Jetico

BCWipe Total WipeOut

Enterprise Edition

User Manual

Introduction

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 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.
From the BCWipe Total WipeOut Enterprise user console, you can:

- Wipe directly from the console
- Switch between online and offline modes
- Run reports

Specifications

Supported Platforms (regardless of operation system installed)

- x86-compatible systems with BIOS or EFI
- x64-compatible systems with BIOS or EFI
- Itanium systems with EFI
- 64-bit SPARC systems with OpenBoot

Supported Drive Interfaces

- FireWire
- IDE
- SAS
- SATA
- SCSI
- USB

Supported Wiping Standards and Schemes

- 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

Supported Drive-Specific Commands

- Device Configuration Overlay (DCO) hidden sectors detection and reset.
- Host Protected Area (HPA) hidden sectors detection and reset.
- Firmware assisted wiping by ATA SECURITY ERASE command.

Installation

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

- For small offices and evaluation purposes, BCWipe Total WipeOut Enterprise can use an embedded Java database (default setting) with no additional actions required.
- For intensive operations and higher reliability, a separate database server is recommended:
  - MySQL 5.0 or newer. See Configuration for details.
  - PostgreSQL 9.0 or newer. See Configuration for details.

DHCP service

DHCP service is required for the following online wiping operations:

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

Installation

1. Start BCWipe_Total_WipeOut_Enterprise.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.

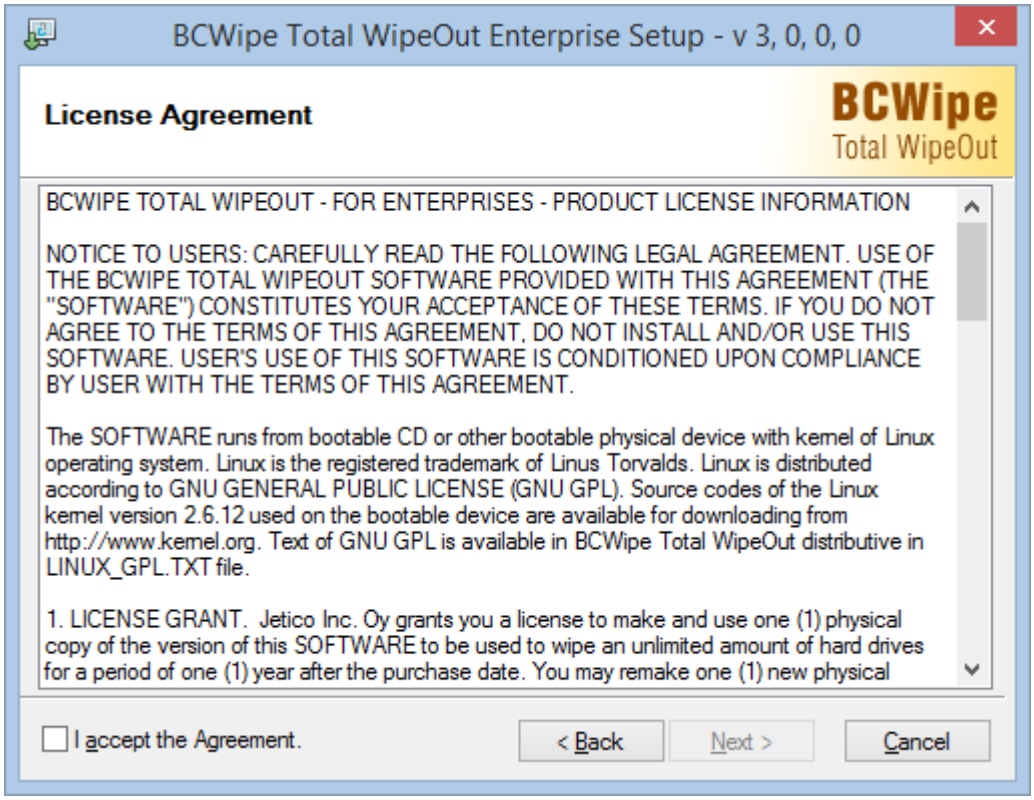
2. Follow the steps outlined in the setup dialog windows.

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.

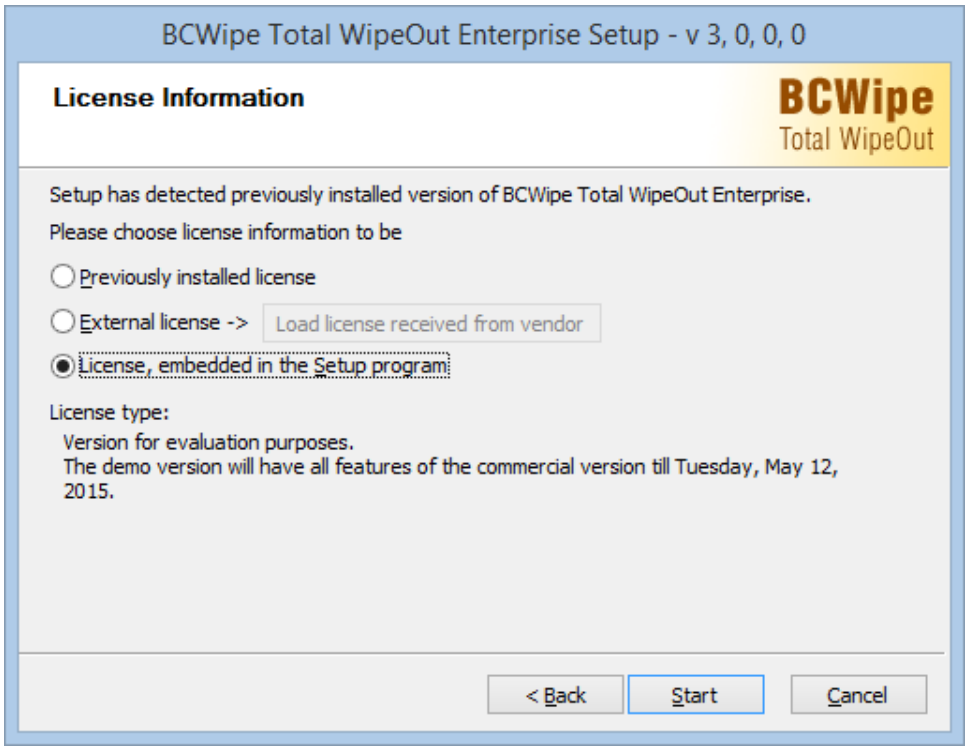
3. Read the License Agreement.

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



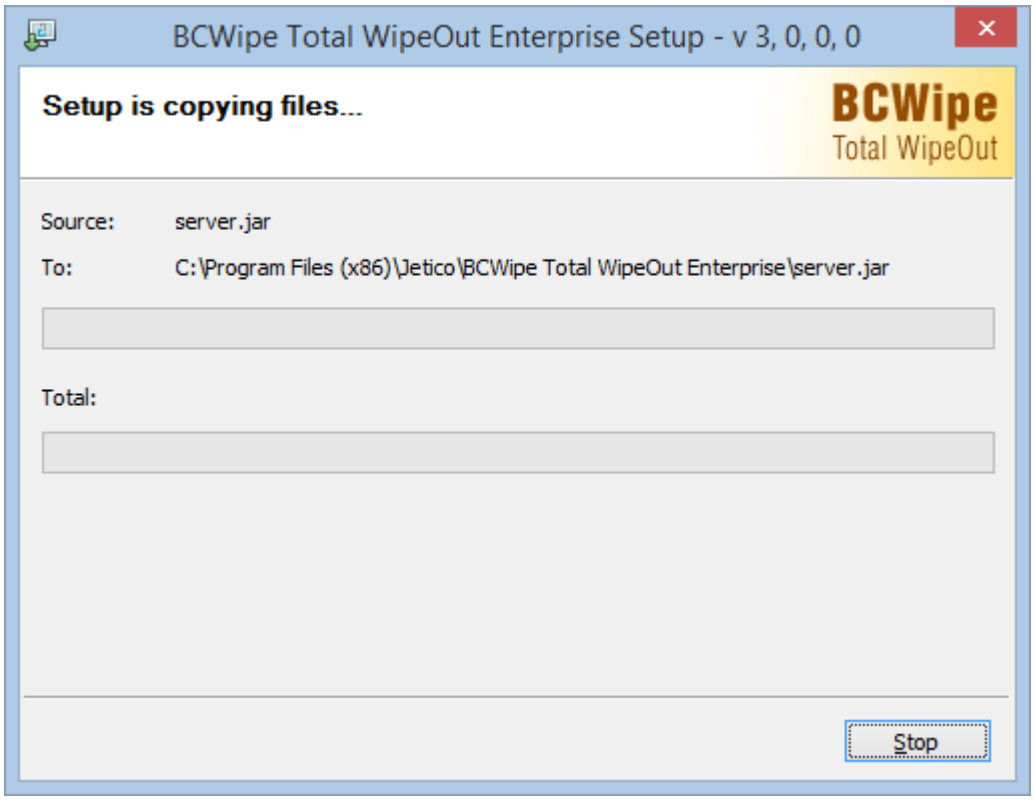
4. Select your license type.

- 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.

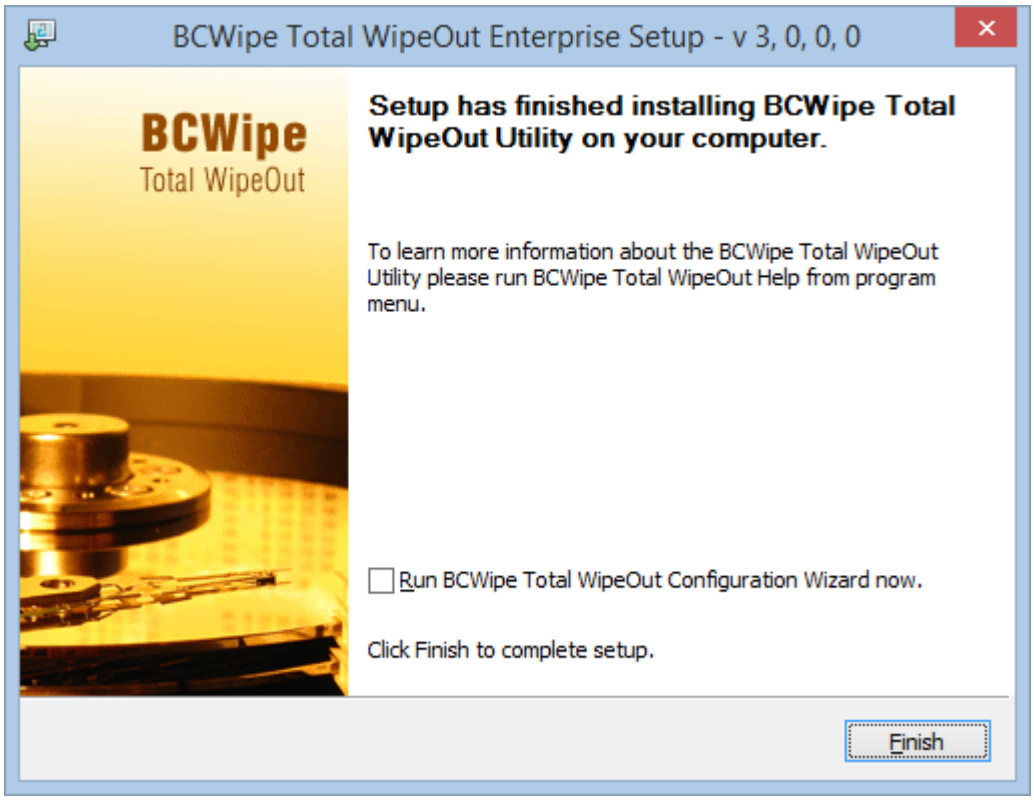


Click ***Start*** to continue installation.

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

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

See also:

Configuration Files
Server Settings
Preparing Environment for Network Boot

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-Server Options. If you want to enable network boot in a single scope, select IPv4-Scope-Scope Options instead.
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.

See also:

Booting BCWipe Total WipeOut

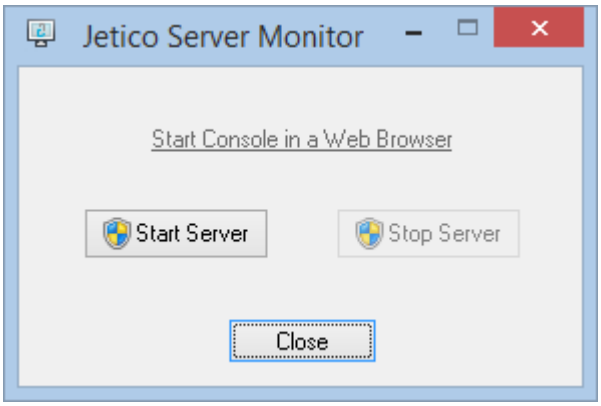
Getting Started

- Starting and Stopping the Server
- Login Page
- Wiping Overview

Starting and Stopping the Server

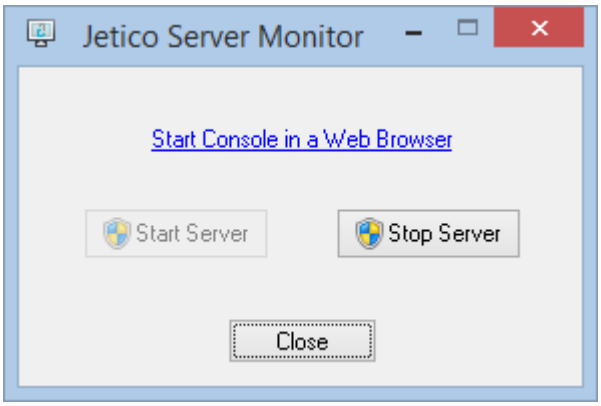
Starting the Server

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***.
Within 5 to 10 seconds 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.



See also:

Login Page
BCWipe Total WipeOut Console User Interface

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.

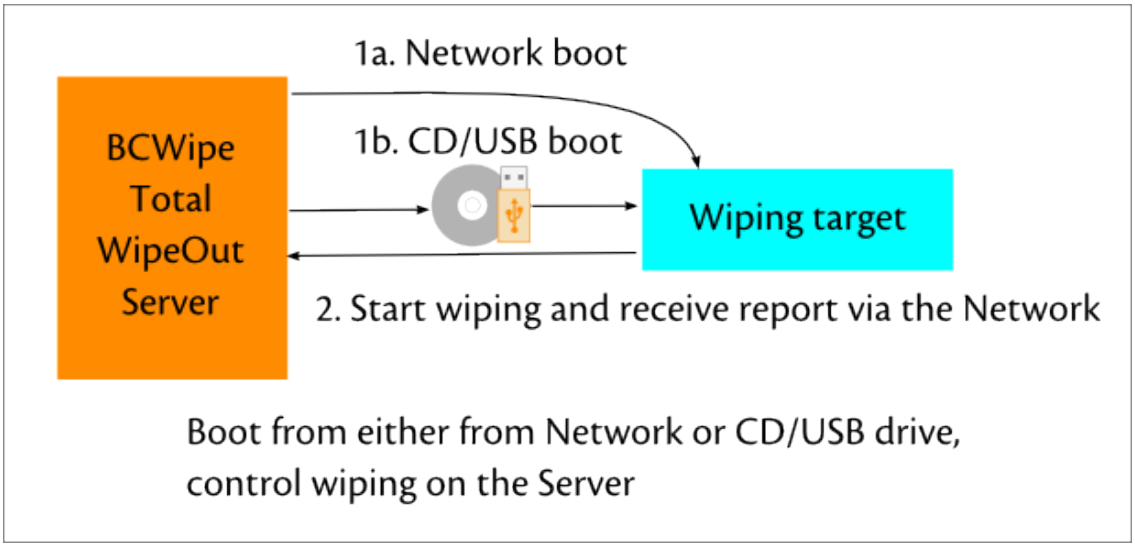
See also:

User Management

Wiping Overview

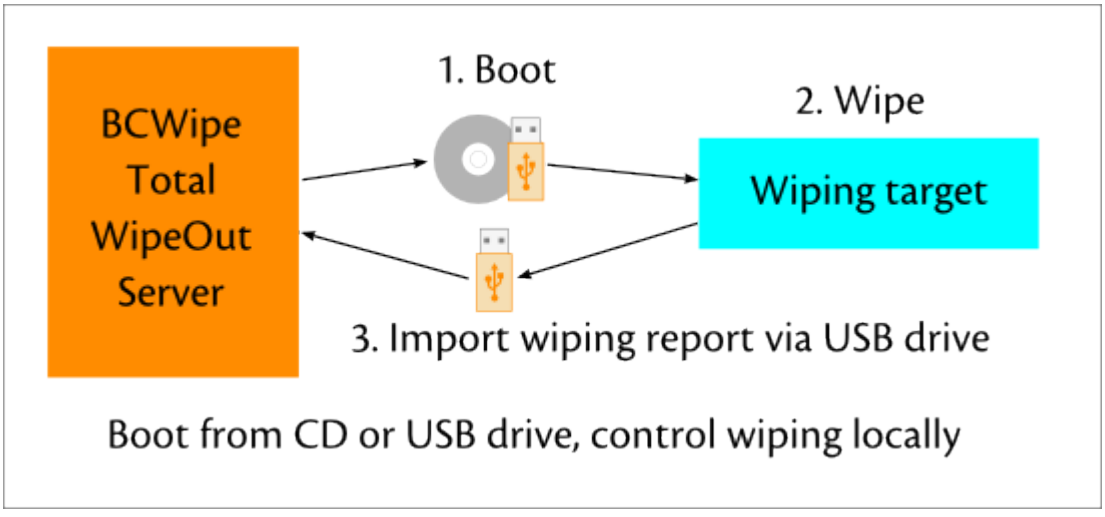
BCWipe Total WipeOut Enterprise can wipe drives in either Online Mode or Offline Mode.

Online Mode



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

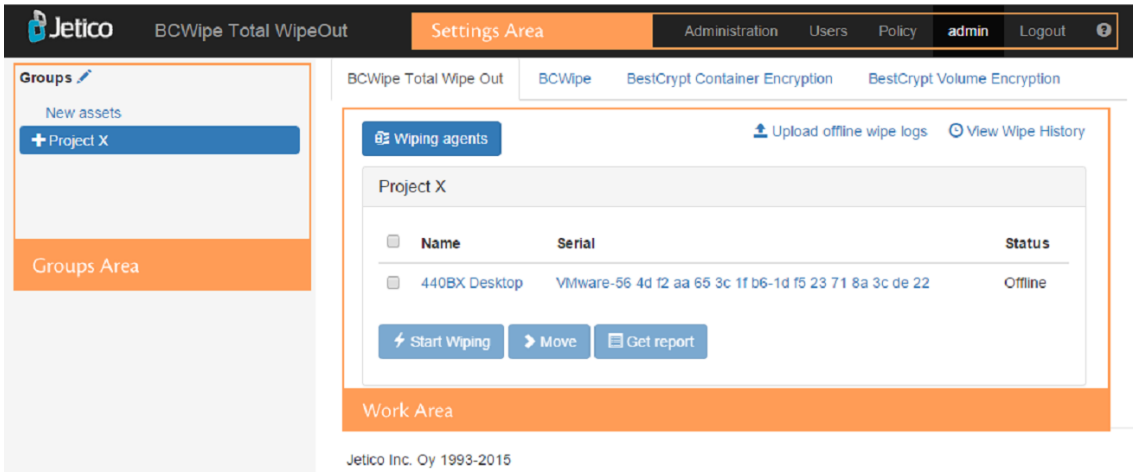


1. Using a bootable CD or USB drive containing your preferred wiping policy (see Making a Bootable USB Drive), boot the target system. If booting from a CD, insert a USB flash drive as well to store wiping reports.
2. Select and wipe drives on the target system.
3. Import the wiping report from the USB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

User Interface

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.



See also:

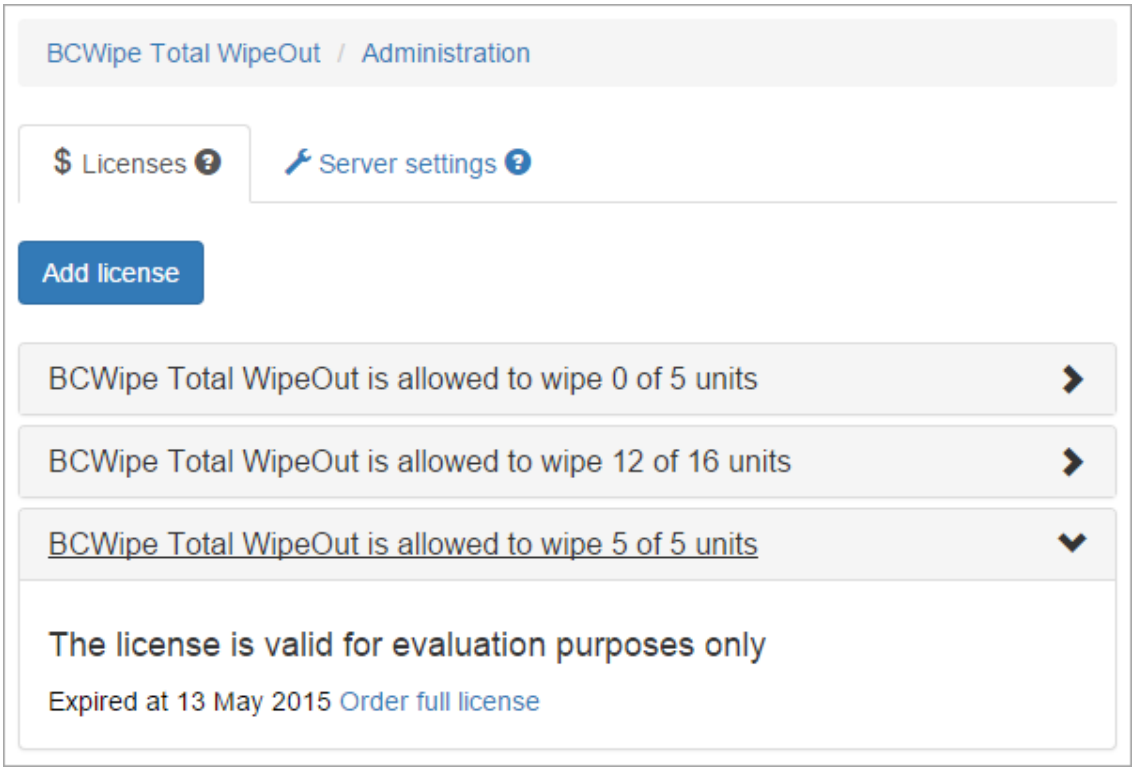
[Assets]
[Wiping Agents]
[Policy Management]
[Groups]

Administration

- Licenses
- Server Settings

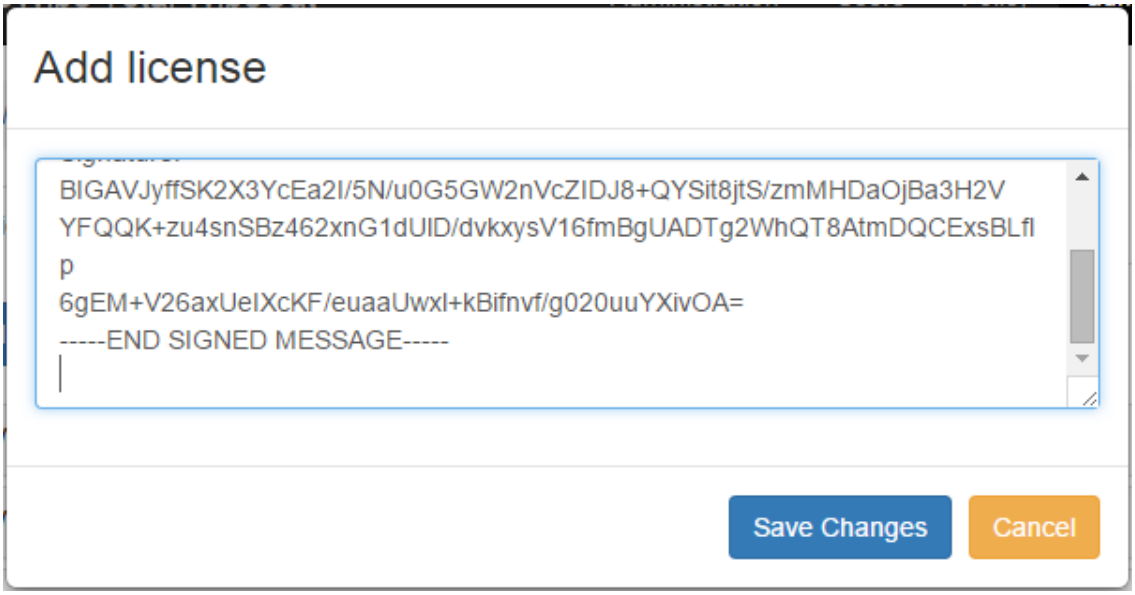
Licenses

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.



Adding a License

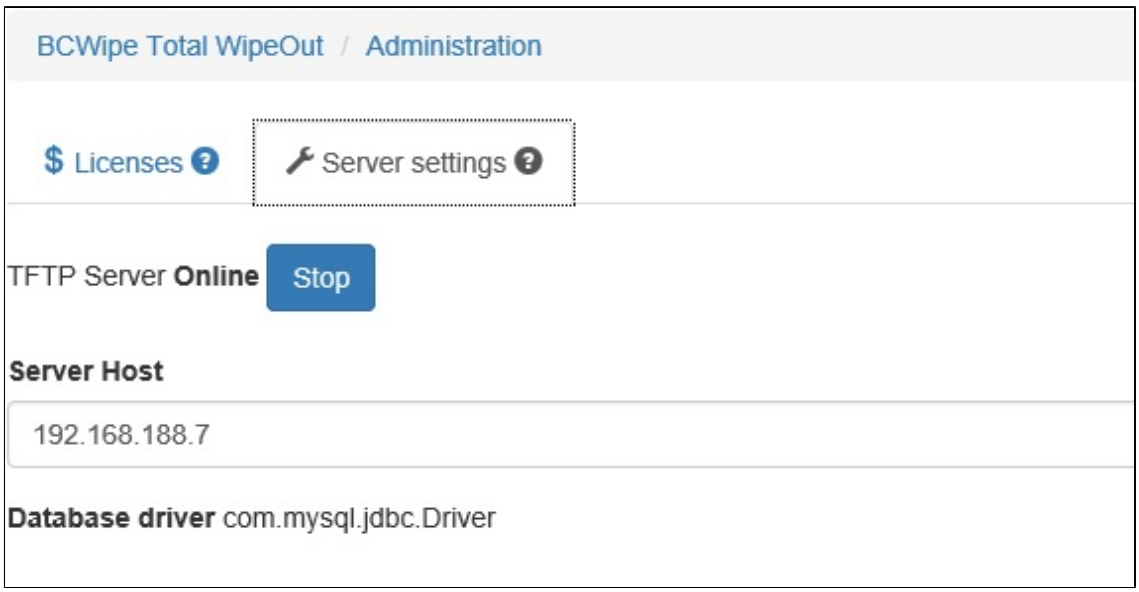
To add a license, click ***Add License***. Copy and paste the license text to the "Add License" window, and then click ***Save Changes***.



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.
Besides, it shows currently used Database.

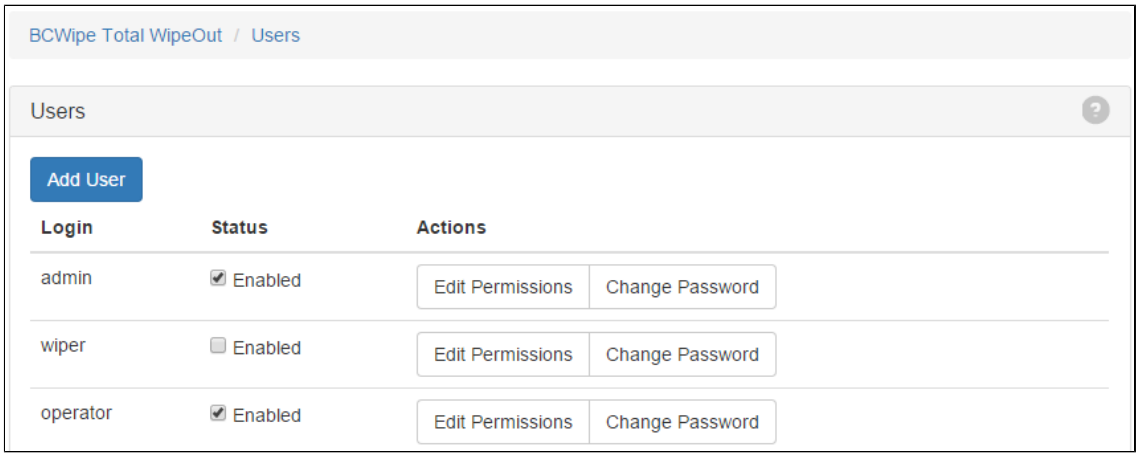


User Management

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

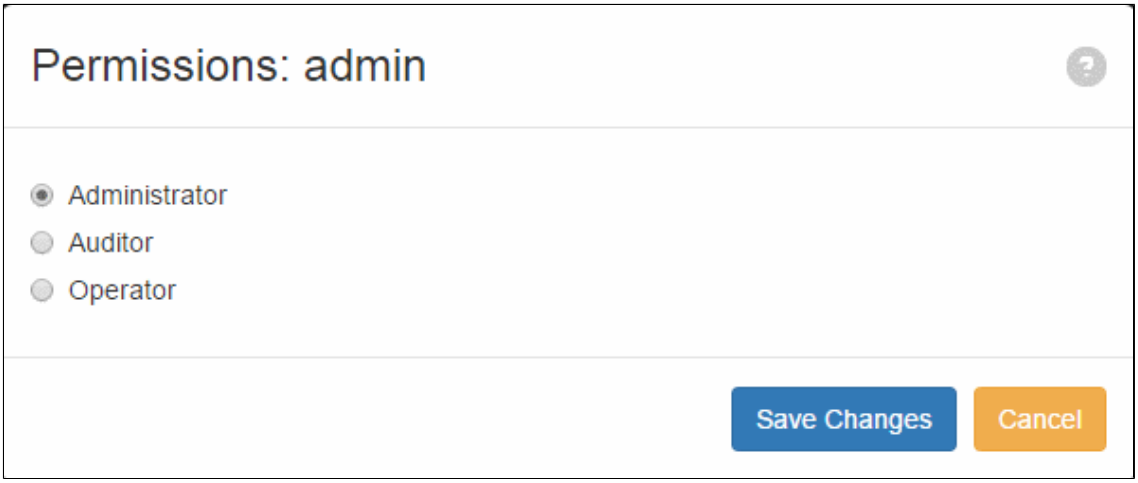
User Management Functions

- 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 manage assets and perform wiping tasks.

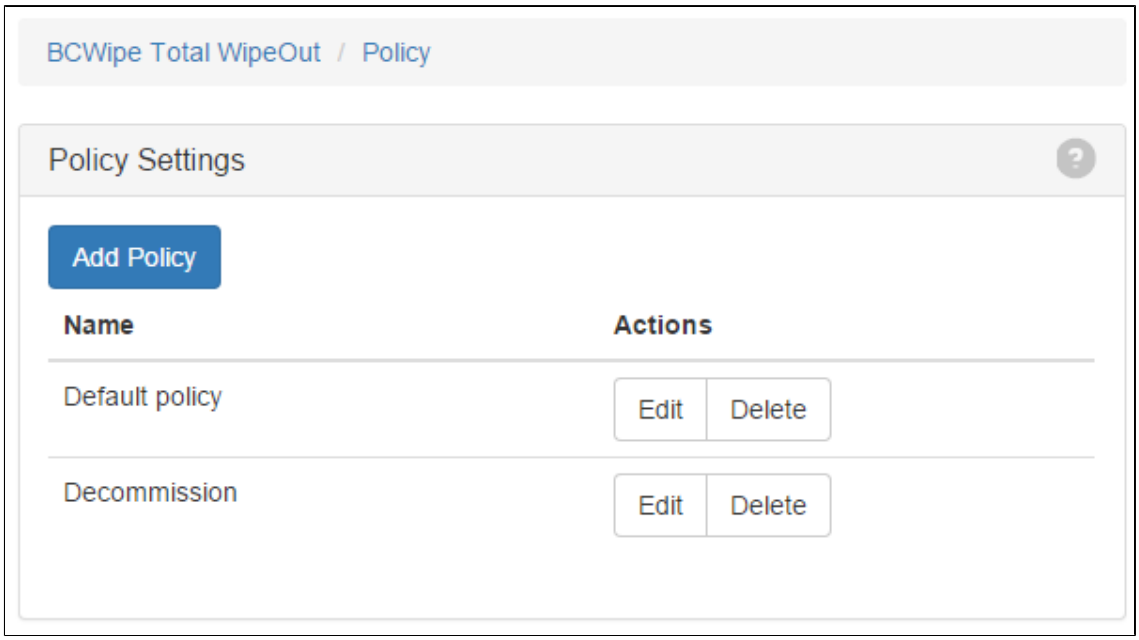


See also:

Start Wiping
Policy Management

Policy Management

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

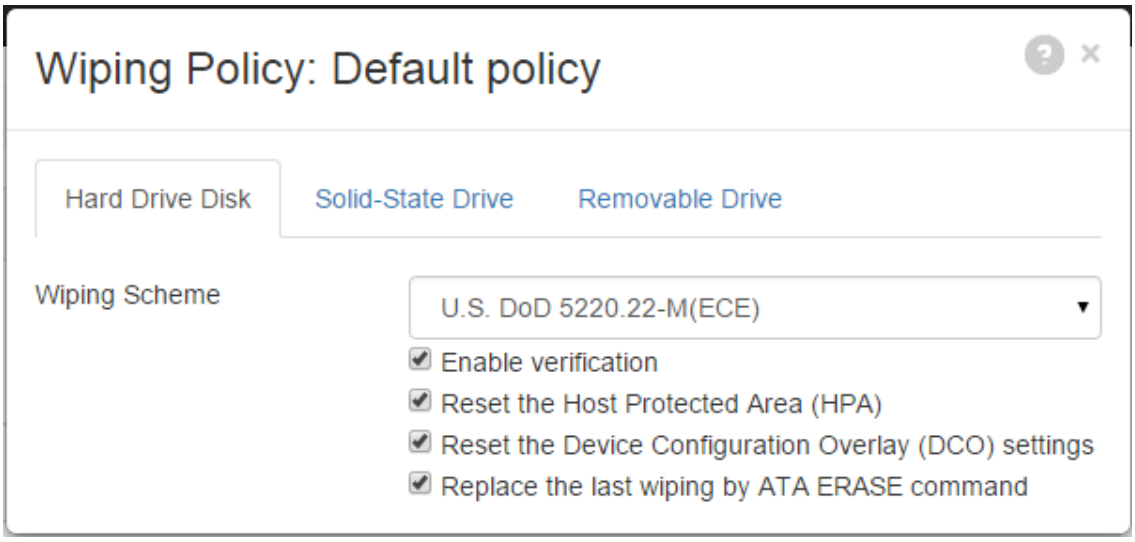


Wiping Policy Settings

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

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

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.



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

• ***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.

• ***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 SECURITY_ERASE command overwrites whole drive including protected, reserved and reallocated sectors.

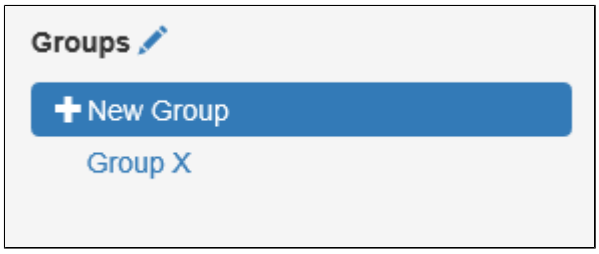
See also:

Wiping Overview

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.



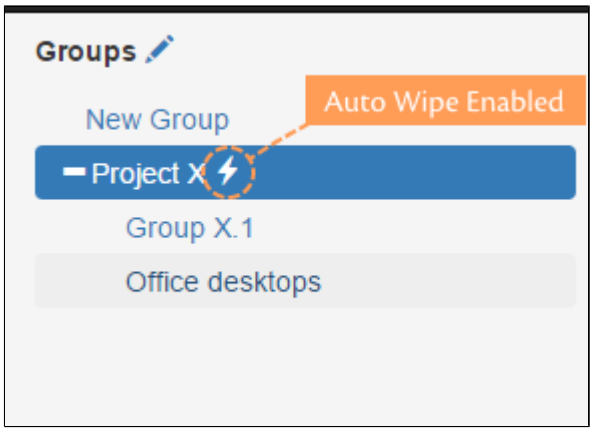
Default Group

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

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

Auto Wipe

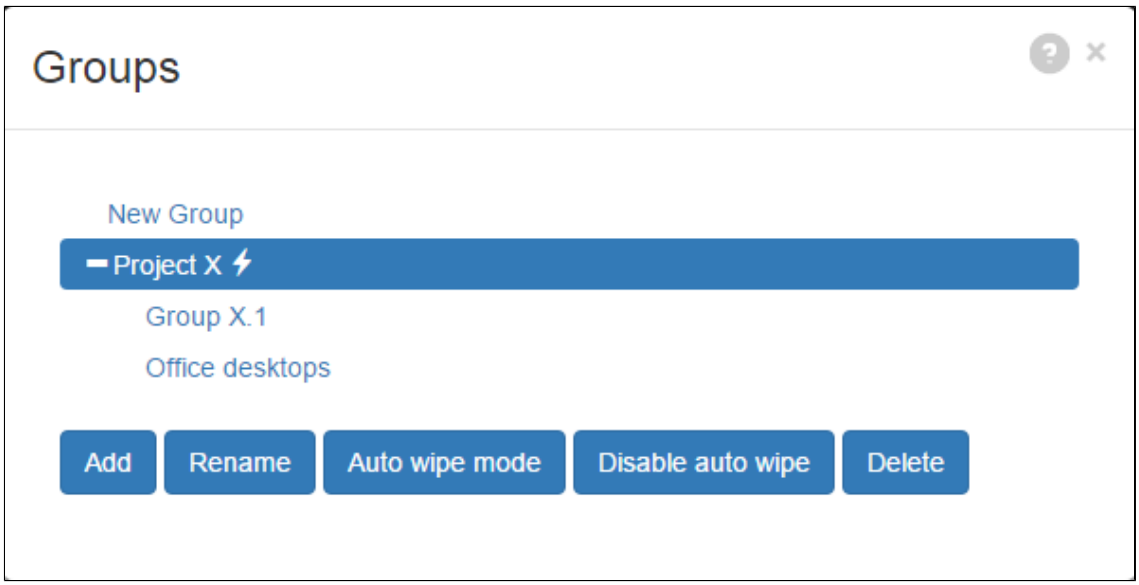
A group can be set to ***Auto Wipe Mode***:



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.

Editing Groups

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



- The ***Add*** button creates a subgroup of the selected group.
- The ***Rename*** button allows you to edit the name of the selected group
- The ***Auto wipe mode*** button allows you to set automatic wiping for the selected group.
- The ***Disable auto wipe*** button turns automatic wiping mode off for the selected group.
- The ***Delete*** button deletes the selected group. 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.

See also:

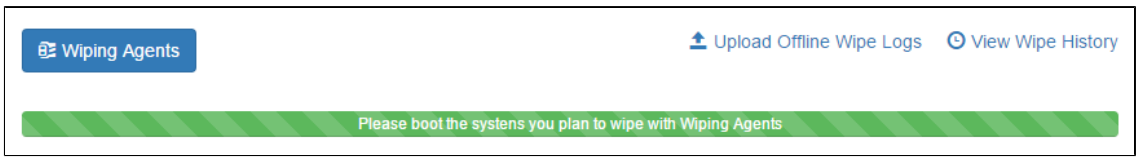
Assets
BCWipe Total WipeOut Console User Interface

Work Area

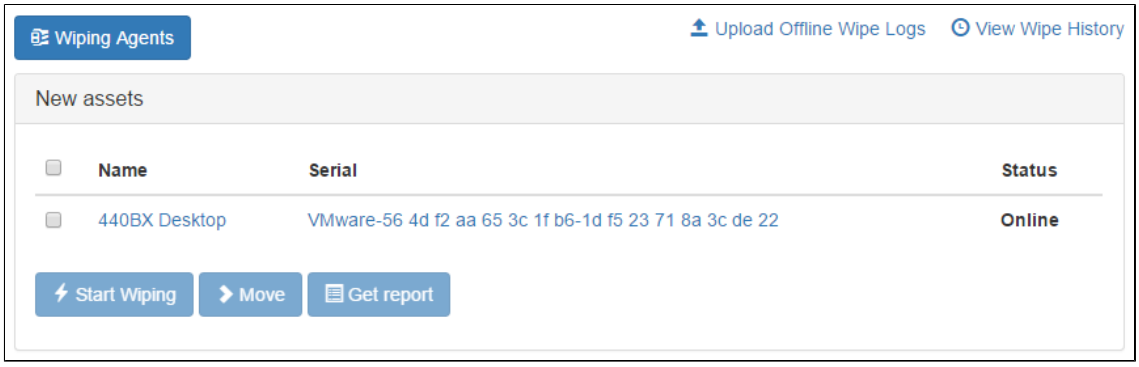
- Assets
- Start Wiping
- Get Report
- Wiping Agents
- Upload Offline Wipe Logs
- View Wipe History

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 Agent starts and connects to the server, an asset will appear with the ***Online*** status:



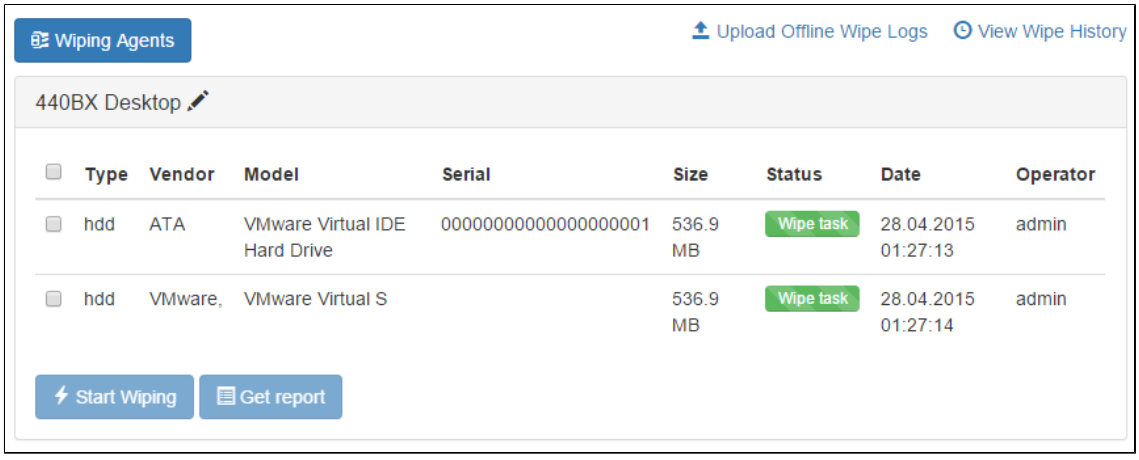
At this point, you can select an asset and perform the following operations:

- 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.

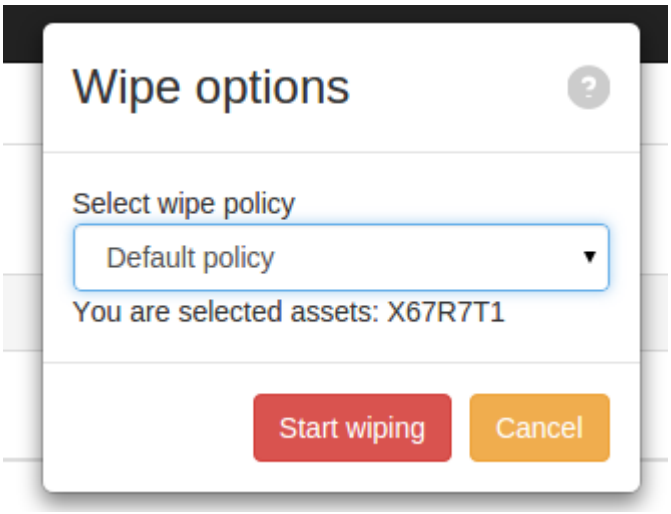
Asset Details

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.



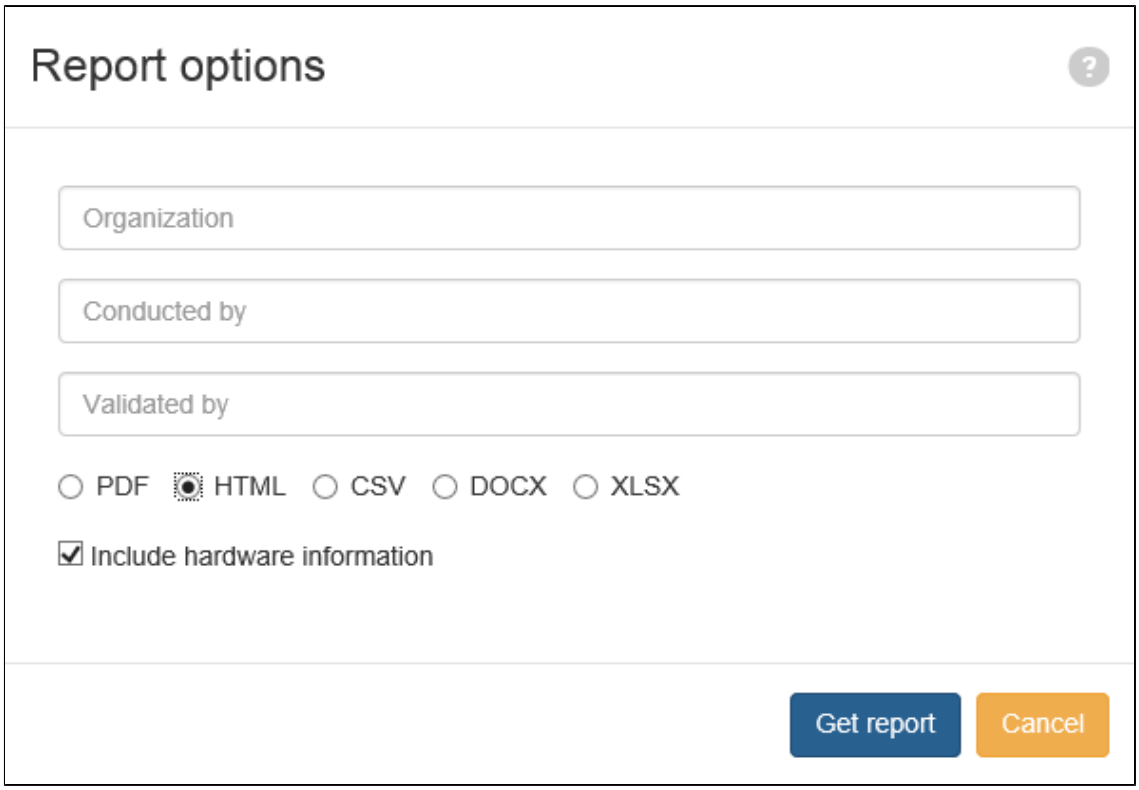
1. Select your desired wiping policy from the drop-down menu.
2. Press ***Start Wiping*** to confirm or ***Cancel*** to cancel the operation.

See also:

Wiping Agents User Interface
Booting BCWipe Total WipeOut
BCWipe Total WipeOut Console User Interface

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.

Finally, select the desired report format and click ***Get report*** to generate it.

Note: Reports open automatically in a new browser window or tab. Please adjust your browser's popup-blocker settings to allow the report window to appear.

See also:

Upload Offline Wipe Logs

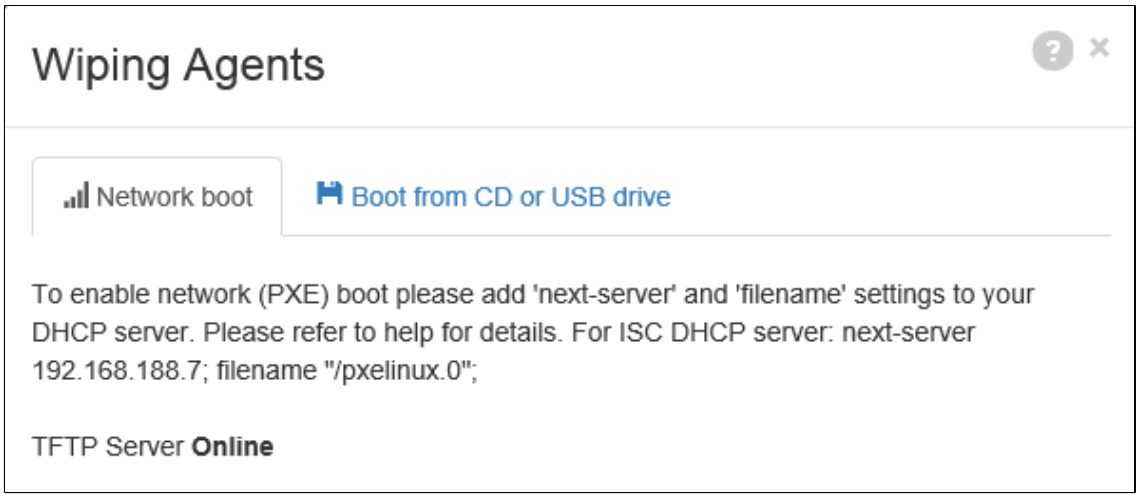
Wiping Agents

BCWipe Total WipeOut uses 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
Intel Mac systems	-	yes	yes
Intel Itanium (IA64)	-	yes	yes
SPARC64	-	yes	-

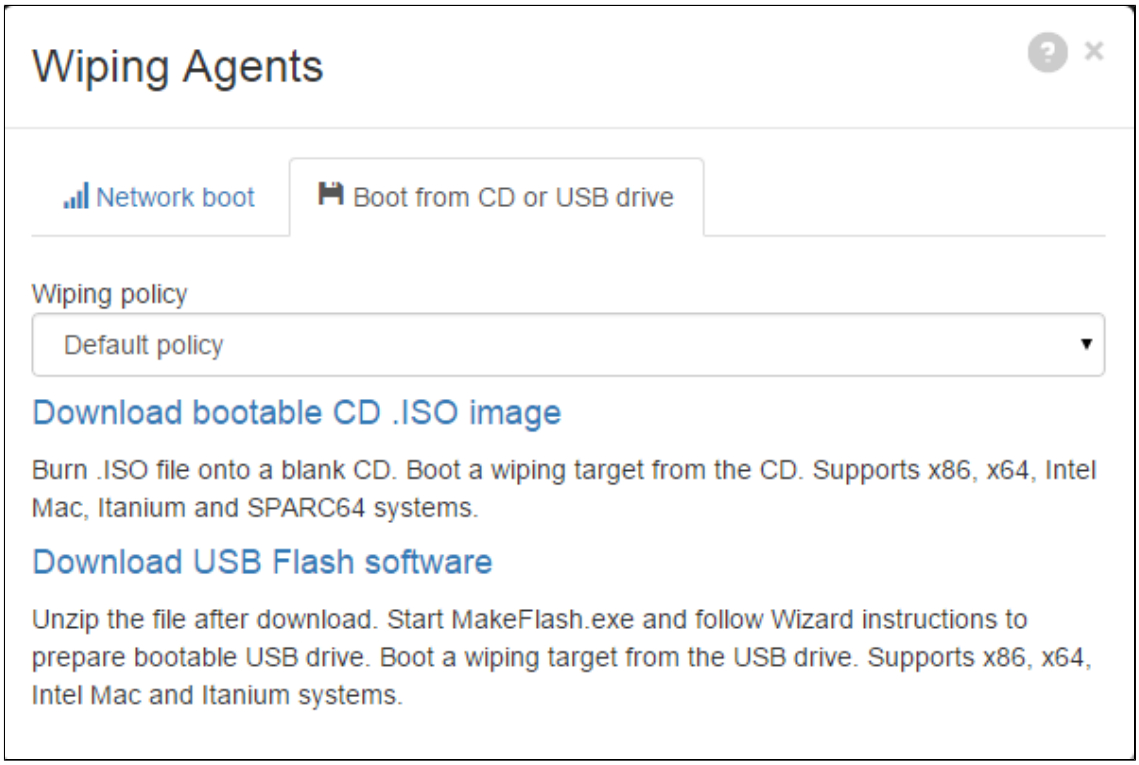
Network Boot

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.
2. Click ***Download bootable CD .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
Making a Bootable USB Drive

Upload Offline Wipe Logs

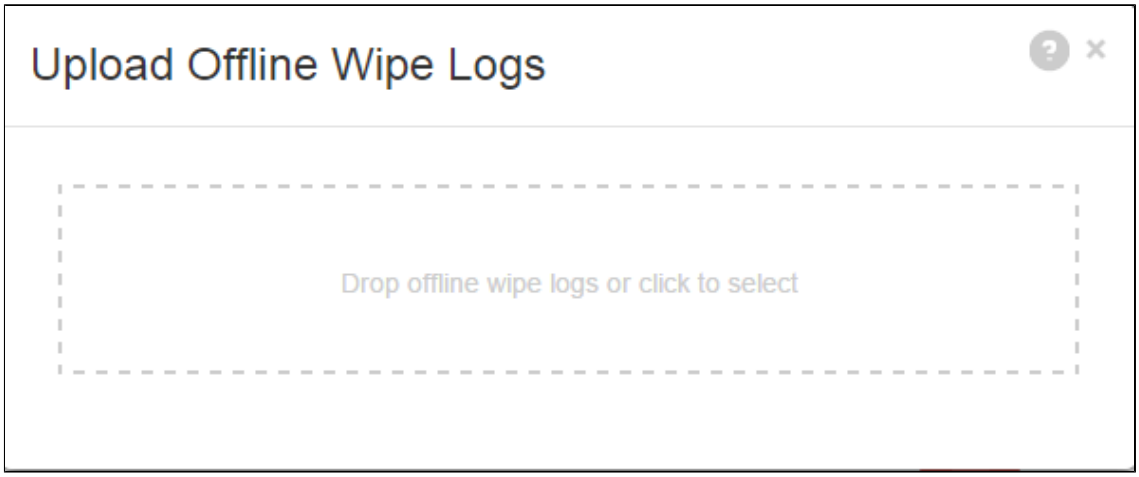
When Wiping Agents does not have a network connection to the BCWipe Total WipeOut server, it operates in Offline Mode.
In Offline Mode, BCWipe Total WipeOut:

- 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.



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

See also:

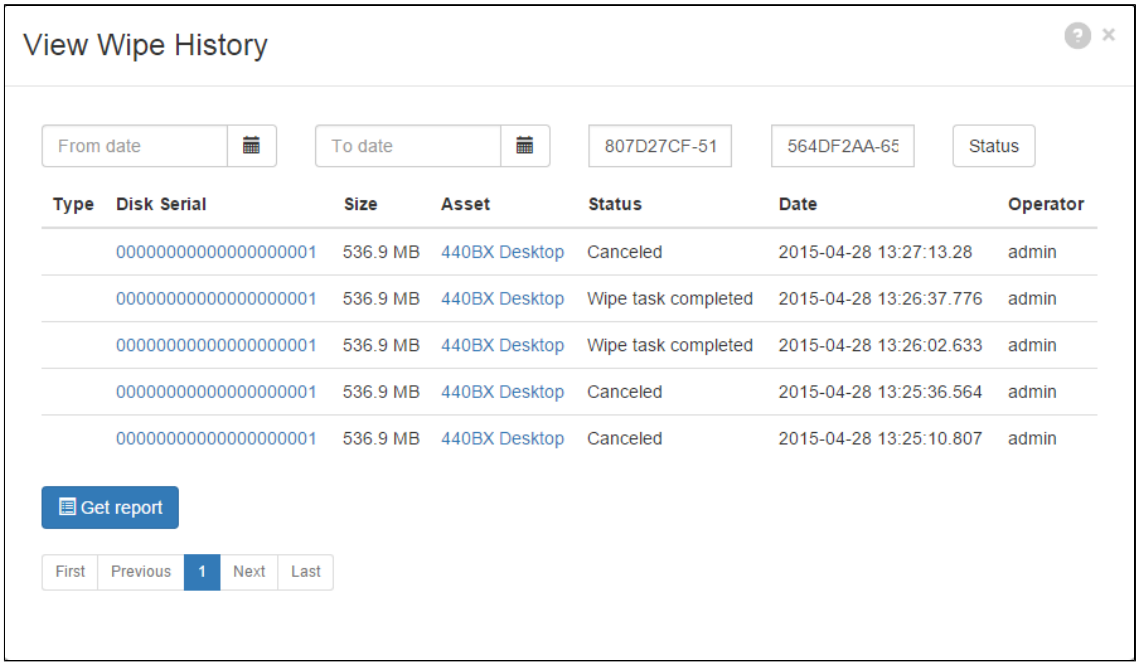
Get Report
Wiping Agents User Interface

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.



See also:

Wiping Overview
BCWipe Total WipeOut Console User Interface

Wiping Agents

- Booting BCWipe Total WipeOut
- Wiping Agents User Interface
- Making a Bootable USB Drive

Booting BCWipe Total WipeOut

Booting from Network (PXE)

BCWipe Total WipeOut Enterprise supports booting from network for x86-compatible BIOS-based systems and x86-compatible EFI systems in legacy mode.

x86 and x64 systems -- BIOS / x86 and x64 systems -- EFI in legacy mode

1. Prepare your environment for booting from network.
2. Turn off the system.
3. Power on the system and invoke your BIOS 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

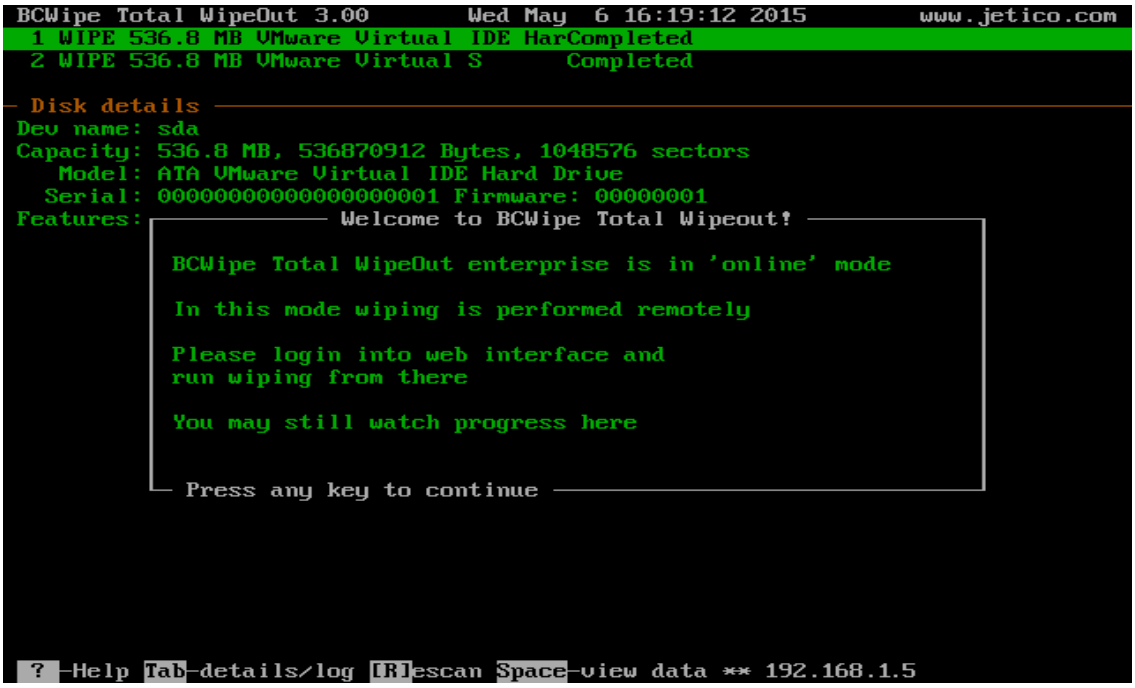
BCWipe Total WipeOut can create a bootable CD for SPARC. Bootable USB sticks are not supported for SPARC systems.

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.

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.

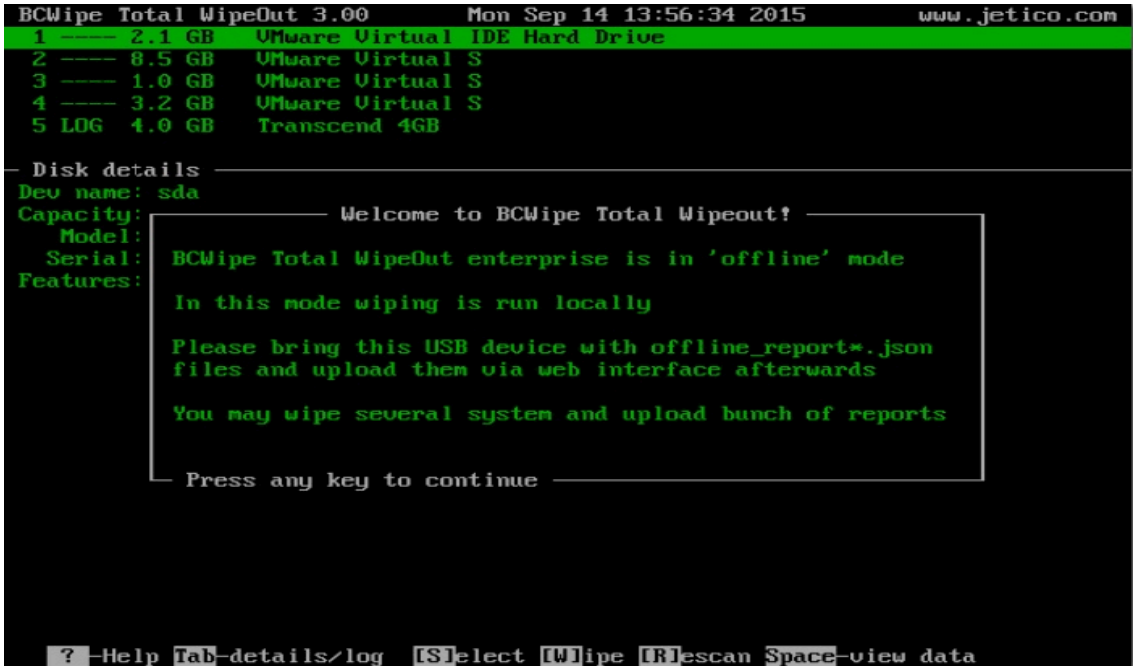


Offline Mode

In Offline Mode, you will be instructed to select drives for wiping and start the wiping process.

The keys for controlling Wiping Agents in offline mode are:

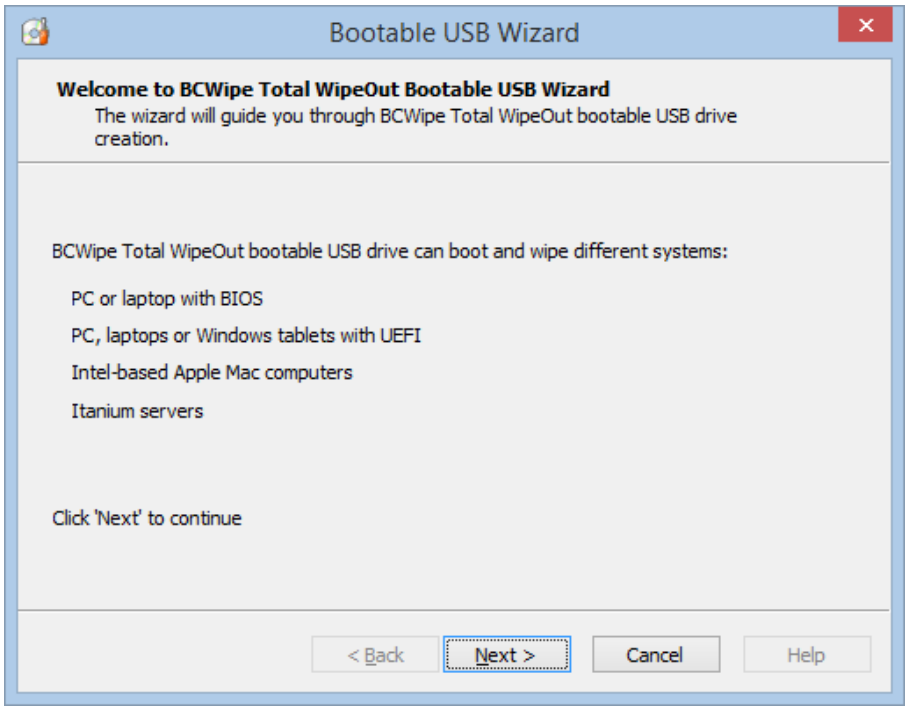
- S: Toggle wiping on a disk
- W: Start wiping on selected disks
- R: Rescan disks



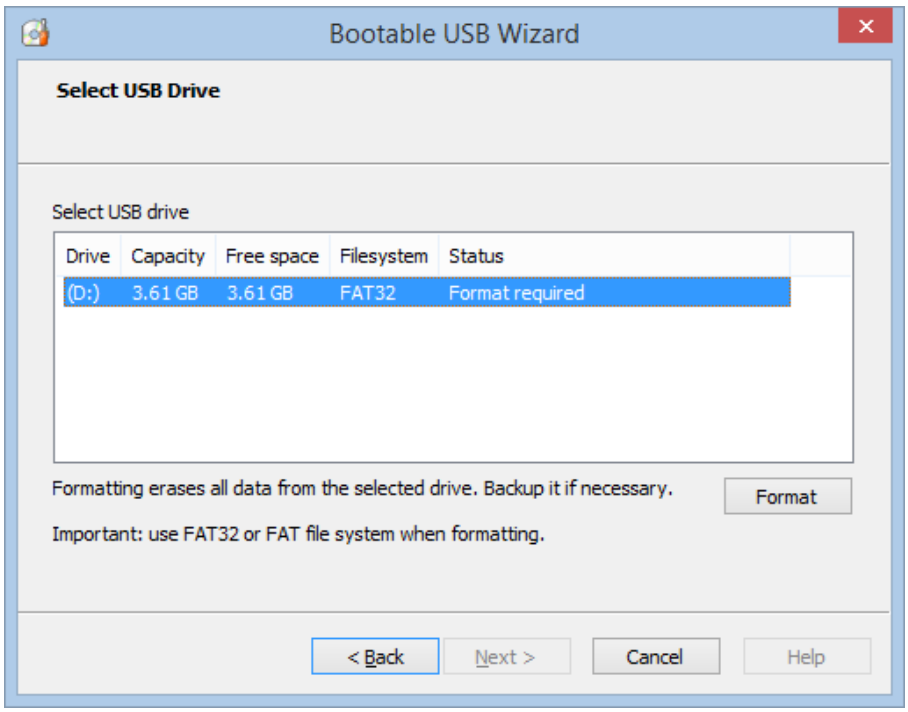
Making a Bootable USB Drive

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

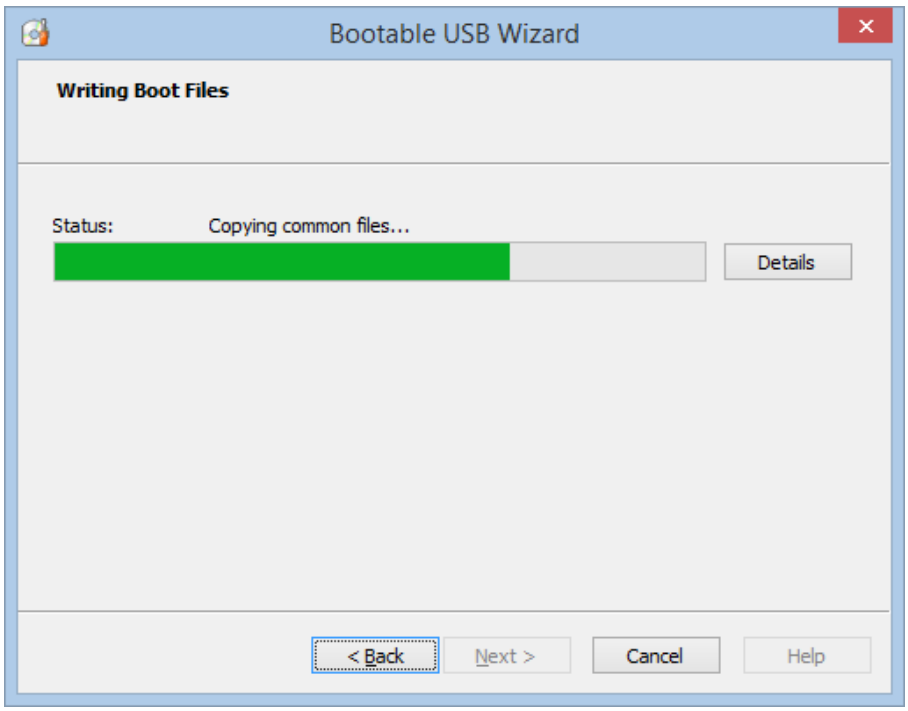
1. Log in to BCWipe Total WipeOut console
2. Open the Wiping Agents dialog and select the Boot from CD or USB Drive tab.
3. Click the ***Download USB Flash software*** link and save *bcwipeflash.zip* on the disk.
4. Unzip bcwipeflash.zip. Start *MakeFlash.exe*.
5. Read the welcome message, then click ***Next***.



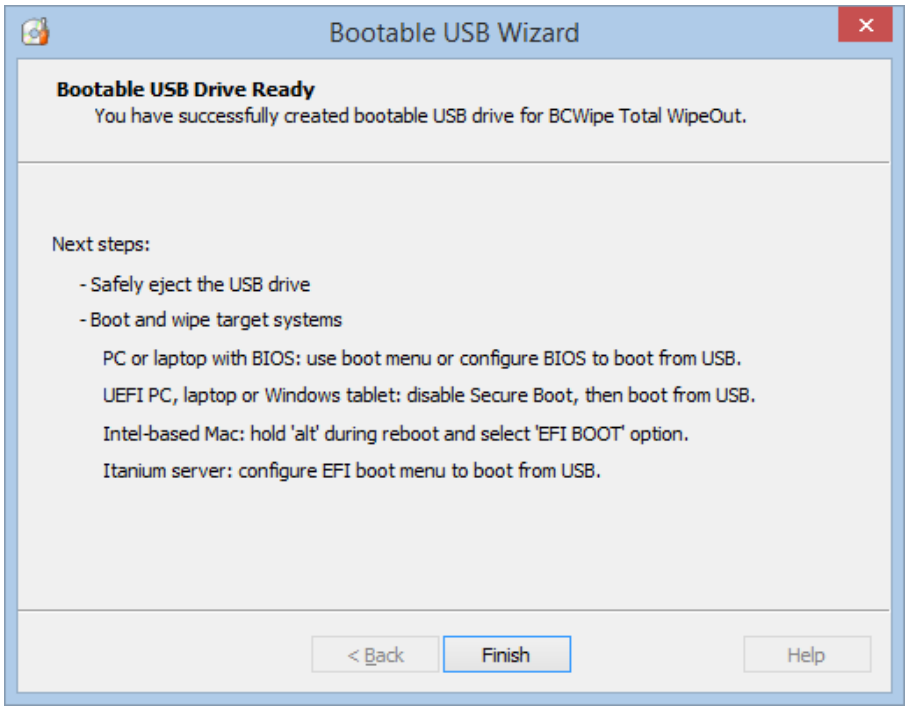
6. Select USB drive from the list. Click the Format button to format the disk with FAT or FAT32 if required. Then, click ***Next***.



7. The wizard will copy the boot files to USB drive. Click ***Next*** when complete.



8. Review the booting instructions. Click ***Finish***. Safely eject the USB drive.



See also:

[Upload Offline Wipe Logs]
[Wiping Agents]

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
spring.jpa.hibernate.ddl-auto: update

# Dont change properties below, please
spring.thymeleaf.cache: false
security.basic.enabled: false
server.port: 8443
spring.thymeleaf.mode: LEGACYHTML5
```

Database Settings

```
# Apache Derby Embeded database
spring.datasource.url: jdbc:derby:database;create=true
spring.datasource.driver-class-name:
org.apache.derby.jdbc.EmbeddedDriver

# MySQL database
#spring.datasource.url=jdbc:mysql://localhost/test
#spring.datasource.username=root
#spring.datasource.password=
#spring.datasource.driver-class-name=com.mysql.jdbc.Driver

# 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
```

Logging Settings

```
logging.config=file:./log4j.properties

log4j.rootCategory=INFO, CONSOLE, FILE

PID=????
LOG_PATTERN=[%d{yyyy-MM-dd HH:mm:ss.SSS}] ${PID} %5p [%t]  %c{1}:
%m%n

log4j.appender.FILE=org.apache.log4j.RollingFileAppender
# Set the maximum file size before rollover
log4j.appender.FILE.MaxFileSize=10MB
```

```
# Set the the backup index
log4j.appender.FILE.MaxBackupIndex=5
log4j.appender.FILE.File=jcm.log
log4j.appender.FILE.ImmediateFlush=true
log4j.appender.FILE.Append=true
log4j.appender.FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.FILE.layout.conversionPattern=${LOG_PATTERN}

# CONSOLE is set to be a ConsoleAppender using a PatternLayout.
log4j.appender.CONSOLE=org.apache.log4j.ConsoleAppender
log4j.appender.CONSOLE.layout=org.apache.log4j.PatternLayout
log4j.appender.CONSOLE.layout.ConversionPattern=

log4j.category.com.jetico.jcm.server=INFO
log4j.category.com=ERROR
log4j.category.org=ERROR
```