BCWipe Total WipeOut

Enterprise Edition

User Manual

Table of contents

Wiping Agents

Appendix

Introduction

When you delete sensitive files from a disk on your computer, the operating system does not erase the contents of those files from the disk - it only deletes references to the files from file-system tables. Contents of the deleted file (or file's body) remain on the disk and can be recovered by a forensic analyst.

Wiping is a term used to describe a process of shredding the contents of a file or of disk space. It is impossible to restore data that has been properly wiped.

BCWipe Total WipeOut Enterprise (BCWipe TWO) is a powerful solution for erasing whole drives securely. BCWipe Total WipeOut Enterprise can wipe all hard drives on the computer, including the drive on which the operating system is installed. It destroys the contents of whole hard drives, including partition tables, boot records, file-system structures, operating system files and user files.

Main Features of BCWipe Total WipeOut

Main features of the BCWipe Total WipeOut:

The utility is able to destroy contents of whole hard drives, including partition tables, boot records, filesystem structures, operating system files and user files.

BCWipe Total WipeOut can wipe storage on following hardware platforms, regardless of operating system installed on the computer.

- ❖ x86-compatible systems with BIOS or EFI
- ❖ x64-compatible systems with BIOS or EFI
- ❖ Itanium systems with EFI: Itanium servers running Windows, HP-UX or Linux
- ❖ 64-bit SPARC systems: servers running Solaris or Linux

BCWipe Total WipeOut can wipe all hard drives on the computer including the one where operating system is installed.

Contents of hard drives are wiped regardless of filesystem used to format the drives (FAT, NTFS, HPFS or other).

BCWipe Total WipeOut supports following wiping schemes:

1. U.S. DoD 5220.22-M(ECE)
2. U.S. DoD 5220.22-M(E)
3. U.S. DoE M 205.1-2
4. U.S. Army AR380-19
5. NAVSO P-5239-26 (MFM)
6. NAVSO P-5239-26 (RLL)
7. Canadian RCMP TSSIT OPS-II
8. British HMG IS5 Baseline
9. British HMG IS5 Enhanced
10. German BCI/VSITR
11. Russian GOST R 50739-95
12. Bruce Schneier's 7-pass wiping scheme
13. Peter Gutmann's 35-pass wiping scheme
14. 1-pass random
15. 1-pass zero

- ❖ BCWipe Total WipeOut allows users to create user-defined wiping schemes.
- ❖ BCWipe Total WipeOut can detect and reset Host Protected Area (HPA) on hard drives.
- ❖ BCWipe Total WipeOut defines number of sectors hidden by Device Configuration Overlay (DCO) functionality appeared since ATA-6 standard. BCWipe Total WipeOut can reset the DCO settings for hidden sectors.
- ❖ BCWipe Total WipeOut detects if a disk supports ATA SECURE ERASE command and uses it for wiping.

❖ BCWipe Total WipeOut detects NVMe disks and can run native firmware commands.

❖ BCWipe Total WipeOut automatically removes ATA disk freeze lock.

❖ BCWipe Total WipeOut supports hotplug.

❖ BCWipe Total WipeOut version 4 supports wiping of network devices connected with iSCSI protocol (SAN).

See also:

[BCWipe Total WipeOut Specifications](#)

[Booting BCWipe Total WipeOut Wiping](#)

[Agents User Interface](#)

Central Management of BCWipe Total WipeOut

BCWipe Total WipeOut **Enterprise Edition** allows to erase computers over the network.

The following functions are available in Enterprise Edition, in addition to the [Main features](#).

- Web Console to control wiping operations, download log files and generate reports
- Remote start of wiping process
- Multiuser role-based access to the Web Console
- Media-based wiping policies
- Several booting options (PXE, CD/DVD, USB)
- View wipe history for selected disk or asset
- Add offline log files into the database
- Centralized reports:
  - Available formats: PDF, HTML, CSV, DOCX, XLSX
  - Optionally: include asset details
  - Optionally: add up to three custom fields
  - Optionally: show warnings

See also:

[BCWipe Total WipeOut Console User Interface](#)

[Start Wiping](#)

[Policy Management](#)

[User Management](#)

[Upload Offline Wipe Logs](#)

[View Wipe History](#)

[Get Report](#)

System Requirements

BCWipe Total WipeOut Enterprise requires the following specifications.

Windows Operating System for Console Installation

- Windows XP SP2 or newer: Both 32- and 64-bit server or desktop systems are supported.
- RAM: 1GB minimum, 4GB recommended.
- Disk Space: 500MB minimum, 2GB recommended.

Oracle Java 8

- Download for free from www.java.com/download if not already installed.
- Reboot is recommended after installing Java.

Attention! OpenJDK Java 8 implementation is not supported.

SQL Database (optional)

- ❖ For small offices and evaluation purposes, BCWipe Total WipeOut Enterprise can use embedded Java database (default setting) with no additional actions required.
- ❖ For intensive operations and higher reliability, a separate database server is recommended (See Configuration Files chapter for more details):

  - MySQL 5.0 or newer.

  - PostgreSQL 9.0 or newer.

DHCP server (optional)

DHCP server is required for the following online wiping operations:

- Online wiping with control from the user console
- Booting wiping target over the network

BCWipe Total WipeOut Specifications

- ➢ Supported platforms:

  - ❖ x86-compatible systems with BIOS or EFI: Intel or AMD based computers

  - ❖ x64-compatible systems with BIOS or EFI: Intel or AMD based computers, Intel Macs

  - ❖ Itanium systems with EFI: Itanium servers running Windows, HP-UX or Linux

  - ❖ 64-bit SPARC systems: servers running Solaris or Linux

- ➢ Supported drive types:
  - ❖ HDD

  - ❖ SSD

  - ❖ [Hybrid disks (SSHD)](#)

  - ❖ [NVMe disks:](#) BCWipe Total WipeOut supports the following commands listed in disk's specification:

    - • Write Zeroes

    - • Deallocate (similar to ATA Trim)

    - • User Data Erase

    - • Cryptographic Erase

  - ❖ Flash

  - ❖ NAND

- ➢ Supported protocols/transports:

  - ❖ IDE

  - ❖ SATA

  - ❖ USB

  - ❖ Firewire

  - ❖ SCSI

  - ❖ Serial Attached SCSI (SAS)

  - ❖ SD/MMC/CF cards

  - ❖ iSCSI

- ➢ ATA/SATA hidden disk areas:

- ❖ Host Protected Area (HPA)

- ❖ Device Configuration Overlay (DCO)

- ➢ ATA/SATA disks: ATA SECURE ERASE command

- ➢ Number of parallel wiping operations:
  - ❖ Unlimited

- ➢ Number of supported wiping schemes:

  - ❖ 15

  - ❖ 2 (evaluation mode)

- ➢ Boot options:
  - ❖ PXE (legacy mode)

  - ❖ PXE (EFI x64)

  - ❖ USB

  - ❖ CD/DVD

Installation

1. Start BCWipeTWO-enterprise-setup.exe.

If you see a Java Version Check dialog box (pictured below) instead of the BCWipe Total WipeOut Enterprise Setup welcome screen, please make sure the following conditions are met:

- Oracle Java 8 or newer is installed.

- The **java.exe** program is accessible via system PATH. To check it, start Command Prompt (cmd.exe) and enter the **java -version** command. Upon successful completion, this command will print your Java version information.

- The system was restarted after Java installation.

We also recommend reviewing the system requirements for BCWipe Total WipeOut.

2. Follow the steps outlined in the setup dialog windows.

- Setup dialog windows feature the following buttons: Cancel, Next, and Back.

    Cancel aborts installation.
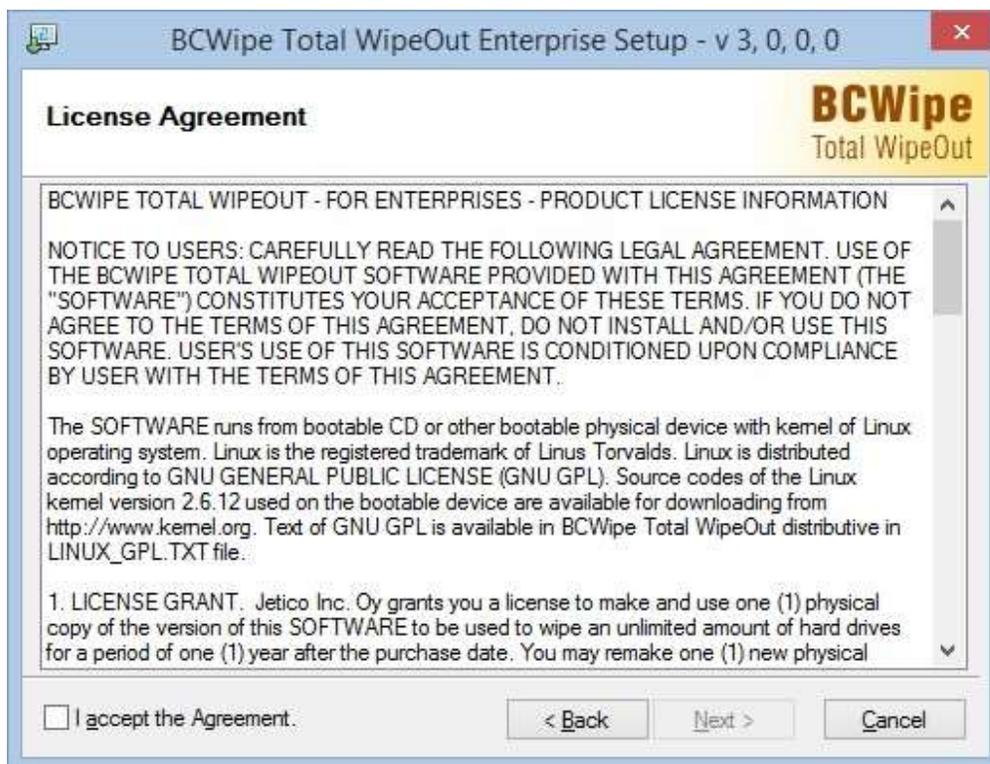
    Next proceeds to the next step of installation.

    Back returns to the previous step of installation.

3. Read the License Agreement.

Read the License Agreement carefully and check 'I accept the Agreement' if you approve. Then click Next.

4. Select your license type.

- Select **Previously installed license** if you are running the installation program to upgrade existing software.

- Select **External license** to prompt an Open File dialog and select a file containing the license information for the software.

- Select **License, embedded in the Setup program** if you have installed a trial version of the software.

Click Start button to continue installation.
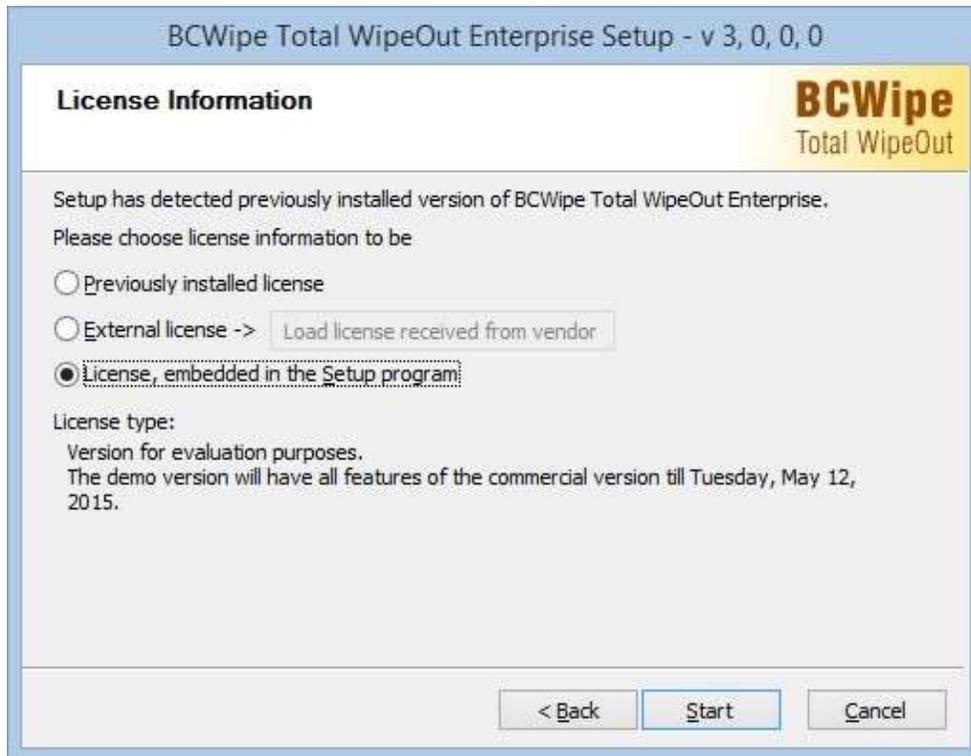
The setup wizard will now copy application files and update system settings.

5. The final step.

After successful installation, please review Post-install Configuration.

Post-install Configuration

BCWipe Total WipeOut Enterprise can be used for demonstration and evaluation purposes with the default settings created by the setup program.

To prepare the server for production, it is highly recommended that the database, security and server settings for network operations are configured as soon as possible after installation.

Database Settings

For small offices and evaluation purposes, BCWipe Total WipeOut Enterprise can use embedded Java database (default setting) with no additional actions required. For intensive operations and higher reliability, a separate database server (MySQL, PostgreSQL) is strongly recommended

Database settings are stored in the **application.properties** file. See the Configuration Files chapter for detailed instructions.

Security Settings

BCWipe Total WipeOut Enterprise installs with the following default administrator account settings:

> username = **admin**
>
> password = **admin**

Please change password for the admin account as soon as possible.

Server Settings for Network Operations

To access the server console from a remote computer, ensure that TCP port 8443 (default value; can be changed in the Configuration Files) is accessible to the remote computer. Create a permissive firewall rule if required.

To allow booting and wiping computers over the network, ensure that UDP port 69 is accessible for remote hosts. Create a permissive firewall rule if required.

Server address for wiping endpoints must be defined in the Server Settings admin section prior to any wiping operation.

Preparing Environment for Network Boot

The recommended modifications depend on which DHCP server version is used in your network environment: Microsoft or ISC.

Microsoft DHCP Server

1. Open the Server Manager and select your DHCP server in the DHCP Server Role.
2. Select **IPv4** in Server Options.
3. Configure options:

- `066 Boot Server Host Name` - enter the BCWipe Total WipeOut server IP address

- `067 BootFILE Name` - enter `/pxelinux.0`

4. Restart the DHCP server

ISC DHCP Server

1. Open the DHCP server configuration file (usually **/etc/dhcp/dhcpd.conf**).

2. Add the following lines to the configuration file:

   `next-server ip_address;` # enter the BCWipe Total WipeOut server IP address

   `filename "/pxelinux.0";`

3. Restart the DHCP server.

Linux DHCP server for EFI and BIOS network boot

Add following lines to the common section of your dhcp.conf (usually **/etc/dhcp/dhcpd.conf**).

option space PXE;
option PXE.mtftp-ip code 1 = ip-address;
option PXE.mtftp-cport code 2 = unsigned integer 16; option
PXE.mtftp-sport code 3 = unsigned integer 16; option PXE.mtftp-
tmout code 4 = unsigned integer 8; option PXE.mtftp-delay code 5 =
unsigned integer 8; option arch code 93 = unsigned integer 16; #
RFC4578

and next lines to your subnet section:

15

class "pxeclients" { match if substring (option vendor-class-identifier, 0, 9) =
"PXEClient"; next-server ip_address; # enter the BCWipe Total WipeOut server IP
address

if option arch = 00:06 { filename "not
supported"; } else if option arch = 00:07 {
filename "grub/x86_64-efi/core.efi";
} else {
filename "pxelinux.0";
}
}

See also:

[Booting BCWipe Total WipeOut](#)

Starting and Stopping the Server

Starting the Server

The BCWipe Total WipeOut Enterprise Setup program configures the server for automatic startup after reboot.

To start the server manually, run the **Jetico Server Monitor** and click Start Server.

After a successful server start, click the **Start Console in a Web Browser** link to open the server console's login page.

Stopping the Server

Run the **Jetico Server Monitor** and click Stop Server to stop the server.

Login Page

BCWipe Total WipeOut Enterprise displays its user interface in a web browser.

User sessions can be connected locally or remotely from desktops or mobile devices.

URL for local connections: https://localhost:8443/

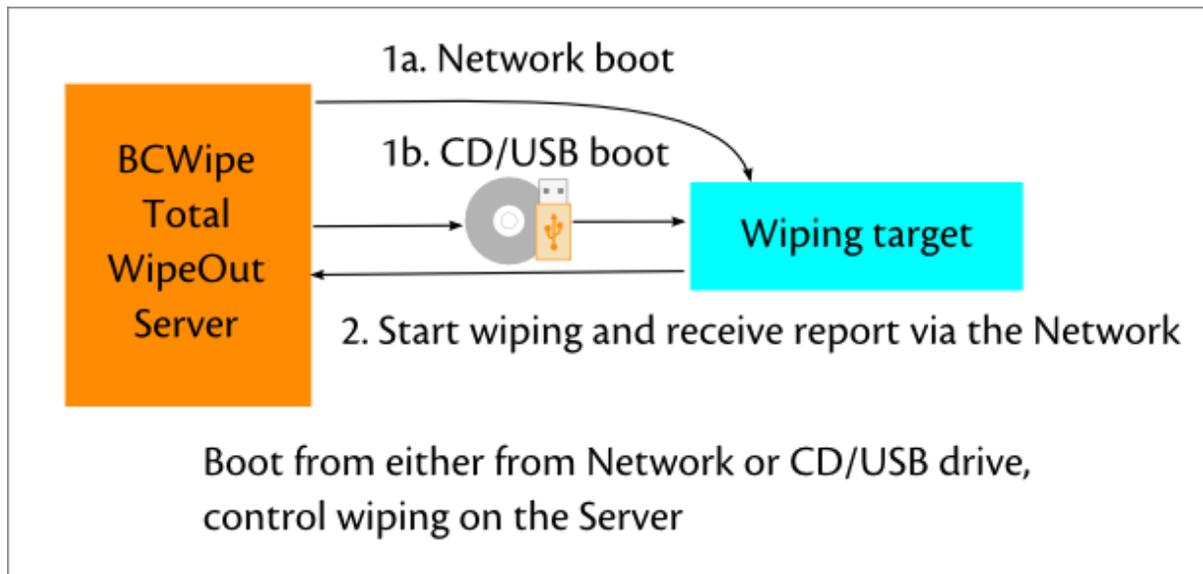**URL for remote connections**: https://<address of server with BCWipe Total WipeOut>:8443/

Attention! The BCWipe Total WipeOut Enterprise installer creates an administrator account with the default username **admin** and default password **admin**. Please change the admin account password after your first login.

Wiping Overview

BCWipe Total WipeOut Enterprise can wipe drives in either **Online Mode** or **Offline Mode**.

Online Mode

1a. Network boot

1b. CD/USB boot

Wiping target

2. Start wiping and receive report via the Network

Boot from either from Network or CD/USB drive,
control wiping on the Server

1. [Boot the wiping target](#) with BCWipe Total WipeOut either over the network (1a) or from a CD or USB drive (1b).

   ♦ As soon as BCWipe Total WipeOut starts on a hardware asset, it registers in the server.

   ♦ An operator selects assets from the inventory and starts wiping with the predefined wiping policy.

   ♦ In Online Mode, BCWipe Total WipeOut wiping software is controlled from the server; no local control is allowed.

2. Upon wiping completion, BCWipe Total WipeOut can generate and send a wiping report to the server via the network.

Offline Mode
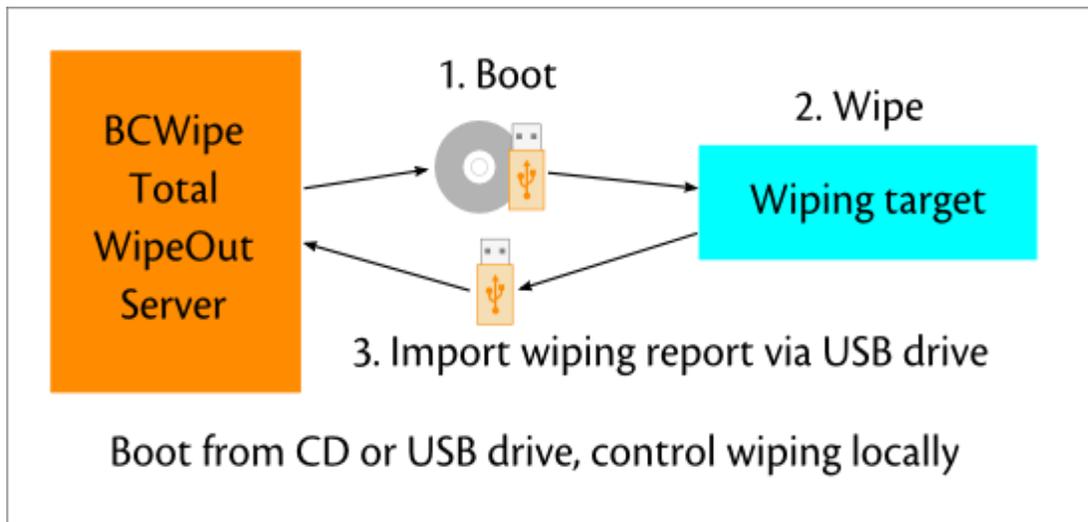
1. Using a bootable CD or USB drive containing your preferred wiping policy (see Making a Bootable USB Drive), boot the target system. If booting from a CD, insert a USB flash drive as well to store wiping reports.
2. Select and wipe drives on the target system.
3. Import the wiping report from the USB drive to the database via the BCWipe Total WipeOut server (see Upload Offline Wipe Logs). A report can be generated after importing the data.

See also:

Boot the wiping target

Making a Bootable USB Drive

Upload Offline Wipe Logs

BCWipe Total WipeOut Console User Interface

The BCWipe Total WipeOut Console contains three main parts:

- The **Groups** area on the left of the screen lists groups of hardware assets.
- The **Settings** area across the top of the screen is a series of shortcuts to server configuration functions.
- The **Work** area in the center of the screen is where the main operations -- wiping and getting reports -- are carried out.
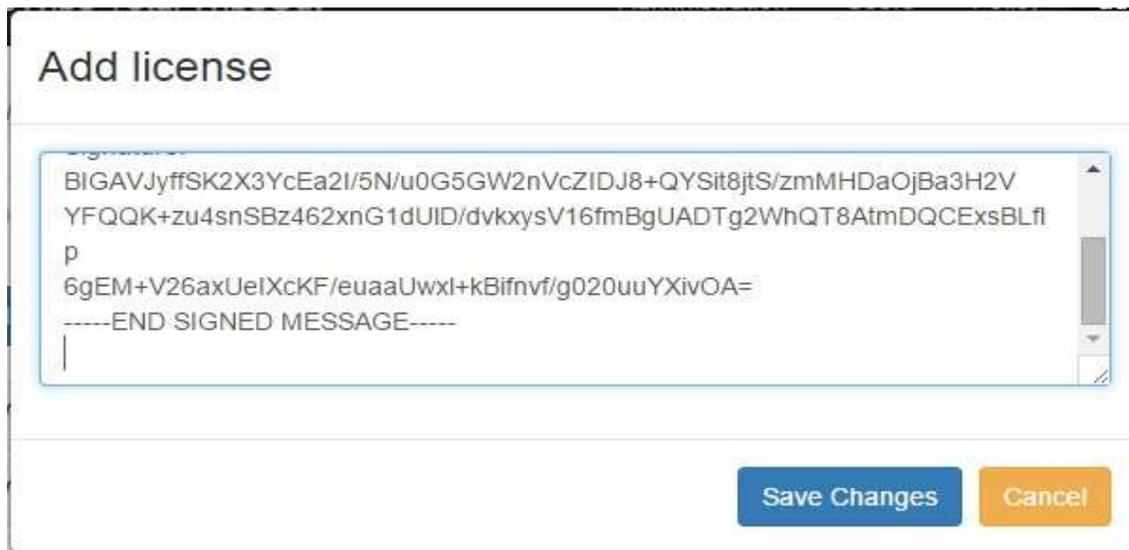
Licenses

The **Licenses** tab contains a list of your product licenses.

This list shows the current status of each license. To view/hide the details, click on the license header.

BCWipe Total WipeOut / Administration

$ Licenses ❷   🔧 Server settings ❷

Add license

BCWipe Total WipeOut is allowed to wipe 0 of 5 units   ❯

BCWipe Total WipeOut is allowed to wipe 12 of 16 units   ❯

BCWipe Total WipeOut is allowed to wipe 5 of 5 units   ❮

The license is valid for evaluation purposes only

Expired at 13 May 2015 Order full license

Adding a License

To add a license, click the Add License button. Copy and paste the license text to the "Add License" window, and then click Save Changes.

Add license

BIGAVJyffSK2X3YcEa2I/5N/u0G5GW2nVcZIDJ8+QYSit8jtS/zmMHDaOjBa3H2V
YFQQK+zu4snSBz462xnG1dUID/dvkxysV16fmBgUADTg2WhQT8AtmDQCExsBLfl
p
6gEM+V26axUeIXcKF/euaaUwxI+kBifnvf/g020uuYXivOA=
-----END SIGNED MESSAGE-----

Save Changes   Cancel

Please make sure you copy the license text in its entirety, including headers:

-----BEGIN/END SIGNED MESSAGE-----,

-----BEGIN/END ARMORED MESSAGE-----,

-----BEGIN/END PUBLIC KEY-----,

 -----BEGIN/END LICENSE-----

Server Settings

The **Server Settings** tab controls the TFTP server and the server address for wiping agents' connections.

BCWipe Total WipeOut / Administration

$ Licenses ❓   🔧 Server settings ❓

TFTP Server **Online** [Stop]

Server Host

192.168.1.5

Policy Management

BCWipe Total WipeOut allows users to preconfigure several wiping policies for different needs.
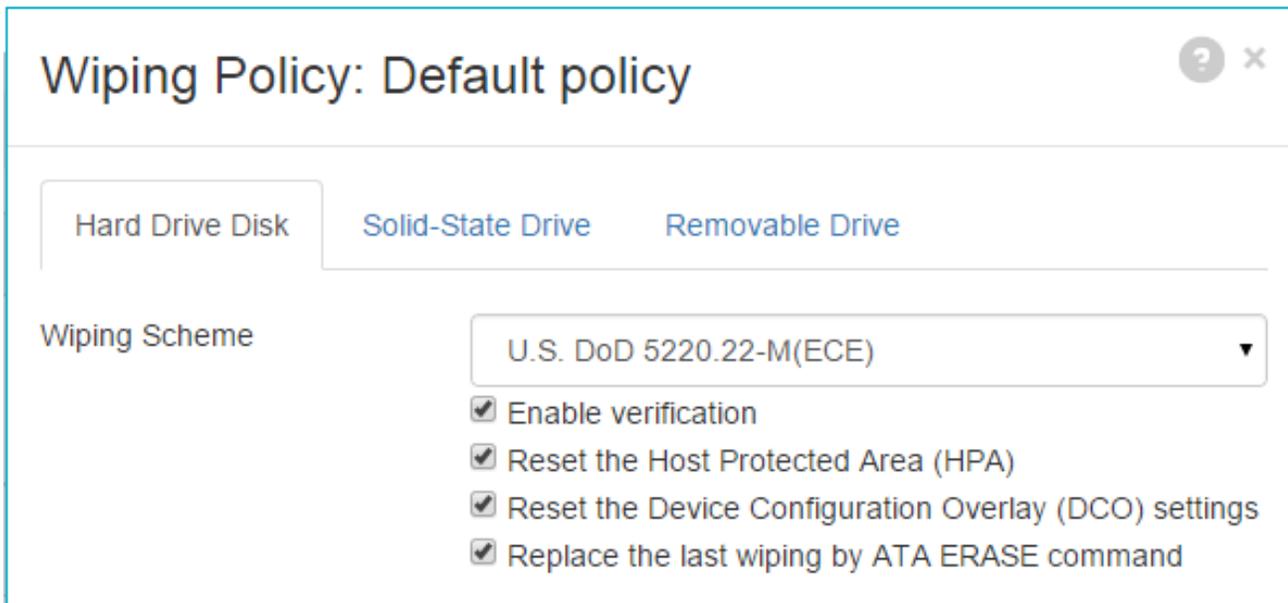
Click Add Policy to create a new policy.

Wiping Policy Settings

The term **Wiping Policy** refers to a set of rules for wiping different types of drives:

- Hard drive disks (HDDs)
- Solid-state drives (SSDs, NVMe)
- Removable drives (USB)

Drive type is detected by Wiping Agents. The result depends on both drive type and controller connection.

For example, a SATA SSD drive connected via eSATA will be detected as a solid-state drive. The same drive connected via USB mobile rack will be detected as a removable drive.

Wiping Policy: Default policy

Hard Drive Disk	Solid-State Drive	Removable Drive

Wiping Scheme

U.S. DoD 5220.22-M(ECE) ▼

☑ Enable verification
☑ Reset the Host Protected Area (HPA)
☑ Reset the Device Configuration Overlay (DCO) settings
☑ Replace the last wiping by ATA ERASE command

The Wiping Policy area allows you to control the following settings:

Wiping Scheme. You may choose one of the following:

- ❖ U.S. DoD 5220.22-M(ECE)
- ❖ U.S. DoD 5220.22-M(E)
- ❖ U.S. DoE M 205.1-2
- ❖ U.S. Army AR380-19
- ❖ NAVSO P-5239-26 (MFM)
- ❖ NAVSO P-5239-26 (RLL)
- ❖ Canadian RCMP TSSIT OPS-II
- ❖ British HMG IS5 Baseline
- ❖ British HMG IS5 Enhanced
- ❖ German BCI/VSITR
- ❖ Russian GOST R 50739-95
- ❖ Bruce Schneier's 7-pass wiping scheme
- ❖ Peter Gutmann's 35-pass wiping scheme
- ❖ 1-pass random
- ❖ 1-pass zero

To add a user-defined wiping scheme, the user should add a new .sch file to the subfolder *\media.src\cfg\tmp\scheme* of the program folder. The file should contain the scheme name, and all wiping passes listed one by one in a new string (refer to other .sch files for example).

* ❖ **Enable Verification.** BCWipe Total WipeOut will read each sector after wiping to verify that the wiping pattern has been written properly. To comply with the DoD 5220.22-M standard, "Enable verification" must be enabled.
* ❖ **Reset the Host Protected Area (HPA)** (ATA/SATA drives only). The HPA feature can be used to hide a range of drive sectors from operating system and programs. "Reset HPA" resets the number of HPA protected sectors to zero, revealing full drive capacity. BCWipe TWO restores HPA after the wiping process is finished.
* ❖ **Reset the Device Configuration Overlay (DCO)** (ATA/SATA drives only). The DCO feature can be used to hide a range of drive sectors from operating system and programs. "Reset DCO" resets DCO settings, revealing full drive capacity.
* ❖ **Replace the last wiping pass with ATA ERASE command** (ATA/SATA drives only). The ATA SECURE ERASE command overwrites whole drive including protected, reserved and reallocated sectors.

ATA disk freeze lock: ATA commands are usually locked by computer's BIOS. BCWipe TWO removes the freeze lock automatically. To do that, it sends the computer to suspend mode, or reboots it.

User Management

The Users page displays the complete list of BCWipe Total WipeOut user accounts and allows authorized persons to manage them.

User Management Functions

- **Add User**: creates a new user
- **Enabled**: when checked, the user can log in and use BCWipe Total WipeOut. When unchecked, the user is not allowed to log in.
- **Edit Permissions**: change the user's permissions
- **Change Password**: change the user's password

User Permissions

- Users with an **Administrator** role have full access to all server functions, including user and license management.
- Users with an **Auditor** role can view wiping results and generate reports.
- Users with an **Operator** role can configure wiping policies, manage assets and perform wiping tasks.

Groups

The Groups Area displays assets arranged into groups. Groups have hierarchical structure; subgroups within groups are allowed. Click the +/- icons to expand/collapse group structures.

The contents of the selected group will be displayed in the Work Area.

On small or low-resolution displays, the Groups Area can be hidden. Click the button to toggle the Groups Area.
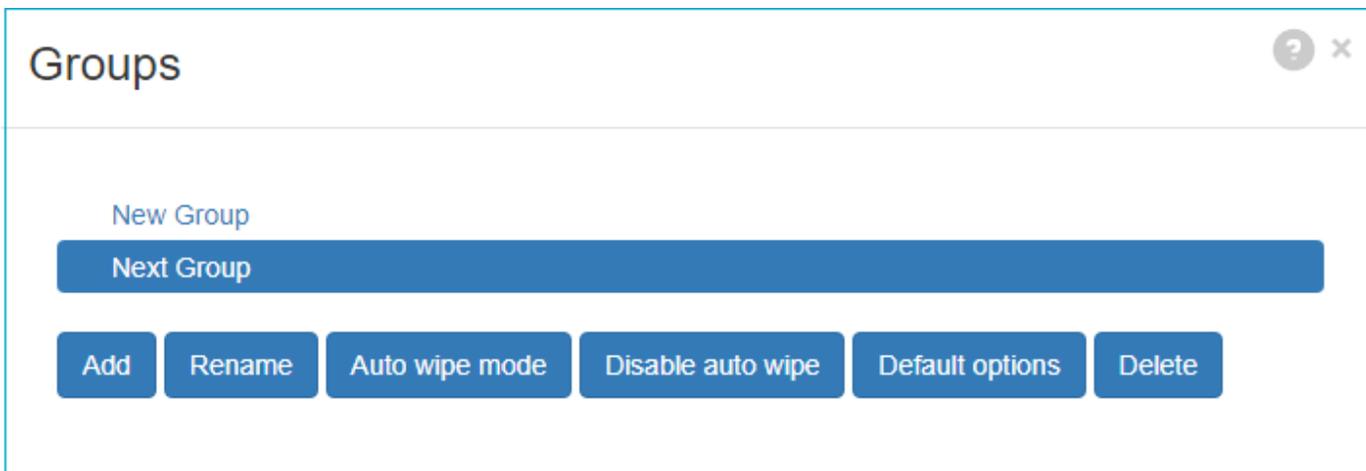
Default Group

BCWipe Total WipeOut creates a special **default group** automatically during installation. The default group is always displayed on top of the groups list.

New assets registered in BCWipe Total WipeOut are added to the default group automatically.

Editing Groups

To modify the groups structure, click the pencil icon to the right of the "Groups" header:

The following commands are availble for selected group:

- **Add** - create a subgroup.
- **Rename** - edit the group name.
- **Auto wipe mode** - set automatic wiping option.
- **Disable auto wipe** turn automatic wiping off.
- **Default options** - set default wiping policy and default options for reports.

- **Delete**. If a non-empty group is deleted, its contents -- both assets and subgroups -- are moved to the default group. The default group cannot be deleted.

Auto Wipe

A group can be set to work in **Auto Wipe Mode**. In this mode wiping with predefined policy is started as soon a computer appears in this group. If Auto Wipe Mode is set for Default Group, wiping will start automatically on all newly added assets.

Auto Wipe Mode affects target asset boot time only. If you simply move an asset to Auto Wipe enabled group, wiping won't start immediately. To start wiping you have to reboot the asset.
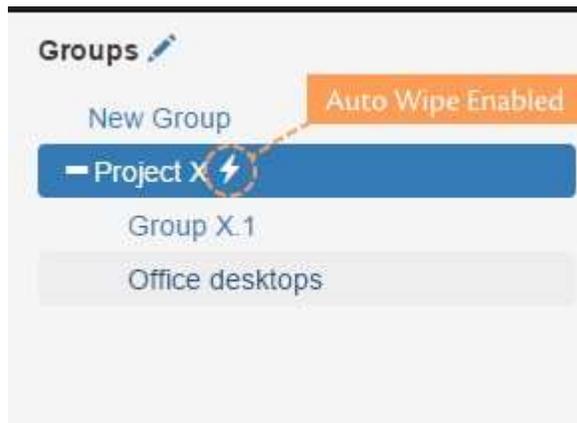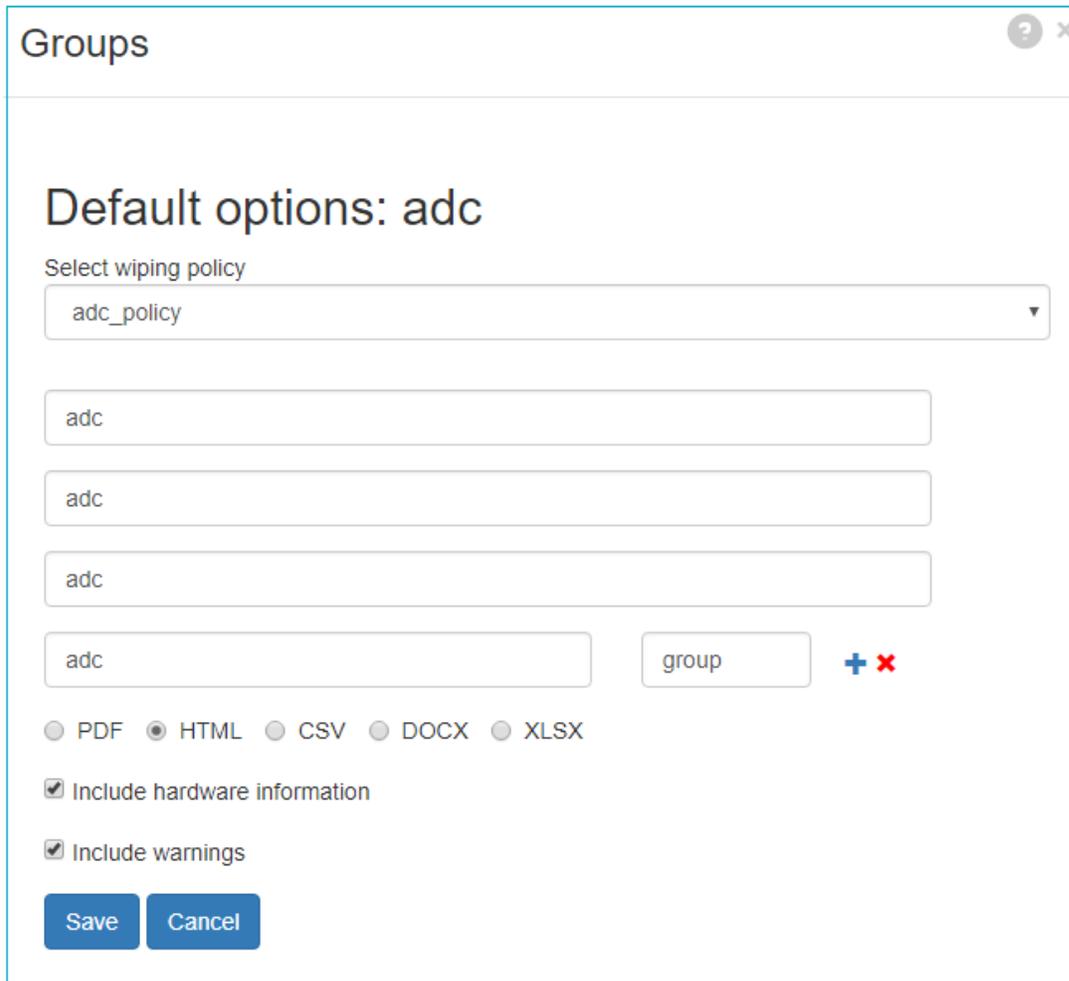

After clicking Auto wipe mode you will be asked to assign a wiping
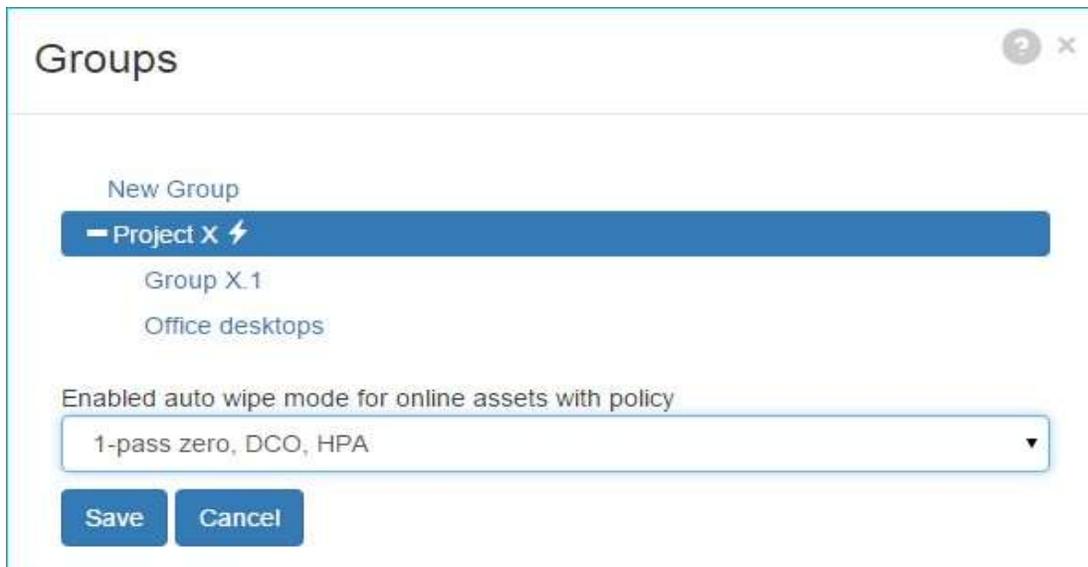
policy:

Default options for a group.

After clicking Default options on the **Edit Groups** dialog, you will be asked to assign a wiping policy and options for reports:

After that, these options will be set automatically for any asset or disk, that belongs to this group, when you click **Start wiping** or **Get report**, so the user does not have to set the options again and again while working with multiple groups.

See also:

Policy Management

Get Report

Wiping Agents

BCWipe Total WipeOut uses so called **Wiping Agents**, a bootable package that boots on the target system itself, to carry out the wiping job on the target system.

BCWipe Total WipeOut supports both network boot and boot from removable (CD or USB) drives.

Refer to the platform compatibility table below for compatibility with different boot media.

	Network Boot	CD	USB Drive
x86-compatible BIOS	yes	yes	yes
x86 or x64 EFI	yes	yes	yes
Intel Mac systems	-	yes	yes
Intel Itanium (IA64)	-	yes	yes
SPARC64	-	yes	-

Click Wiping Agents button to open the window:
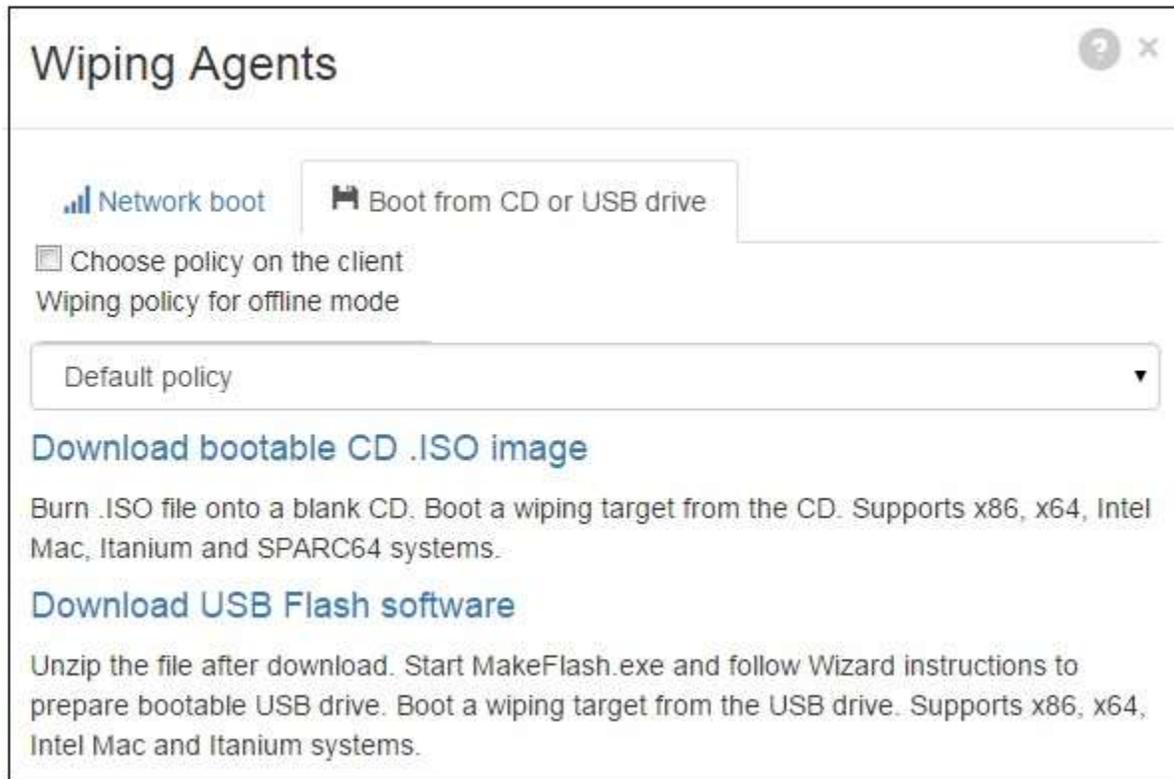
Network Boot

The **Network Boot** tab shows current Network Boot status and basic configuration tips.

See the Preparing Environment for Network Boot chapter for details.

Boot from CD or USB Drive

The **Boot from CD or USB Drive** tab allows you to prepare boot media that enables system wiping either with or without network connection to BCWipe Total WipeOut server.

To prepare boot media:

1. Select a *Wiping Policy*. If there will be no connection to the BCWipe Total WipeOut server, wiping will occur in **Offline Mode**. Mark the checkbox *Choose policy on the client* to create the media with all existing wiping policies embedded.

2. Click *Download bootable CD .ISO image* to download the .ISO image.

3. Burn the .ISO image to a blank CD or DVD.

4. If you are using a Windows system, you may also click *Download USB Flash software*, download and unzip the archive, and follow the wizard instructions that appear when you run *MakeFlash.exe*.

See also:

Booting BCWipe Total WipeOut

Preparing Environment for Network Boot

Assets

When BCWipe Total WipeOut console starts for the first time, no assets appear in the database.

To begin, click the Wiping Agents button to deliver and start Wiping Agent on the target system.

As soon as Wiping Agents starts and connects to the server, an asset will appear with a status of *Online*.

At this point, you can select an asset and perform the following operations:

- Start Wiping for an entire asset.
- Move an asset to another group.
- Get a report for the entire asset.

To view or edit asset details, click the asset name link.

Asset Details

The **Asset Details** view displays detailed information about asset disks, including wiping status. You may select and start wiping or get a report for individual disks.

The Asset Details view also allows you to edit the asset name by clicking the pencil icon.

Start Wiping

When you select assets or individual disks for wiping and click **Start Wiping**, a confirmation dialog appears.

1. Select your desired wiping policy from the drop-down menu.
2. Press **Start Wiping** to confirm or **Cancel** to cancel the operation.
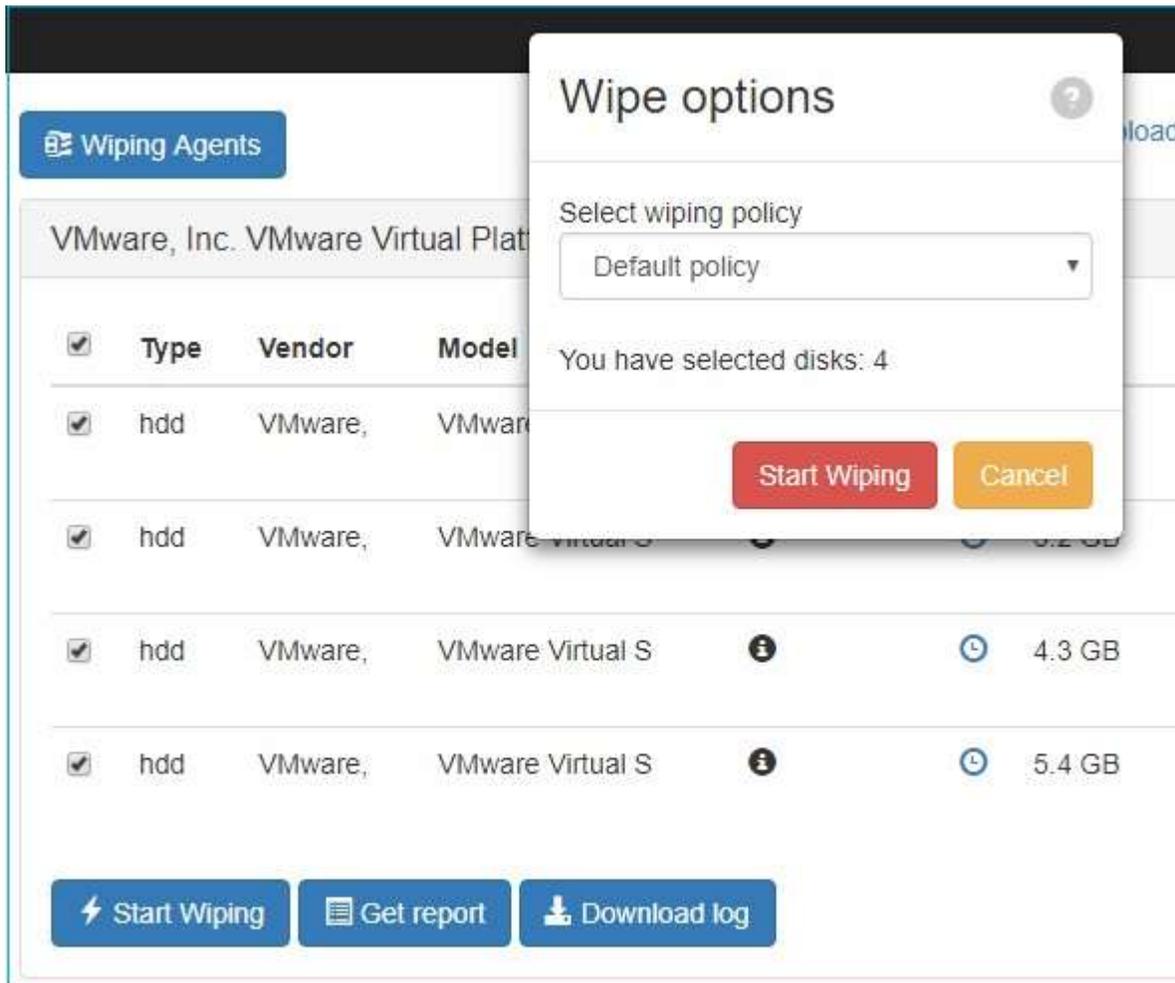
Get Report

When you click **Get Report** either in Assets or in Wipe History, the **Report options** dialog appears.

When prompted, please fill in the following fields:

- ➢ **Organization**: This will be added to report header.
- ➢ **Conducted By**: The wiping operator's name.
- ➢ **Validated By**: The controlling person's name.

Click ✚✖ buttons to add/remove custom fields. Fill in the *Field name* and *Field value*. The custom fields will be added just after 'Organization' name.

Select the desired report format: PFD, HTML, CSV, DOCX, XLSX, and set the option to show/hide hardware information and warnings.

For CSV and XLSX formats, it is possible to select columns that should be presented in the report. The file is generated with separator **';'**.

When all the settings are assigned, click Get report

NOTE: Report is downloaded automatically. Please adjust your browser's popup-blocker settings to allow the download.

Upload Offline Wipe Logs

When Wiping Agents does not have a network connection to the BCWipe Total WipeOut server, it operates in **Offline Mode**.

In Offline Mode, BCWipe Total WipeOut:

- Looks for a writable USB drive and prompts the user if it is missing.
- Allows an operator to select drives and start wiping locally.
- Writes the wiping log to a file named *offline_report_ID.json* in a removable USB drive.

To upload a log file created in Offline Mode:

1. Click **Upload Offline Wipe Logs**.
2. Drag and drop the file named *offline_report_ID.json* to the area prompted.

Alternatively, you can click the prompt area to invoke an Open File browsing dialog and select the offline log file there.

If an asset wiped in Offline Mode was not registered on the BCWipe Total WipeOut server, it is added to the Default Group.

View Wipe History

The **View Wipe History** function provides access to the history of wiping operations.

The wipe history can be filtered by the following fields:

- Date
- Asset type
- Disk
- Wiping status

The **Get Report** button creates a report for all disks satisfying the current filter settings.

View Wipe History

| From date | | To date | | Disk UUID | | e0b15b62-901 | Status |

Type	Disk Serial	Size	Asset	Status	Date	Operator
hdd	6QE00XD1	200 GB	IEV asset	Canceled	21.01.2019 18:03:21	admin
hdd	6QE00XD1	200 GB	IEV asset	Completed	21.01.2019 17:49:57	admin
ssd	S2GLNCAGC18585Z	256.1 GB	IEV asset	Completed	21.01.2019 15:05:18	admin
ssd	S2GLNCAGC18585Z	256.1 GB	IEV asset	Completed	21.01.2019 15:00:02	admin
hdd	5MS0E7NQ	120 GB	IEV asset	Completed	21.01.2019 13:37:53	admin

Get report   **Download log**

First   Previous   **1**   2   3   4   5   Next   Last

Booting BCWipe Total WipeOut

Booting from Network (PXE)

BCWipe Total WipeOut Enterprise supports booting from network for x86-compatible BIOSbased and EFI systems.

x86 and x64 systems -- BIOS and EFI

1. Prepare your environment for booting from network.
2. Turn off the system.
3. Power on the system and invoke your BIOS/EFI configuration.
4. Enable network (PXE) boot and move it to the top of the boot order.
5. Save new BIOS settings.
6. Reboot.

Booting from a CD or USB drive

CD and USB drives created in BCWipe Total WipeOut Enterprise support several computer architectures regardless of operating system installed.

x86 and x64 systems -- BIOS

1. Turn off the system.
2. Power on the system and invoke your BIOS configuration.
3. Move BCWipe Total WipeOut boot media to the top of the boot priority list.
4. Save new BIOS settings.
5. Reboot.

x86 and x64 systems -- EFI

1. Turn off the system.
2. Power on the system and invoke your EFI configuration.
3. Move BCWipe Total WipeOut boot media to the top of the boot priority list.
4. Save new EFI boot settings.
5. Reboot.

Apple Intel-based Mac systems

1. Turn off the system.
2. Insert BCWipe Total WipeOut boot media, either CD or USB.

3. Power on and hold the **alt** key.

4. Select the item called "EFI boot" and press **Enter**.

Itanium systems

1. Turn off the system.

2. Power on the system.

3. Insert BCWipe Total WipeOut boot media, either CD or USB.

4. If your EFI Boot Manager menu already has an appropriate entry, select it and press **Enter**.

5. If not, enter the "Boot Option Maintenace Menu" and create an entry for the BCWipe Total WipeOut boot media.

6. Save the new boot menu entry and select it for booting.

SPARC systems

BCWipe Total WipeOut can create a bootable CD for SPARC. Bootable USB sticks are not supported for SPARC systems.

1. Turn off the system.

2. Power on the system.

3. Insert BCWipe Total WipeOut into the CD drive.

4. Enter `boot cdrom` in the OpenBoot Prompt if your system is not configured to boot the CD automatically.

5. Press **Enter** after the "boot" prompt.

See also:

BCWipe Total WipeOut Specifications

Preparing Environment for Network Boot

Wiping Agents User Interface

Online Mode

In **Online Mode**, Wiping Agents will instruct you to log into the web interface to carry out the wiping procedure.

Although the wiping process is started and managed from remote web console, some commands are still available on the local computer:

- **Tab** - switch between disk details and log areas.
- **iSCSI** - scan network to search for iSCSI devices.
- **R** - (rescan) force program to re-read information about available disks.
- **Space** - run hexadecimal disk viewer.

The menu string also shows the IP address of the server machine.

Offline Mode

The keys that are added to the menu, compared with online mode:

- **S**: Select disk
- **W**: start Wiping on selected disks
- **C**: Cancel the process

```
TWO3 v.4.0.0   (build 8598d9118d1 Thu Jan 31 14:54:08 2019      www.jetico.com
 1 ---- 2.1 GB    VMware Virtual S
 2 LOG  8.0 GB    Flash Disk

─ Disk details ─────────────────────────────────────────────────────────────
Dev name: sda
Capacity: 2.1 GB, 2147483648 Bytes, 4194304 sectors
   Model: VMware, VMware Virtual S
  Serial:
            ──────────── Welcome to BCWipe Total WipeOut! ────────────
           │                                                          │
           │  BCWipe Total WipeOut enterprise is in 'offline' mode    │
           │                                                          │
           │  In this mode wiping is run locally                      │
           │                                                          │
           │  Please bring this USB device with offline_report*.json  │
           │  files and upload them via web interface afterwards      │
           │                                                          │
           │  You may wipe several system and upload bunch of reports │
           │                                                          │
           └─ Enter─OK ───────────────────────────────────────────────




   ?─Help Tab─details/log [i]SCSI menu [S]elect [W]ipe [C]ancel [R]escan Space─view data
```

See also:

[Wiping Overview](#)

Making a Bootable USB Drive

Please note: The BCWipe Total WipeOut bootable USB drive-making package works on Windows systems only.

1. Log in to BCWipe Total WipeOut console

2. Open the Wiping Agents dialog and select the **Boot from CD or USB Drive** tab.

3. Click the **Download USB Flash software** link and save *bcwipeflash.zip* on the disk.

4. Unzip *bcwipeflash.zip*. Start **MakeFlash.exe**.
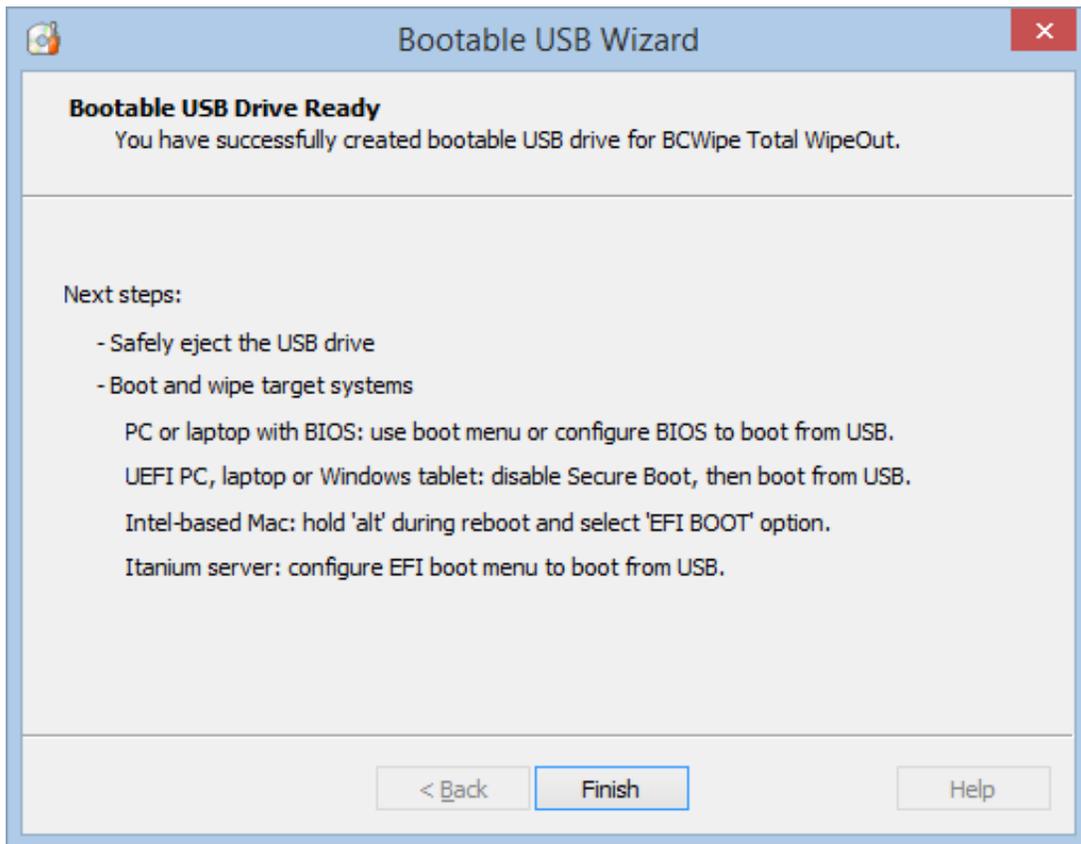
5. Read the welcome message, then click Next.

6. Select USB drive from the list. Click the Format button to format the disk with FAT or FAT32 if required. Then, click Next.

7. The wizard will copy the boot files to USB drive. Click Next when complete.
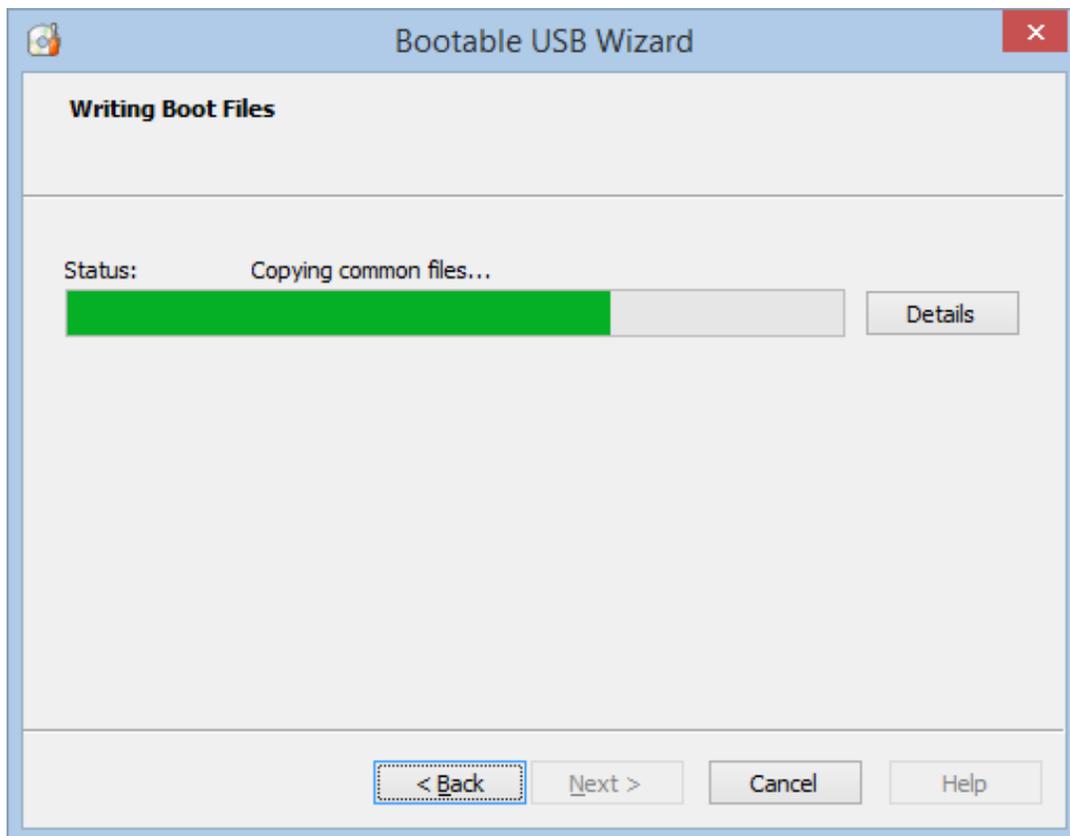
8. Review the booting instructions. Safely eject the USB drive. Click Finish.

See also:

Upload Offline Wipe Logs

Configuration Files

BCWipe Total WipeOut Enterprise can be safely used with the default settings initially created by the setup program.

Configurable BCWipe Total WipeOut Enterprise parameters are stored in the **application.properties** and **log4j.properties** text files located in the installation folder.

To edit the configuration files:

- Administrator privileges are required.
- The BCWipe Total WipeOut server must be stopped first.

Attention! It is strongly recommended that you back up all configuration files prior to making any changes.

General Server Settings

```
 jcm.locale: en
server.address: 0.0.0.0
tftp.port: 69
 server.ssl.key-store: key.jks
server.ssl.key-store-password: secret
server.ssl.key-password: password



# Dont change properties below, please
spring.thymeleaf.cache: true
security.basic.enabled: false server.port:
8443
spring.thymeleaf.mode: LEGACYHTML5 spring.jpa.hibernate.ddl-auto:
none logging.config=file:./log4j.properties
```

Database Settings

```
# H2 Embeded database
spring.datasource.url: jdbc:h2:./database spring.datasource.driver-class-name:
org.h2.Driver
liquibase.change-log: classpath:/db/db.changelog-h2-master.xml
```

```
# MySQL database
#spring.datasource.url=jdbc:mysql://localhost/test?autoReconnect=true&serv
erTimezone=GMT
#spring.datasource.username=root
#spring.datasource.password=root
#spring.datasource.driver-class-name=com.mysql.cj.jdbc.Driver
#liquibase.change-log: classpath:/db/db.changelog-mysql-master.xml

# PostgreSQL database
#spring.datasource.url=jdbc:postgresql://localhost/test
#spring.datasource.username=postgres
#spring.datasource.password=postgres
#spring.datasource.driver-class-name=org.postgresql.Driver
```

NOTE: To change database, comment the old database strings with # mark, and uncomment the new database strings. Remember that all the current settings and assets will be lost.