BounceBack Ultimate

USER GUIDE

Introduction

BounceBack Ultimate 2020 is the newest version of our legendary backup and recovery software for Window 7, 8, and 10 PCs. It's the only backup solution available that allows instant recovery from disasters such as hard drive crashes, virus corruption, and ransomware. No recovery process is required… you're up and running instantly after a disaster. Simply restart the system and select to run from the backup drive. That's it, no need to create rescue media or boot into a rescue environment. Whenever you start your PC, BounceBack Ultimate allows you to select starting from either your system drive or the BounceBack backup drive. If the internal system drive has crashed, most PCs will automatically start from the backup drive. The system will then run normally since all applications, settings, and connectivity are identical when running from the backup drive. This level of backup protection is unmatched.

If a disaster occurs, user can continue to operate from the backup drive indefinitely. A full system restore can be performed at user's leisure, and whenever a replacement system drive has been installed. Performing a full system restore from the booted backup drive is literally a 3 or 4 click process.

Types of Backups

BounceBack Ultimate provides the ability to make different types of backups. A **Full System Backup**, **VHD Image Backup,** and **Data Backup**.

Full System Backup (Drive Mirror)

These are backups that you should run when BounceBack Ultimate is first installed. This type of backup job will copy all partitions on the internal system drive, plus the files contained within each partition to the backup drive. Please note, this process initializes your backup drive to match your system drive's partitioning and as a result, existing data on the backup drive will be erased. When a Full System Backup (Drive Mirror) is utilized for backup, the backup drive must be dedicated to backup use only.

VHD Image Backup

A VHD image backup creates a virtualized drive that exists in a single file on the backup drive. This file can be mounted by Windows to appear as a normal physical drive. BounceBack Ultimate then partitions the virtualized drive similar to a mirror backup. All partitions and files within the system are then transferred to the virtual drive. When the backup completes, the virtual drive is unmounted and appears as a single large file on the backup drive. BounceBack Ultimate will automatically size the VHD to match the size of the OS, applications, plus any data.

Data Backup

Creating a Data Backup job is a nice way to complement your Full System backup. Versions of your documents, spreadsheets, or pictures (data files from your libraries) are created each time a backup is launched and are easily accessible through Access & Restore Data screen. Each time a backup is launched, user is given the option of purging all previous versions. Data Backups can also perform real-time backup. This results in documents being backed up immediately to the backup drive when they change.

Getting Started

- **Installing the software.** To install BounceBack Ultimate, locate the installer file and double click. It is required to be logged in to Windows with an Administrator account for this installation. You may need to temporarily disable Anti-Virus & Anti-Malware scanners and Firewall software for the install. Your activation code is either on a sticker attached to the CD sleeve, emailed when you purchased, or available online at My Account page at http://store.cmsproducts.com.
- **Making your initial Full System Backup.** On the welcome screen, you have the option to select Full System Backup or Data Backup. Make sure your backup drive is connected, Full System Backup should already be selected by default, if not, select and click next. On the next screen your external backup drive should already be selected as target drive, if you have more than one drive connected, select the one you prefer to use. On the next screen select your preferred options and click next. Depending on the size of your drive and your computer's transfer speed, this may take a while. BounceBack will display detailed backup and transfer stats.

For detailed instructions on backup options, look for the relevant sections in this guide.

Supported Backup Drives

Supported backup drives include USB external drives, internal SATA drives, plus any interface that is recognized by the system at boot time. This also includes Thunderbolt drives on many PCs.

Selecting a high-performance drive versus a drive of lessor quality will have a huge impact on user experience when running from the backup drive. This is especially true for flash drives. Many of the high capacity USB 3.0 flash drives sold today are based on inferior USB 2.0 technology. These drives may provide painfully long startup times when booted. The latest external SSD drives can provide performance similar to the system drive.

Full System Backup vs VHD Image Backup

Most users will find Full System Backups easier to implement and use. Bootable VHDs are not supported by Windows Home edition and therefore not available to all users. An advantage of VHDs for Windows Pro and Enterprise users is that the backup drive can contain multiple bootable VHDs. When users choose to create recurring VHD backups, they are in a sense creating a snapshot in time of the entire system. Similar to Full System Backups, BounceBack Ultimate supports specifying which VHD to start from when they create a Windows boot menu. VHD backups will also automatically boot if the internal drive has crashed. In addition to booting a VHD, users can mount their VHDs to compare data with the running system, or to other VHDs. This can be accomplished using the Access & Restore Data feature.

Feature	Full System Backups	VHD Image Backups
Backup Drive is Bootable	✓	✓
Supports All Windows Versions	✓	✓*
Supports BitLocker Full-Disk Encryption	✓	✗
Drive Can Contain Multiple Bootable Backups	✗	✓
Drive Can Contain Bootable Backups from Other PCs	✗	✓
Supports Scheduled Full-System Backups	✓	✓
Supports Scheduled Incremental Backups	✓	✗
Drive Can Contain Non-Backup Data	✗	✓
Backup Drive Can Replace the Internal Drive	✓	✓

* Windows Professional and Enterprise only

A VHD backup will generally require a larger capacity backup drive. A 4TB backup drive can contain several full system VHD backups for the average user. BounceBack Ultimate will optionally delete the oldest VHD if there's no space available when a new VHD backup is scheduled for launch. There is a tradeoff with security as VHD backups do not support BitLocker encryption. Full System Backups are vulnerable if a Full System Backup fails as the drive can be rendered unbootable. If multiple VHDs exist on the backup drive, you always have other VHDs to revert back to.

Ransomware Protection

A ransomware strike on a PC results in the encryption of the system drive at the block level, and below the file system. This encryption can even go over top of a BitLocker encrypted drive. This renders the PC inoperable. A small program will then launch informing the user that payment of a ransom is required to have the drive unencrypted. If the encryption key is not provided by the attacker, the system is lost. Protection against ransomware attacks normally involves anti-virus software designed to catch attacks before they infect the system. Judging by the number of ransoms paid by corporations and government agencies, this approach is not always effective. Since ransomware attacks normally target all drives on the system, backup drives are frequently infected along with the rest of the system. This is especially true for desktop and server PCs where the backup drive is always connected.

BounceBack Ultimate now provides a unique approach to ransomware protection. Users can select to disable the backup drive when a backup is not in progress. If ransomware strikes, the protected drive won't be seen by the system and won't be accessible for attack. Recovering from a ransomware infection is a simple process… reboot and start from the backup drive. After wiping the system drive, a full system restore can be performed from the booted backup drive. BounceBack Ultimate will automatically enable the drive prior to a backup, then disable it when the backup completes. Backup drive protection can be disabled or enabled from the Access & Restore Data screen.

Backup Scheduling

All backups can be launched on a recurring schedule. Users have the option of launching multiple daily, weekly, or monthly backups. Scheduled Full System Backups can be either incremental or Full System. Scheduled VHD Image backups can only be a Full System backup. When a scheduled backup completes, BounceBack Ultimate can optionally shut down the system.

Backup Exclusion Process

When the backup drive is not large enough to fit all of the data from the system, BounceBack Ultimate allows users to select files and folders to exclude from the backup process. The user interface does not allow selection of data that would render the backup drive unbootable. It also does not allow selecting applications for exclusion. If the user selects all items allowed for exclusion, then they will create a **minimal boot drive**. This is a backup that only contains the Windows operating system plus all applications installed on the system. If the backup drive is not large enough to contain a minimal boot drive, then the backup process is halted, and the user is asked to connect a larger drive.

The bars represented in the hard drive display are color-coded to correspond with the data exclusion totals. As data is selected for exclusion, the amount required before the backup will fit is updated. The blue bar on the hard drive will then slide to the left. Once this bar is inside of the drive display, the Next button is enabled, and the user is allowed to continue.

For VHD backups, the user has the option of selecting a VHD capacity smaller than the recommended size. When this occurs, the backup process will always ask the user to exclude data from the VHD backup process as well.

Access & Restore Data

Access & Restore Data screen allows easy access to backup data stored on the backup drive for each of the three backup types; Full System Backup, VHD Image Backup, and Data Backup. This is where users can compare versions of documents, plus perform restores at the folder and file level. Double-clicking a document will open that document in the appropriate app.

Users can turn the Windows boot menu on or off here. For Full System Backups, the boot menu is set to the entire backup drive. For VHD Image Backups, the boot menu can be set to any VHD on the backup drive.

This is also where ransomware protection for the backup drive can be turned on or off. Ransomware protection is supported for both Full System and VHD Image Backups.

Full System Backup

For Full System Backups encrypted with BitLocker, the backup drive can be locked or unlocked, plus passwords can be changed by the user.

VHD Image Backup

Each VHD on the backup drive can be mounted or unmounted. Mounting results in drive letters being automatically assigned to the drives within the VHD. The list of all VHDs lives in the application folder, plus the root of the backup drive. If the user connects a backup drive containing VHDs that has never been seen by the system, the restore program will automatically make available all VHDs on the new backup drive. VHDs can also be deleted.

Data Backup

Data backups are displayed corresponding to each full or incremental backup. This allows easy access to comparing the contents of documents across multiple versions. Any data version can also be deleted.