b>1. Introduction and Installation</b>	<b>6</b>
1.1 Overview	6
1.2 Copyright and Confidentiality Statement	6
1.3 System Requirements	6
1.4 Windows Installation	6
<b>2. Using The Blancco Drive Eraser Configuration Tool</b>	<b>11</b>
2.1 In Windows-systems:	11
2.2 In Linux-systems:	11
2.3 Load a New Image	11
<b>3. Configuring Blancco Drive Eraser</b>	<b>12</b>
3.1 General	12
3.1.1 Image information	13
3.1.2 Localization settings	13
3.1.3 Screensaver settings	14
3.1.4 User interface settings	14
3.1.5 Device view	14
3.1.6 Configuration File Export & Import	15
3.2 Process	15
3.2.1 License options	16
3.2.2 Process options	16
3.2.3 Show more	17
3.2.4 Connected devices	18
3.3 Workflow	18
3.3.1 Workflow options	19
3.3.2 External workflow	19
3.3.3 Embedded workflow	19
3.4 Security	20

---

3.4.1 Security options .....	20
3.4.2 Trusted Platform Module .....	23
3.4.3 Controller options .....	24
3.4.4 Device enrollment detection .....	24
3.4.5 Format settings .....	25
3.4.6 Power saving settings .....	25
3.5 Hardware tests .....	25
3.6 Report .....	27
3.6.1 Report settings .....	28
3.6.2 Report digital signature key .....	28
3.6.3 Customer details .....	29
3.6.4 Operator details .....	29
3.6.5 Asset report settings .....	29
3.6.6 Fingerprint settings .....	29
3.7 Custom fields .....	30
3.7.1 Eye icon .....	31
3.7.2 Regular Expressions for Custom Fields .....	32
3.8 Communication .....	33
3.8.1 Blanco Management Console .....	34
3.8.2 Network share .....	34
3.8.3 VNC remote control .....	36
3.9 Networking .....	38
3.9.1 Static/dynamic network settings .....	38
3.9.2 Global Network Settings .....	39
3.9.3 Networking .....	40
3.9.4 WLAN connectivity .....	40
3.9.5 Proxy .....	41
3.9.6 Network security .....	41

---

3.10 OS .....	42
3.10.1 Boot options .....	42
3.10.2 CD tray eject .....	45
3.10.3 Restart / Shutdown .....	46
3.10.4 List of hybrid drives .....	46
3.11 Other buttons .....	46
3.11.1 Language .....	46
3.11.2 Load new image .....	47
3.11.3 Save .....	47
3.11.4 Save as .....	47
4. Configuring Blanco Drive Verifier .....	48
4.1 General .....	48
4.2 Process .....	48
4.3 Workflow .....	48
4.4 Security (BDV) .....	48
4.4.1 Device enrollment detection .....	50
4.4.2 Power saving settings .....	50
4.5 Verification .....	51
5. Uninstallation .....	53
5.1 Uninstaller script .....	53
5.1.1 In Windows-systems .....	53
5.1.2 In Linux-systems .....	53
6. Contact Information .....	54

# 1. Introduction and Installation

## 1.1 Overview

Blancco Drive Eraser Configuration Tool (BDECT or DECT or CT) permits to preconfigure a Blancco Drive Eraser (BDE or DE) or Blancco Drive Verifier image (BDV or DV) ISO image.

This tool should not be shared with unauthorized personnel: any person having access to both the CT and the Drive Eraser ISO-file has the ability to change the image configuration. This could result in a breach in the security policy of the organization (e.g. changing the erasure standard/options mandated by the organization's policy).

## 1.2 Copyright and Confidentiality Statement

No part of this manual, including the products and software described in it, may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means, except documentation kept by the purchaser of Drive Eraser Configuration Tool. The information contained in this document is subject to change without notice. Products and corporate names appearing in this manual may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owner's benefit, without intent to infringe.

Copyright © 2023 Blancco Technology Group. All rights reserved.

This document is strictly confidential and personal to its recipients and may contain legally privileged and/or copyrighted, trademarked, patented or otherwise restricted information viewable by the intended recipient only. Blancco Technology Group makes no representations and gives no warranties of whatever nature in respect of this document, including but not limited to the accuracy or completeness of any information, facts and/or opinions contained therein. By accessing this document, you acknowledge, accept and agree to the foregoing.

## 1.3 System Requirements

- Windows Server 2016, any Windows 10 or Linux OS with support for appimages.
  - If the software is run in a Windows virtual machine, then 3D acceleration must be disabled on that virtual machine. This has been tested on VirtualBox.
- Administrator rights (root access) to the system.
- 500 MB available space in hard disk.
- Latest operating system updates installed.

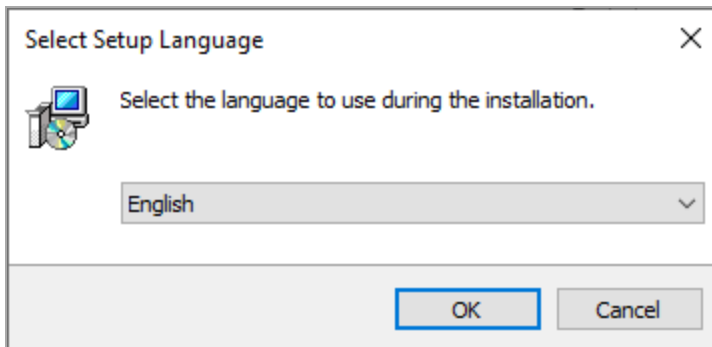
In Windows, the screen resolution ("Scale and Layout" setting) is must not be set above 100%. If this setting is above 100%, Blancco Drive Eraser Configuration Tool won't work correctly.

**IMPORTANT:** Starting from version 3.0, CT is designed to work with Drive Eraser 6.10 or newer.

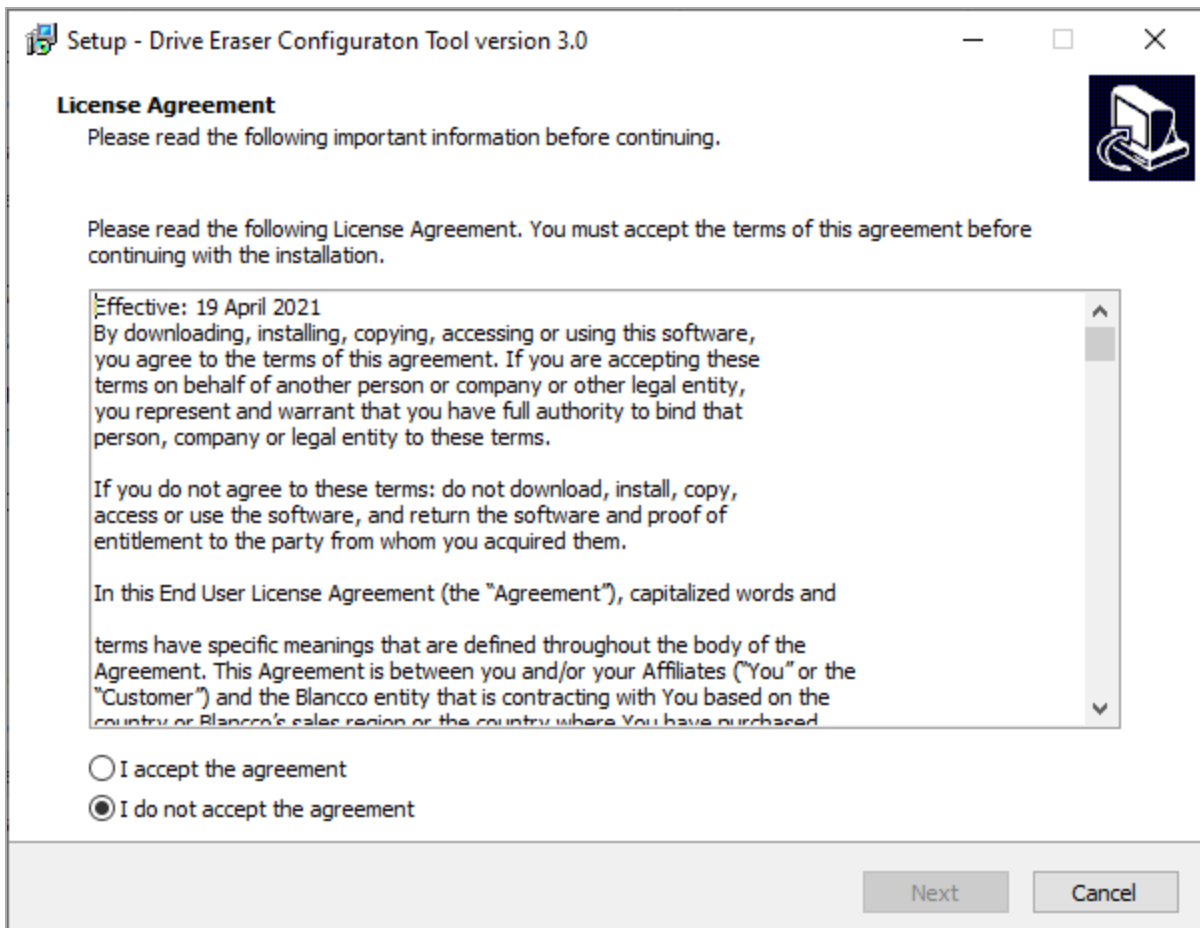
## 1.4 Windows Installation

Before continuing make sure that you have uninstalled any previous version of Blancco Drive Eraser Configuration Tool, please follow the instructions in the "Uninstallation" section.

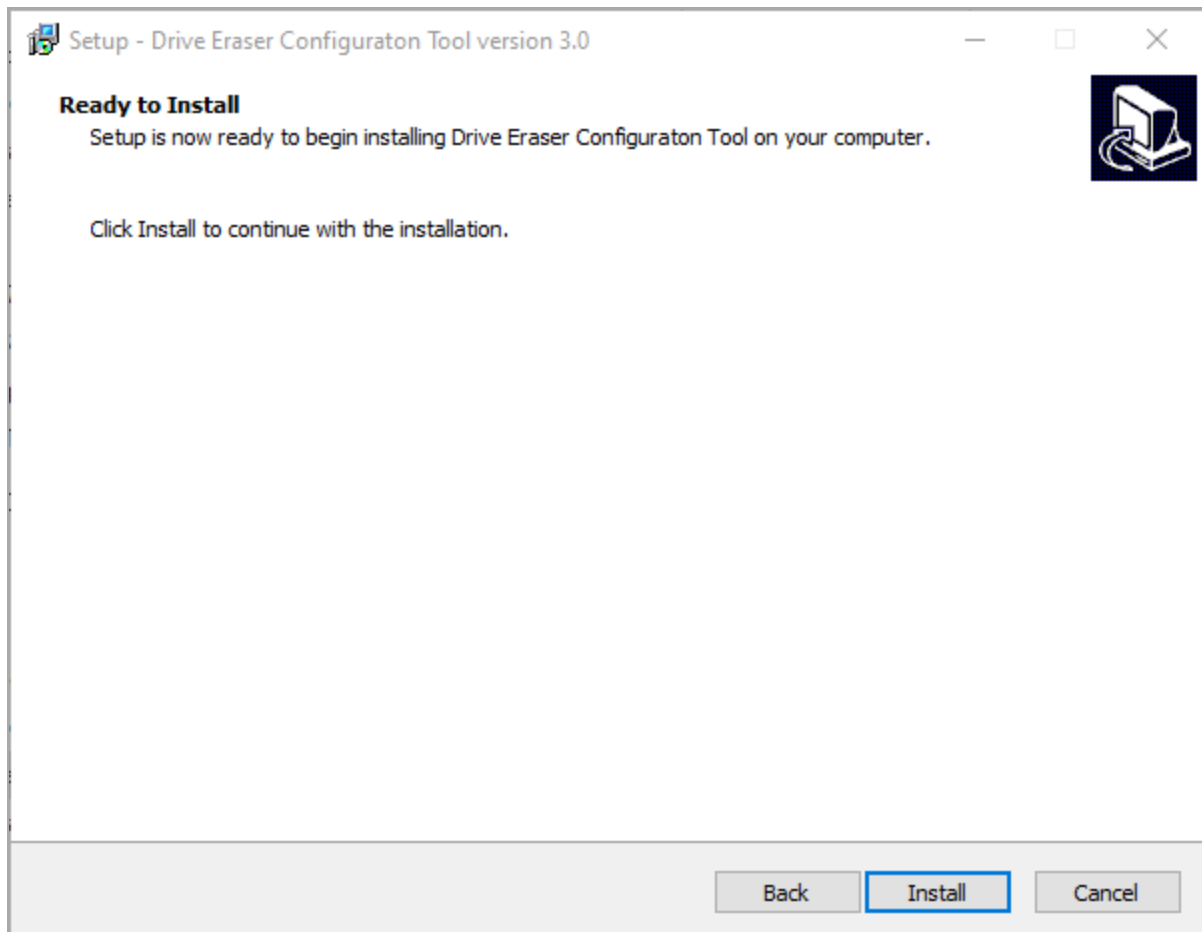
- Double click the installation executable provided by Blancco to start the installation wizard. Make sure you run the installation package with administrator rights.
- Select your installation language:



- Read the License Agreement (visit <http://www.blancco.com/en/eula>) and if you approve of it, select “I accept the terms of this license agreement.” and press “Next”:

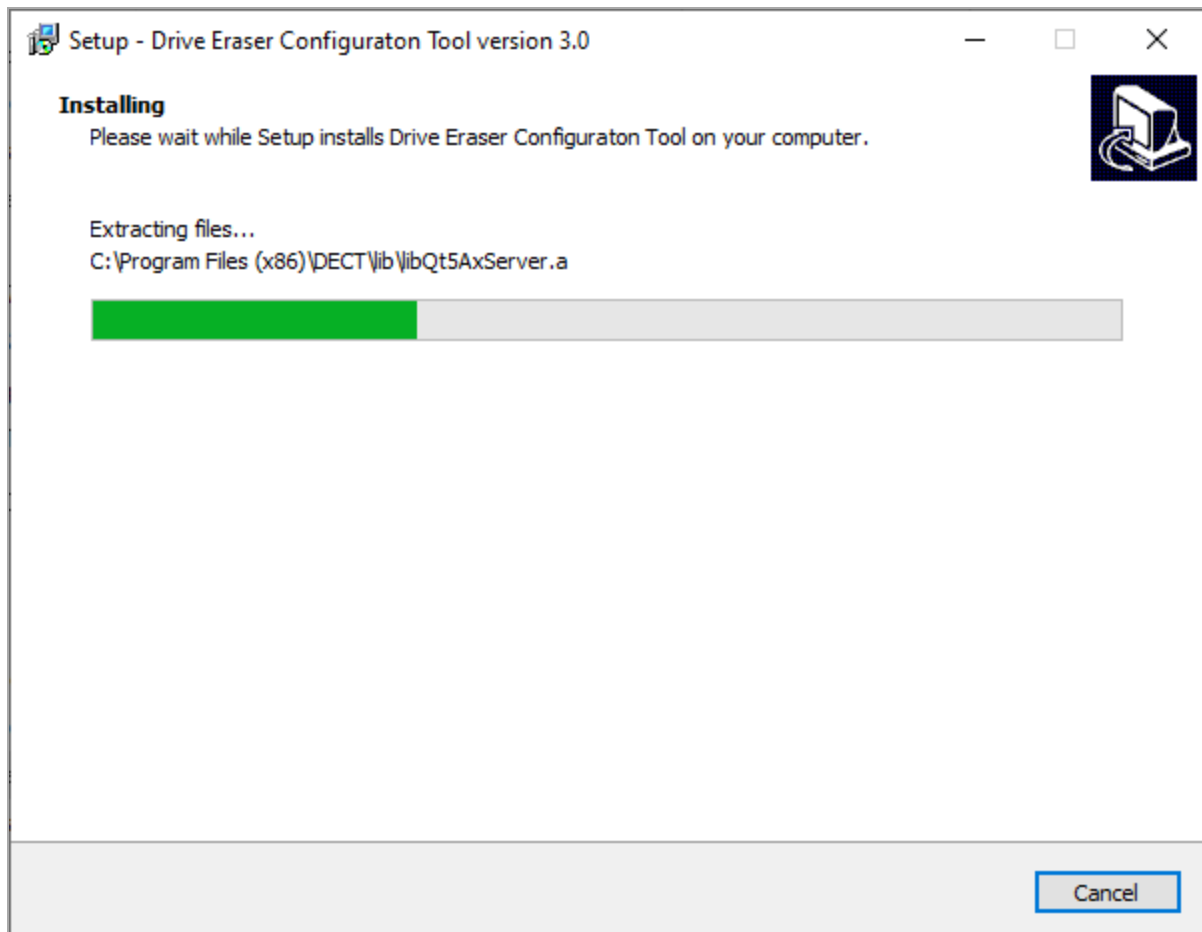


- Software is now ready to install to the default location:

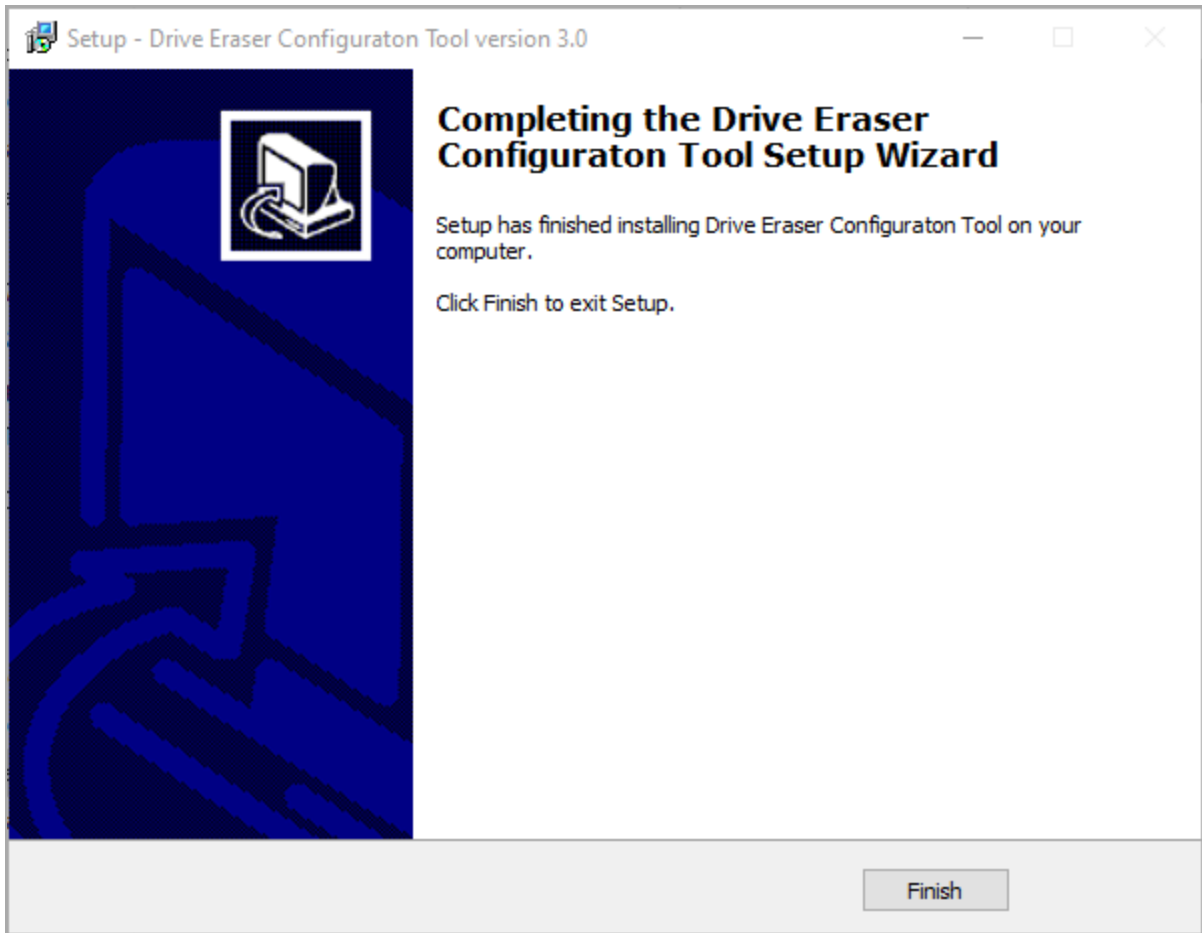


- Choose the Blancco Drive Eraser Configuration Tool installation path:
  - in Windows-systems it is by default: **C:\Program Files\Blancco\Blancco Drive Eraser Configuration Tool 3**
- Wait until installation has finished:





- Installation is now complete. Click **Finish** to close the wizard.



## 2. Using The Blancco Drive Eraser Configuration Tool

Start Blancco Drive Eraser Configuration Tool (CT)

### 2.1 In Windows-systems:

Start the CT service by clicking the "[installation location]\dect.exe.

### 2.2 In Linux-systems:

Start the CT service by starting the .appimage file delivered by Blancco (make sure that you have execution permissions on the file).

### 2.3 Load a New Image

The CT page will open. Click on Load-button to load new image:



- Select a valid Blancco Drive Eraser ISO image, and then click OPEN".
- You can also change the UI language from this window.

## 3. Configuring Blancco Drive Eraser

With CT, it is possible to configure all of the main options of Blancco Drive Eraser. Note that the availability of configuration options depends on Blancco Drive Eraser product variant and version.

The screenshot shows the 'Blancco Drive Eraser Configuration Tool | Version 3.6.0RC2' interface. On the left is a sidebar menu with categories: General, Process, Workflow, Security, Hardware tests, Report, Custom fields, Communication, Networking, and OS. The 'General' category is selected. The main area displays configuration options under several sections: 'Image information' (Product name, Product version, Volume Edition, Licensed to, Usage description), 'Localization settings' (Language, Keyboard layout, UTC offset), 'Screensaver settings' (Enable, Timeout, Notification of exceptions), 'User interface settings' (Scaling), and 'Device view'. The 'Process' category is highlighted in the sidebar. The 'General' category is selected in the sidebar. The 'Image information' section shows 'Product name' and 'Product version' as read-only fields, 'Volume Edition' as a dropdown set to '7.6.0', and 'Licensed to' and 'Usage description' as text input fields. The 'Localization settings' section shows 'Language' as a dropdown set to 'English', 'Keyboard layout' as a dropdown set to 'English (United States)', and 'UTC offset' as a dropdown set to '+00:00 (Z)'. The 'Screensaver settings' section shows 'Enable' as a checked checkbox, 'Timeout (seconds)' as a text input set to '30', and 'Notification of exceptions' as an unchecked checkbox. The 'User interface settings' section shows 'Scaling' as a dropdown set to '100 %'. The 'Device view' section is currently empty. At the bottom right are three buttons: 'Load', 'Save', and 'Save as'.

Category	Section	Option	Value
General	Image information	Product name	
		Product version	7.6.0
		Volume Edition	7.6.0
		Licensed to	
		Usage description	
	Localization settings	Language	English
		Keyboard layout	English (United States)
		UTC offset	+00:00 (Z)
	Screensaver settings	Enable	<input checked="" type="checkbox"/>
		Timeout (seconds)	30
Notification of exceptions		<input type="checkbox"/>	
User interface settings	Scaling	100 %	
	Device view		

### 3.1 General

This menu will allow the general options to be configured.

Image information

Product name

Volume Edition

Product version

7.6.0

Licensed to

Usage description

Localization settings

Language

English

Keyboard layout

English (United States)

UTC offset

+00:00 (Z)

Screensaver settings

Enable

☒

Timeout (seconds)

30

Notification of exceptions

☐

User interface settings

Scaling

100 %

Device view

### 3.1.1 Image information

Name	Default/Example Value	Description
Licensed to *	[Company name]	This field can be edited to match the Licensee or the company using the image. Only visible in the report.
Product name	[Volume Edition / Enterprise Subscription Edition / Enterprise Volume Edition]	Product variant, e.g. Volume Edition. Not editable.
Product version	[6.x series]	Version of the product e.g. 6.0.0. Not editable.
Usage description	Laptops, Enforce SSD	Short description of how the product is meant to be used. For example, an image that erases servers and removes RAID configurations could be "Server, kill RAID". 30 chars maximum.

\* This field can be disabled on special images.

### 3.1.2 Localization settings

Name	Default/Example Value	
Language	English	Default language of the software. All supported languages are shown on the dropdown menu.
Keyboard Layout	English (US)	Default keyboard layout for the software. Blancco Drive Eraser currently supports tens of different

Name	Default/Example Value	
		keyboard layouts.
UTC Offset	+00:00 (Z)	The default time zone used in the software. This time zone is used in the report if the MC cannot be contacted to provide the time zone and time.

### 3.1.3 Screensaver settings

Name	Default/Example Value	
Enable	(checked)	Whether or not the screensaver is on by default.
Lock	(unchecked)	Only available if <b>Process</b> has been set as "Automatic". When turned on, local user cannot exit the screensaver.
Timeout (seconds)	30	Default timeout for screensaver in seconds (period of inactivity before the screensaver starts). Possible values range from 5 seconds to 86400 seconds (1 day).
Notification of exceptions	(unchecked)	To display a notification of erasure exceptions on the screensaver. If enabled, after the erasure is complete any exception that has occurred will blink the screensaver from green (success) to yellow (warning).
Configuration import/export	-	There are two options: "Import from file" and "Export to file". <ul style="list-style-type: none"> <li>Export to file - With this option, current configuration settings can be exported to a configuration file. That file can then be imported to a CT (see below).</li> <li>Import from file - With this option, a configuration file can be imported to this CT. Importing a configuration file imports all the settings set in the ISO used to create the file.</li> </ul> <p>Note that exporting/importing configurations is possible only between same Drive Eraser versions. When successful, notification will be shown on screen.</p>

### 3.1.4 User interface settings

Name	Default/Example value	Description
Scaling	100%	User can change how the program interface scales. This is useful for devices with bigger resolutions. Default value is 100% and you can scale it up to 200% (25% increase in each option).

### 3.1.5 Device view

Name	Default/Example value	Description
Device view by default	List	User can choose the default view for the devices in Drive Eraser. Options are either List or Grid, but default is List. Note that this option can be changed by clicking the icons in Drive Eraser as well.

### 3.1.6 Configuration File Export & Import

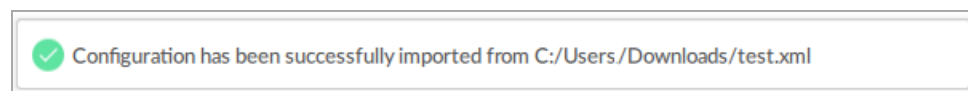
The feature to export a DE configuration creates an XML file (DEconfig.xml), which contains most of the image settings. The DE settings are listed in the following categories:

- Settings that can be modified via CT:
  - Group 1: general settings, hardware tests (including memory test), erasure standards & options, process options, custom fields, most of the BMC & network settings, most of the OS settings.
    - All these settings are exported in the DEconfig.xml file. They can be changed by manually modifying the .xml file (e.g. changing the erasure/process options, changing the IP address of the machine, adding/removing custom fields...). They can then be imported into another DE image.
  - Group 2: BMC & network credentials. These settings are also exported in the DEconfig.xml but they are encrypted, so modifying them manually is not recommended.
  - Group 3: boot options, list of hybrid drives. These settings configure other image files and won't be exported in the DEconfig.xml file.
- Settings that cannot be modified via CT: product version, product name, configuration version.
  - These settings should not be changed. If they are changed, CT will reject the configuration file during the import.
- Some settings (RAID, hotplug, some custom field settings) require a special combination. If such combination is not valid, these settings will be ignored. Also, if the XML file structure is broken, the settings will be ignored. If you are not sure, do not modify these settings and let the CT do the configuration for you.

You can import an older configuration into a new image (e.g. a DE 6.2.0 configuration into a DE 6.5.0 image) but not the other way around (e.g. a DE 6.5.0 configuration into a DE 6.2.0 image). Note that:

- Such backward compatibility does not apply to all DE/B5 versions available.
- Importing an old configuration into a new image will replace the new configuration. In practice, this means that any new settings and features available on the newer image will disappear from CT. For example, if the user is importing settings from version 6.2 to version 6.5 image, the new 6.5 image will behave in CT as it would be a version 6.2 image.
  - For this reason, it is recommended to export/import configurations from same BDE versions.

After importing or exporting the configurations, the program will show a small notification:



### 3.2 Process

This tab will allow the process options to be configured.

License options

License container

Blanco Management Console

Process options

Process

Workflow

Automatic report backup

### 3.2.1 License options

Name	Default/Example Value	Description
License container	Local HASP	Whether the license consumption is done via Local HASP or Blanco Management Console.

### 3.2.2 Process options

Name	Default/Example Value	Description
Process	Manual	<p>The erasure process can be set to Workflow, Automatic, Semi-automatic or Manual. For more information about the erasure processes, see Blanco Drive Eraser User Manual.</p> <p>Note that using Workflow-process requires BMC/Blanco Cloud to function. If you want to create a remote workflow image, "Process" needs to be set to "Workflow" and "Control" needs to be set to "BMC remote" (all the control happens in BMC) or "Combined" (the control happens locally via BMC).</p>
Automatic report backup	[unchecked]	Only available if <b>Process</b> has been set as "Manual". If enabled, a backup copy of the report will be automatically sent to the BMC or saved to a USB stick after an erasure.
Lock the screensaver	[unchecked]	<p>Only available if <b>Process</b> has been set as "Automatic".</p> <p>Locks the screensaver on the BDE once it has been activated.</p>
Post-process action	None	<p>Blanco Drive Eraser can automatically restart or shutdown. This functionality cannot be activated when Process is set to <b>Manual</b> or <b>Workflow</b>.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>None</b> – The default value. No automatic restart or shutdown.</li> <li>• <b>Restart, after process</b> – Machine is automatically restarted, after the process has finished.</li> <li>• <b>Restart, after successful</b></li> </ul>



Name	Default/Example Value	Description
		<p><b>process</b> - Machine is automatically restarted, after the process has finished in a successful state.</p> <ul style="list-style-type: none"> <li>• <b>Shutdown, after process</b> – Machine is automatically shut down, after the process has finished.</li> <li>• <b>Shutdown, after successful process</b> – Machine is automatically shut down, after the process has finished in a successful state.</li> </ul>
Process control	Local user interface	<p>Defines if the erasure is controlled locally via the user interface, remotely from BMC or depends on a Job Specification. Note that remote control and Job specification require the Management Console settings to be filled in the <b>Communication</b> menu.</p> <p>Note that Job specification is only supported on the Blancco Drive Eraser 6.x series, not on the 7.x series.</p> <p>If "Workflow" process is selected, then only the selection "Local user interface" makes workflows available.</p> <p>If "Blancco Management Console remote" or "Combined (Management Console and Local UI)" is selected:</p> <ul style="list-style-type: none"> <li>• Other workflow settings are unavailable (Workflow-tab is greyed out).</li> <li>• "Remote monitoring" is unavailable.</li> </ul>
Remote monitoring	[unchecked]	<p>Only available if Erasure control has been set to Local user interface (the operator controls the erasure locally).</p> <p>If enabled, the Management Console can monitor (not affect) the erasure process. Note that the monitoring requires the Management Console settings to be filled in, either via the configuration tool or via the client software.</p>

### 3.2.3 Show more

Name	Default/Example Value	Description
Show drive partitions	[unchecked]	If enabled, the drive partitions are shown on the GUI and they can be separately erased.
Show removable flash devices	[unchecked]	If selected, removable flash devices are shown in the software user interface and are erasable as any other drive.

### 3.2.4 Connected devices

Name	Default/Example Value	Description
Report per connected device	[unchecked]	<p>If enabled, an individual report is created for each connected device (instead of a report per machine). This feature can only be enabled if:</p> <ul style="list-style-type: none"> <li>• The "Manual" process and the "Local user interface" are selected</li> <li>• Or the "Workflow" process is selected (in v6.13.0 this forces this feature on and it cannot be disabled if that process is active, v6.14 and newer don't force the feature anymore).</li> </ul> <p>When the feature is enabled:</p> <ul style="list-style-type: none"> <li>• Standard Hardware tests are disabled (only applies to client version 6.13 and older).</li> <li>• RAID logical disks removal is enforced</li> <li>• Chromebook Hardware tests can be enabled.</li> </ul>
Hotplug	[unchecked]	<p>This option enables/disables the support for hot plugging drives. <b>Timeout (seconds)</b> is used to modify the timeout for the hotplug procedure (default value is 30 seconds). The minimum timeout is 30 seconds and the maximum is 86400 seconds (24 hours).</p> <p>This option is visible only if the "Report per connected device" mode above is turned on.</p>
Chromebook support	[unchecked]	<p>Only available if <b>Report per connected device</b> option is turned on. This option enables/disables the Chromebook processing support. The <b>Port</b> fields set the ports used to connect to the Chromebook devices. You must set values for both the HTTP and HTTPS ports, the default values are 80 and 443 respectively (it is recommended to leave the default values to simplify the Chromebook processing).</p> <p>Enter a value between 1-65535.</p>

### 3.3 Workflow

This tab will allow the workflow options to be configured.

Workflow options

Workflow container ISO image

External workflow

Load default workflow ☒

### 3.3.1 Workflow options

Name	Default/Example Value	Description
Workflow container	Blanco Management Console	<p>Where the workflow is stored and fetched from.</p> <p>Options are:</p> <ul style="list-style-type: none"> <li>Blanco Management Console - Workflow is fetched from Blanco Management Console. Note that this requires a connection to Blanco Management Console to be set and active.</li> <li>ISO image - The workflow is embedded to the ISO image. See "Embedded workflow" below for more information</li> </ul>

### 3.3.2 External workflow

Note that these options are only available if "Workflow container" has been set to "Blanco Management Console".

Name	Default/Example Value	Description
Load default workflow	[checked]	Automatically load the workflow, which has been set as the default workflow in Blanco Management Console.
Load workflow by name	Workflow_name_here	Only available if "Load default workflow" is not active. Load a workflow from Blanco Management Console named in this field

### 3.3.3 Embedded workflow

Note that these options are only available if "Workflow container" has been set to "ISO image".

Name	Default/Example Value	Description
Import from file	-	Import a workflow file from the computer. Note that before importing from a file, a workflow needs to be exported from a BMC
Export to file	-	<p>Only available if a workflow has been selected from the list of workflows.</p> <p>Export an embedded workflow to a file on the local computer.</p>
Remove	-	Only available if a workflow has been selected from the list of workflows.

Name	Default/Example Value	Description
		Export an embedded workflow to a file on the local computer.
List of workflows	-	A table containing a list of all workflows currently loaded to the ISO image.  To select a file, use checkbox next to the workflow's name.
Main workflow	workflow_name_here	Which workflow is used as the main (default) workflow in this ISO image.

## 3.4 Security

This menu contains options for the erasure's security features.

Security options

Erasure standard

...

HMG Infosec Standard 5, Lower Sta... ▾

Action if erasure is not possible

Interrupt process ▾

Enforce Blancco SSD method on SSDs

☐

Enable fallback from NIST Purge to NIST Clear

☐

Fail process if write errors

☒

Fail threshold

5

### 3.4.1 Security options

Name	Default/Example Value	Description
Erasure standard	HMG Infosec Standard 5, Lower Standard	<p>Default standard used in the erasure procedure. Blancco Drive Eraser currently supports more than 24 different erasure standards. See Blancco Drive Eraser manual for more information on the erasure standards.</p> <p>User can enable/disable the erasure standards, by opening the edit-view by using the edit button (three dots) next to the standards list. Enabling/disabling is then done by using the checkboxes next to the standard names in the edit-menu. After enabling/disabling standards, click "Save" to save the changes, or "Cancel" to undo all changes. Note that at least one erasure standard must be enabled.</p> <p><b>Overwriting pattern type</b> options are available when selecting NIST 800-88 Clear. This allows user to change in what way the overwriting process is done. Byte value can be changed with the "Static" option.</p>
Action if erasure is not possible	Interrupt process	<p>If erasure cannot be started for some reason, the action selected here will be taken. The possible actions are:</p> <ul style="list-style-type: none"> <li>Interrupt process - Completely interrupt and stop the process</li> <li>Continue the process and report</li> </ul>

Name	Default/Example Value	Description
		failure - Continue the process until the process is finished and mark the erasure as "failed" in the report.
Enforce Blancco SSD method on SSDs	[unchecked]	If enabled, for all detected SSD drives the overwrite standard is switched automatically to the "Blancco SSD Erasure" method. Other drives are still erased with the default overwrite standard. Note that this feature requires that the "Blancco SSD Erasure" is enabled as an overwrite standard (see enabling/disabling standards above).
Enable fallback from NIST Purge to NIST Clear	[unchecked]	If enabled and the "NIST 800-88 Purge" erasure fails, or the standard is not supported, the process falls back automatically to the "NIST 800-88 Clear" erasure standard.  Note that this option is unavailable if the "Erasure process" is set to "Workflow".
Fail process if write errors	[checked]	If enabled, the threshold on write error count is defined here. If during the erasure the write error count reaches this threshold, then the erasure will automatically stop and fail. The default threshold is 5 errors. Additionally, the report will show an error message informing about this. Minimum error threshold is 1 and maximum is 1000.
Fail process if read errors	[checked]	If enabled, the threshold on read error count is defined here. If during the erasure the read error count reaches this threshold, then the erasure will automatically stop and fail. The default threshold is 5 errors. Additionally, the report will show an error message informing about this. Minimum error threshold is 1 and maximum is 1000.
Remove hidden areas	[checked]	This option defines how the hidden areas on the drives (HPA and DCO) are handled. If enabled, the hidden areas will be detected and automatically removed. If disabled, the hidden areas will be detected but not removed.
Erase remapped sectors	[checked]	This option defines how remapped sectors are handled during the erasure process. If this option is enabled, remapped sectors are automatically erased if they exist and if the drive supports this functionality. If this option is disabled, the remapped sectors are detected but are not erased.
Fail erasure if the number is too high	[unchecked]	If this option is enabled, the fail threshold becomes active and it is set to 1 or to the value it was before it was disabled.  The <b>Fail Threshold</b> option is used to set a number for the maximum amount of allowed remapped sectors. If the detected

Name	Default/Example Value	Description
		<p>amount of remapped sectors is equal or greater than this value, then the erasure will automatically stop and fail.</p> <p>This option requires that "Erase remapped sectors" option is turned on.</p>
Fail erasure if unsuccessful	[unchecked]	<p>If this option is enabled, the whole erasure will fail if:</p> <ul style="list-style-type: none"> <li>• The drive has at least one remapped sector,</li> <li>• the erasure of remapped sectors is not supported by the drive or it is supported but fails.</li> </ul> <p>This feature is only available on client version 6.1.1 or newer. This option requires that "Erase remapped sectors" option is turned on.</p>
Fail process if the speed is too low (MB/s)	[unchecked]	<p>Fail the process if the erasure speed is lower than the value set in the "Fail threshold" field.</p> <p>Disabled by default. Default value is 1 and the value range is 1-10000. The unit is Megabytes/second.</p>
Fail process by timeout (hours)	[unchecked]	<p>Fail the process if its duration is longer than the value in the "Fail threshold" field.</p> <p>Disabled by default. Default value is 48h. Custom range is from 1 hour to 1 year (8760h)</p>
Execute self-tests on drives	[None]	<p>This option sets the drive's S.M.A.R.T self-test to "None" (no testing – default option), "Short", "Conveyance" or "Extended". For more information about the self-tests, see the client software's user manual.</p>
Fail process if unsuccessful	[unchecked]	<p>If this option is enabled and the selected self-tests fail, the erasure process is aborted, and the erasure process is failed. The reason for the failure is marked to the report.</p> <p>This option is only available if "Execute self-tests on drives" is enabled on the option above.</p>
Verification level	1%	<p>This setting defines the verification level of the erasure. The verification process reads data from the drive and makes sure that the overwriting patterns were correctly written. The minimum verification corresponds to checking 1% of the surface of the drive (fast process), while the full verification corresponds to checking 100% of the surface of the drive (slower).</p> <p>Note that switching the erasure standard always resets the verification level to the one specified for that standard. When this happens, the following warning is</p>

Name	Default/Example Value	Description
		displayed: "The verification percentage was modified based on the erasure standard minimum requirements".
Simultaneous operations limit	[50]	<p>Maximum number of simultaneous erasures. If the number of simultaneous erasures is less than the limit, then new erasures can be started until the limit is met.</p> <p>If the number of erasures exceeds this value, the excess and new erasures are put to erasure queue and are paused until they can be started.</p> <p>Note that the maximum number supported here can differ between client software editions.</p>
Disable block SID authentication	No, skip	<p>Block SID Authentication (BSA) is a type of lock that prevents running firmware commands on the machine drives. This setting allows preconfiguring a dialog to turn on/off that lock, a timeout can also be set to close the dialog (0-86400 seconds). The options are: I No, skip - BSA is not turned off, the lock is kept. I Yes, proceed - BSA is turned off, the lock is removed. Note that this requires rebooting the machine and accepting the disabling.</p>
Preserve recovery partition	[unchecked]	<p>If this option is enabled, erasure process can be resumed if it has been terminated in an uncontrolled manner (power outage, system failure, etc...).</p> <p>See Blancco Drive Eraser user manual for more information.</p>
Resume erasure if interrupted	[unchecked]	<p>If this option is enabled, erasure process can be resumed if it has been terminated in an uncontrolled manner (power outage, system failure, etc...).</p> <p>See Blancco Drive Eraser user manual for more information.</p>
Lock the erasure settings	[unchecked]	If this option is enabled, the user of BDE cannot change the erasure settings.
Estimate the remaining drive life	[unchecked]	<p>Activating this setting will display in the report an estimate on the time left on each drive, based on several internal attributes. Read more in the BDE user manual.</p>

**Note! To erase SSD and NVMe drives that support firmware based erasure commands , the recommended erasure standards available in Blancco Drive Eraser software are "Blancco's SSD Erasure" and "NIST 800-88 Purge".**

However, if your erasure policy mandates that a different process should be applied for these drives, other options can be selected but a message will appear on the report highlighting that an SSD was erased.

### 3.4.2 Trusted Platform Module

Name	Default/Example Value	Description
Clear TPM at startup	No, skip	This setting allows to reset the TPM chip,

Name	Default/Example Value	Description
		<p>which clears all the information contained in it. Read more in the BDE manual.</p> <p>Note that turning this setting on might reboot the machine.</p> <p>If "Timeout (seconds)" is selected, then there is a time limit for the user to make a selection, before the value selected on the "Clear TPM at startup" is automatically selected. Timeout value can be configured (0-86400 seconds). If no timeout is selected, then the software will wait in the selection screen until user selects one of the options.</p>

### 3.4.3 Controller options

Name	Default/Example Value	Description
Logical disk (RAID)	Show	<p>When set to "Show", logical disks defined within a RAID will not be removed; they are visible on the screen and accessible for erasure. When set to "Remove", this option will allow the removal of all logical disks defined within a RAID; RAID configuration will be dismantled and physical disks will be accessible for erasure (erasure of physical disks is much more secure). This setting is not available in the PC Edition.</p>
Reconfigure controller mode	Yes, proceed	<p>This setting allows to reconfigure the controller mode (e.g., from RAID to JBOD mode) which permits a better control of the connected drives. For more information, see Blancco Drive Eraser documentation. The possible values are "Yes, proceed" (default value) and "No, skip".</p> <p>If "Timeout (seconds)" is selected, then there is a time limit for the user to make a selection, before the value selected on the "Reconfigure controller mode" is automatically selected. Timeout value can be configured (0-86400 seconds). If no timeout is selected, then the software will wait in the selection screen until user selects one of the options.</p>

### 3.4.4 Device enrollment detection

Name	Default/Example Value	Description
Persistent software	[unchecked]	<p>If this option is enabled, any persistent software (embedded in the BIOS) will be detected and reported. The most popular persistent software is Computrace (by Absolute Software) and it is used for tracking computer hardware.</p>



### 3.4.5 Format settings

Name	Default/Example Value	Description
Format drive after erasure	[unchecked]	If this option is enabled, when the drive has been erased, the drive is formatted to the file system type chosen on the "File system type" dropdown menu. The supported drive interfaces are ATA, SATA, SCSI and SAS.
File system type	NTFS	File system type the drive is formatted to. Default type is NTFS. Options are: <ul style="list-style-type: none"><li>• NTFS</li><li>• FAT32</li><li>• exFAT</li></ul> This menu becomes active only if "Format drive after erasure" above is enabled.

### 3.4.6 Power saving settings

Name	Default/Example Value	Description
Spin down idle disks	[checked]	When enabled, this option allows the client software to spin down disks when they have been idle for 5 minutes.  Also, when this option is enabled, maximum of one erasure can be started per second. This is to prevent power peaks.  Enabled by default.

## 3.5 Hardware tests

This menu contains options to enable/disable hardware tests and to modify test specific options. CT can also be used to configure hardware tests on Chromebooks. For more information, read the Blancco Drive Eraser user manual.

#### Hardware test settings

☒ Enable

Select hardware tests	Required	Pass thresholds	Duration
<input checked="" type="checkbox"/> Battery capacity	<input type="checkbox"/>	<div><div></div></div> 60 %	
<input checked="" type="checkbox"/> Battery discharge	<input type="checkbox"/>	<div><div></div></div> 50 %	<div><div></div></div> 10 min
<input checked="" type="checkbox"/> BIOS logo	<input type="checkbox"/>		
<input checked="" type="checkbox"/> CPU	<input type="checkbox"/>		

If the **Required** checkbox is selected for a specific test, then the test cannot be unselected from the Blancco Drive Eraser UI and will be run if the user starts the hardware tests manually. If "Chromebook support" has

been enabled on the image, then the "Required" checkbox is not available for the selected tests (all selected tests are automatically on run on ChromeBooks).

Note that with manual tests, user interaction is required.

For more information about specific tests, see the Blancco Drive Eraser User Manual.

Name	Default/Example Value	Description
Enable hardware tests	<i>(unchecked)</i>	Enable/disable all hardware tests. If enabled, the "Hardware tests" step in Blancco Drive Eraser will become visible (hidden otherwise).
Battery Capacity	<i>(checked)</i>	<p>The Battery Capacity test checks the capacity and voltage of the internal battery (on laptops and tablets). Default value is 60% (compliant with e-Steward 2020 Guidelines).</p> <p>The <b>Pass Threshold</b> option is used to determine what level of battery capacity is good enough to pass. The range is 1-100 (%). If the pass threshold is set, for example, to 80% - if the laptop's battery can hold at least 80% of its original capacity, then the test won't fail.</p>
Battery discharge	<i>(checked)</i>	<p>The Battery discharge tests the device's battery discharge rate. The test will fail if the battery discharge is more than set in the <b>Pass threshold</b> (default value – 50 percentage points or p.p) within the time set in Duration (default value 10 minutes). These values are compliant with the e-Steward 2020 Guidelines.</p> <p><b>Warning!</b> The battery discharge test puts the CPU under heavy load which drains the battery. Running it on a poor battery can fail the erasure which might corrupt the drive. Consider applying an external heat dissipation in case of CPU overheating.</p>
BIOS logo	<i>(checked)</i>	BIOS logo test is used to check if the BIOS logo of the computer matches the manufacturer's logo, or if it has been customized.
CPU	<i>(checked)</i>	The CPU test checks the functionality of the processor.
Display	<i>(checked)</i>	Manual test for the display.
Keyboard	<i>(checked)</i>	Manual test for the keyboard. You can choose from "Compact" (no num pad) and "Full size" keyboards. There is also an option to select a different keyboard layout.
Network	<i>(checked)</i>	Test created per detected Ethernet interface. It is also possible to configure pingable IP addresses in CT.
Speaker	<i>(unchecked)</i>	Tests the laptop integrated speakers by playing a voice/audio sample.
Microphone	<i>(checked)</i>	Record and play a 5-second sample. Audio is shown as an amplitude meter for input and output. System master volume is 100% by default.

Name	Default/Example Value	Description
Memory	<i>(unchecked)</i>	The memory test checks the low and the extended memory (RAM) of a computer. Note that, depending on the amount of memory in the machine, this test can last from 20 seconds to several minutes.  The <b>Number of passes</b> is used to determine how many passes (1-99) is done on the memory test. Note that higher number of passes will make the test to take a longer time.
Motherboard	<i>(checked)</i>	The motherboard test checks the CMOS checksum and battery, the RTC and the DMI.
Optical Drive	<i>(checked)</i>	Manual test for the optical drive. This test has separate selections for <b>Write</b> (writing test), <b>Read</b> (reading test) and <b>Blank</b> (blanking test).
Pointer Device	<i>(checked)</i>	Manual test for the pointer device.
PC Speaker	<i>(checked)</i>	Manual test for the PC speaker (beeper connected to motherboard)
USB ports	<i>(checked)</i>	Manual test for testing the USB-ports of the machine. Note that this requires an external USB adapter (USB memory stick for example).
Webcam	<i>(checked)</i>	Manual test for the webcam. The user can take snapshots to verify if the camera is functional."
WiFi	<i>(checked)</i>	The test checks the detected WiFi-interfaces. If no configurations are made by the user, test will list available networks (manual pass/fail)  Test will fail automatically if no network could be reached or IP is missing.
Touchscreen	<i>(checked)</i>	Manual test for the touchscreen. The tests checks whether the touchscreen functions properly or has some issues by asking the user to touch grid on the screen.

### 3.6 Report

In this menu, report, asset report and fingerprint related settings can be configured. Here the "Customer details" and "Operator details" report fields can also be configured.

Report settings

Report format by default

xml

Report view by default

Standard

Locked

☐

Report digital signature key

Custom key label

Image contains no custom key

Generate

Upload

Customer details

### 3.6.1 Report settings

Name	Default/Example Value	Description
Report format by default	XML	The default report format(s) used by the client software to save and/or send reports. Releases before 6.7.0 offer 3 options (XML, PDF, XML+PDF), releases >= 6.7.0 offer 2 options (XML, PDF+XML).
Report view by default	Standard	The default report view (Standard or Advanced).
Locked	[unchecked]	If enabled, the report view cannot be changed by the user of the client software.

### 3.6.2 Report digital signature key

Name	Default/Example Value	Description
Custom key label	-	<p>These options are available on BDE 6.12.0 or higher and are used for managing a new key pair used to generate and verify a custom digital signature in the report. The key pair is generated using the RSA algorithm and it is 2048 bits long. If a key is uploaded, it must follow the PEM format and be 2048 bits long.</p> <p><b>Remove</b> removes the currently uploaded / generated private key from the image.</p> <p><b>Upload</b> is used to upload an external private key to the image. Note that allowed custom key size is between 2048 bits and 4096 bits. The accepted formats are PKCS#1 and PKCS#8 (unencrypted).</p> <p><b>Generate</b> creates a key pair, the private key is embedded into the image and both the private and the public keys can be downloaded.</p>

Name	Default/Example Value	Description
		Note: Whether you upload or generate a key pair, <b>it is strongly recommended that you store both keys in a secure environment</b> . The public key must be uploaded later in the BMC (5.4.0 or higher) in order to verify the custom digital signature (it won't be verified otherwise). A user-friendly label can be input during the pair generation or upload, its sole purpose is to allow a user to easily locate a key pair in both BDE and BMC. It is recommended to give key pairs distinct labels to prevent confusion. If no label is given during the pair generation or upload, a unique label is generated by CT.

### 3.6.3 Customer details

Name	Default/Example Value	Description
Enable	(checked)	Enable/disable customer related fields. Enabled by default.
Customer name	Example Company	Name of the company which owns the machines to erase (can be different than the Licensee).
Customer location	Example City	Location/address of the aforementioned customer.

### 3.6.4 Operator details

Name	Default/Example Value	Description
Enable	(checked)	Enable/disable operator related fields. Enabled by default.
Erasure provider	Example Provider Name	Name of the erasure provider which processes the machines.
Erasure technician	Example Erasure Technician Name	Name of the erasure technician.

### 3.6.5 Asset report settings

Name	Default/Example Value	Description
Write asset report	(unchecked)	If enabled, an asset report will be written on each erased drive after the erasure process has been successfully completed (drive was successfully erased, and the report was successfully saved/sent). The asset report is made bootable and is displayed as a static picture if the machine is rebooted with the erased drive.

### 3.6.6 Fingerprint settings

Name	Default/Example Value	Description
Write fingerprint	(unchecked)	This checkbox defines if the digital fingerprint is written in one sector of each erased drives after the erasure process has finished. Meant for fast verification of the erasure on servers. For more information about the digital fingerprint, see the Blancco Drive Eraser User Manual.






Name	Default/Example Value	Description
Location (sector)	200	In which sector the digital fingerprint is written on ("0" being the first sector).  If the "Write asset report" option is on, the sector value must be equal or greater than 200.

### 3.7 Custom fields



In this menu, custom fields can be added, deleted and modified. Custom fields are usually created and filled in by the Operator i.e. the person or company that carries out the drives' erasure.

Each user can customize them:

- By giving them any name he wishes.
- By filling them in with any default value.
- By setting them as normal or mandatory fields.
- By setting them as:
  - Fillable text boxes.
  - Dropdown lists with pre-filled values allowing the selection of one item.
  - Dropdown lists with pre-filled values allowing the selection of multiple items.
- Examples of custom fields' names: "Asset ID", "Asset type", "Asset value", "Destroy asset"...

Custom fields									
ID	Field name	Type	Values 	Preview	Required	Per connected device	Locked	Regular expression	Hint
1	Operator name	Multidropist	John,Jack,Peter		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
2	Warehouse	Droplist	~,New York,Paris,Joensuu		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
3	Drive ID	Textfield			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
4	Drive grade	Droplist	~,A,B,C		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Name	Default/Example Value	Description
FIELD NAME	Custom 1-n	Name of the custom field. This name can be modified by the user and is displayed in the Blancco Drive Eraser client software. Maximum length of the name is 220 characters.  Cannot be empty. Also, two or more fields cannot have identical names.
DEFAULT VALUE	Custom value~	Default value of the field - can be modified by the user by adding a (~) symbol right after it. Value maximum length is 1000 characters.
TYPE	textfield	Whether the field is a normal text box (textfield), a normal dropdown-list (droplist) or a dropdown-list with multiple selection of items (multidropist).  In order to create a dropdown and multidropdown custom field, first add a value on the field "Default value". Only then, the value of the field "Type" can be changed to "droplist" or "multidropist". As long as the

Name	Default/Example Value	Description
		<p>field "Default value" is empty, the custom field is considered a textbox and "Type" is locked on the value "textfield".</p> <p>With dropdown and multidropdown lists, each entry has to be separated by a comma (.). The string ,1,2,3 would give a dropdown-list with a first entry as empty, second as "1", third as "2" and fourth entry as "3". Duplicated entries are always removed. If the field is mandatory, empty entries are removed. If the rules described previously leave no value in the field and the field is mandatory, it will become a textfield (but will remain mandatory).</p>
REQUIRED (Checkbox)	[unchecked]	<p>Is the field mandatory (checked) or not (unchecked).</p> <p>Not available if "Erasure Process" is set to "Workflow".</p>
PER CONNECTED DEVICE (Checkbox)	[unchecked]	<p>If "Report per connected device" (see <a href="#">Security</a>) is enabled, the custom field behaves as an individual field per device (meant to contain information unique for each loose drive, Chromebook, etc.). This option is unavailable if the "Security – Report per connected device" setting is unchecked. Note that default values for custom fields are purged when "per connected device" option is used.</p>
LOCKED (Checkbox)	[unchecked]	<p>Locks the field. A locked field cannot be edited by the user running Blancco Drive Eraser (the field is greyed out).</p> <p>Note that a locked field requires a value in the <b>Default value</b> field. The field cannot be set as <b>Required</b> or <b>per device</b>.</p>
Delete field-button		Deletes the field.
Add field-button		Adds a new custom field.
Regular expression	n/a	Regular expression enforced on this field. See the chapter <a href="#">Regular Expressions for Custom fields</a> for more information.
Hint	n/a	Hint for the regular expression. This will be displayed to the user of the BDE.

Note that:

- The custom fields are text boxes, empty and not required by default.
- Any required custom field that is left empty here will have to be filled in during the Blancco Drive Eraser session before the user can save or send the report.
- There are by default 2 custom fields ("Custom 1" and "Custom 2"): these fields can be renamed, modified or deleted at will.

### 3.7.1 Eye icon



Clicking the eye icon on top right corner opens "Custom fields form preview" window, where you can view how the operator sees the custom fields. To see the "Per drive fields", there must be custom fields configured and ticked with "Per connected device".

Per drive fields:

### 3.7.2 Regular Expressions for Custom Fields

Each custom field can also be configured to require that the input given on the client software must follow predefined rules. The rules are set by using regular expressions.

The regular expression, which will determine what kind of input is accepted for that field, is inserted on the **Regular Expression** field. This software uses JavaScript's regular expression syntax.

For example, the regular expression `(A|F)[0-9]{3}` would require that the value is either "A" or "F" followed by 3 numerical characters (e.g. A245 would be an accepted input).

Note that the regular expressions are validated according to the rules of JavaScript's validation implementation. Any character not in the set of approved characters is considered a word break. This set of characters is limited to Roman alphabet in both upper- and lower-case, decimal digits, and the underscore character. Accented characters, such as "é" or "ü" are treated as word breaks. See JavaScript's documentation on regular expressions for more information.

Note that the following expression looks right:

`[0-9]{4|6}`

One might expect it to match a 4- or 6-digit long input. This is not the case. The expression in this case consists of two alternatives:

Alternative 1: `[0-9]{4}` (e.g. 1{4})

Alternative 2: `6`



Engine used by the Drive Eraser, will mark this expression as syntactically incorrect, because the curly braces have no open/close matching. Some of the resources available in the internet though, will find no error.

Regular expressions must be checked and tested prior using them in a Production environment. External tools (like <https://regexr.com>) should be used to validate the regular expressions entered in CT. Newer versions of Blancco Drive Eraser will purge invalid regular expressions.

The **Hint** can contain an indication of the kind of input that is expected, it is displayed on the client software's UI for this specific custom field. For the example above, the hint could be "A or F and three numbers". Note that a custom field with a regular expression cannot receive a predefined value (it will be purged).

### 3.8 Communication

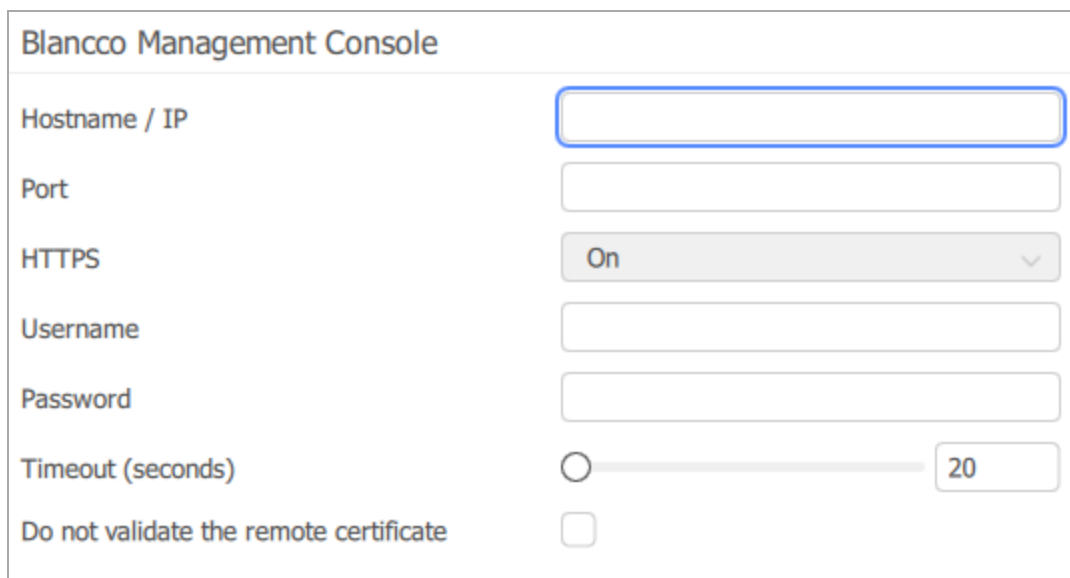
This menu contains options related to the connectivity with the server running the Blancco Management Console.

If the machine to erase is connected to a network where a BMC server is running, it is possible to configure the settings to establish a communication with it and:

- Consume licenses remotely via the network (HASP is connected to the BMC server, not to the machine).
- Send the asset report, issue report and/or erasure report to the BMC server (no need to save the report on an external device).

Note that:

- The IP address of the server (or its hostname if defined) running the BMC in your local network must be input. The communication protocol is always **https**.
- If one of these settings is missing, the machine to erase will not be able to communicate with the BMC server or send reports to it. However, you will be able to save reports on an external device (such as a USB-stick).



The screenshot shows the 'Blancco Management Console' settings page. It features several input fields and a checkbox. The 'Hostname / IP' field is highlighted with a blue border. The 'Port' field is empty. The 'HTTPS' field is a dropdown menu set to 'On'. The 'Username' and 'Password' fields are empty. The 'Timeout (seconds)' field is a slider set to 20. The 'Do not validate the remote certificate' checkbox is unchecked.

Blancco Management Console	
Hostname / IP	<input type="text"/>
Port	<input type="text"/>
HTTPS	On <input type="button" value="v"/>
Username	<input type="text"/>
Password	<input type="password"/>
Timeout (seconds)	<input type="range" value="20"/>
Do not validate the remote certificate	<input type="checkbox"/>

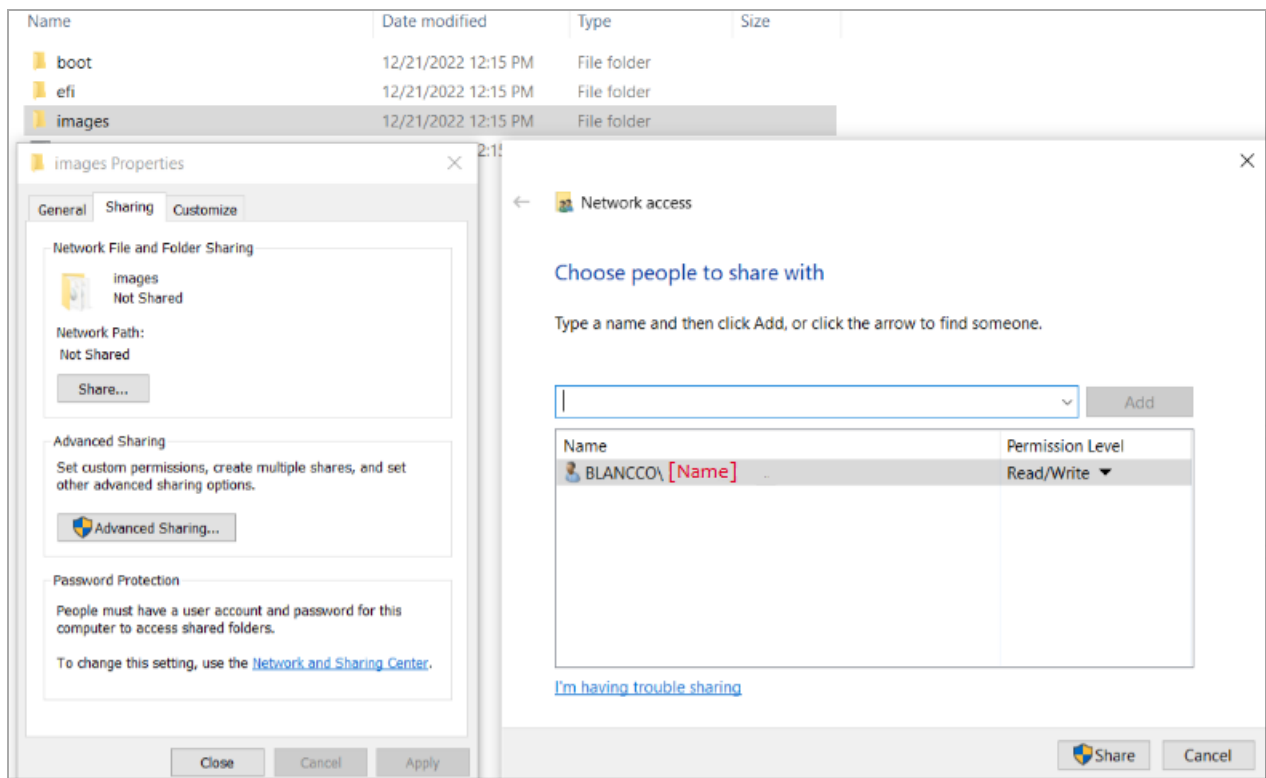
### 3.8.1 Blancco Management Console

Name	Default/Example Value	Description
Hostname / IP	<i>n/a</i>	IP-address of the server running the BMC in your local network. Example: 10.1.1.1 cloud.blancco.com https://172.16.1.98:8443
Port	<i>n/a</i>	Port number of the BMC. This port was set up when installing the BMC; it is the port 8443 by default (HTTPS protocol always enforced). Please check the BMC manual for more information.
HTTPS	<i>On</i>	Locked field, HTTPS capability is always On.
Username	<i>n/a</i>	Username for accessing the BMC. Values should be between 3 to 64 characters long.
Password	<i>n/a</i>	Password for the user set in "Username" for accessing the BMC. Values should be minimum 6 characters and maximum 64 characters long.
Timeout (seconds)	20	Time out for the BMC communication (how long the connection to BMC is tried). Possible values range from 20 seconds to 600 seconds (10 minutes). It is recommended to increase this value if you face recurring connectivity problems with the BMC.
Do not validate the remote certificate	<i>[unchecked]</i>	If activated, the TLS certificate offered by the Blancco Management Console <b>is not validated</b> .  Turned off by default.  Note that certificate validation is not possible if BMC address is an IP-address or localhost. In this case, this option is activated and cannot be modified.

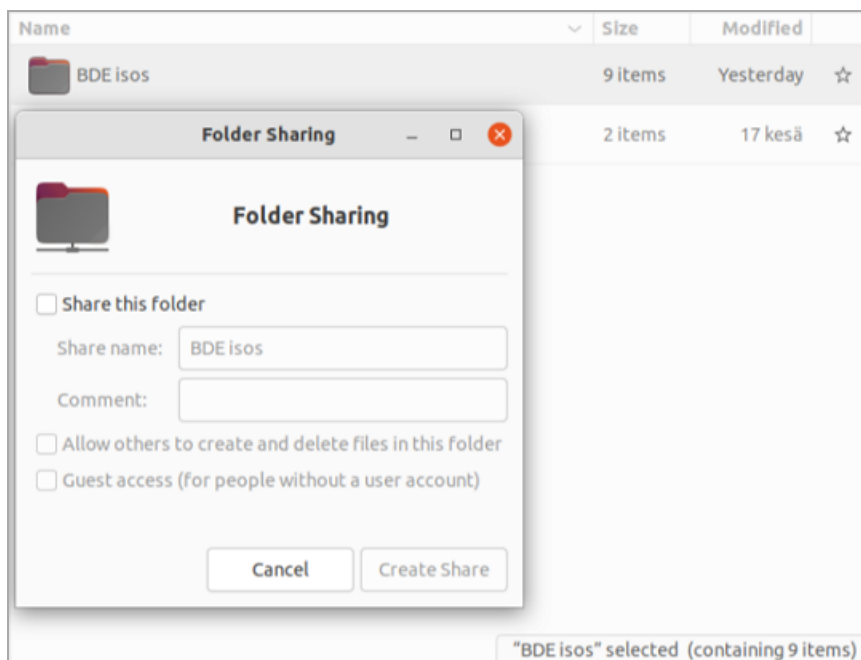
### 3.8.2 Network share

A network shared folder is a folder that has properties and permissions to be shared within a local network.

For example (Windows): Right click > Properties > Sharing:



For devices using Ubuntu: right click > Local network share:



Or via command line in Linux (<https://www.techrepublic.com/article/how-to-set-up-quick-and-easy-file-sharing-with-samba/>)

Using a network shared folder is interesting in case BDE is connected to a LAN without any internet connectivity or BMC. Once mounted in BDE, a network shared folder can be used as a location to save

reports. The network shared folder can be accessed by using different communication protocols, such as SSH, SMB, FTP, SFTP, NFS. BDE currently focuses only on SMB (Server Message Block) via a free software called "Samba".

To customize network share feature in CT:

### Network share

Hostname / IP

Path

Username

Password

••••••••

Domain *Optional*

Protocol

SMB

Name	Default/Example value	Description
Hostname / IP	n/a	IP or Hostname of the device performing the network share. Hostname can be either valid DNS resolvable name or IPv4 address of the server.
Path	n/a	Directory path of the location for saving BDE reports. Path is the share name of server and it can also contain one or more subdirectories. Those subdirectories must exist in the server before connection is established. Slash "/" is used for separator. Path is case insensitive and can contain spaces.
Username	n/a	Username must be at least 3 and maximum 64 characters.
Password	n/a	Password must be at least 6 and maximum 64 characters.
Domain	n/a	This setting is optional, but a server might need it for authentication.
Protocol	SMB	The network shared folder can be accessed by these protocols. There are multiple options, but currently the only communication protocol for BDE is Server Message Block (SMB).

### 3.8.3 VNC remote control

BDE is able to utilize VNC software for remote controlling a machine. These settings can only be changed in CT.

The settings are located under the **Communication** tab:

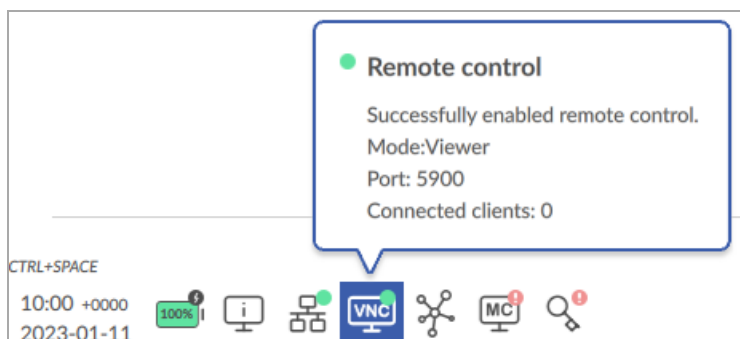
Communication	Password	<input type="text"/>
	Domain <i>Optional</i>	<input type="text"/>
Networking	Protocol	SMB <span>▼</span>
OS	VNC remote control	
Debug	Enabled	<input checked="" type="checkbox"/>
	Mode	VNC Repeater <span>▼</span>
	Hostname / IP	10.1.2.3
	Port	5432
	Password <i>Optional</i>	<input type="password"/>

When enabled, user can choose from two modes:

- **VNC viewer**

- In this mode BDE/BDV machine is in the same network with the user's host machine.
- User should run VNC viewer software of his choice and connect directly from the host machine to the BDE/BDV machine.

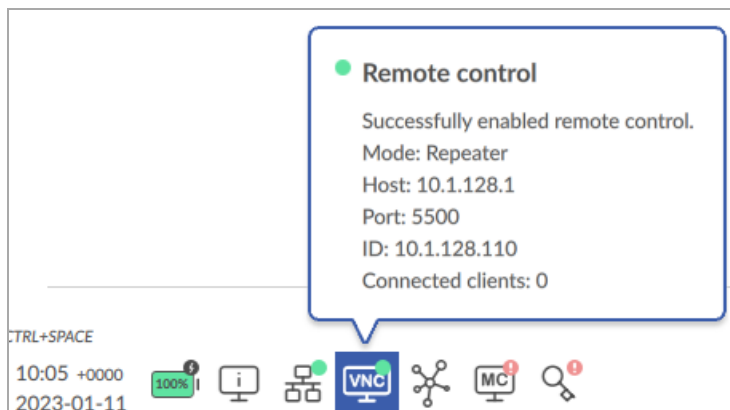
In BDE, the Viewer mode looks like this:



- **VNC Repeater**

- In this mode BDE/BDV machine is in the network that is not accessible by the user's host machine, but there is a another machine that both BDE/BDV and user's host machine can access.
- User should run VNC repeater software of his choice which acts like a proxy, sitting in the middle between the server and viewer. All data for the session is passed through the repeater. BDE/BDV connects to the repeater and the host machine running the VNC viewer software connects to the repeater.

- In BDE, the Repeater mode looks like this:



In the Repeater mode, Hostname / IP address of the repeater machine must be entered.

Port is the IP port of the VNC server that can accept remote connections. In **Viewer mode**, default port is 5900. In **Repeater mode**, the default port is 5500. Port number can freely be selected from a range of 1-65535 as long as port is not reserved for any other use.

**Note:** In the repeater mode, default port 5900 is in use for the repeater to connect so that a direct connection is also possible to that port.

Password is optional, so it can be left empty. Note that in some VNC viewer clients, empty password is not allowed, which means that the connection will not work.

## 3.9 Networking

This menu contains options related to the connectivity to the network of the machine that runs Blancco Drive Eraser.

### 3.9.1 Static/dynamic network settings

If the DHCP is turned on (it is turned on by default), the image automatically get its network related settings from the DHCP-server (dynamic network settings).

For those users that wish to configure a static network, the DHCP can be turned off (the DHCP box left unchecked) and the network settings can be input manually. If these settings are invalid, Blancco Drive Eraser cannot access the network.

Global network settings

Disable network entirely

☐

Enable SSH connections

☐

Report network information

☒

Networking

Wired enabled

☒

DHCP

☒

VLAN

Wireless

Wireless enabled

☐

Proxy

Hostname / IP

Port

Username

Password

Network security

Enabled

☐

### 3.9.2 Global Network Settings

Name	Default/Example Value	Description
Disable network entirely	[unchecked]	If selected, all network connections, wired and wireless, are disabled.
Enable SSH connections	[unchecked]	Whether SSH connections to client software are allowed or not.
Report network information	[checked]	When selected, the report will contain full network information. If not selected, all MAC, IP and DNS information is removed from the reports. Note that this setting does not

Name	Default/Example Value	Description
		affect the content of the issue report.

### 3.9.3 Networking

Name	Default/Example Value	Description
Wired enabled	<i>[checked]</i>	Whether wired network connection is enabled or not.
DHCP	<i>[checked]</i>	If checked, BDE will automatically get its network settings from the DHCP server (dynamic IP address, subnet mask, etc.). If unchecked, BDE needs to have its network settings statically defined (see the settings below).
Interface selection	<i>First suitable interface</i>	This setting is available if "DHCP" is unchecked. Selecting "First suitable interface" will apply the static network settings to the first network adapter that can use them. Selecting "Loop until connect to BMC" will loop through all detected network adapters and apply the static network settings to each one of them until one achieves a successful connection to BMC.
IP address	<i>192.168. 1.99</i>	This setting is available if "DHCP" is unchecked. This is the static IP address that BDE will use to connect to the network.
Subnet mask	<i>255.255. 255.0</i>	This setting is available if "DHCP" is unchecked. Address of the subnet mask of the network.
Default gateway	<i>192.168. 1.1</i>	This setting is available if "DHCP" is unchecked. Address of the default gateway of the network.
DNS1	<i>10.0.0.1</i>	This setting is available if "DHCP" is unchecked. Address of the primary DNS of the network.
DNS 2	<i>10.0.0.2</i>	This setting is available if "DHCP" is unchecked. Address of the secondary DNS of the network.
VLAN	<i>n/a</i>	VLAN ID. Acceptable value range is 1-4094. Note that if wireless is enabled, this field is purged and turned off.

### 3.9.4 WLAN connectivity

Things to note:

- The SSID or "network name" of the WLAN must be input, except for WPA-PSK encryption type empty password and SSID are allowed.
- The settings (password, encryption type, is network hidden) depend entirely on the wireless network characteristics. If the settings are incorrect, the machine to erase will not be able to communicate with the BMC server or send reports to it. However, you will be able to save reports on an external device (such as a USB-stick).
- In case both the LAN and the WLAN are available and the settings are valid, the communication with the BMC will use the first suitable network. LAN has higher priority over WLAN.
- WLAN settings are accessible only from the CT (not directly from the Blancco Drive Eraser GUI).



Wireless

Wireless enabled ☒

Encryption type WPA-PSK

Hidden SSID No

Wlan SSID ●●●●●●●●

Password ●●●●●●●●●●

Name	Default/Example Value	Description
Wireless Enabled	<i>[unchecked]</i>	Whether or not the WLAN connectivity is enabled.
Encryption type	<i>WPA-PSK</i>	Encryption Type of the wireless network. The types are: WPA-PSK, WPA-EAP, WEP and none (no encryption used).  Note that all EAP types, that don't require anything external (certificates and/or authentication server), are supported.
Hidden SSID	<i>No</i>	Is the SSID broadcast (public) or hidden.
WLAN SSID	<i>n/a</i>	The SSID value of the WLAN. Compulsory, if wireless is enabled.
Password	<i>n/a</i>	Password of the wireless network. Compulsory, if "Encryption Type" is anything else than "none".

### 3.9.5 Proxy

If a proxy is used for network connection, these fields must be filled.

Proxy

Hostname / IP

Port

Username

Password

Name	Default/Example Value	Description
Hostname/IP	<i>10.1.1.1</i>	IP-address of the proxy.
Port	<i>8080</i>	Port number for the proxy.
Username	<i>Username</i>	Username for the proxy.
Password	<i>StrongPassword</i>	Password for the proxy.

### 3.9.6 Network security

If network security is enabled, then the support for 802.1x authentication is enabled. This will allow network connection over network adapters and WP2 enterprise Wi-Fi.

Name	Default/Example Value	Description
Enabled	<i>(not checked)</i>	Whether or not this feature is enabled.
Protocol	<i>PEAPv0/EAP-MSCHAPv2</i>	Selected protocol.
Identity	<i>IdentityName</i>	Identity of the network.
Password	<i>StrongPassword</i>	Password for the network.
Use CA certificate	<i>(not checked)</i>	Whether or not the CA (Certificate Authority) certificate uploaded below is used or not.
Filename	<i>Image contains no certificate / [certificate name]</i>	<p>Name of the uploaded certificate.</p> <p>Upload a CA certificate from clicking the Upload-button. This will open the file explorer. Use that to navigate to and select the CA certificate.</p> <p>If a certificate is uploaded, click the Remove-button to remove it.</p>

Note that the CA Certificate -file must be in a valid format. Valid format is a X509V3 in PEM container and the maximum reserved size for storing them is 10 KB. If the certificate is in wrong format, it is possible to convert it.

Example, where DER is converted to PEM format with openssl:

```
openssl x509 -inform DER -outform PEM -text -in mykey.der -out mykey.pem
```

## 3.10 OS

This menu contains some extra settings that have an influence on the way the software boots and behaves.

### 3.10.1 Boot options

The Boot Options allow Blancco Drive Eraser to be booted with alternative settings, if there are issues with the default booting.

Boot options

Preset

FLR during startup [DEFAULT]

CD ejection

After boot-up

☒

After completed erasure

☐

After report sending/saving

☐

At shutdown

☐

Restart / Shutdown

Preset

none

List of hybrid drives

Import from file

Export to file

The Blancco Drive Eraser image can be booted in several different ways, each way enabling a different set of features.

These options are:

**FLR during startup** – This is the default option. The Freeze lock removal process is carried out during the booting phase, before loading all the system drivers, to increase the chances to wake up the machine after the freeze lock removal.

**Normal startup (native resolution)** – Blancco Drive Eraser is loaded using any available driver that corresponds to the graphical card of the machine (the standard/universal graphical driver is just a fallback).

**Normal startup (safe resolution)** – Blancco Drive Eraser is loaded using a standard/universal graphical driver. The screen resolution of the GUI is static (1024\*768).

**Installer** – This booting option allows to install the software on a machine (persistent installation). To be used to process loose drives or Chromebooks, for instance. All erasure reports are stored on the installation drive but can be exported to an external USB stick or sent to BMC.

**Show startup messages** – This is the same option than the second one, except that startup messages are shown in the screen instead of the animated loading screen.

**Customized startup** – When this option is selected a text field named "Command line "will appear:

Boot options

Preset

Customized startup

Command line

archisobasedir=arch archisolabel=BLANCCO co

This text field can be used to freely configure the booting parameters. The following booting parameters are validated by the Drive Eraser Configuration Tool:

Parameter	Possible values / Extra options	Description
cr		Enable manual Crash Reporter mode.
debug		Enable more kernel messages. Meant for troubleshooting. Opposite of "quiet".
fir	flr=15 flr=10 flr=20 flr=30 flr=60 flr=forced flr=disabled	Enable Freeze Lock Removal during bootup. By default, there is 10 second alarm in which time computer should be able to suspend itself and resume when alarm is set. In CT, there is a sanity check that timeout value is between 5 and 60 seconds. That check can be bypassed by modifying the parameters during boot up. "flr = [15-60]" is used to modify the timeout. "flr=15", would be 15 seconds. If parameter is not given or is unknown value, default timeout (10 seconds) will be used instead. "flr=forced" forces the flr to occur always. "flr=disabled" disables freeze lock removal completely from being attempted.
intremap	intremap=nosid intremap=on intremap=off intremap=no_x2apic_optout intremap=nopost	"intremap" means interrupt remapping, which is a software capability for rerouting signals from a peripheral device. This option allows the kernel to replace the remapping tables created by the machine's BIOS. The user can choose the value out of the following: "on", "off", "nosid", "no_x2apic_optout", "nopost". "intremap=nosid" setting is Required for Macbook 12, 13,3, 9,1 screen / boot to work properly.
kms		Enables kernel mode setting (chances are it will be enabled anyway unless explicitly disabled). This lets the kernel to set the graphic driver.
loglevel	loglevel=0	Amount of kernel messages during booting. "loglevel=0" shows only the emergency-level kernel messages, to clean up booting.
memtest	memtest=00	Specifies the number of memory tests passes to be performed. 17 different test patterns are available. memtest=00 means that memory tests are disabled. If enabled, 17 passes are done by default, which will go through all of the test patterns. Maximum number of rounds is 99.
noapic		This option disables APIC. Disabling APIC removes the ability to make use of IRQ sharing or device IRQ remapping. APIC (Advanced Programmable Interrupt Controller) is the replacement for the old PIC chip that, in the past, was embedded on motherboards and allowed the configuration of interrupts for peripherals like soundcards, IDE controllers, sharing/redirecting of interrupts.
nomodeset		Selecting this option instructs the kernel to not load video drivers

Parameter	Possible values / Extra options	Description
		and use BIOS modes instead.
quiet		Disable most kernel messages. Opposite of "debug".
rd.driver.blacklist=nouveau modprobe.blacklist=nouveau		nouveau driver of NVIDIA Intel graphic card is known to cause issues (e.g. laptops with Optimus technology).  Manually adding these both of these options will allow using i915 VGA Intel controller instead and solve black screen issue on such machines.
nouveau.modeset	nouveau.modeset=0	Whether the driver should be enabled. 0 for disabled, 1 for enabled, 2 for headless. Helps with some HP ZBook models.  More information: <a href="https://nouveau.freedesktop.org/KernelModuleParameters.html">https://nouveau.freedesktop.org/KernelModuleParameters.html</a>
pci	pci=noms, noaer	"pci" is used for various PCI subsystem options.  "pci=noms, noaer" is used to solve issues with Lenovo 88E8057 ethernet controller.
radeon.runpm=0		Disables PX runtime power management.  Resolves some Radeon graphics driver troubles on some machines with switchable dual graphics cards (integrated Intel + AMD/ATI).
random.trust_cpu=1	1 = on 0 = off	Enable or disable trusting the use of the CPU's random number generator (if available) to fully seed the kernel's CRNG.
rd.udev.log-priority=3		Clean up the systemd startup message: "starting version..."
splash		Show Blancco Drive Eraser splash screen during boot.  Remove the parameter to boot Macbook 7.1, 7.2, 11.1, 11.3
verbose		Flag for Drive Eraser init scripts. It disables the splash screen and show the messages on the screen.
vmalloc=400M		Increases the default (128MB) memory allocation for virtually contiguous memory. Is needed for PXE booting, since the ISO-image will first be loaded to this memory area before booting.
ip=dhcp BOOTIF=\${netX/mac}		If there are problems with PXE/iPXE with some Legacy BIOS/UEFI combinations.  replace \${netX/mac} with the mac address of the network interface you are booting from.
acpi=off		Allows internal SSD to be detected properly on some HP EliteDesk models.

For unvalited parameters, see - <https://www.kernel.org/doc/html/v4.15/admin-guide/kernel-parameters.html>

For more information, see the Blancco Drive Eraser manual, chapter "Bootting options" and <https://support.blancco.com>.

### 3.10.2 CD tray eject

Blancco Drive Eraser can automatically eject the trays of all the optical drives connected to and recognized by the machine. The ejection can be selected to occur at the following moments:

- After boot-up – Immediately after Blancco Drive Eraser has booted up. Selected by default.
- After completed erasure – After the erasure(s) have been completed.

- After report sending/saving – After a report has been sent to the Blancco Management Console or saved to a USB-stick.
- At shutdown – When exiting Blancco Drive Eraser.

Note that:

- The main purpose of the CD tray ejection is to prevent potential data breaches that may occur in case of optical disks containing personal/professional data being forgotten inside a machine that is erased and that is shipped away. In that regard, Blancco recommends to always leave at least one option selected.
- The CD ejection feature is also used to monitor the different phases of the erasure process (booting, erasure, report, shutdown). In that regard, several ejections can be selected.

### 3.10.3 Restart / Shutdown

Blancco Drive Eraser can automatically restart or shutdown. This functionality cannot be activated when **Process** is set to **Manual** or **Workflow** (see [Security](#)). The following options are available:

- **none** – The default value. No automatic restart or shutdown.
- **Restart, after erasure** – Machine is automatically restarted, after the erasure process has finished.
- **Restart, after successful erasure** – Machine is automatically restarted, after the erasure process has finished in a successful state.
- **Shutdown, after erasure** – Machine is automatically shut down, after the erasure process has finished.
- **Shutdown, after successful erasure** – Machine is automatically shut down, after the erasure process has finished in a successful state.

### 3.10.4 List of hybrid drives

The list of hybrid files embedded in Blancco Drive Eraser can be modified with this menu.

To export the current list of hybrid drives, click the “Export to file”. This exports a file called “hybrid\_list.txt”. This list can be modified (add/remove hybrid drive models).

To import a modified hybrid drive list, click the “Import from file”. The file must be a .txt file and the hybrid drives information must be in the format:

```
Manufacturer;model
```

Example: Seagate;ST1000DX001

For more information on hybrid drives, see the Blancco Drive Eraser manual.

## 3.11 Other buttons

The rest of UI functionalities are described here.

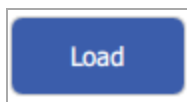
### 3.11.1 Language

Clicking this button will open the dropdown-menu from which the UI language can be changed.



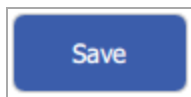
### 3.11.2 Load new image

With this button you can load another Blancco Drive Eraser image for configuration.



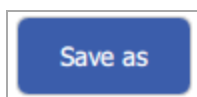
### 3.11.3 Save

Press this button to save all the changes done so far. Note that this won't create a new image file yet.



### 3.11.4 Save as

Press this button to save the configured image (ISO image). You can save the image locally or on a network drive.



Once you have saved the image, you can:

- Use it to burn a CD
- Add it to a bootable USB-stick (you can use the Blancco USB Creator tool for that purpose)
- Add it as a bootable image on a Preboot eXecution Environment or PXE (network booting)

## 4. Configuring Blancco Drive Verifier

With CT, it is possible to configure all of the main options of Blancco Drive Verifier. Note that the availability of configuration options depends on Blancco Drive Verifier product variant and version.

After loading a Blancco Drive Verifier image in the software, you will be able to adjust the settings. Note that inaccessible settings show up in gray color.

### 4.1 General

This menu will allow the general options to be configured. For more information on these settings, refer to "General" on page 12

### 4.2 Process

This menu contains options for processes, such as controlling the software remotely. For more information on these settings, refer to [Process](#).

### 4.3 Workflow

This menu contains options to configure the workflow. For more information on these settings, refer to [Workflow](#).

### 4.4 Security (BDV)

This menu contains options for security features for verification.



Security options

Verification standard

...

All sectors the same

Byte value

0x00

Fail process if read errors

☒

Fail threshold

5

Fail process if the speed is too low (MB/s)

☐

Fail threshold

1

Execute self-tests on drives

None

Fail process if unsuccessful

☐

Verification level

☐

1

%

Simultaneous operations limit

50

Disable block SID authentication

No, skip

Timeout (seconds)

☒

5

Lock the verification settings

☐

Device enrollment detection

Persistent software

☐

Power saving settings

Spin down idle disks

☐

Name	Default/Example Value	Description
Verification standard:	All sectors the same	Default standard used in the erasure procedure. Blancco Drive Verifier currently supports 4 different verification standards. See Blancco Drive Verifier manual for more information. The user can hide some standards from the BDV user interface via the edit button (three dots) next to the standard list.
Byte value	-	Byte value (a.k.a pattern) that BDV will search throughout the drive, used if the standard is "All bytes the same".
Fail process if read errors	[checked]	If enabled, the threshold on read error count is defined here. If during the verification the read error count reaches this threshold, then the verification will automatically stop and fail. The default threshold is 5 errors. Additionally, the report will show an error message informing about this. Minimum error threshold is 1 and maximum is 1000
Fail process if the speed is too low (MB/s)	[unchecked]	Fail the verification if the verification speed is lower than the value set in the "Fail threshold" field. Disabled by default. Default value is 1 and the value range is

Name	Default/Example Value	Description
		1-10000. The unit is Megabytes/second.
Fail process by timeout (hours)	[unchecked]	Fail the process if its duration is longer than the value in the "Fail threshold" field.  Disabled by default. Default value is 48h. Custom range is from 1 hour to 1 year (8760h)
Execute self-tests on drives	[None]	This option sets the drive's S.M.A.R.T self-test to " <b>None</b> " (no testing – default option), " <b>Short</b> ", " <b>Conveyance</b> " or " <b>Extended</b> ". For more information about the self-tests, see the client software's user manual.
Fail process if unsuccessful	[unchecked]	If this option is enabled and the selected self-test fails, the verification process is aborted and failed. The reason for the failure is marked to the report. This option is only available if the previous setting "Execute self-tests on drives" is enabled.
Verification level	1%	This setting defines the verification level. The verification process reads data from the drive at randomly selected intervals and makes sure that the drive is covered with periodic patterns. The minimum verification corresponds to checking 1% of the surface of the drive (fast process), while the full verification corresponds to checking 100% of the surface of the drive (slower process).
Simultaneous operations limit	[50]	Maximum number of simultaneous verifications. If the number of simultaneous verifications is less than the limit, then new verifications can be started until the limit is met. If the number of verifications exceeds this value, the excess and new verifications are put in a verification queue and are paused until they can be started.
Disable block SID authentication	No, skip	Block SID Authentication (BSA) is a type of lock that prevents running firmware commands on the machine drives. This setting allows pre-configuring a dialog to turn on/off that lock, as well as a timeout (sub-setting). This setting has more to do with an erasure process, see " <a href="#">Configuring Blancco Drive Eraser</a> "
Lock the verification settings	[unchecked]	If this option is enabled, the user of BDV cannot change the verification settings.
Estimate remaining drive life	[unchecked]	Activating this setting will display in the report an estimate on the time left on each drive, based on several internal attributes. Read more in the BDE user manual.

#### 4.4.1 Device enrollment detection

For more information on these settings, refer to the "[Security](#)" chapter.

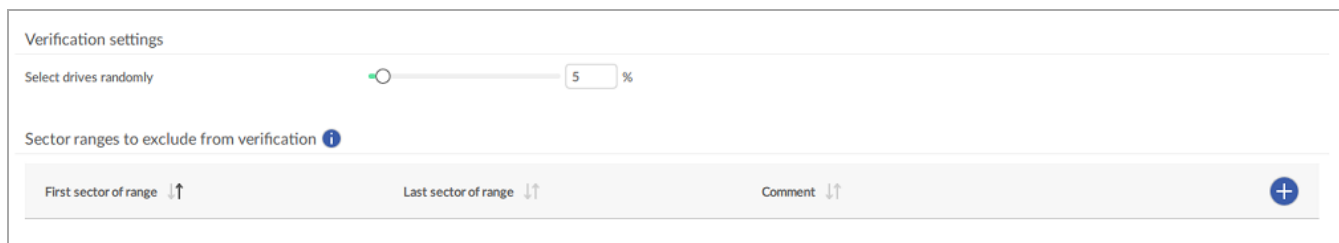
#### 4.4.2 Power saving settings

For more information on these settings, refer to the "[Security](#)" chapter.

## 4.5 Verification

In the Verification settings tab, you can define how many drives should be verified, as well as what are the sectors that should be excluded from the verification.

The slider "Select drives randomly" is set to 5% by default: if this value is not set to 100%, only a subset of the drives will be automatically selected for verification, nevertheless, a minimum of one drive per asset will always be verified.



First sector of range	Last sector of range	Comment
-----------------------	----------------------	---------

**Example 1:** the percentage of drives to be verified is set to 5% and BDV is run on a laptop that has one drive: the drive in question will be verified consistently.

**Example 2:** the percentage of drives to be verified is set to 5% and BDV is run on a server that has five drives: one drive will be randomly selected for verification.

**Example 3:** the percentage of drives to be verified is set to 5% and BDV is run on a server that has forty drives: two drives will be randomly selected for verification.

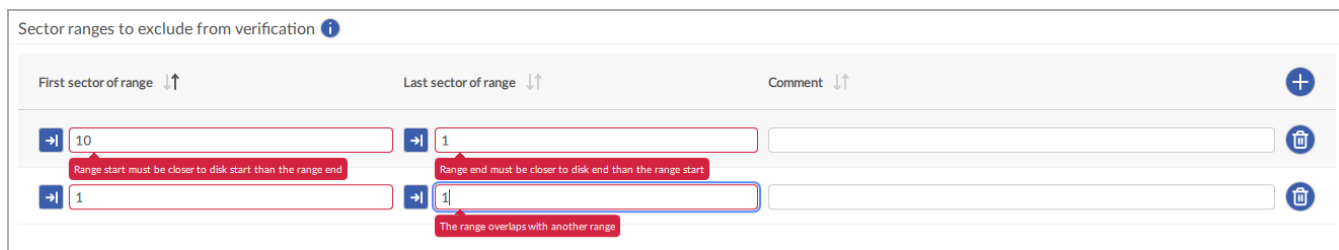
**Example 4:** the percentage of drives to be verified is set to 5% and BDV is run on a server that has one hundred drives: five drives will be randomly selected for verification.

If you want all your drives to be consistently verified, set the percentage to 100%. The 5% default value corresponds to the percentage of assets that need to be verified according to the R2v3 certification (<https://sustainableelectronics.org/welcome-to-r2v3/>).

The typical sectors to be excluded from the verification are those containing a Fingerprint or those containing a Bootable Asset Report. More information on the Fingerprint and the Bootable Asset Report in the BDE user manual.

Configure a range of sectors to exclude from the verification by clicking the + button. A range has a first sector and a last sector but you can also decide from where you start counting (from the beginning or from the end of the drive), you can also add a comment per range (e.g. "Fingerprint sectors"). The counting direction is chosen with the blue arrows.

Some rules do apply: no sector overlapping is possible, if the first sector is counted backwards the last cannot be counted forward, the last sector cannot be smaller than the first sector (if both are forward) etc.













First sector of range	Last sector of range	Comment
10	1	
1	1	

With the arrows next to the ranges and comment row, you can choose how to sort the different options, i.e. in ascending order.

Note: If the second button turns gray, it means it is not interactive anymore. To change it back to blue, click the left button so it sets back to "Counting from beginning of the drive".

Some possible combinations are listed below (the explanation is in the Comment section):

Sector ranges to exclude from verification ⓘ		
First sector of range ↓↑	Last sector of range ↓↑	Comment ↓↑
 0	 9	Excludes the first 10 sectors of the drive
 200	 300	Excludes all the sectors between #201 and #301 counting from the beginning of the drive
 9	 0	Excludes the last 10 sectors of the drive
 100	 50	Excludes all the sectors between #51 and #101 counting from the end of the drive
 2000	 3000	Excludes all the sectors between #2001 (from the beg. of the drive) and #3001 (from the end of the drive)

## 5. Uninstallation

### 5.1 Uninstaller script

#### 5.1.1 In Windows-systems

Uninstall the CT just like any other Windows program: Start Menu -> Settings -> Apps -> Apps & Features -> CT -> Uninstall

#### 5.1.2 In Linux-systems

Simply delete the .appimage file of the CT.

## 6. 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/resources/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!



# Drive Eraser Configuration Tool

**Manual del usuario para la versión 3.8.0**

**2023-08-02**

# Índice

---

1. Introducción e instalación .....	59
1.1 Descripción general .....	59
1.2 Declaración de copyright y confidencialidad .....	59
1.3 Requisitos del sistema .....	59
1.4 Instalación en Windows .....	59
2. Uso de Blancco Drive Eraser Configuration Tool .....	64
2.1 En sistemas Windows: .....	64
2.2 En sistemas Linux: .....	64
2.3 Cargar una nueva imagen .....	64
3. Configuración de Blancco Drive Eraser .....	65
3.1 General .....	65
3.1.1 Información de imagen .....	66
3.1.2 Configuración de localización .....	66
3.1.3 Configuración de salvapantallas .....	67
3.1.4 Configuración de la interfaz de usuario .....	67
3.1.5 Vista del dispositivo .....	68
3.1.6 Exportación e importación de archivo de configuración .....	68
3.2 Proceso .....	69
3.2.1 Opciones de licencia .....	69
3.2.2 Opciones de proceso .....	69
3.2.3 Mostrar más .....	71
3.2.4 Dispositivos conectados .....	71
3.3 Flujo de trabajo .....	72
3.3.1 Opciones de flujo de trabajo .....	72
3.3.2 Flujo de trabajo externo .....	73
3.3.3 Flujo de trabajo integrado .....	73
3.4 Seguridad .....	73



---

3.4.1 Opciones de seguridad .....	74
3.4.2 Trusted Platform Module .....	77
3.4.3 Opciones de controlador .....	78
3.4.4 Detección de inscripción de dispositivos .....	78
3.4.5 Ajustes de formato .....	79
3.4.6 Configuración de ahorro de energía .....	79
3.5 Pruebas de hardware .....	79
3.6 Informe .....	82
3.6.1 Configuración de informes .....	82
3.6.2 Clave de firma digital de informes .....	83
3.6.3 Detalles del cliente .....	83
3.6.4 Datos del operador .....	84
3.6.5 Configuración de informes de activos .....	84
3.6.6 Configuración de huella digital .....	84
3.7 Campos personalizados .....	84
3.7.1 Icono de ojo .....	86
3.7.2 Expresiones regulares para campos personalizados .....	87
3.8 Comunicación .....	88
3.8.1 Blancco Management Console .....	89
3.8.2 Recurso compartido de red .....	89
3.8.3 Control remoto VNC .....	91
3.9 Red .....	93
3.9.1 Configuración de red estática/dinámica .....	93
3.9.2 Configuración de red global .....	94
3.9.3 Red .....	95
3.9.4 Conectividad WLAN .....	95
3.9.5 Proxy .....	96
3.9.6 Seguridad de red .....	96

---

3.10 SO .....	97
3.10.1 Opciones de arranque .....	97
3.10.2 Expulsión de bandejas de CD .....	101
3.10.3 Reinicio / apagado .....	101
3.10.4 Lista de discos híbridos .....	101
3.11 Otros botones .....	102
3.11.1 Idioma .....	102
3.11.2 Cargar nueva imagen .....	102
3.11.3 Guardar .....	102
3.11.4 Guardar como .....	102
4. Configuración de Blancco Drive Verifier .....	104
4.1 General .....	104
4.2 Proceso .....	104
4.3 Flujo de trabajo .....	104
4.4 Seguridad (BDV) .....	104
4.4.1 Detección de inscripción de dispositivos .....	107
4.4.2 Configuración de ahorro de energía .....	107
4.5 Verificación .....	107
5. Desinstalación .....	109
5.1 Guion de desinstalación .....	109
5.1.1 En sistemas Windows .....	109
5.1.2 En sistemas Linux .....	109
6. Información de contacto .....	110

# 1. Introducción e instalación

## 1.1 Descripción general

Blancco Drive Eraser Configuration Tool (BDECT, DECT o CT) permite preconfigurar una imagen ISO de Blancco Drive Eraser (BDE o DE) o de Blancco Drive Verifier (BDV o DV).

Esta herramienta no debe compartirse con personal no autorizado: cualquier persona que tenga acceso a CT y al archivo de imagen ISO de Drive Eraser puede cambiar la configuración de la imagen. Esto podría tener como resultado un incumplimiento en la política de seguridad de la organización (por ejemplo, el cambio de la norma/opciones de borrado establecidas por la política de la organización).

## 1.2 Declaración de copyright y confidencialidad

Ninguna parte de este manual, lo que incluye los productos y software descritos en él, puede reproducirse, transmitirse, transcribirse, almacenarse en un sistema de recuperación ni traducirse a ningún idioma de ninguna forma y por ningún medio, excepto la documentación que guarda el comprador de Drive Eraser Configuration Tool. La información contenida en este documento está sujeta a cambios sin previo aviso. Los productos y nombres corporativos que aparecen en este manual pueden ser o no marcas registradas y tener o no copyrights de sus respectivas empresas y se utilizan solo para identificación o explicación en beneficio del cliente sin ninguna intención de cometer una infracción.

Copyright © 2023 Blancco Technology Group. Todos los derechos reservados.

Este documento es estrictamente confidencial y privado para sus destinatarios y puede contener información privilegiada legalmente y de copyright, marca registrada, patente o cualquier otro tipo de información restringida que es solo para que la vea el destinatario previsto. Blancco Technology Group no hace representaciones ni otorga garantías de ninguna naturaleza en relación a este documento, lo que incluye, sin limitarse a, la exactitud ni exhaustividad de ninguna información, hechos y opiniones que contenga. Al acceder a este documento, confirma que acepta y está de acuerdo con lo anterior.

## 1.3 Requisitos del sistema

- Windows Server 2016, cualquier sistema operativo Windows 10 o Linux con soporte para appimages.
  - Si el software se ejecuta en una máquina virtual Windows, deberá deshabilitarse la aceleración 3D en dicha máquina virtual. Esto se ha probado en VirtualBox.
- Derechos de administrador (acceso raíz) del sistema.
- 500 MB de espacio disponible en el disco duro.
- Actualizaciones más recientes del sistema operativo instaladas.

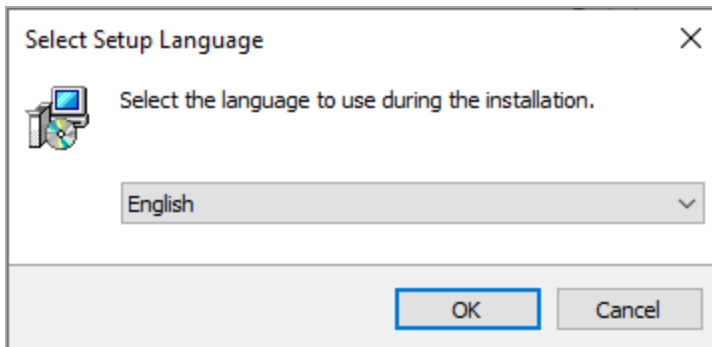
En Windows, la resolución de la pantalla (ajuste "Escala y diseño") no debe definirse por encima del 100 %. Si este ajuste es superior al 100 %, Blancco Drive Eraser Configuration Tool no funcionará correctamente.

**IMPORTANTE:** A partir de la versión 3.0, CT está diseñado para funcionar con Drive Eraser 6.10 o posterior.

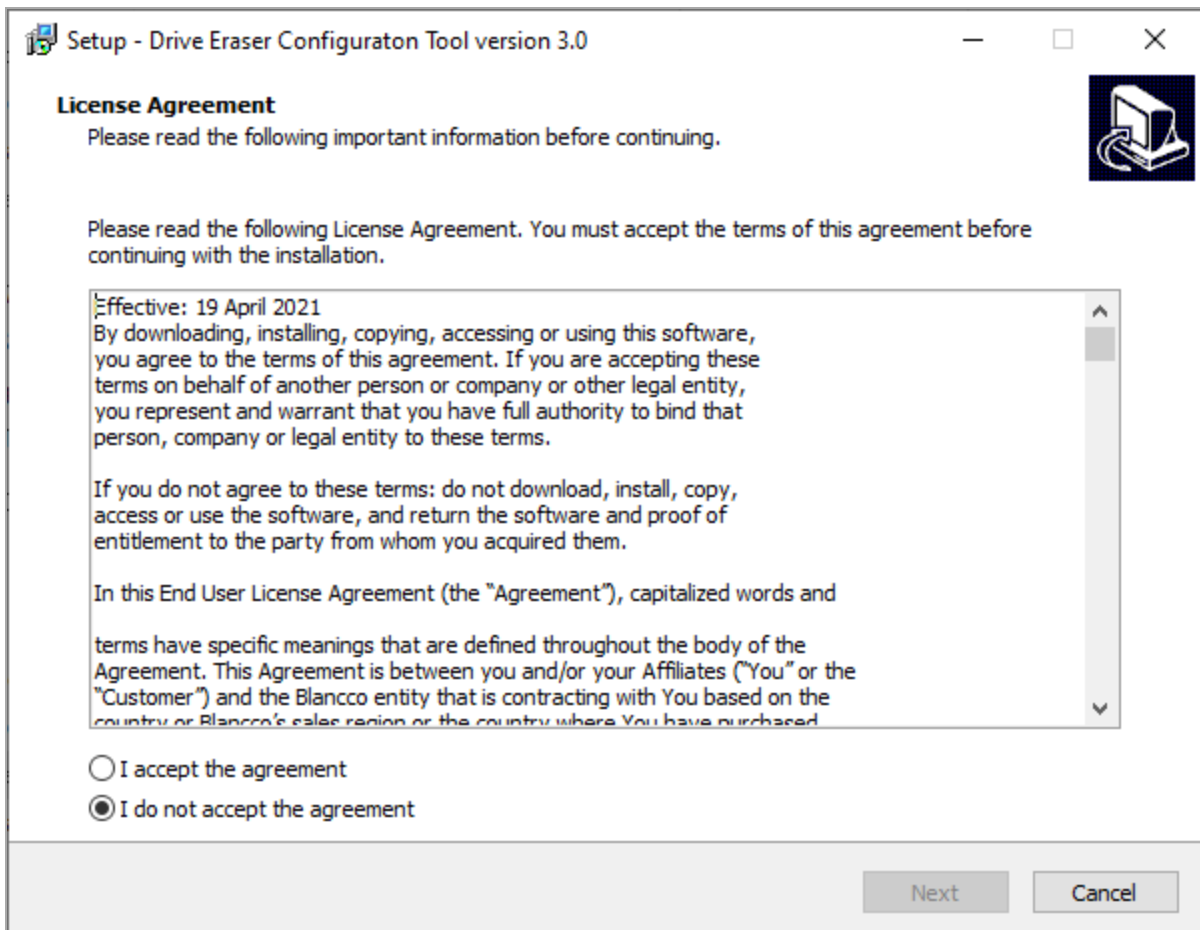
## 1.4 Instalación en Windows

Antes de continuar, asegúrese de haber desinstalado cualquier versión anterior de Blancco Drive Eraser Configuration Tool; siga las instrucciones de la sección "Desinstalación".

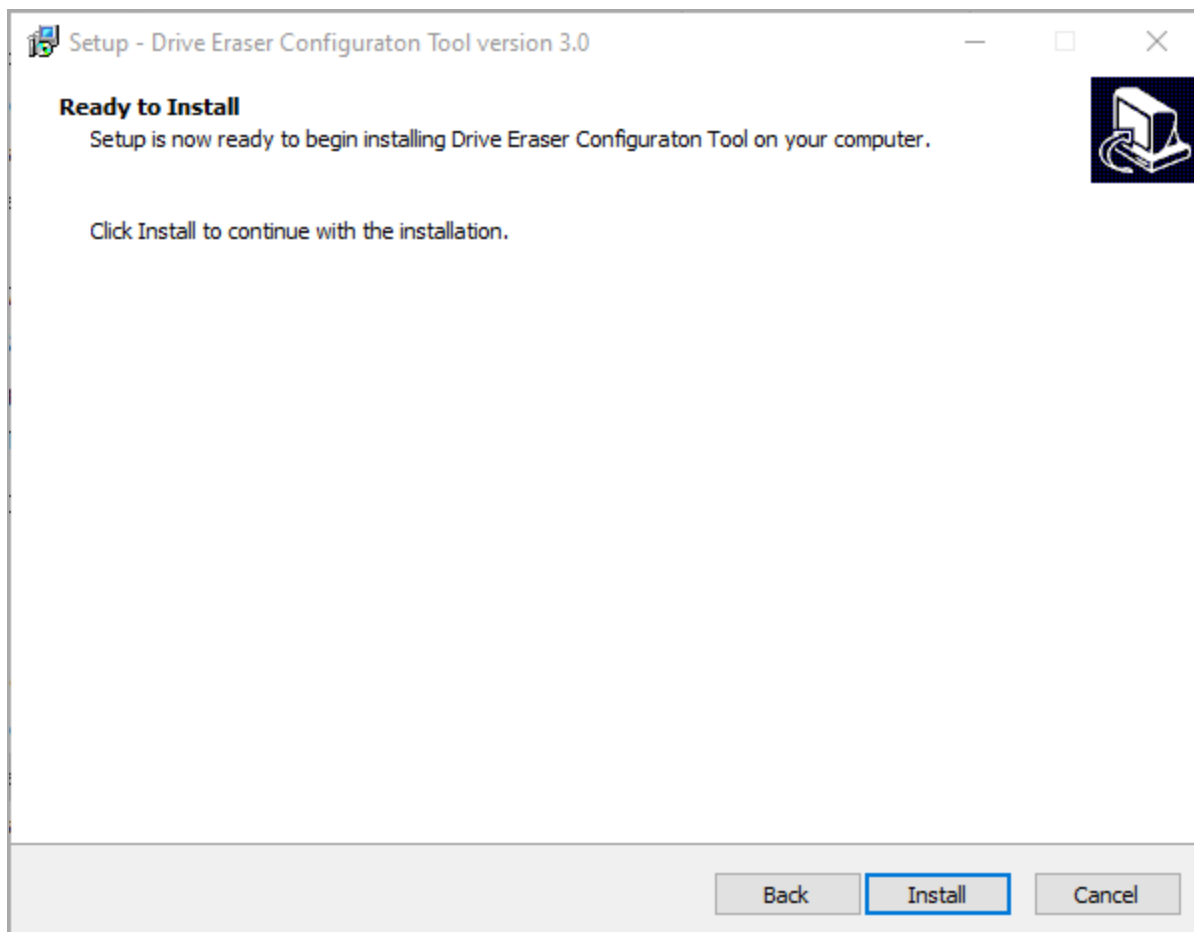
- Haga doble clic en el ejecutable de instalación suministrado por Blancco para iniciar el asistente de instalación. Asegúrese de ejecutar el paquete de instalación con derechos de administrador.
- Seleccione su idioma de instalación:



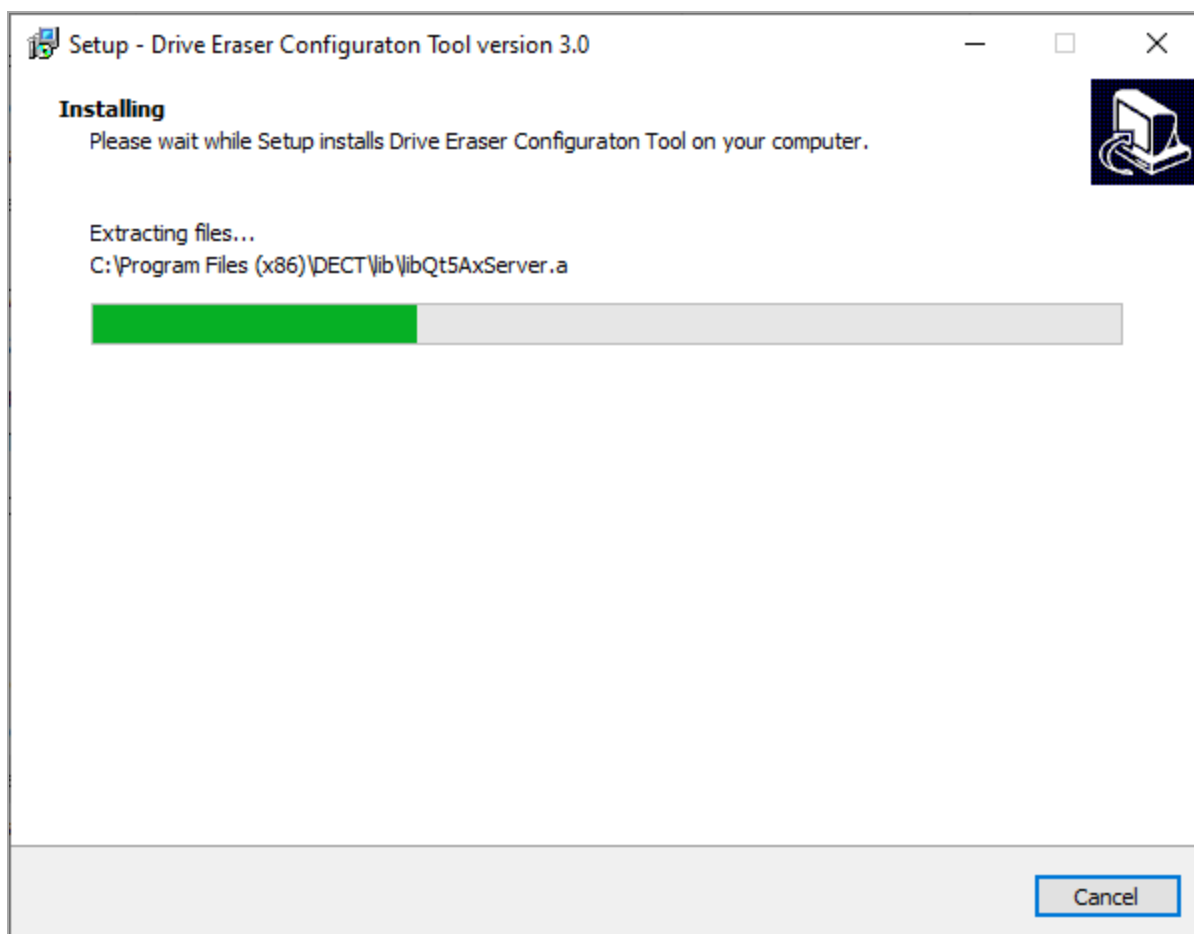
- Lea el Contrato de licencia (visite <http://www.blancco.com/en/eula>) y, si está de acuerdo con él, seleccione **"Acepto los términos de este contrato de licencia."** y haga clic en **"Siguiente"**:



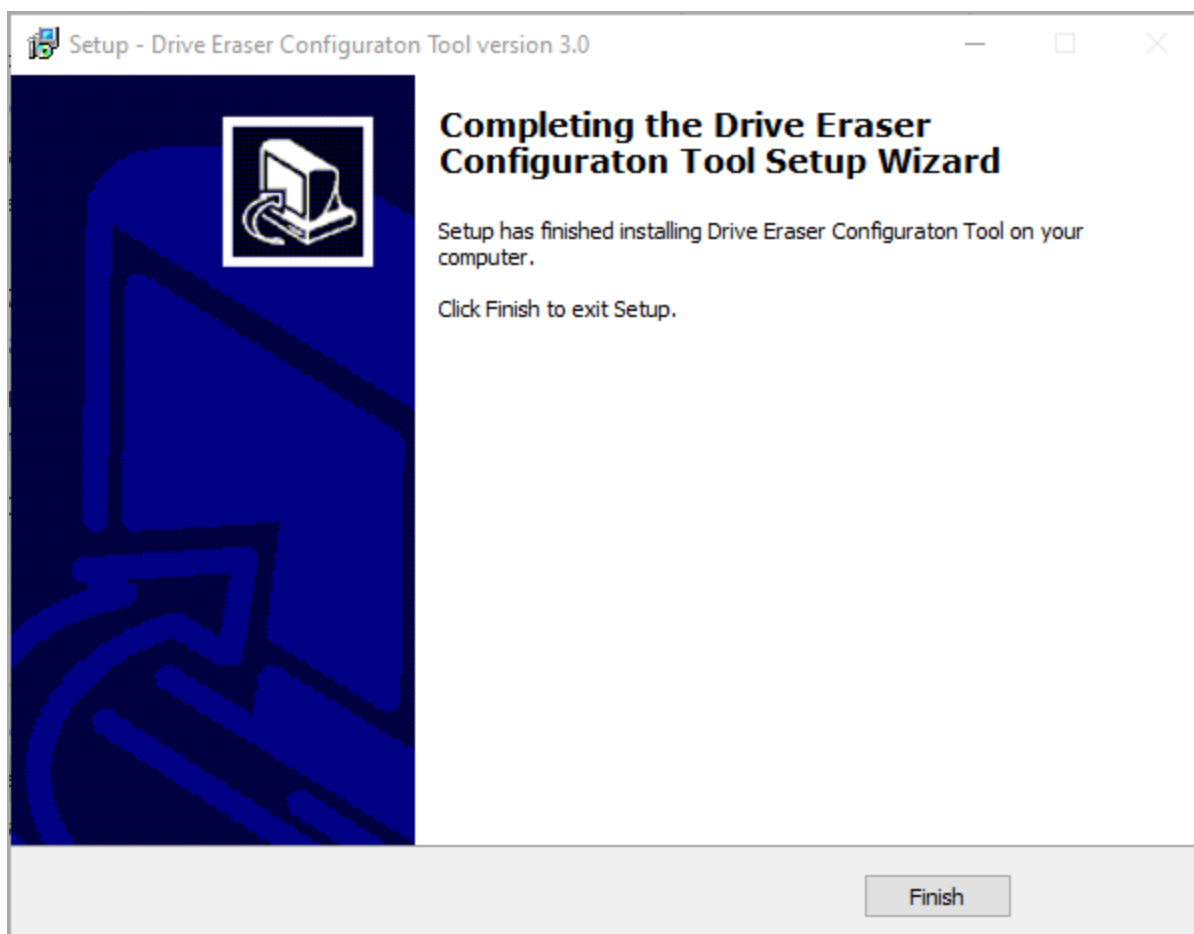
- El software ya está listo para instalarse en la ubicación predeterminada:



- Elija la ruta de instalación de Blancco Drive Eraser Configuration Tool:
  - en los sistemas Windows, de forma predeterminada es: **C:\Archivos de Programa\Blancco\Blancco Drive Eraser Configuration Tool 3**
- Espere a que finalice la instalación:



- La instalación ya se ha completado. Haga clic en "**Finalizar**" para cerrar el asistente.



## 2. Uso de Blancco Drive Eraser Configuration Tool

Iniciar Blancco Drive Eraser Configuration Tool (CT)

### 2.1 En sistemas Windows:

Inicie el servicio CT haciendo clic en [ubicación de la instalación]\dect.exe.

### 2.2 En sistemas Linux:

Inicie el servicio CT iniciando el archivo .appimage suministrado por Blancco (asegúrese de que tiene permisos de ejecución sobre el archivo).

### 2.3 Cargar una nueva imagen

Se abrirá la página de CT. Haga clic en el botón Cargar para cargar la nueva imagen:



- Seleccione una imagen ISO de Blancco Drive Eraser válida y, a continuación, haga clic en “ABRIR”.
- También puede cambiar el idioma de la interfaz de usuario desde esta ventana.



## 3. Configuración de Blancco Drive Eraser

Con CT, es posible configurar todas las opciones principales de Blancco Drive Eraser. Recuerde que la disponibilidad de las opciones de configuración depende del producto concreto y versión de Blancco Drive Eraser.

**blancco**  
Drive Eraser Configuration Tool | Version 3.6.0RC2

English ▾ Help

**General**

Image information

Product name

Product version

Volume Edition

7.6.0

Licensed to

Usage description

Localization settings

Language

English ▾

Keyboard layout

English (United States) ▾

UTC offset

+00:00 (Z) ▾

Screensaver settings

Enable

☒

Timeout (seconds)

30

Notification of exceptions

☐

User interface settings

Scaling

100 % ▾

Device view

Load Save Save as

### 3.1 General

Este menú permitirá configurar las opciones generales.

Image information

Product name

Volume Edition

Product version

7.6.0

Licensed to

Usage description

Localization settings

Language

English

Keyboard layout

English (United States)

UTC offset

+00:00 (Z)

Screensaver settings

Enable

☒

Timeout (seconds)

30

Notification of exceptions

☐

User interface settings

Scaling

100 %

Device view

### 3.1.1 Información de imagen

Nombre	Valor predeterminado/de ejemplo	Descripción
Licencia otorgada a *	[Nombre de empresa]	Este campo puede editarse para que coincida con el licenciatario o la empresa que utiliza la imagen. Solo se puede ver en el informe.
Nombre de producto	[Volume Edition / Enterprise Subscription Edition / Enterprise Volume Edition]	Variante de producto, por ejemplo, Volume Edition. No editable.
Versión de producto	[serie 6.x]	Versión del producto, por ejemplo, 6.0.0. No editable.
Descripción de uso	Portátiles, Imponer SSD	Breve descripción del uso previsto del producto. Por ejemplo, una imagen que borre servidores y elimine configuraciones RAID podría ser "Servidor, eliminar RAID". Máximo 30 caracteres.

\* Este campo puede deshabilitarse en imágenes especiales.

### 3.1.2 Configuración de localización

Nombre	Valor predeterminado/de ejemplo	
Idioma	Inglés	Idioma predeterminado del software. Todos los idiomas admitidos se muestran en el menú desplegable.

Nombre	Valor predeterminado/de ejemplo	
Diseño de teclado	English (US)	El diseño de teclado predeterminado para el software. Blancco Drive Eraser admite en la actualidad muchos diseños diferentes de teclados.
Diferencia respecto de UTC	+00:00 (Z)	La zona horaria predeterminada utilizada en el software. Esta zona horaria se utiliza en el informe si no se puede contactar con MC para que indique la zona horaria y la hora.

### 3.1.3 Configuración de salvapantallas

Nombre	Valor predeterminado/de ejemplo	
Habilitar	(activado)	Define si el salvapantallas está activado o no de forma predeterminada.
Bloquear	(no activado)	Solo disponible si <b>Proceso</b> tiene seleccionado el valor "Automático". Cuando está activado, el usuario local no puede salir del salvapantallas.
Tiempo inactivo (segundos)	30	El tiempo inactivo predeterminado para el salvapantallas en segundos (el periodo de inactividad que transcurre antes de que se inicie el salvapantallas). Los valores posibles van de 5 segundos a 86 400 segundos (1 día).
Notificación de excepciones	(no activado)	Para mostrar una notificación de excepciones de borrado en el salvapantallas. Si está habilitado, una vez completado el borrado, cualquier excepción que se haya producido hará que el salvapantallas parpadee de verde (correcto) a amarillo (advertencia).
Importación/exportación de configuración	-	Hay dos opciones: "Importar desde archivo" y "Exportar a archivo". <ul style="list-style-type: none"> <li>Exportar a archivo: con esta opción puede exportar los ajustes de la configuración actual a un archivo de configuración. Ese archivo puede importarse después a un CT (consulte a continuación).</li> <li>Importar desde archivo: con esta opción puede importar un archivo de configuración a este CT. Al importar un archivo de configuración, se importan todos los ajustes definidos en la imagen ISO utilizada para crear el archivo.</li> </ul> Recuerde que las configuraciones de exportación/importación solo son posibles entre las mismas versiones de Drive Eraser. Cuando se realice correctamente, aparecerá una notificación en la pantalla.

### 3.1.4 Configuración de la interfaz de usuario

Nombre	Valor predeterminado/de ejemplo	Descripción
Escalado	100 %	El usuario puede cambiar cómo se escala la interfaz del programa. Esto es útil para dispositivos con mayores resoluciones.  El valor predeterminado es 100 % y puede escalarlo hasta 200 % (25 % de incremento en cada opción).

### 3.1.5 Vista del dispositivo

Nombre	Valor predeterminado/de ejemplo	Descripción
Vista del dispositivo predeterminada	Lista	<p>El usuario puede elegir la vista predeterminada de los dispositivos en Drive Eraser. Las opciones son Lista o Cuadrícula, pero la predeterminada es Lista.</p> <p>Recuerde que esta opción también se puede cambiar haciendo clic en los iconos de Drive Eraser.</p>

### 3.1.6 Exportación e importación de archivo de configuración

La función para exportar una configuración DE crea un archivo XML (DEconfig.xml), que contiene la mayoría de los ajustes de imagen. La configuración DE se enumera en las siguientes categorías:

- Ajustes que pueden modificarse a través de CT:
  - Grupo 1: ajustes generales, pruebas de hardware (incluida la prueba de memoria), normas y opciones de borrado, opciones de proceso, campos personalizados, la mayoría de los ajustes de BMC y de red, la mayoría de los ajustes de SO.
    - Todos estos ajustes se exportan al archivo DEconfig.xml. Pueden cambiarse modificando manualmente el archivo .xml (p. ej., cambiando las opciones de borrado/proceso, cambiando la dirección IP de la máquina, añadiendo/eliminando campos personalizados...). Pueden importarse a otra imagen DE.
  - Grupo 2: credenciales de BMC y red. Estos ajustes también se exportan en el archivo DEconfig.xml, pero están encriptados, por lo que no se recomienda modificarlos manualmente.
  - Grupo 3: opciones de arranque, lista de unidades híbridas. Estos ajustes configuran otros archivos de imagen y no se exportarán en el archivo DEconfig.xml.
- Ajustes que no pueden modificarse a través de CT: versión de producto, nombre de producto y versión de configuración.
  - Estos ajustes no deben cambiarse. Si se cambian, CT rechazará el archivo de configuración durante la importación.
- Algunos ajustes (RAID, conexión en caliente, algunos ajustes de campo personalizados) requieren una combinación especial. Si esa combinación no es válida, estos ajustes no se tendrán en cuenta. Además, si se rompe la estructura de archivos XML, los ajustes se ignorarán. Si no tiene la seguridad, no modifique estos ajustes y deje que CT haga la configuración.

Puede importar una configuración más antigua en una nueva imagen (p. ej., una configuración DE 6.2.0 en una imagen DE 6.5.0), pero no al revés (p. ej., una configuración DE 6.5.0 en una imagen DE 6.2.0).

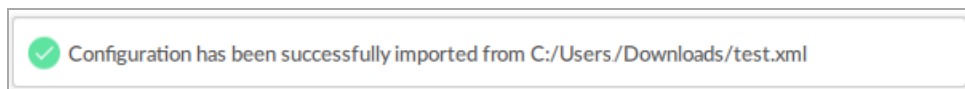
Recuerde que:

- La compatibilidad con versiones anteriores no se aplica en todas las versiones de DE/B5 disponibles.
- La importación de una configuración anterior a una nueva imagen sustituirá la nueva configuración. En la práctica, esto significa que los nuevos ajustes y funciones disponibles en la imagen más reciente desaparecerán de CT. Por ejemplo, si el usuario va a importar ajustes de una imagen de la versión 6.2 a la versión 6.5, la nueva imagen 6.5 se comportará en CT como si fuera una imagen de

la versión 6.2.

- Por este motivo, se recomienda exportar/importar configuraciones de las mismas versiones de BDE.

Tras importar o exportar las configuraciones, el programa mostrará una pequeña notificación:



## 3.2 Proceso

Esta pestaña permitirá configurar las opciones de proceso.

The image shows two configuration panels. The first panel, titled "License options", contains a "License container" dropdown menu set to "Blanco Management Console". The second panel, titled "Process options", contains a "Process" dropdown menu set to "Workflow" and an "Automatic report backup" checkbox which is currently unchecked.

### 3.2.1 Opciones de licencia

Nombre	Valor predeterminado/de ejemplo	Descripción
Contenedor de licencias	HASP local	Indica si el consumo de licencias se realiza mediante HASP local o mediante Blanco Management Console.

### 3.2.2 Opciones de proceso

Nombre	Valor predeterminado/de ejemplo	Descripción
Proceso	Manual	<p>El proceso de borrado se puede configurar como Flujo de trabajo, Automático, Semiautomático o Manual. Para obtener más información acerca de los procesos de borrado, consulte el Manual del usuario de Blanco Drive Eraser.</p> <p>Recuerde que el uso del proceso Flujo de trabajo requiere BMC/Blanco Cloud para funcionar. Si desea crear una imagen de flujo de trabajo remoto, "Proceso" se debe establecer en "Flujo de trabajo" y "Control" se debe establecer en "BMC remoto" (todo el control se produce en BMC) o en "Combinado" (el control se produce localmente a través de BMC).</p>
Copia de seguridad automática de informe	[no activado]	Solo disponible si <b>Proceso</b> tiene seleccionado el valor "Manual". Si está habilitado, tras el borrado se enviará automáticamente una copia de seguridad del informe a BMC o se guardará en una llave USB.

Nombre	Valor predeterminado/de ejemplo	Descripción
Bloquear el salvapantallas	[no activado]	<p>Solo disponible si <b>Proceso</b> tiene seleccionado el valor "Automático".</p> <p>Bloquea el salvapantallas en BDE una vez activado.</p>
Acción posproceso	Ninguno	<p>Blancco Drive Eraser puede reiniciarse o apagarse automáticamente. Esta funcionalidad no se puede activar cuando Proceso está definido como <b>Manual</b> o <b>Flujo de trabajo</b>.</p> <p>Están disponibles las siguientes opciones:</p> <ul style="list-style-type: none"> <li>• <b>Ninguno:</b> el valor predeterminado. Sin reinicio ni apagado automático.</li> <li>• <b>Reiniciar, después del proceso:</b> el equipo se reinicia automáticamente una vez que ha finalizado el proceso.</li> <li>• <b>Reiniciar, después de un proceso completado con éxito:</b> el equipo se reinicia automáticamente una vez que el proceso ha finalizado con un estado correcto.</li> <li>• <b>Apagar, después del proceso:</b> el equipo se apaga automáticamente una vez que ha finalizado el proceso.</li> <li>• <b>Apagar, después de un proceso completado con éxito:</b> el equipo se apaga automáticamente una vez que el proceso ha finalizado con un estado correcto.</li> </ul>
Control de proceso	Interfaz de usuario local	<p>Define si el borrado se controla localmente a través de la interfaz de usuario, remotamente desde BMC o depende de una especificación de trabajo. Recuerde que el control remoto y la especificación de trabajo requieren que se introduzcan los valores de Management Console en el menú <b>Comunicación</b>.</p> <p>Tenga en cuenta que la especificación de trabajo solo se admite en la serie 6.x de Blancco Drive Eraser, no en la serie 7.x.</p> <p>Si se selecciona el proceso "Flujo de trabajo", los flujos de trabajo solo están disponibles con la selección "Interfaz de usuario local".</p> <p>Si se selecciona "Blancco Management Console remoto" o "Combinado (Management Console e interfaz de usuario local)":</p> <ul style="list-style-type: none"> <li>• Otros ajustes de flujo de trabajo no están disponibles (la pestaña Flujo de trabajo se muestra en color gris).</li> </ul>

Nombre	Valor predeterminado/de ejemplo	Descripción
		<ul style="list-style-type: none"> <li>"Monitorización remota" no está disponible.</li> </ul>
Monitorización remota	[no activado]	<p>Solo disponible si Control de borrado tiene seleccionado Interfaz local de usuario (el operador controla localmente el borrado).</p> <p>Si está habilitado, Management Console puede monitorizar (sin intervención) el proceso de borrado. Recuerde que la monitorización requiere que se introduzcan los valores de Management Console, ya sea a través de la herramienta de configuración o a través del software cliente.</p>

### 3.2.3 Mostrar más

Nombre	Valor predeterminado/de ejemplo	Descripción
Mostrar particiones de unidad	[no activado]	Si está habilitado, se muestran las particiones de unidad en la interfaz gráfica de usuario y pueden borrarse de forma separada.
Mostrar dispositivos flash extraíbles	[no activado]	Si está seleccionada esta opción, los dispositivos flash extraíbles se muestran en la interfaz de usuario del software y se pueden borrar como cualquier otra unidad.

### 3.2.4 Dispositivos conectados

Nombre	Valor predeterminado/de ejemplo	Descripción
Informe por dispositivo conectado	[no activado]	<p>Si está habilitado, se crea un informe individual para cada dispositivo conectado (en lugar de un informe por equipo). Esta característica solo se puede habilitar si:</p> <ul style="list-style-type: none"> <li>Se seleccionan el proceso "Manual" y la "Interfaz de usuario local"</li> <li>O bien, se selecciona el proceso "Flujo de trabajo" (en v6.13.0, fuerza la activación de esta característica y no se puede deshabilitar si el proceso está activo; en v6.14 o versiones más recientes, ya no se fuerza la característica).</li> </ul> <p>Cuando la característica está habilitada:</p> <ul style="list-style-type: none"> <li>Se deshabilitan las pruebas de hardware estándar (solo se aplica a la versión de cliente 6.13 y anteriores).</li> <li>Se aplica la eliminación de discos lógicos RAID</li> <li>Se pueden habilitar las pruebas de hardware de Chromebook.</li> </ul>
Conexión en caliente	[no activado]	Esta opción habilita/deshabilita la compatibilidad para unidades de conexión

Nombre	Valor predeterminado/de ejemplo	Descripción
		<p>en caliente. <b>Tiempo inactivo (segundos)</b> se utiliza para modificar el tiempo en espera para el procedimiento de conexión en caliente (el valor predeterminado es 30 segundos). El tiempo inactivo mínimo son 30 segundos, y el máximo, 86 400 segundos (24 horas).</p> <p>Esta opción solo está visible si el modo "Informe por dispositivo conectado" está activado.</p>
Compatibilidad con Chromebook	[no activado]	<p>Solo disponible si la opción <b>Informe por dispositivo conectado</b> está activada. Esta opción habilita/deshabilita el soporte de procesamiento de Chromebook. Los campos de <b>Puerto</b> definen los puertos utilizados para conectarse a los dispositivos Chromebook. Debe definir valores para los puertos HTTP y HTTPS; los valores predeterminados son 80 y 443 respectivamente (se recomienda dejar los valores predeterminados para simplificar el procesamiento de Chromebook).</p> <p>Introduzca un valor entre 1 y 65 535.</p>

### 3.3 Flujo de trabajo

Esta pestaña permitirá configurar las opciones de flujo de trabajo.

The screenshot shows a configuration window titled 'Workflow options'. It contains a 'Workflow container' dropdown menu with 'ISO image' selected. Below this is an 'External workflow' section. At the bottom, there is a 'Load default workflow' checkbox that is checked.

#### 3.3.1 Opciones de flujo de trabajo

Nombre	Valor predeterminado/de ejemplo	Descripción
Contenedor de flujos de trabajo	Blancco Management Console	<p>Donde se almacena el flujo de trabajo y desde donde se recopila.</p> <p>Las opciones son:</p> <ul style="list-style-type: none"> <li>• Blancco Management Console: el flujo de trabajo se recopila de Blancco Management Console. Tenga en cuenta que esta opción requiere que se establezca y active una conexión a Blancco Management Console.</li> <li>• Imagen ISO: el flujo de trabajo se integra en la imagen ISO. Consulte "Flujo de trabajo integrado" a continuación para obtener más información</li> </ul>



### 3.3.2 Flujo de trabajo externo

Tenga en cuenta que estas opciones solo están disponibles si "Contenedor de flujos de trabajo" se ha establecido en "Blancco Management

Console".

Nombre	Valor predeterminado/de ejemplo	Descripción
Cargar flujo de trabajo pre-determinado	[activado]	Cargue automáticamente el flujo de trabajo que se haya establecido como flujo de trabajo predeterminado en Blancco Management Console.
Cargar flujo de trabajo por nombre	Aquí_nombre_flujo_de_trabajo	Solo está disponible si "Cargar flujo de trabajo predeterminado" no está activo. Cargue un flujo de trabajo de Blancco Management Console con nombre en este campo

### 3.3.3 Flujo de trabajo integrado

Tenga en cuenta que estas opciones solo están disponibles si "Contenedor de flujos de trabajo" se ha establecido en "Imagen ISO".

Nombre	Valor predeterminado/de ejemplo	Descripción
Importar desde archivo	-	Importe un archivo de flujo de trabajo desde el ordenador. Tenga en cuenta que, antes de importar desde un archivo, es necesario exportar un flujo de trabajo desde BMC
Exportar a archivo	-	Solo está disponible si se ha seleccionado un flujo de trabajo de la lista de flujos de trabajo. Exporte un flujo de trabajo integrado a un archivo del equipo local.
Eliminar	-	Solo está disponible si se ha seleccionado un flujo de trabajo de la lista de flujos de trabajo. Exporte un flujo de trabajo integrado a un archivo del equipo local.
Lista de flujos de trabajo	-	Una tabla que contiene una lista de todos los flujos de trabajo cargados actualmente en la imagen ISO. Para seleccionar un archivo, use la casilla de verificación situada junto al nombre del flujo de trabajo.
Flujo de trabajo principal	aquí_nombre_flujo_de_trabajo	El flujo de trabajo que se utiliza como flujo de trabajo principal (pre-determinado) en esta imagen ISO.

## 3.4 Seguridad

Este menú contiene opciones para las funciones de seguridad del borrado.

Security options

Erasure standard

...

HMG Infosec Standard 5, Lower Sta... ▾

Action if erasure is not possible

Interrupt process ▾

Enforce Blancco SSD method on SSDs

☐

Enable fallback from NIST Purge to NIST Clear

☐

Fail process if write errors

☒

Fail threshold

5

### 3.4.1 Opciones de seguridad

Nombre	Valor predeterminado/de ejemplo	Descripción
Norma de borrado	HMG Infosec Standard 5, Lower Standard	<p>La norma predeterminada utilizada en el procedimiento de borrado. Blancco Drive Eraser admite actualmente más de 24 normas de borrado diferentes. Consulte el manual de Blancco Drive Eraser para obtener más información acerca de las normas de borrado.</p> <p>El usuario puede habilitar/deshabilitar las normas de borrado, abriendo la vista de edición mediante el botón editar (tres puntos) que está junto a la lista de normas. La habilitación/deshabilitación se realiza con las casillas de verificación que están junto a los nombres de norma en el menú de edición. Tras habilitar/deshabilitar las normas, haga clic en "Guardar" para guardar los cambios o en "Cancelar" para cancelar todos los cambios. Recuerde que al menos debe habilitar una norma de borrado.</p> <p>Las opciones de <b>Tipo de patrón de sobrescritura</b> están disponibles cuando se selecciona <u>NIST 800-88 Clear</u>. De este modo, el usuario puede cambiar la forma en que se realiza el proceso de sobrescritura. El valor del byte se puede cambiar con la opción "Estático".</p>
Acción si el borrado no es posible	Interrumpir proceso	<p>Si el borrado no puede iniciarse por alguna razón, se llevará a cabo la acción seleccionada aquí. Las acciones posibles son:</p> <ul style="list-style-type: none"> <li>Interrumpir proceso: interrumpe y detiene completamente el proceso</li> <li>Continuar proceso y comunicar fallo: continúa el proceso hasta que finaliza y marca el borrado como "fallido" en el informe.</li> </ul>
Aplicar el método Blancco SSD en todas las unidades SSD	[no activado]	<p>Si está habilitado, se cambia automáticamente al método "Borrado de SSD de Blancco" para todas las unidades SSD detectadas. Otras unidades se siguen borrando con la norma de sobrescritura predeterminada. Recuerde que esta característica requiere que esté habilitado el "Borrado de SSD de Blancco" como norma</p>

Nombre	Valor predeterminado/de ejemplo	Descripción
		de sobrescritura (consulte a continuación la habilitación/deshabilitación de normas).
Habilitar alternativa de NIST Purge a NIST Clear	[no activado]	Si está habilitado y falla el borrado "NIST 800-88 Purge", o la norma no se admite, el proceso recurre automáticamente a la norma de borrado "NIST 800-88 Clear".  Recuerde que esta opción no está disponible si "Proceso de borrado" está configurado como "Flujo de trabajo".
Proceso fallido si hay errores de escritura	[activado]	Si está habilitado, el umbral del total de errores de escritura se define aquí. Si durante el borrado el total de errores de escritura alcanza este límite, el borrado se detendrá automáticamente y fallará. El umbral predeterminado es de 5 errores. Además, el informe mostrará un mensaje de error que lo indica. El umbral de errores mínimo es 1 y el máximo es 1000.
Proceso fallido si hay errores de lectura	[activado]	Si está habilitado, el umbral del total de errores de lectura se define aquí. Si durante el borrado el total de errores de lectura alcanza este límite, el borrado se detendrá automáticamente y fallará. El umbral predeterminado es de 5 errores. Además, el informe mostrará un mensaje de error que lo indica. El umbral de errores mínimo es 1 y el máximo es 1000.
Eliminar las áreas ocultas	[activado]	Esta opción define cómo se manejan las áreas ocultas de las unidades (HPA y DCO). Si está habilitado, las áreas ocultas se detectarán y eliminarán automáticamente. Si está deshabilitado, las áreas ocultas se detectarán, pero no se eliminarán.
Borrar sectores reasignados	[activado]	Esta opción define cómo se manejan los sectores reasignados durante el proceso de borrado. Si esta opción está habilitada, los sectores reasignados se borran automáticamente si existen y si la unidad admite esta funcionalidad. Si la opción está deshabilitada, los sectores reasignados se detectan, pero no se borran.
Fallo borrado si el número es demasiado alto	[no activado]	Si se habilita esta opción, se habilita el umbral de fallos y se establece como 1 o el valor que hubiera antes de deshabilitarse.  La opción <b>Límite de fallo</b> se utiliza para definir el número máximo de sectores reasignados permitidos. Si la cantidad detectada de sectores reasignados es igual o mayor que este valor, el borrado se detendrá automáticamente y será fallido.  Esta opción requiere que la opción "Borrar sectores reasignados" esté activada.
Borrado fallido si no funciona	[no activado]	Si esta opción está habilitada, todo el borrado fallará si: <ul style="list-style-type: none"> <li>La unidad tiene uno o varios sectores reasignados,</li> </ul>

Nombre	Valor predeterminado/de ejemplo	Descripción
		<ul style="list-style-type: none"> <li>el borrado de los sectores reasignados no se admite en la unidad o se admite, pero falla.</li> </ul> <p>Esta característica solo está disponible en la versión de cliente 6.1.1 o más reciente. Esta opción requiere que la opción "Borrar sectores reasignados" esté activada.</p>
Proceso fallido si la velocidad es demasiado baja (MB/s)	[no activado]	<p>Marca el proceso como fallido si la velocidad de borrado es inferior al valor establecido en el campo "Límite de fallo".</p> <p>Deshabilitado de forma predeterminada. El valor predeterminado es 1 y el rango de valores es de 1-10 000. La unidad se indica en megabytes/segundo.</p>
Proceso fallido debido al tiempo límite (horas)	[no activado]	<p>Marca el proceso como fallido si su duración es mayor que el valor del campo "Límite de fallo".</p> <p>Deshabilitado de forma predeterminada. El valor predeterminado es 48 h. El rango personalizado es de 1 hora a 1 año (8760 h)</p>
Ejecutar autodiagnósticos en unidades	[Ninguno]	<p>Esta opción define el autodiagnóstico S.M.A.R.T de la unidad con el valor "Ninguno" (sin pruebas – opción predeterminada), "Breve", "Transporte" o "Extendido". Para obtener más información acerca de las opciones de autodiagnóstico, consulte el manual de usuario del software del cliente.</p>
Proceso fallido si no funciona	[no activado]	<p>Si esta opción está habilitada y falla el autodiagnóstico seleccionado, se cancela el proceso de borrado y falla el proceso de borrado. La razón del fallo se marca en el informe.</p> <p>Esta opción solo está disponible si "Ejecutar autodiagnósticos en unidades" está habilitado en la opción anterior.</p>
Nivel de verificación	1 %	<p>Este ajuste define el nivel de verificación del borrado. El proceso de verificación lee los datos de la unidad y se asegura de que los patrones de sobrescritura se sobrescribieron correctamente. La verificación mínima corresponde a una comprobación del 1 % de la superficie del disco (proceso rápido), mientras que la verificación completa corresponde a la comprobación del 100 % de la superficie de la unidad (más lento).</p> <p>Tenga en cuenta que el cambio de norma de borrado siempre restablece el nivel de verificación al especificado para esa norma. Cuando esto ocurre, aparece la siguiente advertencia: "El porcentaje de verificación se modificó en función de los requisitos mínimos de la norma de borrado".</p>
Límite de operaciones simultáneas	[50]	<p>El número máximo de borrados simultáneos. Si el número de borrados que se están realizando simultáneamente es inferior al</p>

Nombre	Valor predeterminado/de ejemplo	Descripción
		<p>límite, es posible iniciar nuevos borrados hasta que se alcance el límite.</p> <p>Si el número de borrados rebasa este valor, los borrados nuevos o que superen el límite pasan a la cola de borrados y quedan en pausa hasta que sea posible iniciarlos.</p> <p>Recuerde que el número máximo admitido aquí puede diferir de una edición del software cliente a otra.</p>
Deshabilitar Bloquear autenticación SID	No, omitir	<p>Bloquear autenticación SID (BSA) es un tipo de bloqueo que impide ejecutar comandos de firmware en las unidades del equipo. Este ajuste permite preconfigurar un cuadro de diálogo para activar/desactivar ese bloqueo; también se puede establecer un tiempo límite para cerrar el cuadro de diálogo (0-86 400 segundos). Las opciones son: I No, omitir: BSA no se desactiva, el bloqueo se mantiene. I Sí, continuar: BSA se desactiva, el bloqueo se elimina. Tenga en cuenta que esta opción requiere reiniciar el equipo y aceptar la deshabilitación.</p>
Conservar partición de recuperación	[no activado]	<p>Si esta opción está habilitada, el proceso de borrado puede reanudarse si ha terminado de una manera descontrolada (corte de suministro eléctrico, fallo del sistema, etc.).</p> <p>Consulte el Manual del usuario de Blancco Drive Eraser para obtener más información.</p>
Reanudar borrado si se interrumpe	[no activado]	<p>Si esta opción está habilitada, el proceso de borrado puede reanudarse si ha terminado de una manera descontrolada (corte de suministro eléctrico, fallo del sistema, etc.).</p> <p>Consulte el Manual del usuario de Blancco Drive Eraser para obtener más información.</p>
Bloquear la configuración de borrado	[no activado]	<p>Si esta opción está habilitada, el usuario de BDE no puede cambiar la configuración de borrado.</p>
Calcular la vida útil restante de la unidad	[no activado]	<p>Al activar este ajuste, se muestra en el informe una estimación del tiempo que le queda a cada unidad en función de varios atributos internos. Obtenga más información en el manual del usuario de BDE.</p>

**¡Atención! Para borrar unidades SSD y NVMe que admiten comandos de borrado basados en firmware, las normas de borrado recomendadas disponibles en el software de Blancco Drive Eraser son "Borrado de SSD de Blancco" y "NIST 800-88 Purge".**

Sin embargo, si su política de borrado exige que debe aplicarse un proceso diferente para estas unidades, pueden seleccionarse otras opciones, pero aparecerá un mensaje en el informe resaltando que se borró una unidad SSD.

### 3.4.2 Trusted Platform Module

Nombre	Valor predeterminado/de ejemplo	Descripción
Borrar TPM en el arranque	No, omitir	Este ajuste permite restablecer el chip TPM, lo que borra toda la información

Nombre	Valor predeterminado/de ejemplo	Descripción
		<p>contenida en él. Obtenga más información en el manual de BDE.</p> <p>Tenga en cuenta que, al activar esta opción, puede reiniciarse el equipo.</p> <p>Si se selecciona "Tiempo límite (segundos)", existe un límite de tiempo para que el usuario realice una selección, antes de que se seleccione automáticamente el valor seleccionado en "Borrar TPM en el arranque". El valor de tiempo límite se puede configurar (0-86 400 segundos). Si no se selecciona ningún tiempo límite, el software esperará en la pantalla de selección hasta que el usuario seleccione una de las opciones.</p>

### 3.4.3 Opciones de controlador

Nombre	Valor predeterminado/de ejemplo	Descripción
Disco lógico (RAID)	Mostrar	<p>Cuando se selecciona "Mostrar", no se eliminarán los discos lógicos definidos dentro de una RAID; están visibles en la pantalla y accesibles para el borrado.</p> <p>Cuando se selecciona "Eliminar", esta opción permitirá eliminar todos los discos lógicos definidos dentro de una RAID; la configuración de RAID se desmontará y los discos físicos estarán accesibles para el borrado (el borrado de los discos físicos es mucho más seguro). Este ajuste no está disponible en PC Edition.</p>
Reconfigurar modo de controlador	Sí, continuar	<p>Este ajuste permite reconfigurar el modo de controlador (p. ej., de RAID a modo JBOD), lo que permite un mayor control de las unidades conectadas. Para obtener más información, consulte la documentación de Blancco Drive Eraser. Los valores posibles son "Sí, continuar" (valor predeterminado) y "No, omitir".</p> <p>Si se selecciona "Tiempo límite (segundos)", existe un límite de tiempo para que el usuario realice una selección, antes de que se seleccione automáticamente el valor seleccionado en "Reconfigurar modo de controlador". El valor de tiempo límite se puede configurar (0-86 400 segundos). Si no se selecciona ningún tiempo límite, el software esperará en la pantalla de selección hasta que el usuario seleccione una de las opciones.</p>

### 3.4.4 Detección de inscripción de dispositivos

Nombre	Valor predeterminado/de ejemplo	Descripción
Software persistente	[no activado]	Si esta opción está habilitada, se detectará y registrará cualquier software persistente (integrado en la BIOS). El

Nombre	Valor predeterminado/de ejemplo	Descripción
		software persistente más conocido es Computrace (de Absolute Software), y se utiliza para hacer un seguimiento del hardware del ordenador.

### 3.4.5 Ajustes de formato

Nombre	Valor predeterminado/de ejemplo	Descripción
Formatear la unidad después del borrado	[no activado]	Si esta opción está habilitada, cuando la unidad se ha borrado, se formatea la unidad al tipo de sistema de archivos elegido en el menú desplegable "Tipo de sistema de archivos". Las interfaces de unidad admitidas son ATA, SATA, SCSI y SAS.
Tipo de sistema de archivos	NTFS	Tipo de sistema de archivos al que se ha formateado la unidad. El tipo predeterminado es NTFS. Las opciones son: <ul style="list-style-type: none"> <li>• NTFS</li> <li>• FAT32</li> <li>• exFAT</li> </ul> El menú solo se habilita después de habilitar "Formatear la unidad después del borrado".

### 3.4.6 Configuración de ahorro de energía

Nombre	Valor predeterminado/de ejemplo	Descripción
Reducir velocidad de giro de discos inactivos	[activado]	Si está habilitada, esta opción permite al software cliente reducir la velocidad de giro de los discos si han estado inactivos durante 5 minutos.  Además, si esta opción está habilitada, es posible iniciar un máximo de un borrado por segundo. Se hace así para prevenir los picos de potencia.  Habilitado de forma predeterminada.

## 3.5 Pruebas de hardware

Este menú contiene opciones para habilitar/deshabilitar las pruebas de hardware y modificar las opciones específicas de las pruebas. CT también se puede utilizar para configurar pruebas de hardware en Chromebooks. Para obtener más información, consulte el Manual del usuario de Blancco Drive Eraser.

Hardware test settings

☒ Enable

Select hardware tests	Required	Pass thresholds	Duration
<input checked="" type="checkbox"/> Battery capacity	<input type="checkbox"/>	<div><div></div></div> 60 %	
<input checked="" type="checkbox"/> Battery discharge	<input type="checkbox"/>	<div><div></div></div> 50 %	<div><div></div></div> 10 min
<input checked="" type="checkbox"/> BIOS logo	<input type="checkbox"/>		
<input checked="" type="checkbox"/> CPU	<input type="checkbox"/>		

Si la casilla de verificación **Obligatorio** está seleccionada para una prueba específica, la prueba no puede deseleccionarse en la interfaz de usuario de Blancco Drive Eraser y se ejecutará si el usuario inicia manualmente las pruebas de hardware. Si se ha habilitado "Compatibilidad con Chromebook" en la imagen, la casilla de verificación "Obligatorio" no está disponible para las pruebas seleccionadas (todas las pruebas seleccionadas se ejecutan automáticamente en los Chromebooks).

Recuerde que, con las pruebas manuales, es necesaria la interacción por parte del usuario.

Para obtener más información acerca de pruebas específicas, consulte el Manual del usuario de Blancco Drive Eraser.

Nombre	Valor predeterminado/de ejemplo	Descripción
Habilitar pruebas de hardware	(no activado)	Habilitar/deshabilitar todas las pruebas de hardware. Si está habilitado, el paso "Pruebas de hardware" de Blancco Drive Eraser estará visible (en caso contrario, está oculto).
Capacidad de la batería	(activado)	La prueba de Capacidad de la batería comprueba la capacidad y el voltaje de la batería interna (en portátiles y tablets). El valor predeterminado es del 60 % (de conformidad con las directrices e-Steward 2020).  La opción <b>Umbral de prueba superada</b> se utiliza para determinar qué nivel de capacidad de batería es el adecuado para que la prueba sea correcta. El rango es de 1 a 100 (%). Si el umbral de prueba superada tiene, por ejemplo, el valor 80 %, si la batería del portátil puede conservar al menos el 80 % de su capacidad original, la prueba será correcta.
Descarga de la batería	(activado)	La prueba de descarga de la batería prueba la tasa de descarga de la batería del dispositivo. La prueba arrojará fallos si la descarga de la batería es superior al <b>Umbral de prueba superada</b> (valor predeterminado – 50 puntos porcentuales o p.p.) dentro del intervalo establecido en Duración (valor predeterminado 10 minutos). Estos valores se ajustan a las



Nombre	Valor predeterminado/de ejemplo	Descripción
		directrices e-Steward 2020.  <b>¡Advertencia!</b> La prueba de descarga de la batería somete a la CPU a una carga considerable que agota la batería. Si se ejecuta con una batería con poca carga, el borrado podría fallar, lo que podría causar corrupción de la unidad. Plántese aplicar una disipación de calor externa en caso de sobrecalentamiento de la CPU.
Logotipo de la BIOS	(activado)	La prueba de logotipo de la BIOS se utiliza para comprobar si el logotipo de la BIOS del ordenador coincide con el del fabricante o si se ha personalizado.
CPU	(activado)	La prueba de CPU comprueba la funcionalidad del procesador.
Pantalla	(activado)	Prueba manual para la pantalla.
Teclado	(activado)	Prueba manual para el teclado. Puede elegir entre los teclados "Compacto" (sin teclado numérico) y "Tamaño completo". También existe la opción de seleccionar un diseño de teclado diferente.
Red	(activado)	Prueba creada por interfaz Ethernet detectada. También es posible configurar direcciones IP a las que hacer ping en CT.
Altavoz	(no activado)	Prueba los altavoces integrados en el portátil reproduciendo una muestra de voz/audio.
Micrófono	(activado)	Grabe y reproduzca una muestra de 5 segundos. El audio se muestra como un medidor de amplitud para la entrada y la salida. El volumen maestro del sistema está al 100 % de forma predeterminada.
Memoria	(no activado)	La prueba de memoria comprueba la memoria de bajo nivel y la memoria extendida (RAM) de un ordenador. Tenga en cuenta que, dependiendo de la cantidad de memoria de la máquina, esta prueba puede durar de 20 segundos a varios minutos.  El <b>Número de pasadas</b> se utiliza para determinar cuántas pasadas (1-99) se realizan en la prueba de memoria. Tenga en cuenta que un mayor número de pasadas hará que la prueba dure más tiempo.
Placa base	(activado)	La prueba de la placa base comprueba la suma de comprobación del CMOS, la batería, el RTC y la DMI.
Unidad óptica	(activado)	Prueba manual para la unidad óptica. Esta prueba tiene selecciones separadas para <b>Escritura</b> (prueba de escritura), <b>Lectura</b> (prueba de lectura) y <b>Vaciado</b> (prueba de vaciado).
Dispositivo apuntador	(activado)	Prueba manual para el dispositivo apuntador.
Altavoz del PC	(activado)	Prueba manual para el altavoz del PC (zumbador conectado a la placa base)

Nombre	Valor predeterminado/de ejemplo	Descripción
Puertos USB	(activado)	Prueba manual para probar los puertos USB de la máquina. Recuerde que se necesita un adaptador USB externo (por ejemplo, una memoria USB).
Webcam	(activado)	Prueba manual para la webcam. El usuario puede hacer capturas de pantalla para verificar si la cámara funciona".
Wifi	(activado)	La prueba comprueba las interfaces WiFi detectadas. Si el usuario no ha realizado ninguna configuración, la prueba mostrará una lista de las redes disponibles (superada/con fallos manual)  La prueba arrojará fallos automáticamente si no se ha podido acceder a ninguna red o falta la IP.
Pantalla táctil	(activado)	Prueba manual para la pantalla táctil. La prueba comprueba si la pantalla táctil funciona correctamente o tiene algún problema, solicitando al usuario que toque una cuadrícula en la pantalla.

### 3.6 Informe

Este menú permite configurar los ajustes relacionados con los informes, los informes de activos y las huellas digitales. Aquí se configuran también los campos de informe de los "Detalles del cliente" y los "Datos del operador".

#### Report settings

Report format by default

xml

Report view by default

Standard

Locked

☐

#### Report digital signature key

Custom key label

Image contains no custom key

Generate

Upload

#### Customer details

#### 3.6.1 Configuración de informes

Nombre	Valor predeterminado/de ejemplo	Descripción
Formato de informe predeterminado	XML	Los formatos de informe predeterminados que utiliza el software del cliente para guardar y enviar informes. Las versiones anteriores a 6.7.0 ofrecen 3 opciones (XML, PDF, XML+PDF), las versiones >=

Nombre	Valor predeterminado/de ejemplo	Descripción
		6.7.0 ofrecen 2 opciones (XML, PDF+XML).
Vista de informe predeterminada	Estándar	La vista de informe predeterminada (Estándar o Avanzada).
Bloqueado	[no activado]	Si se habilita, el usuario del software cliente no puede cambiar la vista de informe.

### 3.6.2 Clave de firma digital de informes

Nombre	Valor predeterminado/de ejemplo	Descripción
Etiqueta de clave personalizada	-	<p>Estas opciones están disponibles en BDE 6.12.0 o posterior y se utilizan para gestionar un nuevo par de claves utilizadas para generar y verificar una firma digital personalizada en el informe. El par de claves se genera mediante un algoritmo RSA y tiene una longitud de 2048 bits. Si se carga una clave, esta debe seguir el formato PEM y tener una longitud de 2048 bits.</p> <p><b>Eliminar</b> elimina la clave privada cargada actualmente / generada de la imagen.</p> <p><b>Cargar</b> se utiliza para subir una clave privada externa para la imagen. Tenga en cuenta que el tamaño permitido de la clave personalizada está entre 2048 y 4096 bits. Los formatos aceptados son PKCS#1 y PKCS#8 (no cifrados).</p> <p><b>Generar</b> crea un par de claves: la clave privada se integra en la imagen y es posible descargar tanto la clave privada como la pública.</p> <p>Nota: Tanto si carga un par de claves como si las genera, <b>se recomienda encarecidamente que conserve ambas claves en un entorno seguro</b>. La clave pública se debe cargar más tarde en BMC (5.4.0 o posterior) para verificar la firma digital personalizada (no se verificará de otra manera). Se puede introducir una etiqueta fácil de recordar durante la generación o carga del par; su único propósito es permitir al usuario localizar fácilmente un par de claves tanto en BDE como en BMC. Se recomienda asignar etiquetas diferentes a los pares de claves para evitar confusiones. Si no se asigna ninguna etiqueta durante la generación o la carga del par, CT genera una etiqueta única.</p>

### 3.6.3 Detalles del cliente

Nombre	Valor predeterminado/de ejemplo	Descripción
Habilitar	(activado)	Habilitar/deshabilitar los campos relacionados con el cliente.

Nombre	Valor predeterminado/de ejemplo	Descripción
		Habilitado de forma predeterminada.
Nombre del cliente	Empresa de ejemplo	Nombre de la empresa propietaria de los equipos que se desea borrar (puede ser diferente del Licenciario).
Ubicación del cliente	Población de ejemplo	Ubicación/dirección del cliente mencionado.

### 3.6.4 Datos del operador

Nombre	Valor predeterminado/de ejemplo	Descripción
Habilitar	(activado)	Habilitar/deshabilitar los campos relacionados con el operador. Habilitado de forma predeterminada.
Proveedor de borrado	Nombre de proveedor de ejemplo	Nombre del proveedor de borrado que procesa los equipos.
Persona que realiza el borrado	Nombre de ejemplo de persona que realiza el borrado	Nombre de la persona que realiza el borrado.

### 3.6.5 Configuración de informes de activos

Nombre	Valor predeterminado/de ejemplo	Descripción
Escritura de informe de activos	(no activado)	Si está habilitado, se escribirá un informe de activos en cada unidad borrada, una vez que el proceso de borrado se haya completado correctamente (si la unidad se borró con éxito y el informe se guardó/envió con éxito). El informe de activos se configura como un informe de arranque y se muestra como una imagen estática si el equipo se reinicia con la unidad borrada.

### 3.6.6 Configuración de huella digital

Nombre	Valor predeterminado/de ejemplo	Descripción
Escritura de huella digital	(no activado)	Esta casilla de verificación define si la huella digital se escribe en un sector de cada unidad borrada una vez terminado el proceso de borrado. Está destinada a la verificación rápida del borrado de los servidores. Para obtener más información acerca de la huella digital, consulte el Manual del usuario de Blancco Drive Eraser.
Ubicación (sector)	200	En qué sector se escribe la huella digital ("0" es el primer sector).  Si la opción "Escritura de informe de activos" está activada, el valor del sector debe ser igual o superior a 200.

## 3.7 Campos personalizados


En este menú, puede añadirse, eliminarse y modificarse campos personalizados. Los campos personalizados normalmente son creados y cumplimentados por el operador, es decir, la persona o empresa que realiza el borrado de las unidades.

Cada usuario puede personalizarlos:

- Asignándoles el nombre que desee.
- Complimentándolos con cualquier valor predeterminado.
- Configurándolos como campos normales u obligatorios.
- Definiéndolos como:
  - Campos de texto que se pueden rellenar.
  - Listas desplegables con valores rellenados previamente que permiten seleccionar un elemento.
  - Listas desplegables con valores rellenados previamente que permiten seleccionar varios elementos.
- Ejemplos de nombres de campos personalizados: "ID de activo", "Tipo de activo", "Valor de activo", "Destruir activo"...

ID	Field name	Type	Values	Preview	Required	Per connected device	Locked	Regular expression	Hint
1	Operator name	Multidropist	John,Jack,Peter		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
2	Warehouse	Droplist	~,New York,Paris,Joensuu		<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
3	Drive ID	Textfield			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
4	Drive grade	Droplist	~,A,B,C		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

Nombre	Valor predeterminado/de ejemplo	Descripción
NOMBRE DEL CAMPO	<i>Custom 1-n</i>	Nombre del campo personalizado. Este nombre puede ser modificado por el usuario y aparece en el software cliente de Blancco Drive Eraser. La longitud máxima del nombre es 220 caracteres.  No puede estar vacío. Además, dos o más campos no pueden tener nombres idénticos.
VALOR PREDETERMINADO	<i>n/a</i>	Valor predeterminado del campo; puede ser modificado por el usuario. La longitud máxima del valor es 1000 caracteres.
TIPO	<i>textfield</i>	Si el campo es un cuadro de texto normal (textfield), una lista desplegable normal (droplist) o una lista desplegable con múltiple selección de elementos (multidropist).  Para crear un campo personalizado desplegable o multidesplegable, añada un valor en el campo "Valor predeterminado". Solo entonces, el valor del campo "Tipo" puede cambiarse a "droplist" o "multidropist". Mientras el campo "Valor predeterminado" esté vacío, el campo personalizado se considera un cuadro de texto y el "Tipo" está bloqueado con el valor "textfield".  Con las listas desplegables y multidesplegables, cada entrada tiene que separarse con una coma (.). La cadena ,1,2,3 generaría una lista desplegable con una primera entrada vacía, la segunda con "1", la tercera con "2" y la cuarta con "3". Las entradas duplicadas siempre se eliminan. Si el campo es obligatorio, las entradas

Nombre	Valor predeterminado/de ejemplo	Descripción
		vacías se eliminan. Si las reglas descritas anteriormente no dejan ningún valor en el campo y el campo es obligatorio, se convertirá en un campo de texto (pero seguirá siendo obligatorio).
OBLIGATORIO (casilla de verificación)	[no activado]	Indica si el campo es obligatorio (activado) o no (no activado).  No está disponible si "Proceso de borrado" está configurado como "Flujo de trabajo".
POR DISPOSITIVO CONECTADO (casilla de verificación)	[no activado]	Si "Informe por dispositivo conectado" (consulte <a href="#">Seguridad</a> ) está habilitado, el campo personalizado se comporta como un campo individual por dispositivo (destinado a contener información única para cada unidad suelta, Chromebook, etc.). Esta opción no está disponible si la opción "Seguridad – Informe por dispositivo conectado" está desactivada. Recuerde que los valores predeterminados para los campos personalizados se purgan cuando se utiliza la opción "por dispositivo conectado".
BLOQUEADO (casilla de verificación)	[no activado]	Bloquea el campo. El campo bloqueado no puede editarlo el usuario que ejecuta Blancco Drive Eraser (el campo está atenuado).  Recuerde que un campo bloqueado requiere un valor en el campo <b>Valor predeterminado</b> . El campo no puede tener el valor <b>Obligatorio</b> o <b>por dispositivo</b> .
Botón Eliminar campo		Elimina el campo.
Botón Añadir campo		Añade un nuevo campo personalizado.
Expresión regular	n/a	Expresión regular aplicada a este campo. Consulte el capítulo <a href="#">Expresiones regulares para campos personalizados</a> para obtener más información.
Sugerencia	n/a	Sugerencia para la expresión regular. Se mostrará al usuario de BDE.

Recuerde que:

- Los campos personalizados son cuadros de texto, están vacíos y no son obligatorios de forma predeterminada.
- Cualquier campo personalizado obligatorio que se deje vacío aquí tendrá que rellenarse durante la sesión de Blancco Drive Eraser para que el usuario pueda guardar o enviar el informe.
- De forma predeterminada, hay 2 campos personalizados ("Custom 1" y "Custom 2"): estos campos pueden renombrarse, modificarse o eliminarse a voluntad.

### 3.7.1 Icono de ojo



Al hacer clic en el icono de ojo en la esquina superior derecha, se abre la ventana "Vista previa del formulario de campos personalizados", donde puede visualizar cómo ve el operador los campos

personalizados. Para ver los "Campos por unidad", debe haber campos personalizados configurados y marcados con "Por dispositivo conectado".

Campos por unidad:

### 3.7.2 Expresiones regulares para campos personalizados

Todos los campos personalizados también pueden configurarse para que exijan que los datos introducidos en el software cliente sigan unas reglas predefinidas. Las reglas se definen mediante expresiones regulares.

La expresión regular, que determinará qué tipo de entrada se acepta para ese campo, se inserta en el campo **Expresión regular**. Este software utiliza la sintaxis de expresiones regulares de JavaScript.

Por ejemplo, la expresión regular `(A|F)[0-9]{3}` requeriría que el valor sea "A" o "F" seguido de 3 caracteres numéricos (por ejemplo, A245 sería una entrada aceptada).

Recuerde que las expresiones regulares se validan acorde con las normas de la implementación de validación de JavaScript. Cualquier carácter que no esté en el conjunto de caracteres aprobados se considera una división de palabra. Este conjunto de caracteres se limita al alfabeto latino en mayúsculas y minúsculas, dígitos decimales y carácter de subrayado. Los caracteres acentuados, como "é" o "ü" se tratan como divisiones de palabras. Consulte la documentación de JavaScript sobre expresiones regulares para obtener más información.

Recuerde que la siguiente expresión parece correcta:

`[0-9]{4|6}`

Podría esperarse que coincida con una entrada de 4 o 6 dígitos. No es el caso. La expresión en este caso consta de dos alternativas:

Alternativa 1: `[0-9]{4}` (p. ej., 1{4})

Alternativa 2: 6}

El motor utilizado por Drive Eraser marcará esta expresión como sintácticamente incorrecta, porque las llaves no tienen coincidencia de apertura/cierre. Sin embargo, algunos de los recursos disponibles en Internet no detectarán el error.

Deben verificarse y comprobarse las expresiones regulares antes de utilizarlas en un entorno de producción. Deben utilizarse herramientas externas (como <https://regexr.com>) para validar las expresiones regulares introducidas en CT. Las versiones más recientes de Blancco Drive Eraser purgarán las expresiones regulares no válidas.

La **Sugerencia** puede contener una indicación de qué tipo de entrada se espera, se muestra en la interfaz de usuario del software del cliente para este campo personalizado específico. Para el ejemplo anterior, la sugerencia podría ser "A o F y tres números". Recuerde que un campo personalizado con una expresión regular no puede recibir un valor predefinido (se purgará).

### 3.8 Comunicación

Este menú contiene opciones relacionadas con la conectividad con el servidor que ejecuta Blancco Management Console.

Si el equipo que va a borrar está conectado a una red donde se está ejecutando un servidor de BMC, es posible configurar los valores para establecer una comunicación con él y:

- Consumir licencias de forma remota a través de la red (el HASP está conectado al servidor de BMC, no al equipo).
- Enviar el informe de activos, el informe de problemas y/o el informe de borrado al servidor de BMC (no es necesario guardar el informe en un dispositivo externo).

Recuerde que:

- Debe introducir la dirección IP del servidor (o su nombre de host si está definido) que ejecuta el BMC en su red local. El protocolo de comunicación es siempre **https**.
- Si falta alguno de estos valores, el equipo que se va a borrar no podrá comunicarse con el servidor de BMC ni enviarle informes. Sin embargo, podrá guardar los informes en un dispositivo externo (como una llave USB).



Blanco Management Console

Hostname / IP

Port

HTTPS

On

Username

Password

Timeout (seconds)

20

Do not validate the remote certificate

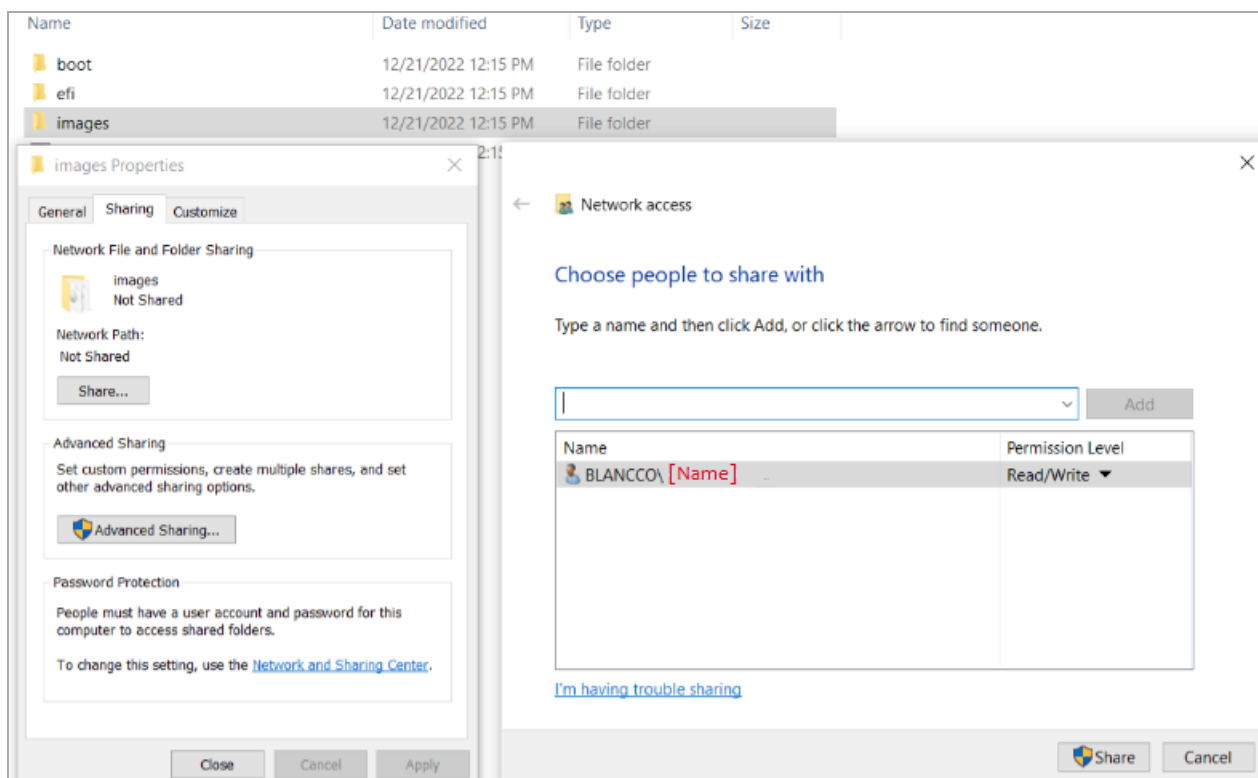
### 3.8.1 Blanco Management Console

Nombre	Valor predeterminado/de ejemplo	Descripción
Nombre de host / IP	n/a	La dirección IP del servidor que está ejecutando BMC en su red local. Ejemplo: 10.1.1.1 cloud.blanco.com https://172.16.1.98:8443
Puerto	n/a	Número de puerto de BMC. Este puerto se configuró al instalar BMC; es el puerto 8443 de forma predeterminada (siempre se aplica el protocolo HTTPS). Consulte el manual de BMC para obtener más información.
HTTPS	Activado	Campo bloqueado, la capacidad HTTPS está siempre activada.
Nombre de usuario	n/a	Nombre de usuario para acceder a BMC. Los valores deben tener una longitud de entre 3 y 64 caracteres.
Contraseña	n/a	Contraseña del usuario definido en "Nombre de usuario" para acceder a BMC. Los valores deben tener un mínimo de 6 caracteres y un máximo de 64.
Tiempo inactivo (segundos)	20	Tiempo de espera para la comunicación con BMC (cuánto tiempo se intenta la conexión con BMC). Los valores posibles van de 20 segundos a 600 segundos (10 minutos). Se recomienda aumentar este valor si tiene problemas recurrentes de conectividad con BMC.
No validar el certificado remoto	[no activado]	Si se activa, el certificado TLS ofrecido por Blanco Management Console <b>no está validado</b> . Desactivado de forma predeterminada. Recuerde que la validación del certificado no es posible si la dirección de BMC es una dirección IP o bien localhost. En este caso, esta opción está activada y no se puede modificar.

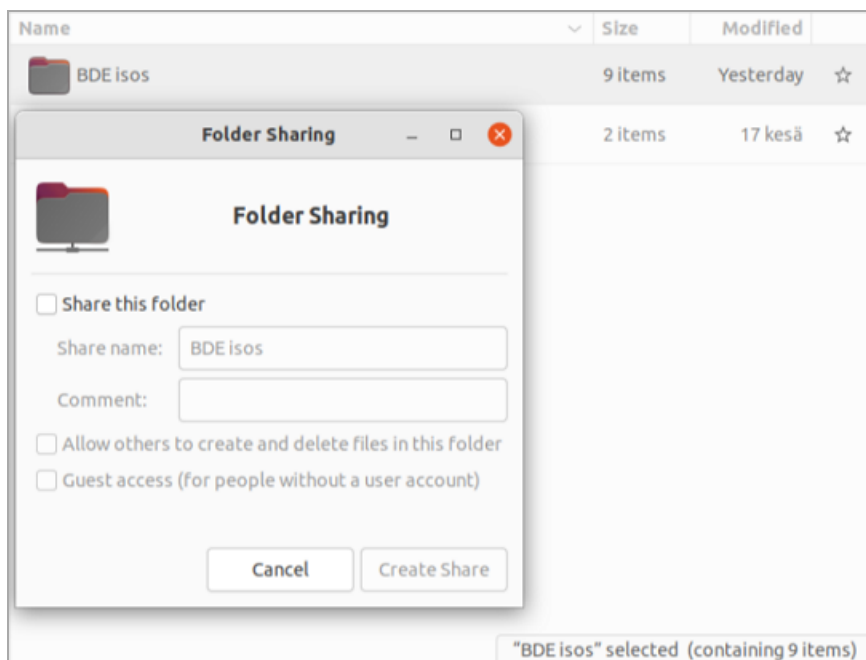
### 3.8.2 Recurso compartido de red

Una carpeta compartida en red es una carpeta que tiene propiedades y permisos para compartir dentro de una red local.

Por ejemplo (Windows): Clic derecho > Propiedades > Compartir:



Para dispositivos con Ubuntu: Clic derecho > Recurso compartido de red local:



O mediante línea de comandos en Linux (<https://www.techrepublic.com/article/how-to-set-up-quick-and-easy-file-sharing-with-samba/>)

El uso de una carpeta compartida en red es interesante en el caso de que BDE esté conectado a una LAN sin conexión a Internet ni BMC. Una vez montada una carpeta compartida en red en BDE, puede utilizarse

como ubicación para guardar informes. Es posible acceder a la carpeta compartida en red utilizando diferentes protocolos de comunicación, como SSH, SMB, FTP, SFTP, NFS. Actualmente, BDE se centra únicamente en SMB (Server Message Block) mediante un software gratuito llamado "Samba".

Para personalizar la característica de recurso compartido de red en CT:

Network share

Hostname / IP

Path

Username

Password

••••••••

Domain *Optional*

Protocol

SMB

Nombre	Valor predeterminado/de ejemplo	Descripción
Nombre de host / IP	n/a	IP o nombre de host del dispositivo que comparte el recurso compartido de red. El nombre de host puede ser un nombre DNS resoluble válido o la dirección IPv4 del servidor.
Ruta	n/a	Ruta del directorio de la ubicación donde se guardan los informes de BDE. La ruta es el nombre del recurso compartido del servidor y puede contener también uno o varios subdirectorios. Esos subdirectorios deben existir en el servidor antes de que se establezca la conexión. Se utiliza la barra diagonal "/" como separador. La ruta no distingue entre mayúsculas y minúsculas y puede contener espacios.
Nombre de usuario	n/a	El nombre de usuario debe tener un mínimo de 3 y un máximo de 64 caracteres.
Contraseña	n/a	La contraseña debe tener un mínimo de 6 y un máximo de 64 caracteres.
Dominio	n/a	Este ajuste es opcional, pero puede que un servidor lo necesite para la autenticación.
Protocolo	SMB	Es posible acceder a la carpeta compartida en red mediante estos protocolos. Existen múltiples opciones, pero actualmente el único protocolo de comunicación para BDE es Server Message Block (SMB).

### 3.8.3 Control remoto VNC

BDE puede utilizar el software VNC para el control remoto de un equipo. Estos ajustes solo pueden modificarse en CT.

Los ajustes se encuentran en la pestaña **Comunicación**:

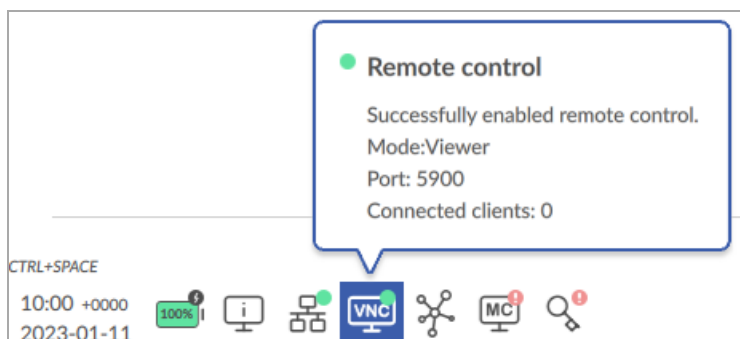
Communication	Password	<input type="text"/>
	Domain <i>Optional</i>	<input type="text"/>
Networking	Protocol	SMB <span>▼</span>
OS	VNC remote control	
Debug	Enabled	<input checked="" type="checkbox"/>
	Mode	VNC Repeater <span>▼</span>
	Hostname / IP	10.1.2.3
	Port	5432
	Password <i>Optional</i>	<input type="password"/>

Cuando está habilitado, el usuario puede elegir entre dos modos:

- **Visor VNC**

- En este modo, el equipo BDE/BDV está en la misma red que el equipo host del usuario.
- El usuario debe ejecutar el software visor VNC de su elección y conectarse directamente desde el equipo host al equipo BDE/BDV.

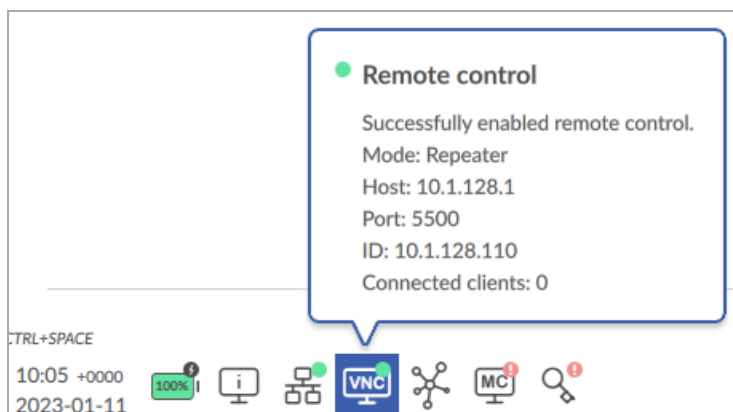
En BDE, el modo Visor tiene este aspecto:



- **Repetidor VNC**

- En este modo, el equipo BDE/BDV se encuentra en la red a la que no puede acceder el equipo host del usuario, pero hay otro equipo al que pueden acceder tanto BDE/BDV como el equipo host del usuario.
- El usuario debe ejecutar el software repetidor VNC de su elección que actúa como un proxy, situándose en medio entre el servidor y el visor. Todos los datos de la sesión pasan por el repetidor. BDE/BDV se conecta al repetidor y el equipo host que ejecuta el software visor VNC se conecta al repetidor.

- En BDE, el modo Repetidor tiene este aspecto:



En el modo Repetidor, debe introducirse el nombre de host / dirección IP del equipo repetidor.

Puerto es el puerto IP del servidor VNC que puede aceptar conexiones remotas. En el **modo Visor**, el puerto predeterminado es 5900. En el **modo Repetidor**, el puerto predeterminado es 5500. El número de puerto puede seleccionarse libremente entre 1 y 65535 siempre que el puerto no esté reservado para ningún otro uso.

**Nota:** En el modo repetidor, se utiliza el puerto predeterminado 5900 para que el repetidor se conecte de modo que también sea posible una conexión directa a ese puerto.

La contraseña es opcional, por lo que puede dejarse vacía. Tenga en cuenta que en algunos clientes del visor VNC no se permite dejar vacía la contraseña, lo que supone que la conexión no funcionará.

## 3.9 Red

Este menú contiene opciones relacionadas con la conectividad a la red del equipo que ejecuta Blancco Drive Eraser.

### 3.9.1 Configuración de red estática/dinámica

Si el DHCP está activado (lo está de forma predeterminada), la imagen obtiene automáticamente su configuración relacionada con la red del servidor DHCP (configuración de red dinámica).

Para aquellos usuarios que deseen configurar una red estática, se puede desactivar el DHCP (dejar sin marcar la casilla DHCP) e introducir manualmente la configuración de red. Si esta configuración no es válida, Blancco Drive Eraser no podrá acceder a la red.

Global network settings

Disable network entirely

☐

Enable SSH connections

☐

Report network information

☒

Networking

Wired enabled

☒

DHCP

☒

VLAN

Wireless

Wireless enabled

☐

Proxy

Hostname / IP

Port

Username

Password

Network security

Enabled

☐

### 3.9.2 Configuración de red global

Nombre	Valor predeterminado/de ejemplo	Descripción
Deshabilitar red por completo	[no activado]	Si está seleccionado, se deshabilitan todas las conexiones de red, alámbricas e inalámbricas.
Habilitar conexiones SSH	[no activado]	Si se permiten o no las conexiones SSH con el software cliente.
Información de red del informe	[activado]	Si se selecciona, el informe contendrá toda la información de red. Si no se selecciona, toda la información de MAC, IP y DNS se eliminará de los

Nombre	Valor predeterminado/de ejemplo	Descripción
		informes. Tenga en cuenta que este ajuste no afecta al contenido del informe de problemas.

### 3.9.3 Red

Nombre	Valor predeterminado/de ejemplo	Descripción
Cableado habilitado	<i>[activado]</i>	Si está habilitada o no la conexión de red con cable.
DHCP	<i>[activado]</i>	Si está activado, BDE obtendrá automáticamente su configuración de red del servidor DHCP (dirección IP dinámica, máscara de subred, etc.). Si no está activado, BDE necesita que su configuración de red se defina estáticamente (consulte la configuración más abajo).
Selección de interfaz	<i>Primera interfaz adecuada</i>	Este ajuste está disponible si "DHCP" no está activado. Si se selecciona "Primera interfaz adecuada", la configuración de red estática se aplicará al primer adaptador de red que pueda utilizarla. Si se selecciona "Bucle hasta conectarse a BMC", se recorrerán en bucle todos los adaptadores de red detectados y se aplicará la configuración de red estática a cada uno de ellos hasta que alguno logre una conexión correcta con BMC.
Dirección IP	<i>192.168. 1.99</i>	Este ajuste está disponible si "DHCP" no está activado. Esta es la dirección IP estática que BDE utilizará para conectarse a la red.
Máscara de subred	<i>255.255. 255.0</i>	Este ajuste está disponible si "DHCP" no está activado. Dirección de la máscara de subred de la red.
Puerta de enlace predeterminada	<i>192.168. 1.1</i>	Este ajuste está disponible si "DHCP" no está activado. Dirección de la puerta de enlace predeterminada de la red.
DNS1	<i>10.0.0.1</i>	Este ajuste está disponible si "DHCP" no está activado. Dirección del DNS primario de la red.
DNS 2	<i>10.0.0.2</i>	Este ajuste está disponible si "DHCP" no está activado. Dirección del DNS secundario de la red.
VLAN	<i>n/a</i>	ID de VLAN. El rango de valores aceptable es de 1-4094. Recuerde que, si se habilita la conexión inalámbrica, este campo se vacía y se desactiva.

### 3.9.4 Conectividad WLAN

Recuerde que:

- Se debe introducir el SSID o "nombre de red" de la WLAN, excepto para el tipo de encriptación WPA-PSK, que permite dejar vacíos la contraseña y el SSID.
- Los valores (contraseña, tipo de encriptación, red oculta) dependen por completo de las características de la red inalámbrica. Si los valores son incorrectos, el equipo que se va a borrar no podrá comunicarse con el servidor de BMC ni enviarle informes. Sin embargo, podrá guardar los informes en un dispositivo externo (como una llave USB).
- En el caso de que tanto la LAN como la WLAN estén disponibles y la configuración sea válida, la comunicación con BMC utilizará la primera red adecuada. LAN tiene mayor prioridad que WLAN.
- Solo se puede acceder a la configuración de WLAN desde CT (no directamente desde la GUI de Blancco Drive Eraser).

Wireless

Wireless enabled
☒

Encryption type
WPA-PSK

Hidden SSID
No

Wlan SSID

Password

Nombre	Valor predeterminado/de ejemplo	Descripción
Conexión inalámbrica habilitada	<i>(no activado)</i>	Indica si está habilitada o no la conectividad WLAN.
Tipo de encriptación	<i>WPA-PSK</i>	Tipo de encriptación de la red inalámbrica. Los tipos son: WPA-PSK, WPA-EAP, WEP y ninguno (no se utiliza encriptación). Recuerde que se admiten todos los tipos de EAP que no requieren nada externo (certificados o servidor de autenticación).
SSID oculto	<i>No</i>	Si SSID tiene la difusión activada (público) o está oculto.
SSID de WLAN	<i>n/a</i>	El valor SSID de la WLAN. Obligatorio, si la conexión inalámbrica está habilitada.
Contraseña	<i>n/a</i>	La contraseña de la red inalámbrica. Obligatorio, si "Tipo de encriptación" es distinto de "ninguno".

### 3.9.5 Proxy

Si se utiliza un proxy para la conexión de red, estos campos deben rellenarse.

Proxy

Hostname / IP

Port

Username

Password

Nombre	Valor predeterminado/de ejemplo	Descripción
Nombre de host/IP	<i>10.1.1.1</i>	Dirección IP del proxy.
Puerto	<i>8080</i>	Número de puerto del proxy.
Nombre de usuario	<i>Nombre de usuario</i>	Nombre de usuario del proxy.
Contraseña	<i>ContraseñaFuerte</i>	Contraseña del proxy.

### 3.9.6 Seguridad de red

Si la seguridad de la red está habilitada, la compatibilidad con la autenticación 802.1x está habilitada. Con ello se permitirá la conexión a redes a través de adaptadores de red y una wifi de empresa WP2.



Nombre	Valor predeterminado/de ejemplo	Descripción
Activado	<i>(no activado)</i>	Indica si esta característica está habilitada o no.
Protocolo	<i>PEAPv0/EAP-MSCHAPv2</i>	Protocolo seleccionado.
Identidad	<i>IdentityName</i>	Identidad de la red.
Contraseña	<i>ContraseñaFuerte</i>	Contraseña de la red.
Usar certificado de CA	<i>(no activado)</i>	Indica si el certificado de CA (autoridad de certificación) cargado a continuación se utiliza o no.
Nombre de archivo	<i>La imagen no contiene ningún certificado / [nombre de certificado]</i>	Nombre del certificado cargado.  Cargar un certificado de CA al hacer clic en el botón Cargar. De esta forma, se abre el explorador de archivos. Úselo para buscar el certificado de CA y seleccionarlo.  Si se carga un certificado, haga clic en el botón Eliminar para eliminarlo.

Recuerde que el archivo del certificado de CA debe estar obligatoriamente en un formato válido. El formato válido es un X509V3 en contenedor PEM, y el tamaño máximo reservado para almacenarlos es de 10 KB. Si el certificado presenta un formato incorrecto, es posible convertirlo.

Por ejemplo, si un DER se convierte al formato PEM con openssl:

```
openssl x509 -inform DER -outform PEM -text -in mykey.der -out mykey.pem
```

## 3.10 SO

Este menú contiene algunos ajustes adicionales que influyen en la forma en que arranca y se comporta el software.

### 3.10.1 Opciones de arranque

Las opciones de arranque permiten que Blancco Drive Eraser se arranque con valores alternativos si hay problemas con el arranque predeterminado.

Boot options

Preset

FLR during startup [DEFAULT]

CD ejection

After boot-up

☒

After completed erasure

☐

After report sending/saving

☐

At shutdown

☐

Restart / Shutdown

Preset

none

List of hybrid drives

Import from file

Export to file

La imagen de Blancco Drive Eraser puede arrancarse de varias maneras diferentes, cada una de las cuales habilita un conjunto diferente de características.

Estas opciones son:

**Eliminación de bloqueo de inmovilización durante el arranque:** esta es la opción predeterminada. El proceso de eliminación del bloqueo de inmovilización se realiza durante la fase de arranque, antes de cargar los controladores del sistema para aumentar las posibilidades de que se active el equipo tras la eliminación del bloqueo de inmovilización.

**Arranque normal (resolución nativa):** Blancco Drive Eraser se carga utilizando cualquier controlador disponible que corresponda a la tarjeta gráfica del equipo (el controlador gráfico estándar/universal es solo una alternativa).

**Arranque normal (resolución segura):** Blancco Drive Eraser se carga utilizando un controlador gráfico estándar/universal. La resolución de pantalla de la GUI es fija (1024\*768).

**Instalador:** Esta opción de arranque permite instalar el software en un equipo (instalación persistente). Se utiliza para procesar unidades sueltas o Chromebooks, por ejemplo. Todos los informes de borrado se almacenan en la unidad de instalación, pero pueden exportarse a una memoria USB externa o enviarse a BMC.

**Mostrar mensajes de arranque:** esta opción es igual que la segunda, excepto porque los mensajes de arranque se muestran en la pantalla en lugar de la pantalla de carga animada.

**Arranque personalizado:** al seleccionar esta opción, aparece un campo de texto denominado “Línea de comandos”:

Boot options

Preset

Customized startup

Command line

archisobasedir=arch archisolabel=BLANCCO co

Este campo de texto se puede utilizar para configurar libremente los parámetros de arranque. Los siguientes parámetros de arranque son validados por Drive Eraser Configuration Tool:

Parámetro	Valores posibles / Opciones adicionales	Descripción
cr		Habilita el modo de informe de fallos manual.
debug		Habilita más mensajes del kernel. Se utiliza para la resolución de problemas. Lo opuesto a "quiet".
flr	flr=15 flr=10 flr=20 flr=30 flr=60 flr=forced flr=disabled	Habilita la eliminación del bloqueo de inmovilización durante el arranque.  De forma predeterminada, hay una alarma de 10 segundos durante los cuales el ordenador debería ser capaz de suspenderse y reanudarse al establecerse la alarma. En CT, se realiza una comprobación de estado para verificar que el valor del tiempo de espera esté entre 5 y 60 segundos. Esa comprobación se puede omitir modificando los parámetros durante el arranque.  "flr = [15-60]" se utiliza para modificar el tiempo de espera. "flr=15" serían 15 segundos. Si el parámetro no se proporciona o su valor es desconocido, se utilizará en su lugar el tiempo de espera predeterminado (10 segundos).  "flr=forced" fuerza que se aplique siempre la opción flr.  "flr=disabled" deshabilita completamente que se intente la eliminación del bloqueo de inmovilización.
intremap	intremap=nosid intremap=on intremap=off intremap=no_x2apic_optout intremap=nopost	"intremap" significa reasignación de interrupciones, que es una funcionalidad de software para redirigir señales de un dispositivo periférico. Esta opción permite al kernel sustituir las tablas de reasignación creadas por la BIOS de la máquina.  El usuario puede elegir un valor entre los siguientes: "on", "off", "nosid", "no_x2apic_optout", "nopost".  El ajuste "intremap=nosid" es obligatorio para que la pantalla / arranque del Macbook 12, 13,3, 9,1 funcione correctamente.
kms		Habilita la configuración del modo kernel (lo más probable es que esté habilitada de todos modos a menos que se deshabilite explícitamente). Permite al kernel definir el controlador gráfico.
loglevel	loglevel=0	Cantidad de mensajes del kernel durante el arranque.  "loglevel=0" muestra solamente los mensajes del kernel de emergencia para limpiar el arranque.
memtest	memtest=00	Especifica el número de pasadas de pruebas de memoria que se realizarán. Hay disponibles 17 patrones de prueba diferentes.  memtest=00 significa que las pruebas de memoria están deshabilitadas.  Si se habilita, se realizarán 17 pasadas de forma

Parámetro	Valores posibles / Opciones adicionales	Descripción
		predeterminada, que se someterán a todos los patrones de prueba. El número máximo de rondas es 99.
noapic		Esta opción deshabilita APIC. Deshabilitar APIC elimina la capacidad de utilizar IRQ compartido o reasignación IRQ de dispositivos. APIC (Advanced Programmable Interrupt Controller) es la sustitución del chip PIC anterior que, en el pasado, estaba integrado en placas bases y permitía la configuración de interrupciones de periféricos como tarjetas de sonido, controladoras IDE, compartir/redirigir interrupciones.
nomodeset		Al seleccionar esta opción, se indica al kernel que no cargue los controladores de vídeo y utilice en su lugar los modos BIOS.
quiet		Deshabilita la mayoría de los mensajes del kernel. Lo opuesto a "debug".
rd.driver.blacklist=nouveau modprobe.blacklist=nouveau		Se sabe que el controlador nouveau de la tarjeta gráfica Intel NVIDIA causa problemas (p. ej., en portátiles con tecnología Optimus).  Si se añaden manualmente estas dos opciones, se podrá utilizar el controlador Intel i915 VGA en su lugar y resolver el problema de la pantalla negra en estos equipos.
nouveau.modeset	nouveau.modeset=0	Indica si debe habilitarse el controlador. 0 para deshabilitado, 1 para habilitado, 2 para equipo sin periféricos. Ayuda con algunos modelos HP ZBook.  Más información: <a href="https://nouveau.freedesktop.org/KernelModuleParameters.html">https://nouveau.freedesktop.org/KernelModuleParameters.html</a>
pci	pci=noms, noaer	"pci" se utiliza para varias opciones del subsistema PCI.  "pci=noms, noaer" se utiliza para solucionar problemas con el controlador ethernet Lenovo 88E8057.
radeon.runpm=0		Deshabilita la administración de energía del tiempo de ejecución PX.  Resuelve algunos problemas del controlador de gráficos Radeon en algunos equipos con tarjetas gráficas duales conmutables (Intel integrada + AMD/ATI).
random.trust_cpu=1	1 = activado 0 = desactivado	Habilitar o deshabilitar la confianza en el uso del generador de números aleatorios de la CPU (si está disponible) para sembrar completamente el CRNG del kernel.
rd.udev.log-priority=3		Limpia el mensaje de arranque de systemd: "starting version...".
splash		Muestra la pantalla de presentación de Blancco Drive Eraser durante el arranque.  Elimine el parámetro para arrancar Macbook 7.1, 7.2, 11.1, 11.3
verbose		Marcador para los guiones de inicialización de Drive Eraser. Deshabilita la pantalla de presentación y muestra los mensajes en la pantalla.
vmalloc=400M		Aumenta la asignación de memoria predeterminada (128 MB) para la memoria virtualmente contigua. Es necesario para el arranque PXE, ya que la imagen ISO se cargará primero en esta área de memoria antes de arrancar.
ip=dhcp BOOTIF=\${netX/mac}		Si hay problemas con PXE/IPXE con algunas combinaciones Legacy BIOS/UEFI.  Sustituya \${netX/mac} por la dirección mac de la interfaz de red desde la que está arrancando.
acpi=off		Permite detectar correctamente la SSD interna en algunos modelos de HP EliteDesk.

Para los parámetros no validados, consulte: <https://www.kernel.org/doc/html/v4.15/admin-guide/kernel-parameters.html>

Para obtener más información, consulte el manual de Blancco Drive Eraser, capítulo “Opciones de arranque”, y <https://support.blancco.com>.

### 3.10.2 Expulsión de bandejas de CD

Blancco Drive Eraser puede expulsar automáticamente las bandejas de todas las unidades ópticas conectadas y reconocidas por el equipo. Es posible seleccionar que la expulsión se produzca en los siguientes momentos:

- Después del arranque: inmediatamente después de que Blancco Drive Eraser se haya arrancado. Seleccionado de forma predeterminada.
- Después del borrado completado: después de que el borrado o borrados se hayan completado.
- Después del envío/guardado de un informe: después de que se haya enviado un informe a Blancco Management Console o se haya guardado en una memoria USB.
- En el apagado: al salir de Blancco Drive Eraser.

Recuerde que:

- El objetivo principal de la expulsión de las bandejas de CD es evitar las posibles pérdidas de información que puedan producirse en caso de que se olviden discos ópticos con datos personales/profesionales dentro de un equipo que se borra y se envía a otro lugar. A este respecto, Blancco recomienda dejar siempre seleccionada al menos una opción.
- La función de expulsión de CD también se utiliza para monitorizar las distintas fases del proceso de borrado (arranque, borrado, informe, apagado). En este sentido, se pueden seleccionar varias expulsiones.

### 3.10.3 Reinicio / apagado

Blancco Drive Eraser puede reiniciarse o apagarse automáticamente. Esta funcionalidad no se puede activar cuando **Proceso** está definido como **Manual** o **Flujo de trabajo** (consulte [Seguridad](#)). Están disponibles las siguientes opciones:

- **ninguno**: el valor predeterminado. Sin reinicio ni apagado automático.
- **Reiniciar, tras borrado**: el equipo se reinicia automáticamente una vez ha finalizado el proceso de borrado.
- **Reiniciar, tras borrado correcto**: el equipo se reinicia automáticamente una vez que el proceso de borrado ha finalizado con un estado correcto.
- **Apagar, tras borrado**: el equipo se apaga automáticamente una vez ha finalizado el proceso de borrado.
- **Apagar, tras borrado correcto**: el equipo se apaga automáticamente una vez que el proceso de borrado ha finalizado con un estado correcto.

### 3.10.4 Lista de discos híbridos

La lista de archivos híbridos integrados en Blancco Drive Eraser puede modificarse con este menú.

Para exportar la lista de discos híbridos actual, haga clic en “Exportar hacia archivo”. Se exporta un archivo denominado “hybrid\_list.txt”. Esta lista puede modificarse (añadir/eliminar modelos de discos híbridos).

Para importar una lista de discos híbridos modificados, haga clic en “Importar desde archivo”. El archivo debe ser un archivo .txt y la información de los discos híbridos debe estar en formato:

```
Manufacturer;model
```

Ejemplo: Seagate;ST1000DX001

Para obtener más información acerca de los discos híbridos, consulte el manual de Blancco Drive Eraser.

### 3.11 Otros botones

A continuación, se describe el resto de las funcionalidades de la interfaz de usuario.

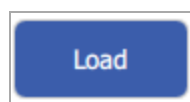
#### 3.11.1 Idioma

Al hacer clic en este botón, se abrirá el menú desplegable en el que puede modificarse el idioma de la interfaz de usuario.



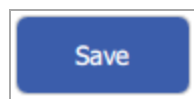
#### 3.11.2 Cargar nueva imagen

Con este botón puede cargar otra imagen de Blancco Drive Eraser para la configuración.



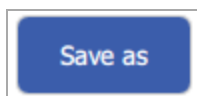
#### 3.11.3 Guardar

Pulse este botón para guardar todos los cambios realizados hasta el momento. Tenga en cuenta que esto no creará un nuevo archivo de imagen todavía.



#### 3.11.4 Guardar como

Pulse este botón para guardar la imagen configurada (imagen ISO). Puede guardar la imagen localmente o en una unidad de red.



Una vez que ha guardado la imagen, puede:

- Utilizarla para grabar un CD
- Incorporarla a una llave USB de arranque (puede utilizar para este fin la herramienta Blancco USB Creator)
- Añadirla como una imagen de arranque a un Preboot eXecution Environment o PXE (arranque de red)

## 4. Configuración de Blancco Drive Verifier

Con CT, es posible configurar todas las opciones principales de Blancco Drive Verifier. Recuerde que la disponibilidad de las opciones de configuración depende del producto concreto y versión de Blancco Drive Verifier.

Tras cargar una imagen de Blancco Drive Verifier en el software, podrá ajustar la configuración. Tenga en cuenta que los ajustes inaccesibles aparecen en color gris.

### 4.1 General

Este menú permitirá configurar las opciones generales. Para obtener más información sobre estos ajustes, consulte "General" en la página 65

### 4.2 Proceso

Este menú contiene opciones para procesos, como controlar el software de forma remota. Para obtener más información sobre estos ajustes, consulte [Proceso](#).

### 4.3 Flujo de trabajo

Este menú contiene opciones para configurar el flujo de trabajo. Para obtener más información sobre estos ajustes, consulte [Flujo de trabajo](#).

### 4.4 Seguridad (BDV)

Este menú contiene opciones para las características de seguridad de verificación.



Security options

Verification standard

...

All sectors the same

Byte value

0x00

Fail process if read errors

☒

Fail threshold

5

Fail process if the speed is too low (MB/s)

☐

Fail threshold

1

Execute self-tests on drives

None

Fail process if unsuccessful

☐

Verification level

☐

1

%

Simultaneous operations limit

50

Disable block SID authentication

No, skip

Timeout (seconds)

☒

5

Lock the verification settings

☐

Device enrollment detection

Persistent software

☐

Power saving settings

Spin down idle disks

☐

Nombre	Valor predeterminado/de ejemplo	Descripción
Estándar de verificación:	Igual para todos los sectores	La norma predeterminada utilizada en el procedimiento de borrado. Blancco Drive Verifier admite actualmente 4 estándares de verificación diferentes. Consulte el manual de Blancco Drive Verifier para obtener más información. El usuario puede ocultar algunos estándares de la interfaz de usuario de BDV mediante el botón de edición (tres puntos) situado junto a la lista de estándares.
Valor de byte	-	Valor de byte (también denominado patrón) que BDV buscará en toda la unidad, utilizado si el estándar es "Igual para todos los bytes".
Proceso fallido si hay errores de lectura	[activado]	Si está habilitado, el umbral del total de errores de lectura se define aquí. Si durante la verificación el total de errores de lectura alcanza este umbral, la verificación se detendrá automáticamente y fallará. El umbral predeterminado es de 5 errores. Además, el informe mostrará un mensaje de error que lo indica. El umbral de errores mínimo es 1 y el máximo es 1000

Nombre	Valor predeterminado/de ejemplo	Descripción
Proceso fallido si la velocidad es demasiado baja (MB/s)	[no activado]	Marca la verificación como fallida si la velocidad de verificación es inferior al valor establecido en el campo "Límite de fallo". Deshabilitado de forma predeterminada. El valor predeterminado es 1 y el rango de valores es de 1-10 000. La unidad se indica en mega-bytes/segundo.
Proceso fallido debido al tiempo límite (horas)	[no activado]	Marca el proceso como fallido si su duración es mayor que el valor del campo "Límite de fallo".  Deshabilitado de forma predeterminada. El valor predeterminado es 48 h. El rango personalizado es de 1 hora a 1 año (8760 h)
Ejecutar autodiagnósticos en unidades	[Ninguno]	Esta opción define el autodiagnóstico S.M.A.R.T de la unidad con el valor " <b>Ninguno</b> " (sin pruebas – opción predeterminada), " <b>Breve</b> ", " <b>Transporte</b> " o " <b>Extendido</b> ". Para obtener más información acerca de las opciones de autodiagnóstico, consulte el manual de usuario del software del cliente.
Proceso fallido si no funciona	[no activado]	Si esta opción está habilitada y falla el autodiagnóstico seleccionado, el proceso de verificación se cancela y falla. La razón del fallo se marca en el informe. Esta opción solo está disponible si el ajuste anterior "Ejecutar autodiagnósticos en unidades" está habilitado.
Nivel de verificación	1 %	Este ajuste define el nivel de verificación. El proceso de verificación lee los datos de la unidad a intervalos seleccionados aleatoriamente y se asegura de que la unidad esté cubierta con patrones periódicos. La verificación mínima corresponde a una comprobación del 1 % de la superficie del disco (proceso rápido), mientras que la verificación completa corresponde a la comprobación del 100 % de la superficie de la unidad (proceso más lento).
Límite de operaciones simultáneas	[50]	El número máximo de verificaciones simultáneas. Si el número de verificaciones que se están realizando simultáneamente es inferior al límite, es posible iniciar nuevas verificaciones hasta que se alcance el límite. Si el número de verificaciones rebasa este valor, las verificaciones nuevas o que superen el límite se colocan en una cola de verificaciones y quedan en pausa hasta que sea posible iniciarlas.
Deshabilitar Bloquear autenticación SID	No, omitir	Bloquear autenticación SID (BSA) es un tipo de bloqueo que impide ejecutar comandos de firmware en las unidades del equipo. Este ajuste permite

Nombre	Valor predeterminado/de ejemplo	Descripción
		preconfigurar un cuadro de diálogo para activar/desactivar ese bloqueo, así como un tiempo límite (ajuste secundario). Este ajuste tiene más que ver con un proceso de borrado; consulte <a href="#">"Configuración de Blancco Drive Eraser"</a>
Bloquear la configuración de verificación	[no activado]	Si esta opción está habilitada, el usuario de BDV no puede cambiar la configuración de verificación.
Calcular la vida útil restante de la unidad	[no activado]	Al activar este ajuste, se muestra en el informe una estimación del tiempo que le queda a cada unidad en función de varios atributos internos. Obtenga más información en el manual del usuario de BDE.

#### 4.4.1 Detección de inscripción de dispositivos

Para obtener más información sobre estos ajustes, consulte el capítulo ["Seguridad"](#).

#### 4.4.2 Configuración de ahorro de energía

Para obtener más información sobre estos ajustes, consulte el capítulo ["Seguridad"](#).

### 4.5 Verificación

En la pestaña Configuración de verificación, puede definir cuántas unidades deben verificarse, así como cuáles son los sectores que deben excluirse de la verificación.

El control deslizante "Seleccionar unidades aleatoriamente" está establecido en 5 % de forma predeterminada: si este valor no se define al 100 %, solo se seleccionará automáticamente un subconjunto de las unidades para su verificación; no obstante, siempre se verificará un mínimo de una unidad por activo.

Verification settings

Select drives randomly 5 %

Sector ranges to exclude from verification ⓘ

First sector of range ↓↑	Last sector of range ↓↑	Comment ↓↑

+

**Ejemplo 1:** el porcentaje de unidades para verificar se define en 5 % y BDV se ejecuta en un portátil que tiene una única unidad de disco: la unidad en cuestión se verificará de forma sistemática.

**Ejemplo 2:** el porcentaje de unidades para verificar se define en 5 % y BDV se ejecuta en un servidor que tiene cinco unidades: se seleccionará una unidad aleatoriamente para su verificación.

**Ejemplo 3:** el porcentaje de unidades para verificar se define en 5 % y BDV se ejecuta en un servidor que tiene cuarenta unidades: se seleccionarán dos unidades aleatoriamente para su verificación.

**Ejemplo 4:** el porcentaje de unidades para verificar se define en 5 % y BDV se ejecuta en un servidor que tiene cien unidades: se seleccionarán cinco unidades aleatoriamente para su verificación.

Si desea que todas sus unidades se verifiquen de forma sistemática, defina el porcentaje en 100 %. El valor predeterminado del 5 % corresponde al porcentaje de activos que deben verificarse según la certificación R2v3 (<https://sustainableelectronics.org/welcome-to-r2v3/>).

Los sectores típicos que deben excluirse de la verificación son los que contienen una huella digital o los que contienen un informe de activos de arranque. Obtenga más información acerca de la huella digital y el informe de activos de arranque en el manual del usuario del BDE.

Configure un rango de sectores para excluir de la verificación haciendo clic en el botón +. Un rango tiene un primer sector y un último sector, pero también puede decidir desde dónde empieza a contar (desde el principio o desde el final de la unidad) y también puede añadir un comentario por rango (por ejemplo, "Sectores de huellas digitales"). La dirección de recuento se elige con las flechas azules.

Se aplican algunas reglas: no es posible el solapamiento de sectores; si el primer sector se cuenta hacia atrás, el último no puede contarse hacia delante; el último sector no puede ser más pequeño que el primero (si ambos se cuentan hacia delante), etc.

The screenshot shows the 'Sector ranges to exclude from verification' interface. It has a table with three columns: 'First sector of range', 'Last sector of range', and 'Comment'. There are two rows of input fields. The first row has '10' in the first column and '1' in the second column. The second row has '1' in the first column and '1' in the second column. Red error messages are displayed below the input fields: 'Range start must be closer to disk start than the range end' for the first row, 'Range end must be closer to disk end than the range start' for the second row, and 'The range overlaps with another range' for the second row. There are also blue arrows for sorting and a '+' button for adding new ranges.

Con las flechas situadas junto a los rangos y la fila de comentarios, puede elegir cómo ordenar las distintas opciones, por ejemplo, en orden ascendente.

**Nota:** Si el segundo botón cambia a gris, significa que ya no es interactivo. Para que vuelva a estar en azul, haga clic en el botón izquierdo para que vuelva a tener el valor "Recuento desde el principio de la unidad".

A continuación, se enumeran algunas combinaciones posibles (la explicación se encuentra en la sección Comentarios):

The screenshot shows the 'Sector ranges to exclude from verification' interface with five rows of valid ranges. Each row has a 'First sector of range', a 'Last sector of range', and a 'Comment'. The ranges are: 0 to 9, 200 to 300, 9 to 0, 100 to 50, and 2000 to 3000. The comments explain the ranges: 'Excludes the first 10 sectors of the drive', 'Excludes all the sectors between #201 and #301 counting from the beginning of the drive', 'Excludes the last 10 sectors of the drive', 'Excludes all the sectors between #51 and #101 counting from the end of the drive', and 'Excludes all the sectors between #2001 (from the beg. of the drive) and #3001 (from the end of the drive)'. There are also blue arrows for sorting and a '+' button for adding new ranges.

## 5. Desinstalación

### 5.1 Guion de desinstalación

#### 5.1.1 En sistemas Windows

Desinstale CT como cualquier otro programa de Windows: Menú Inicio -> Configuración -> Aplicaciones -> Aplicaciones y características -> CT -> Desinstalar

#### 5.1.2 En sistemas Linux

Simplemente, elimine el archivo .appimage de CT.

## 6. Información de contacto

Para consultar la base de datos de conocimientos técnicos (preguntas frecuentes) y contactar con la asistencia técnica de Blancco mediante un ticket de asistencia técnica, visite:

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

Para ver vídeos instructivos acerca de los productos Blancco, visite:

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

Para obtener información de contacto y la información más reciente acerca de las soluciones de borrado seguro de datos, visite la página web de Blancco en:

<https://www.blancco.com>

Siempre buscamos la forma de mejorar nuestros productos. ¡Le rogamos que nos comunique cualquier sugerencia!