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 is 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 are up and running instantly after a disaster. Simply restart the system and select to run from the backup drive. 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 https://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

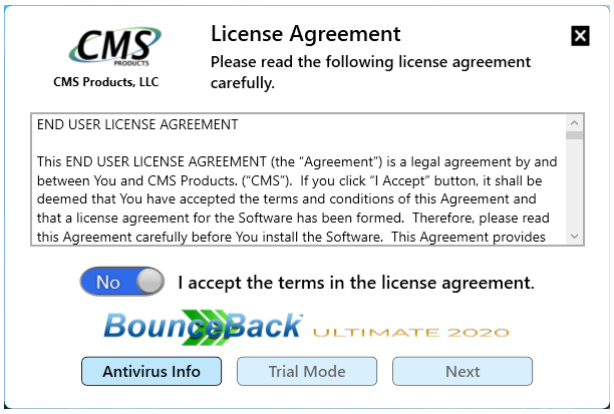
Supported backup drives include USB external drives, internal SATA drives, plus any interface that is recognized by the system at boot time. This also includes Thunderbolt drives on many PCs.

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.

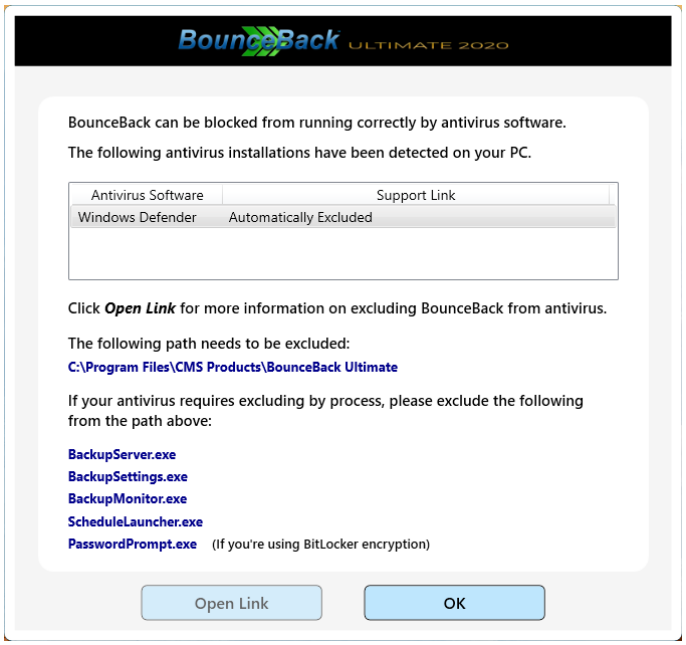
Installation

If you downloaded a zipped file, extract the content of the zipped file to any location on your hard drive and run **BounceBackUltimate2020.exe** by double clicking it.

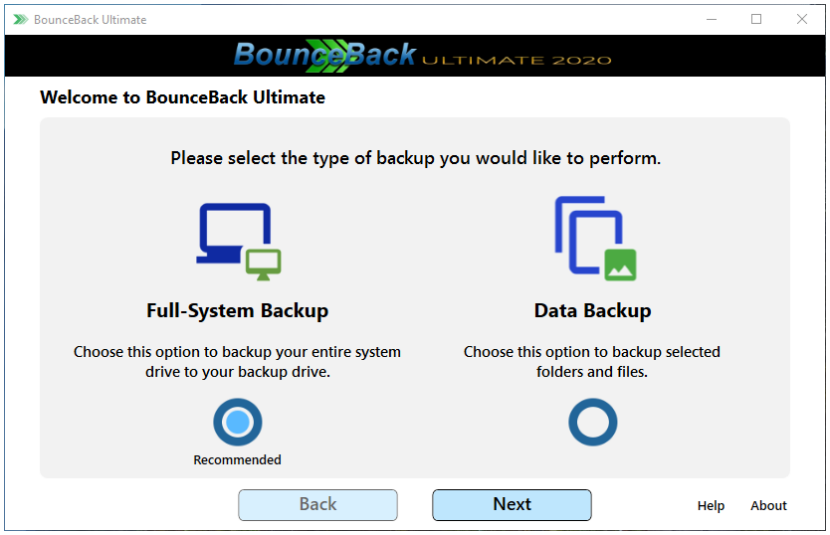
After clicking **Yes** to accept the license agreement, you are prompted to enter your activation code. You should have received an activation code when you purchased the software. If you want to install BounceBack Ultimate in trial mode, click **Trial Mode**.



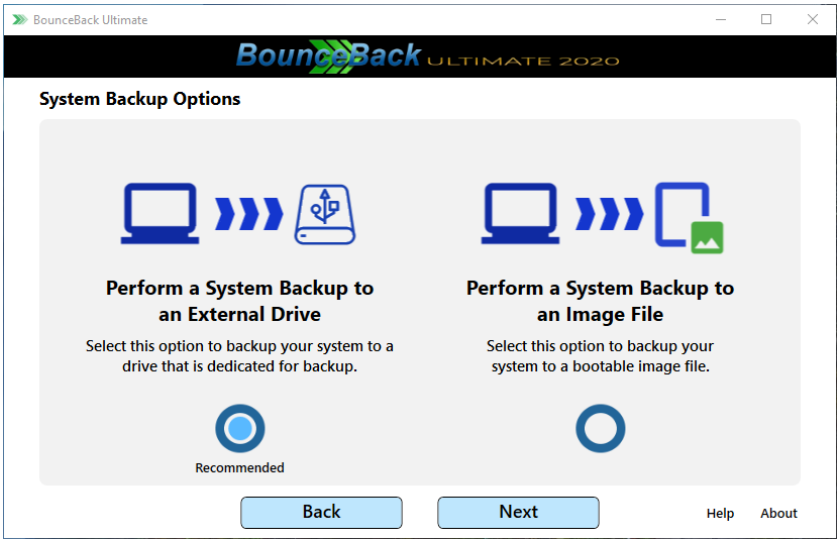
BounceBack Ultimate needs low-level access to your backup drive, some antivirus software may interfere with the backup process. Clicking **Antivirus Info** will display a list of each of your installed antivirus solutions. Clicking Open Link will display instructions in your browser for excluding BounceBack Ultimate from the scanning process for that antivirus program. If you are using Microsoft antivirus, exclusions are built automatically.



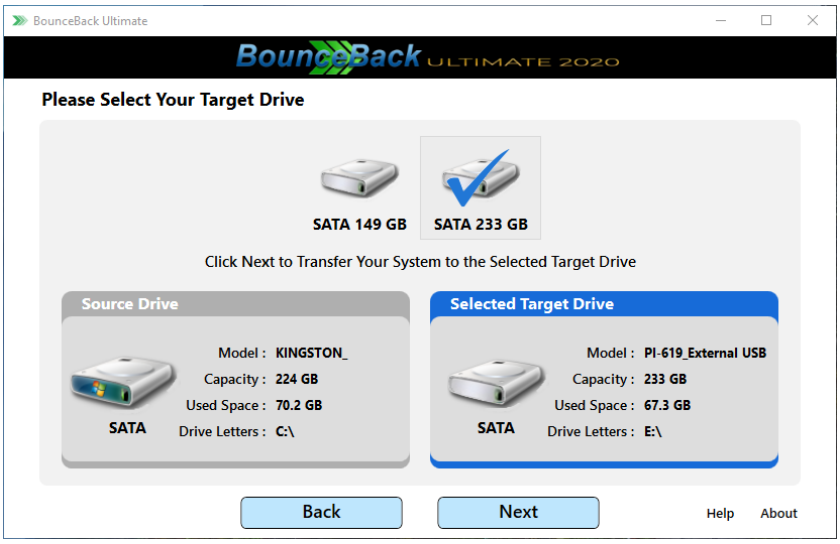
The next step is to select what type of initial backup you would like to perform. If you want to backup your entire system drive, select **Full-System Backup**. If you would prefer to select specific folders and files to backup, select **Data Backup**.



The Full-System Backup option will allow you to create a bootable backup to an external USB drive, and is the recommended method of backing up.

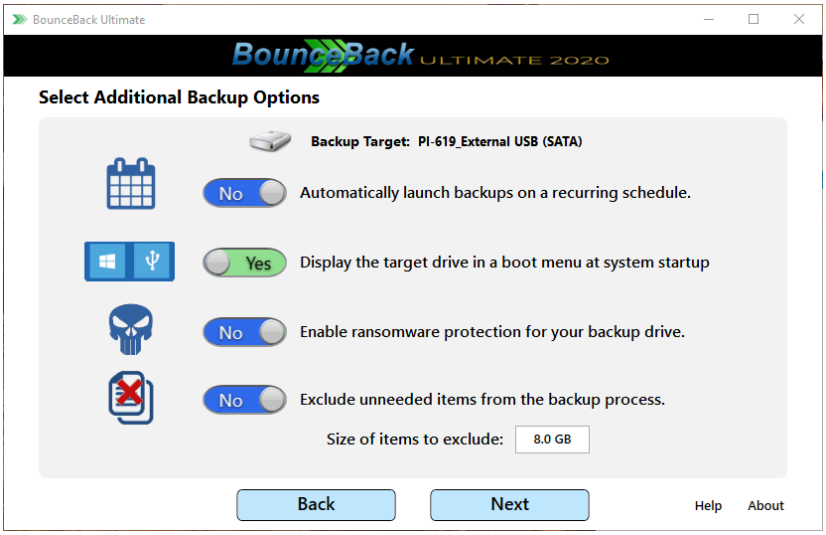


Next, you are asked to select the backup drive you would like to target for your full-system backup. If there is only one drive available, it is automatically selected, otherwise select the external USB drive you intent to use. The system drive is also selected automatically.



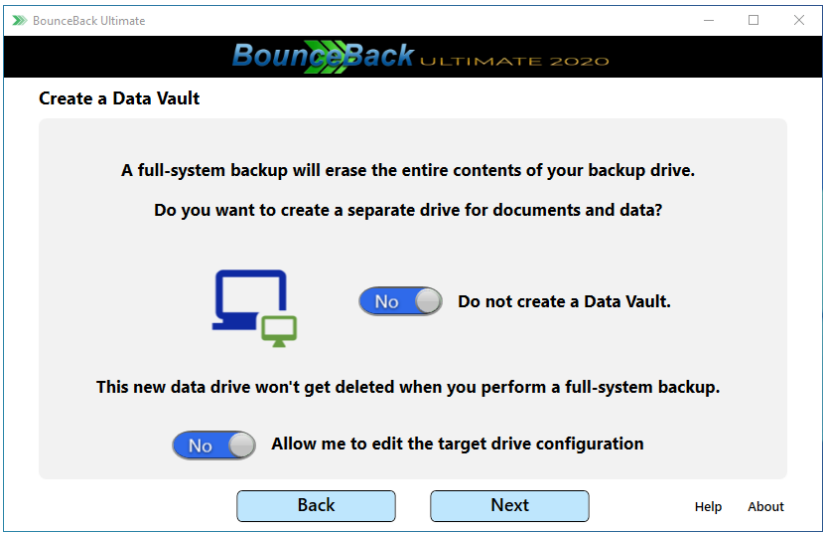
On the next screen, you are presented with three options when creating a bootable backup:

1) Create Backup Schedules (see section on Scheduling Backups)
2) Enable Ransomware Protection (see section on Ransomware Protection)
3) Display a Boot Menu at Startup (see section on Creating a Startup Boot Menu)
4) Exclude unneeded items from the backup process.

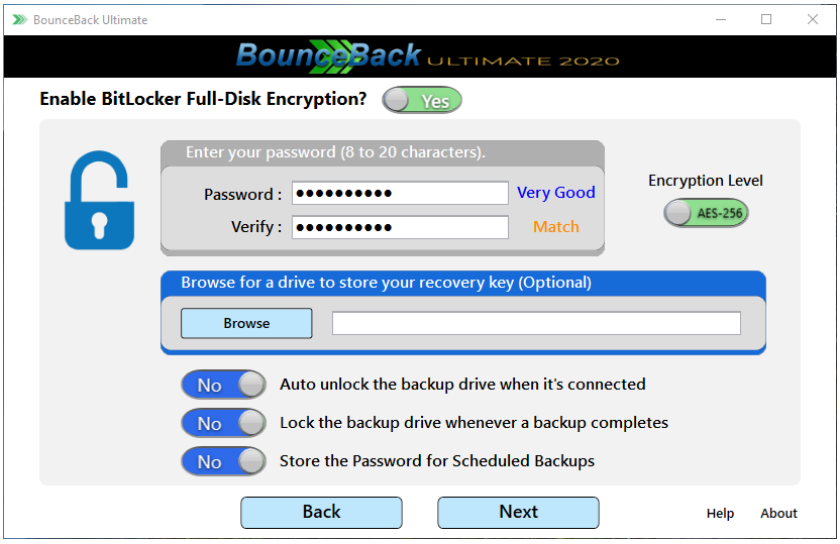


Unneeded items include the Windows temp folder, internet temp folders, plus various cache and log folders. The hibernation file, page file, and crash dump files are also excluded. All items excluded are not needed for backup or the booting process.

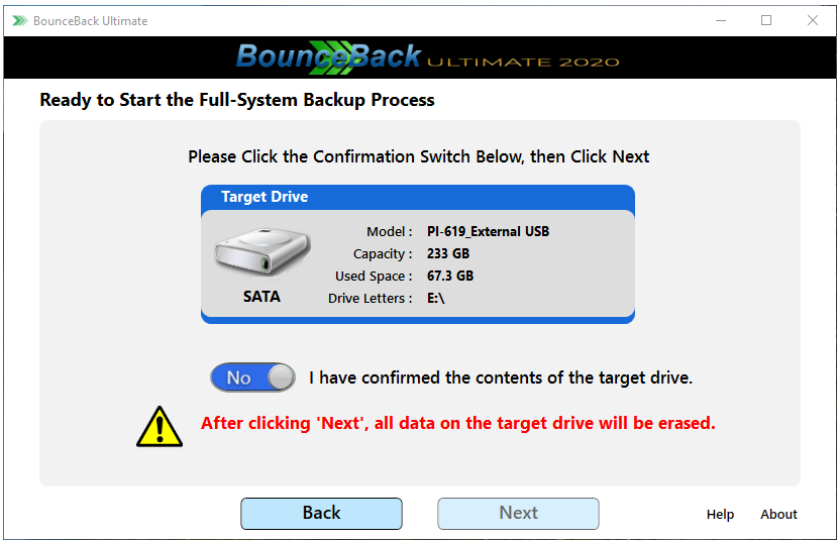
Next, select if you would like to create a Data Vault on your backup Drive. This will allow you to store items on the backup drive that will not get deleted during your next full-system backup.



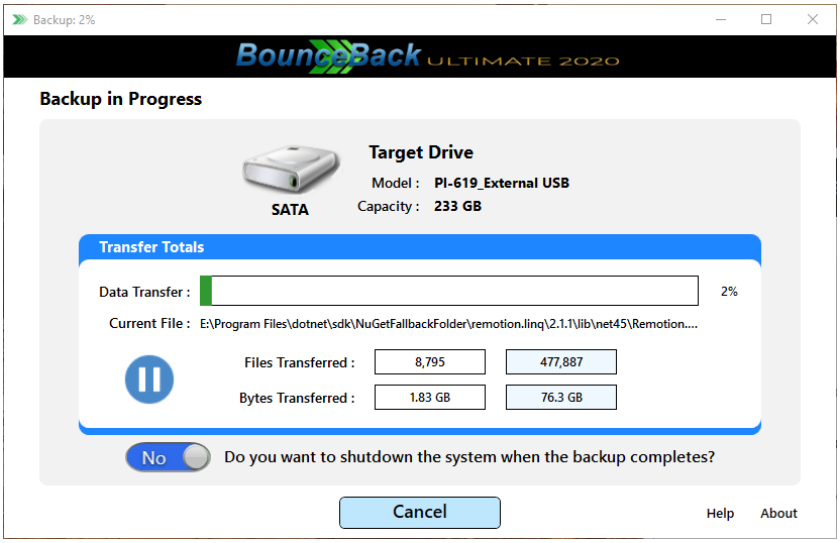
Clicking next will present you a screen with an option to enable BitLocker encryption. If you enable this option, the password you select will be required to unlock the drive when booting from backup drive. Refer to section on BitLocker Full-Disk Encryption for more information.



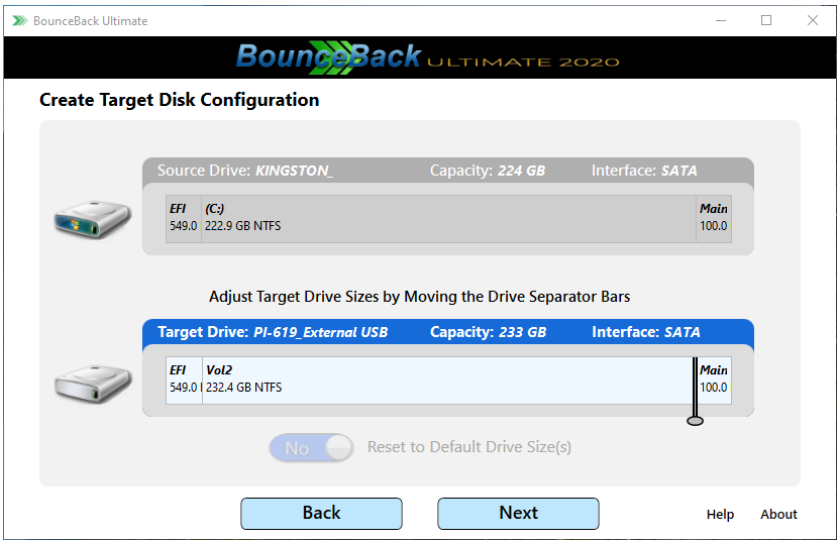
The final installation screen asks you to Click **Yes** to verify that there is no data on the backup drive you want to keep. Clicking **Next** will start the backup process and wipe the drive clean.



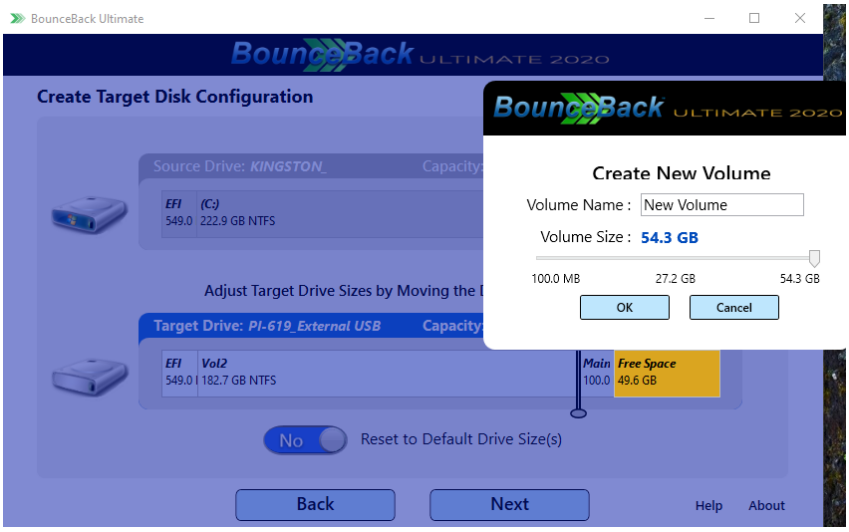
Slide the confirmation button to Yes and click next, BounceBack will start partitioning and formatting your target drive and once ready, it will start copying your files to your backup drive. This process may take a long time and will depend on the speed of your computer, drive, and USB ports as well the amount of data you are backing up.



NOTE: Advanced users can alter the partition structure of their Backup Drive by clicking the **Back** button twice from the confirmation screen.



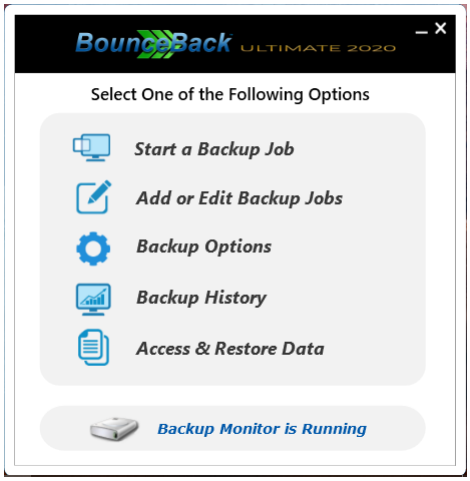
Move the sliders left or right to change the size of a partition. As you move the sliders, the free space of the partition on the left and right will display, along with the new capacity of both partitions. Maintenance partitions created by Windows or the PC OEM cannot be resized.



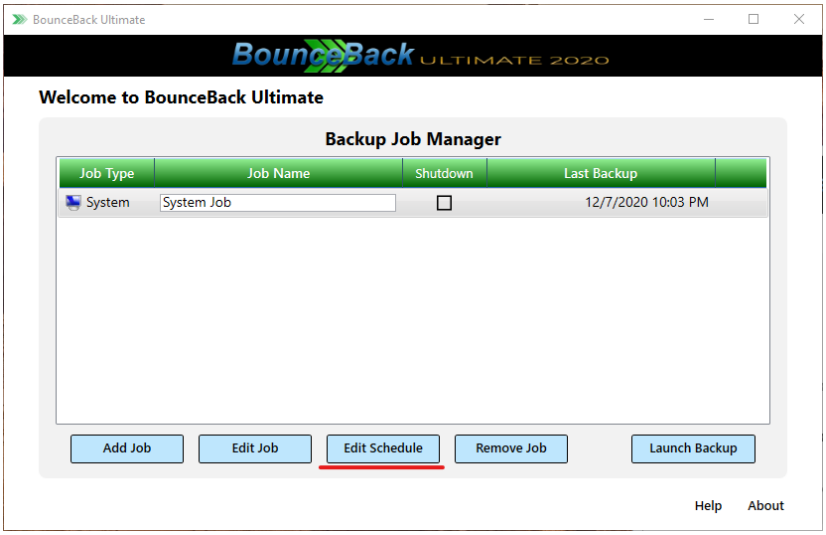
Partitions can also be deleted from this display. Click the **Reset** button at any time to restore the default partition sizes.

Scheduling Backups

BounceBack Ultimate can launch backups on a recurring schedule. Scheduling is supported for full-system and data-only backups. To create a backup schedule, select **Add or Edit Backup Jobs**.



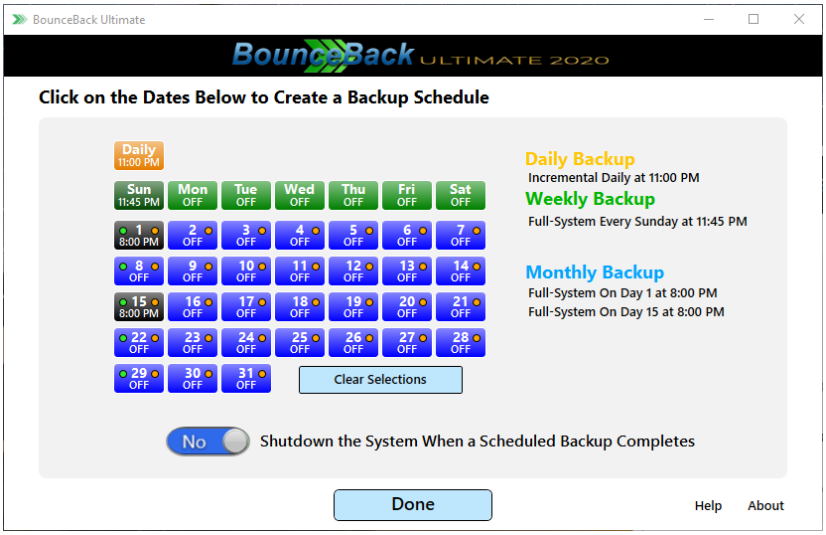
Next, click the **Edit Schedule**.



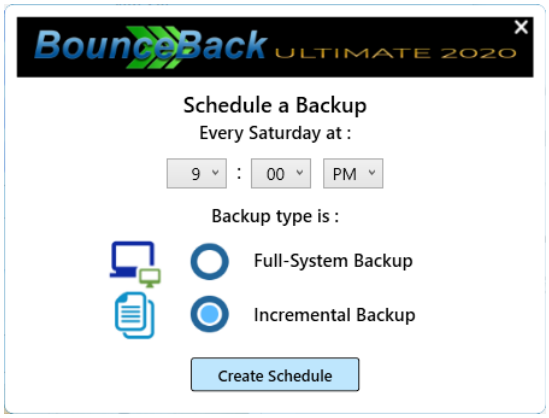
BounceBack Ultimate allows you to create daily, weekly, or monthly backup schedules.

To create a daily backup, click on the orange button on the upper left of the display. Create weekly schedules by clicking any of the 7 green buttons and create monthly schedules with the blue numbered buttons. Remember that you can create multiple triggers for each backup job.

You can also **shut down your PC** after the scheduled backup completes.



In the example above, the same backup job is scheduled for daily incremental backups at 11PM, full-system backups every Saturday, and a full-system backup on the 1st and 15th of every month.



After clicking one of the colored schedule buttons, you are prompted to select the time the backup will start. You can also select if you would like to **Backup Everything**. Select Full-System Backup for system backups, or backup everything in your data backup. Select Incremental Backups, which only backs up changes for backups.

Backup Exclusion

If your backup drive is not large enough to fit all the data on the system, then BounceBack Ultimate allows you to select folders and files to exclude from the backup process. If you select all items allowed for exclusion, then a **minimal boot drive** is created. This is a backup that only contains the Windows operating system plus all applications installed on the system. If your BounceBack is not large enough to contain a minimal boot drive, then the backup process is halted, and you are asked to connect a larger drive.

NOTE: 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.

The bars represented in the Exclusion Window's hard drive display are color-coded to correspond with the **Data Exclusion** totals. As data is selected for exclusion, the storage 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 the drive display, the **Next** button is enabled, and you are allowed to continue.

For image backups, you have the option of selecting an image smaller than the recommended size. When this occurs, the backup process will always ask you to exclude data from the image backup process as well.

Creating a Startup Boot Menu

Creating a startup boot menu will allow you to select which drive you want to start your PC from. If you enable this option, a Boot menu will be displayed each time you start your PC. The default option is to start from your normal system drive. Select the second option if you would like to start from your BounceBack backup drive. This menu will display for 15 seconds, then continue and start normally.

You can select to create a startup boot menu when you initially create a full-system backup.

Your BounceBack software will create a startup boot menu by default. Change the switch from **Yes** to **No** if you do not want to see the startup menu every time you start your PC. If you chose not to create a startup menu, then change your mind, you can create it at any time by editing your backup job. To do this, click the BounceBack icon in the system tray, then select **Add or Edit Backup Jobs**. Next, select **Edit Job** to turn the startup menu on or off.

BounceBack Ultimate supports a legacy style boot menu. Though not as pretty, this version will display earlier in the boot process and allow you to start from your BounceBack quicker. To turn the legacy style menu on or off, click the BounceBack icon in the system tray, then select **Backup Options**.

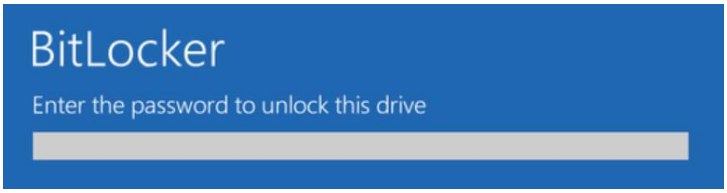
Starting from Your BounceBack

BounceBack is unique among all PC backup applications in that upon completion of your first full-system backup, you can immediately verify that the backup process worked correctly. To do this, start from your BounceBack Ultimate backup drive! All your applications, Windows settings, and internet connectivity, and OneDrive will all work as if you were running from your internal system drive.

If you chose to create a startup boot menu, you will be prompted each time you reboot if you would like to start from your BounceBack Ultimate backup drive. After 15 seconds, your PC will automatically start as normal from your system drive.

If you do not create a startup boot menu, you can use your BIOS boot menu to start from your BounceBack Ultimate backup drive. You do this by tapping the hot key used by your PC manufacturer to access the BIOS boot menu. See the troubleshooting section at the end of this guide for a list of BIOS hotkeys.

If you selected to encrypt your BounceBack, you are prompted to provide your password first.



The type of storage drive you select for your BounceBack will have a big impact on performance. An SSD or a second internal drive can often boot as fast or faster than your internal system drive.

After your PC has started from your BounceBack Ultimate backup drive, a popup message displays informing you that your system is running from your backup drive.

The **Backup Drive Startup Time** measures the time between PC startup up when the popup is displayed. This will not be accurate if a login screen is left idle.

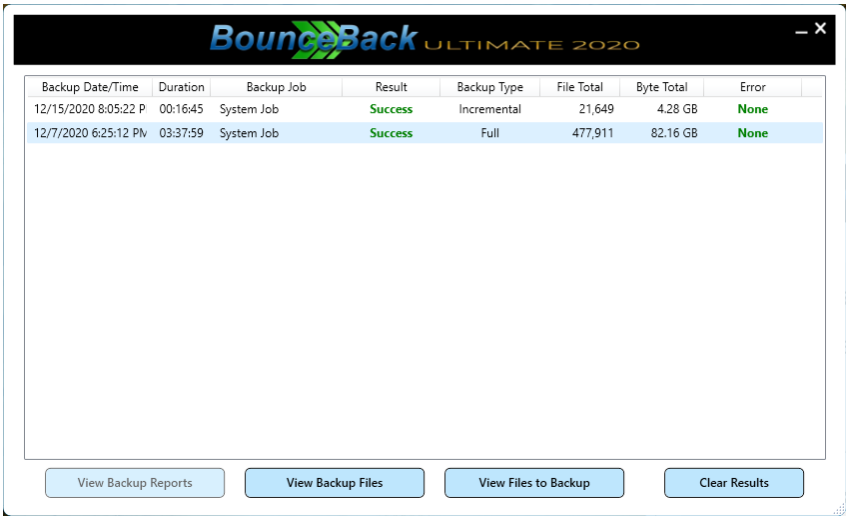
Clicking the Backup Monitor icon in the system tray displays your backup options when running from your BounceBack. Your only option is **Launch Restore Process**. Clicking this option will start the Full-System restore process. This allows you to restore from your booted BounceBack Ultimate backup drive to your internal drive, or to any connected storage device. Any changes made while running from the booted BounceBack will be included in the Full-System restore process.

View Backup History

To get a detailed report of previous backups, please do the following:

1) Right-click the BounceBack icon in the system tray
2) Select **Backup History**

Your backup report includes all your previous incremental and full backups, the time and duration of the backup job, file, and byte totals, plus the result and any errors if applicable.



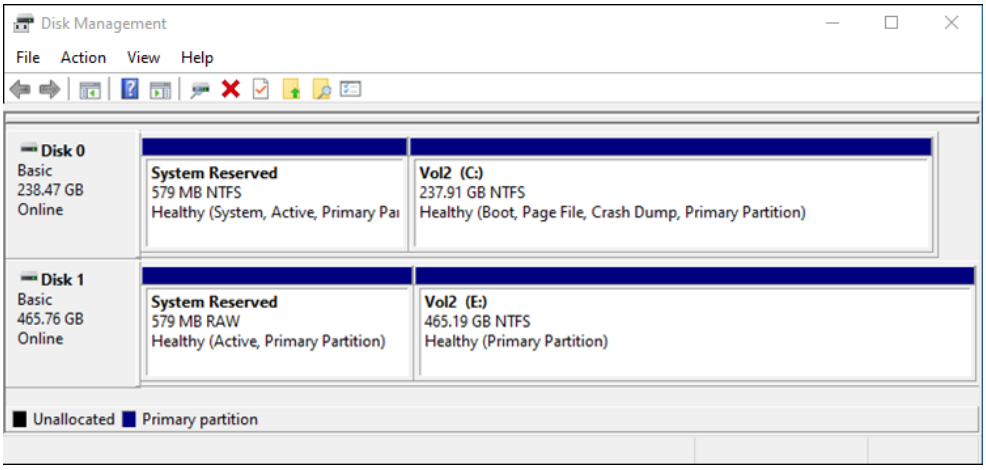
You can also view previous files backed up during incremental backups and view a list of files that are scheduled for your next incremental backup.

Creating a Data Vault

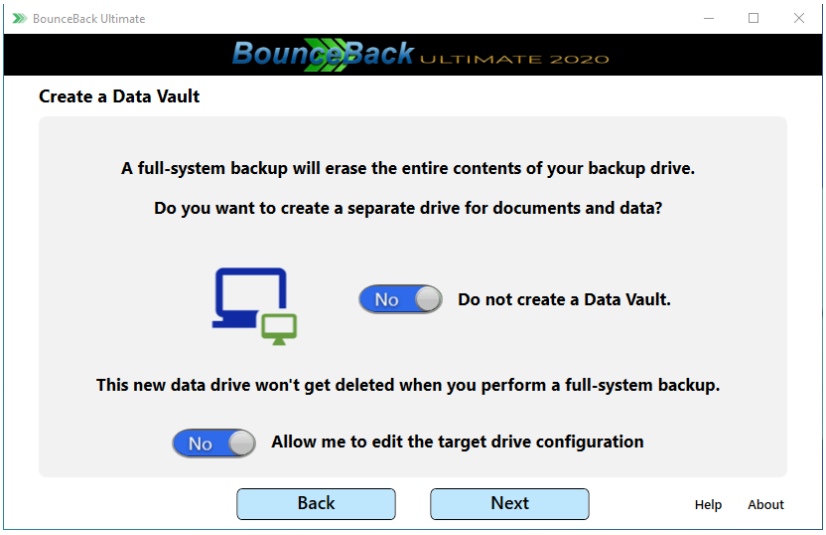
BounceBack Ultimate, in conjunction with full-system backups, allows you to create an extra data drive on your backup drive called a **Data Vault**. When this option is selected, the additional drive is created after the mirror, normally created by a full-system backup. Whenever subsequent full-system backups are performed, the data vault is left intact and not deleted. This allows for storing data that only exists in a data drive and not on the system drive. Users can also perform data-only backups to this drive. BounceBack Ultimate no longer requires separate backup drives for both full-system and data-only backups. The default size of the extra drive can be changed by the user in the UI. This feature is especially useful for large capacity backup drives.

Warning: Turning Data Vault **OFF** will result in the extra drive getting deleted during the next full-system backup, along with any data stored in the extra drive.

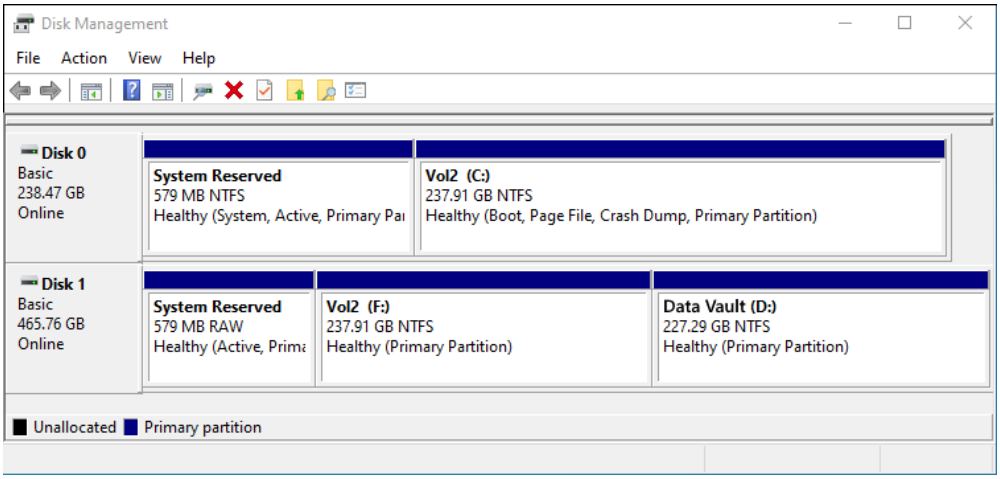
Backup Drive Configuration without Data Vault



Selection process while setting up full-system backup



Backup Drive Configuration with Data Vault

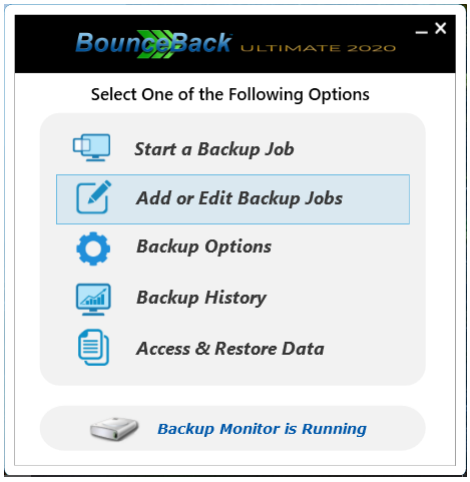


Data-Only Backup

In addition to full-system backups, BounceBack Ultimate also allows selecting folders and files for backup. The resulting backup job can be scheduled for both full and incremental backups, supports ransomware protection, and realtime backup. To create a data-only backup, please do the following:

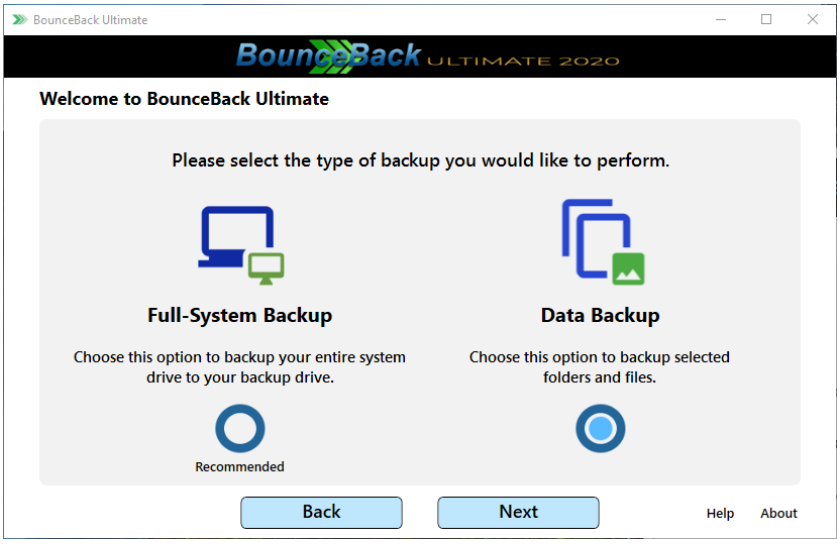
Right-click the BounceBack Ultimate icon in the system tray

Select **Add or Edit Backup Jobs**



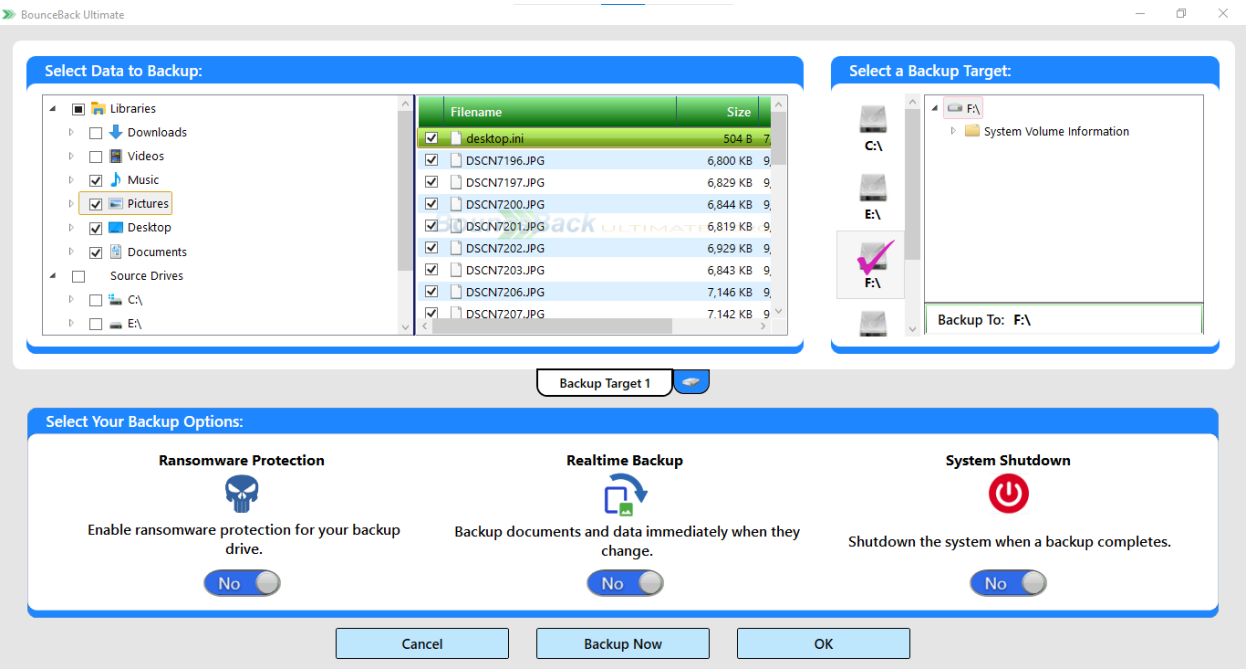
Click the **Add Job**

Select **Data Backup**



The next step is to select the folders and files that you want to backup under the section titled, **Select Data to Backup**. This can be a drive or folders, including the selection of individual files. Once your data is selected, choose where to backup to in the **Select a Backup Target** section.

BounceBack supports backing up to more than one backup target in the same backup job. To do this, click the tab next to **Backup Target 1** below.



Three options are supported for data-only backups to your BounceBack:

1) **Ransomware Protection**
2) **Shutdown System**
3) **Realtime Backup**

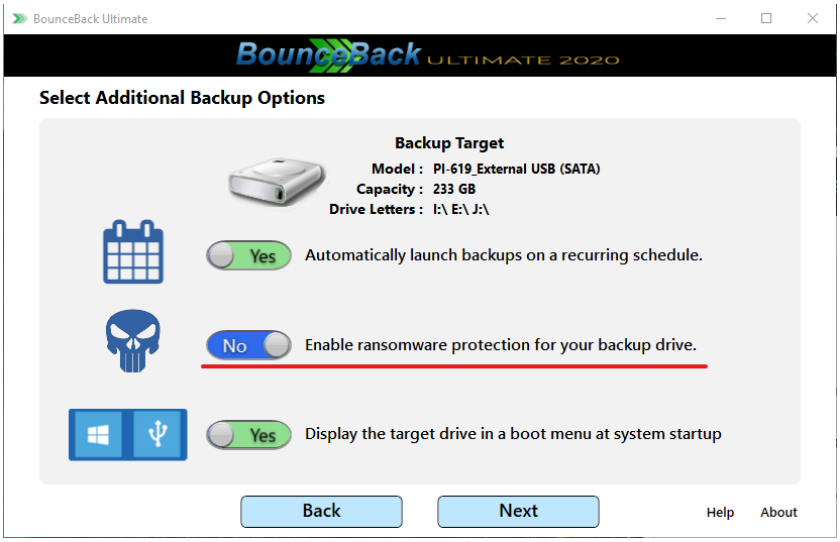
Realtime backup backs up the selected documents or files immediately when they change. This option is best suited for desktop PCs where your BounceBack Ultimate backup drive is always connected. This may also come in handy for laptops that need to backup to network paths.

If you prefer not to utilize the real-time backup option, BounceBack can schedule data-only backups on a daily, weekly, or monthly basis. Both full data and incremental backups can be scheduled. To access and restore your data, please see the **Restoring Folders & Files** section of this guide.

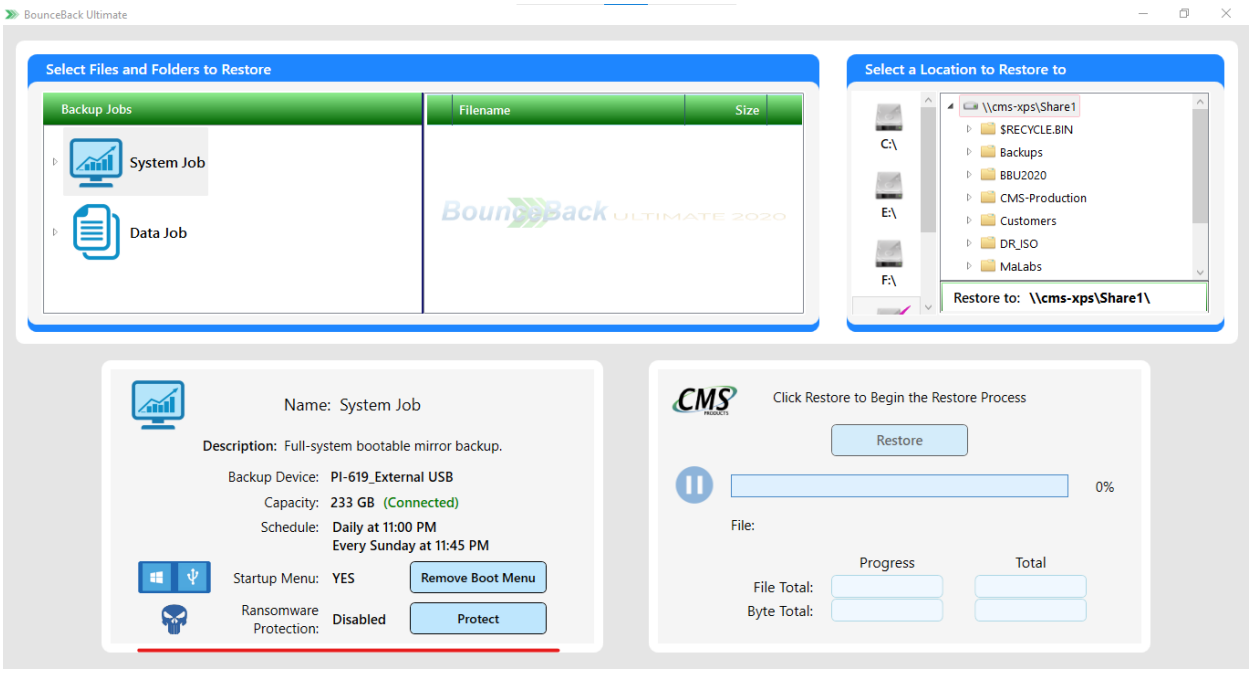
Ransomware Protection

BounceBack Ultimate has a patent-pending technology that allows you to protect your backup drive from ransomware. By disabling the backup drive after a backup job completes, ransomware cannot access the drive or your data. Your backup drive is only visible to the system while a backup job is in progress. If ransomware infects your system at any point, you can reboot and started directly from your backup drive. Ransomware protection is supported for both full-system and data-only backups. It can be enabled when creating a new backup job, or when editing an existing backup.

WARNING: This feature disables access to your backup drive except when a backup is in progress. Do not use this feature if you need to frequently access your backup drive from File Explorer or other applications! To gain access to the drive, you will need to temporarily turn ransomware protection off.



To disable ransomware protection, select **Access & Restore Data** from the BounceBack tray icon.

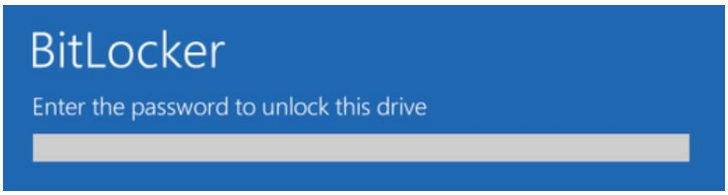


BitLocker Full-Disk Encryption

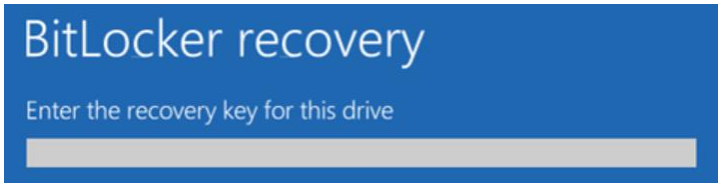
BounceBack Ultimate allows you to create a full-system backup using BitLocker encryption. If your external drive is lost or stolen, the contents cannot be accessed without the correct password. BitLocker can be utilized on your backup drive even if the internal drive is unencrypted or is encrypted with third party encryption. When creating a full-system backup, you are given the option to enable BitLocker encryption.

NOTE: Image backups do not support BitLocker.

The password you select will be required to unlock the drive when starting from your backup drive:



In addition to a password, BounceBack Ultimate supports setting a recovery key. This allows you to unlock the drive from the key in case you forget the password. You can enter your recovery key at startup by clicking **ESC** from the password prompt. The recovery key is saved to a file and can be stored on the local PC, or to a remote location.



Other encryption options include:

Auto Unlock	Your backup drive is automatically unlocked when the drive is connected.
Lock on Completion	Your backup drive will lock after a backup completes.
Store Password	If you schedule your backup jobs, your BitLocker password will be encrypted and stored locally.

You can change your BitLocker password, or lock and unlock the drive at any time by selecting to **Add or Edit Backup jobs** from the Backup Monitor app in the system tray.

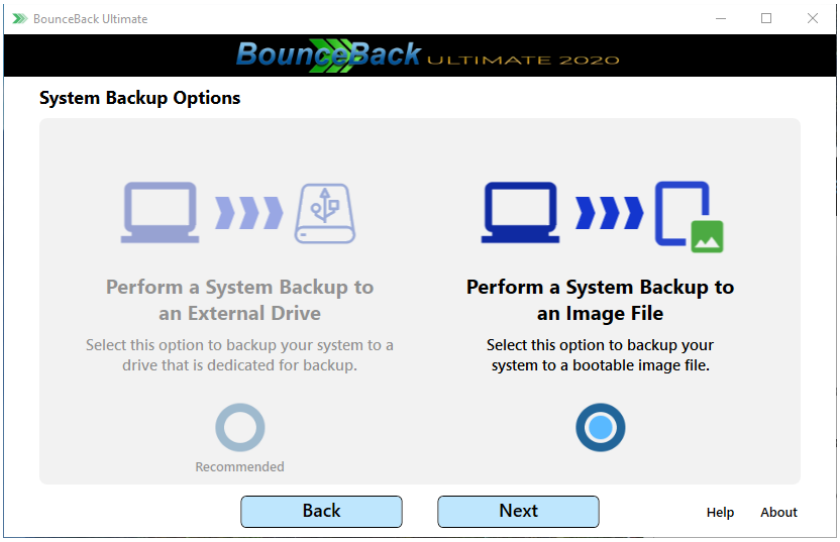
1) Right-click the BounceBack icon in the system tray
2) Select **Add or Edit Backup Jobs**
3) Click the **Edit Job** button, then click **Next**

Image Backup with VHDs

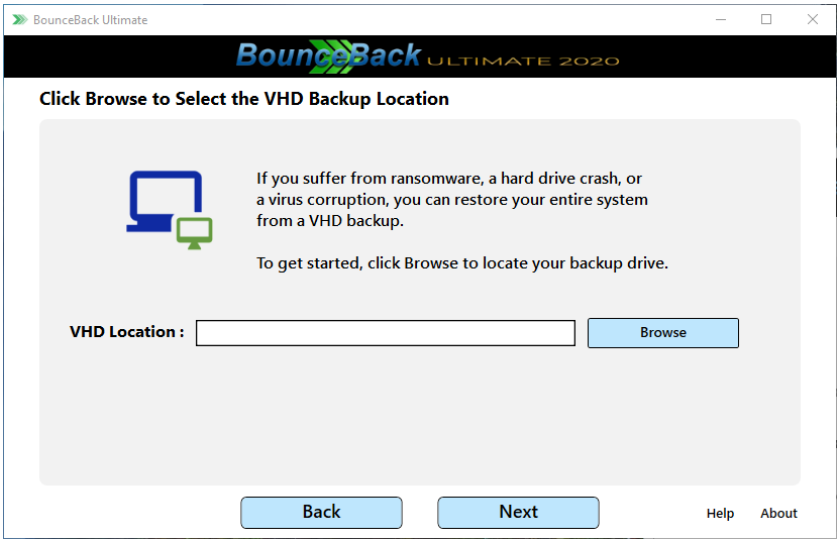
BounceBack Ultimate supports VHD image backups, which allows full-system backups of multiple PCs to the same backup drive. In most instances, these backups can be made bootable on PCs that were not the original backup target. If BounceBack Ultimate is installed on multiple PCs, each PC can be started from the same backup drive!

Image backups are a snapshot of your entire system at the time a backup is performed, which allows you to boot and rollback your system to a previous backup date. Multiple Image backups can also be mounted at the same time to allow access to previous file versions.

To create a Image backup, click the BounceBack icon in the system tray, then select **Add or Edit Backup Jobs**. Select **Full-System Backup**, then **Perform a System Backup to an Image File**.

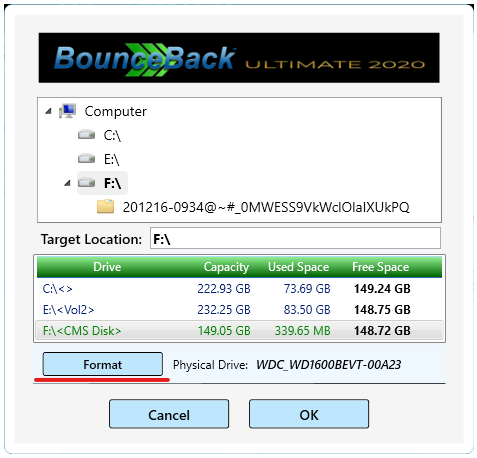


When prompted, click the **Browse** button to select a path to target for your Image backup.

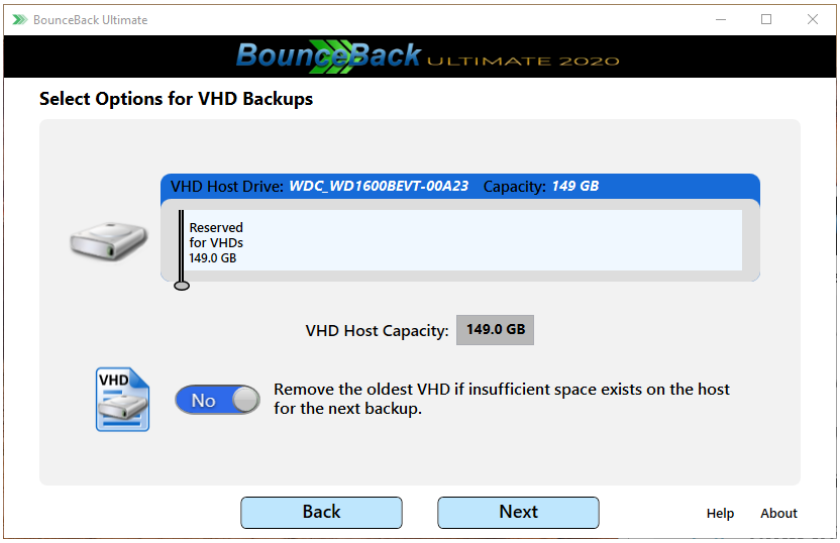


A popup will display allowing you to select the VHD host drive. You can save your Image backup VHD files to the root of the selected drive, or to a subfolder. Backing up to your system drive is not recommended. If the system crashes, you will not be able to boot from your Image backups!

IMPORTANT: Prior to creating your first VHD Image backup, click the format button. This will configure the BounceBack Ultimate to allow booting from your Image backups. You only need to perform this step once. **Formatting the drive will wipe everything from the drive.**



BounceBack will automatically determine the capacity required to backup your system. You can optionally create the VHD image larger or smaller than the recommended capacity. If you select a larger capacity, you can change partition sizes or create new ones.



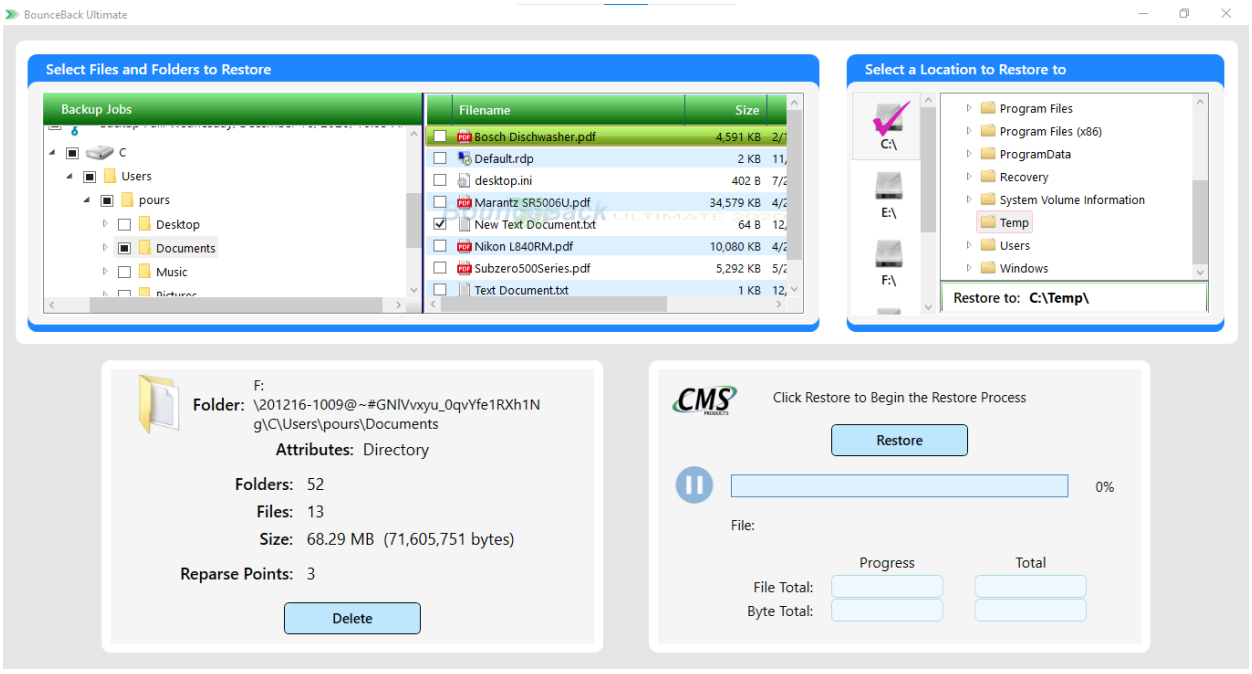
Selecting a smaller capacity will require selecting folders and files to exclude from the backup process.

Restoring Folders & Files

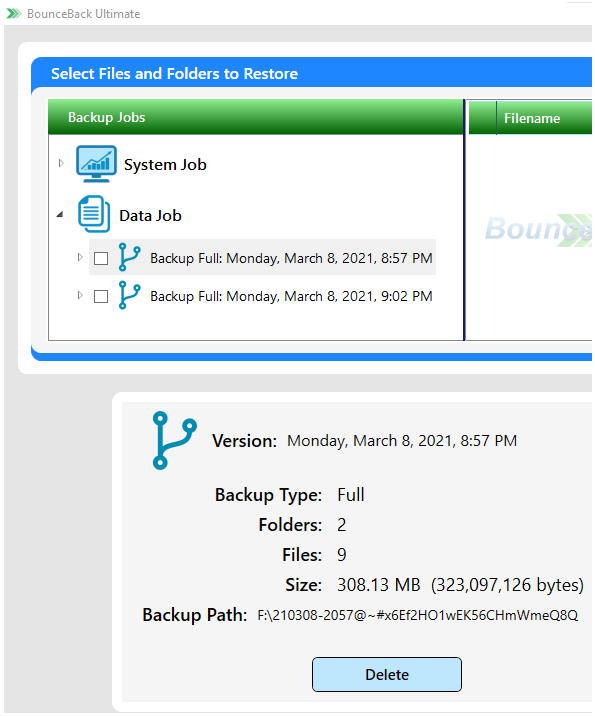
You can access or restore the data from any of your backup jobs by selecting **Access & Restore Data** from the Backup Monitor app in the system tray.

Restore from a Data-Only Backup

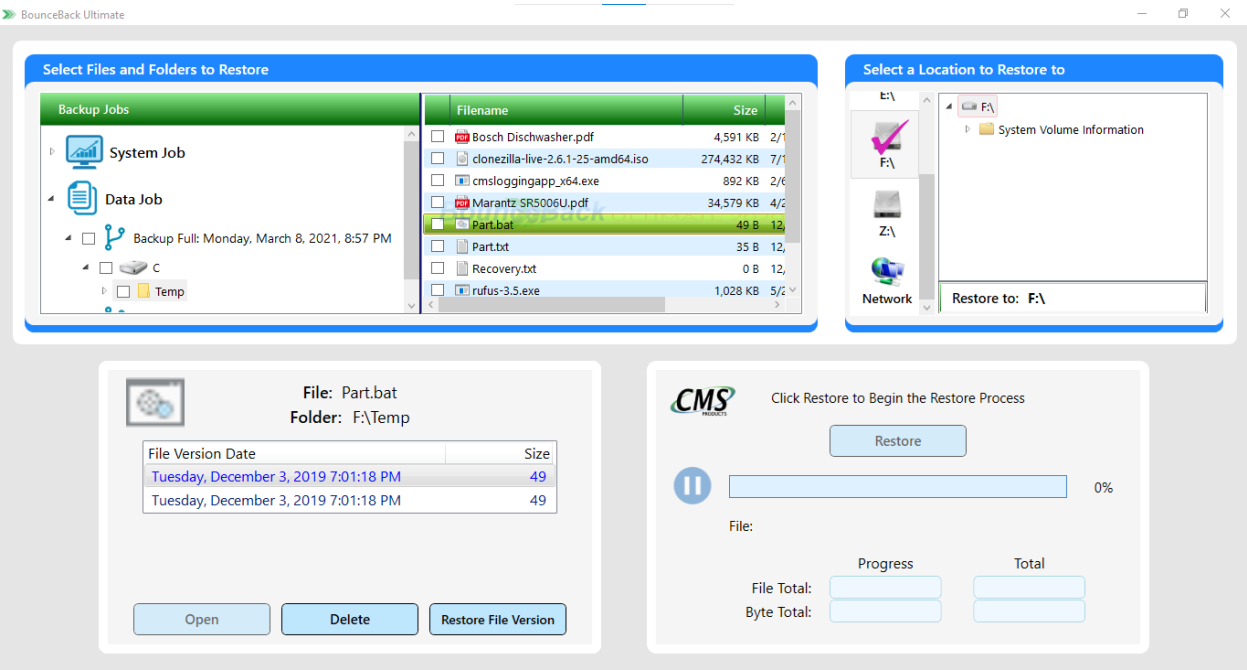
Each time you launch a data backup, BounceBack will create a version for the backup. Each version is accessible in the restore app, including both full and incremental backups. You can view or restore any file from any backup. Folders can also be restored. Clicking on the data Job node in the upper left will display information about your backup drive, plus allow you to toggle ransomware protection for the drive (if enabled).



Clicking on the version node displays version info, clicking a drive or folder node displays file totals.



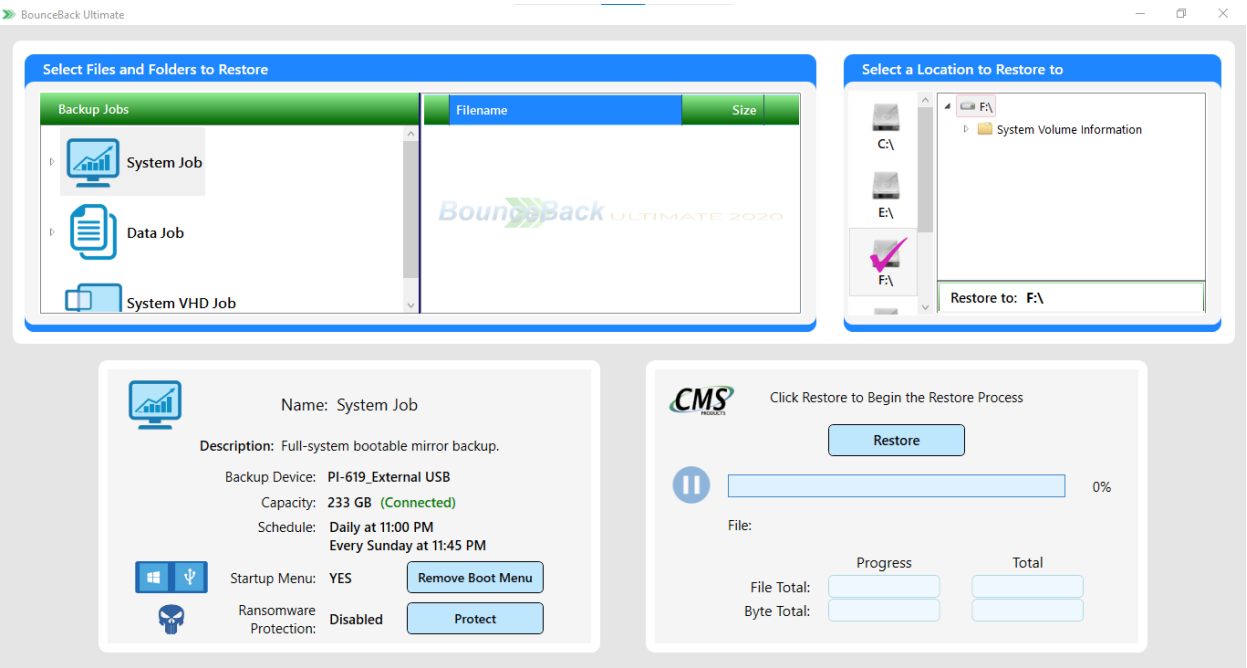
Clicking on a file displays all file versions with their backup dates in the lower left pane. Double-clicking any a version will open the file in the default app for that file type. You can also select an individual file version for restore.



After both source and target are selected, click the **Restore** button to launch the restore process.

Restore from a Full-System Backup

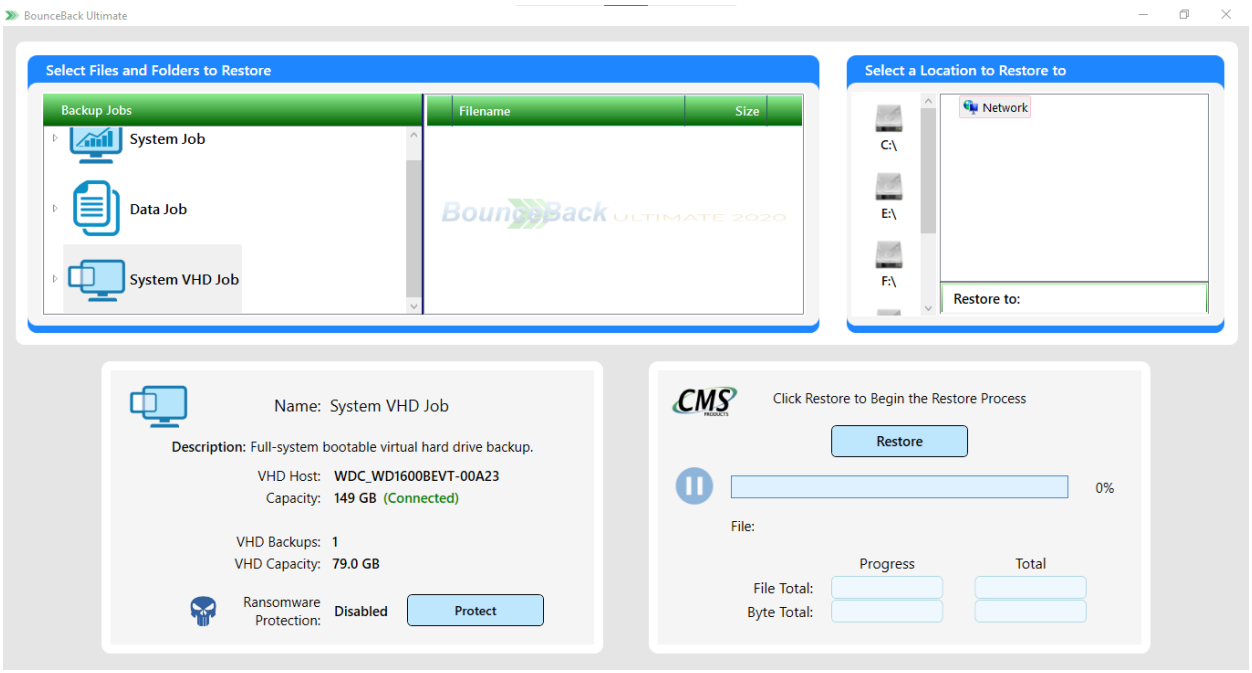
For full-system backups, you have access to all the drive letters, folders, and files on the system. You can control if the startup boot menu is enabled for the backup job. You can also manually turn ransomware protection on and off. As with data backups, folders and files can be opened for viewing, deleted, or selected for restore.



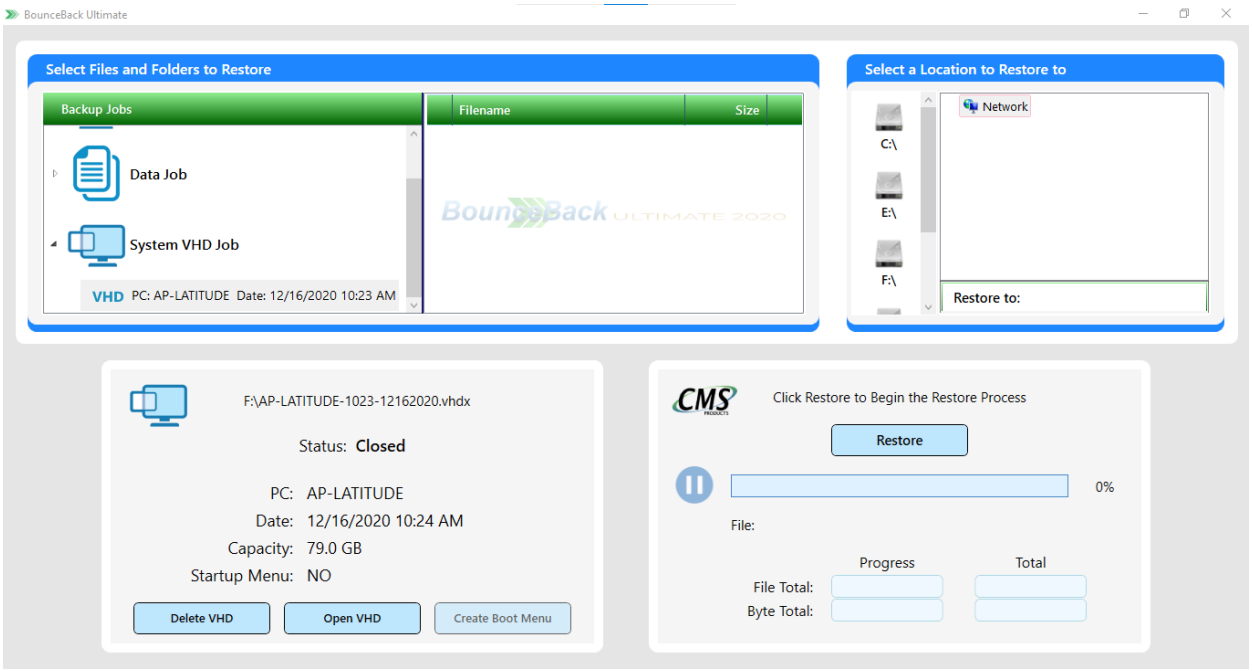
If you are using BitLocker, entering the password is required before you can access the drive.

Restore from an Image Backup

The BounceBack restore feature gives you access to all your images backups. The connection status and capacity of the host drive is displayed, along with the number and capacity of images. This is where you can manually turn ransomware protection on or off for the host drive.



Clicking an image displays the status, plus allows opening or deleting the image.



Clicking the **Open VHD** button will mount the image and assign drive letters to each volume in the full-system backup. As with data backups, folders and files can be accessed, opened for viewing, or can be selected for restore.

Image backups are basically a snapshot of your entire system at a particular date and time. Multiple images can be opened at the same time, allowing you to compare folders and files from different image backups, and from anywhere in your system.

NOTE: You will notice there is a star preceding the image name in the display above. This indicates that this image is set in the startup boot menu. BounceBack Ultimate allows you to select any image to set as the target for the startup boot menu. **This allows booting from any of your image backups!** You can run indefinitely from your backup drive as all your applications and internet connectivity are available. When booted, you are given the option of restoring your system from the booted image to your internal drive, or to other drives attached to the system. Any changes you made while running from your image are also included in the restore process. This unique feature is exclusive to BounceBack Ultimate!

Frequently Asked Questions

Is BounceBack Ultimate supported on the Windows Home Version?

BounceBack Ultimate can run from Windows Home, Professional, and Enterprise.

Is BounceBack Ultimate supported on both USB 2.0 and 3.x drives?

Yes, but USB 3.0 and above is highly recommended.

Are Windows Updates supported on the booted BounceBack Ultimate backup drive?

Yes, if you need to run from your backup drive for an extended period of time, Windows updates will occur normally. When you restore back to another drive, the restore process will include any Windows Updates that occurred when running from the backup drive.

Can I put my PC to sleep when running from BounceBack Ultimate drive?

Yes, sleep is supported. Hibernation is not supported.

What happens if I remove my backup drive while it is running?

If your backup drive is removed, your PC will freeze and allow you up to 60 seconds to reconnect the drive. After 60 seconds, the PC will shut down.

Can I see my internal drive when running from my BounceBack Ultimate backup drive?

Yes, drive letters normally assigned to the backup drive will be assigned to the internal drive.

Does BounceBack Ultimate break my Windows license agreement?

No, Windows allows you to make a single full-system backup of your PC.

Backup Strategy

How can I reliably perform both full-system and data backups to a single backup drive?

Many users will want to create both full-system and data backups, and schedule both backup types on a recurring basis. It is important to note that a full-system backup will wipe the entire contents of your backup drive prior to launching.

Data backup jobs will maintain previous versions of all your files backed up. You always have the option of performing a full backup, or an incremental backup (backup of changed files only). This applies to both full-system and data backups.

IMPORTANT: If you target your full-system backup drive for data backups, a full-system backup will wipe your BounceBack, including all data backup versions and history.

How can I work around this limitation?

Strategy #1

Use a second drive or other backup device as the target for your data backups. This can include flash drives or other USB devices. Your BounceBack Ultimate software allows you to backup data to an unlimited number of devices. This ensures that a full-system backup to your backup drive does not affect your data backups.

Strategy #2 (Windows Professional & Enterprise Only)

Create your full-system backups with the image option instead of the default mirror option. Image backups create a full-system backup in a single large file on your backup drive and will not wipe the contents of the drive. This allows you to create multiple full-system backups on your backup drive, including full-system backups from other PCs. Image backups are also bootable, and portable, just like mirror backups.

Since image backups will not wipe the contents of your backup drive, you can also store your data backups on the same drive.

Mirror Versus Image Backup

Choosing image backups will generally require a larger capacity backup drive. A 4TB backup drive can contain at least 15 full-system image backups on the average PC. BounceBack will optionally delete the oldest if there is no space available when a new backup is launched.

	FULL-SYSTEM MIRROR BACKUP 	IMAGE BACKUP 
Backup drive is Bootable	✓	✓
Supports All Windows Versions	✓	✗
BitLocker Full-Disk Encryption	✓	✗
Supports Multiple Bootable Backups	✗	✓
Supports Bootable Backups of Other PCs	✗	✓
Supports Scheduling Full-System Backups	✓	✓
Supports Scheduling Incremental Backups	✓	✗
Drive Can Contain Other Non-Backup Data	✗	✓
Backup Drive Can Replace the Internal Drive	✓	✗

Notes: Image backup is only supported on Windows Professional and Enterprise versions, while mirror backups support the Windows Home version. BitLocker does not support Windows Home. Image backups do not currently support incremental backups. An image host drive can replace your internal drive, but the format is converted to the virtual drive structure supported by VHDs.

Troubleshooting

How do I boot from My BounceBack backup drive?

Two Methods for Starting from your Backup Drive

1. **The Startup Boot Menu** - You can select to create a startup menu that displays each time you restart your PC. To do this, you need to select the boot menu option prior to creating your first full-system backup. The default for this option is ON when creating your first full-system backup.
2. **The BIOS Boot Menu** – All PCs have a hot-key to access BIOS options. By pressing the BIOS hot-key before your system starts, you can select to start from your backup drive. See below for the hot-keys for various PC manufacturers. If you see two items in the BIOS drive list for your backup drive, the UEFI option is usually correct for newer PCs.

Both mirror and VHD image backups can start with either method. For Image backups, you can select which VHD file you would like to start from.

What should I do if the backup drive will not boot?

Try both booting methods. If the drive fails to startup correctly when using the startup boot menu, try again from the BIOS boot menu.

Check your BIOS settings to ensure booting from USB drives is not blocked. Windows 7 PCs will often require additional changes to BIOS settings.

It is possible that the backup process failed. Perform another full-system backup, then try again to boot the backup drive.

BIOS Settings

When starting some PCs, it may be necessary to press CTL-ALT-DEL if the boot menu does not initially display your backup drive.

A small percentage of PCs may require a BIOS setting change to enable USB boot, especially on Windows 7. These BIOS changes could include:

BIOS Values

Post Settings:	Thorough
Enabled External Device Boot:	Enabled
Quick Boot:	Disabled
Diagnostic Mode:	Enabled

Computer Manufacturer	Type	Model	Boot Menu Key	BIOS Key
ACER			Esc, F12, F9	Del, F2
ACER	netbook	AspireOne, Aspire Timeline	F12	F2
ACER	netbook	Aspire v3, v5, v7	F12	F2
APPLE		After 2006	Option	
ASUS	desktop		F8	F9
ASUS	laptop		Esc	F9
ASUS	laptop	R503C	F8	DEL
ASUS	netbook	Eee PC 1025c	Esc	F2
COMPAQ		Presario	Esc, F9	F10
DELL	desktop	Dimension, Inspiron, Latitude	F12	F2
DELL	desktop	Inspiron One 2020, 2305, 2320, 2330 All-In-One	F12	F2
DELL	laptop	Inspiron	F12	F2
DELL	laptop	Precision	F12	F12
EMACHINES			F12	Tab, Del
GATEWAY			F11, Esc, F10	F2, Del
HP	generic		Esc, F9	Esc, F10, F1
HP	desktop	Media Center	Esc	F10
HP	desktop	Pavilion 23 All In One	Esc	F10
HP	desktop	Pavilion g6 and g7	Esc	F10
HP	desktop	Pavilion HPE PC, h8-1287c	Esc	Esc F10
HP	desktop	Pavilion PC, p6 2317c	Esc	Esc F10
HP	desktop	Pavilion PC, p7 1297cb	Esc	Esc F10
HP	desktop	TouchSmart 520 PC	Esc	Esc F10
HP	laptop	2000	Esc	Esc
HP	notebook	Pavilion	Esc	F10
HP	notebook	ENVY dv6 and dv7 PC	Esc	Esc
INTEL			F10	
LENOVO	desktop		F12, F8, F10	F1, F2
LENOVO	laptop		F12	F1, F2
LENOVO	laptop	IdeaPad P500	F12 or Fn + F11	F2
NEC			F5	F2
PACKARD BELL			F8	F1, Del
SAMSUNG			F12, Esc	
SAMSUNG	netbook	NC10	Esc	F2
SAMSUNG	ultrabook	Series 5 Ultra and Series 7 Chronos	Esc	F2
SHARP				F2
SONY		VAIO, PCG, VGN	F11	F1, F2, F3
SONY		VGN Esc	F10	F2
TOSHIBA		Protege, Satellite, Tecra	F12	F1, Esc
TOSHIBA		Equium F12	F12	F12

Prevent Virus Protection from Interfering with BounceBack

Your virus protection can block or interfere with the operation of the BounceBack Ultimate software. This can result in slow backups or the software crashing. It is a good idea to create antivirus exclusions for BounceBack even if you do not have these issues. BounceBack Ultimate will automatically create an exclusion for Windows Defender. The following folders need to be excluded for BounceBack.

For 32-bit systems:

C:\Program Files\CMS Products\BounceBack Ultimate

For 64-bit systems:

C:\Program Files\CMS Products\BounceBack Ultimate\x64

If you are unsure if you have a 32 or 64-bit system, exclude both. Some anti-viruses may require you to exclude individual processes. If so, these files should be excluded in the folders above:

BackupServer.exe

BackupSettings.exe

BackupMonitor.exe

ScheduleLauncher.exe

PasswordPrompt.exe (if you are using BitLocker)

Here are links to popular antivirus websites with instructions on creating exclusions:

Bitdefender
https://www.bitdefender.com/consumer/support/answer/13427/

NortonLifeLock
https://support.norton.com/sp/en/us/home/current/solutions/v36687854

PCMatic
https://forums.pcmatic.com/topic/203530-manually-adding-a-programservice-to-whitelist/

Avast
https://support.avast.com/en-us/article/Antivirus-scan-exclusions/

AVG
https://support.avg.com/answers?id=906b00000008tbFAAQ

Kasperski
https://support.kaspersky.com/11481#block2

Total AV
https://support.totalav.com/en/kb/article/148/how-can-i-exclude-certain-files-or-folder-paths-from-scanning

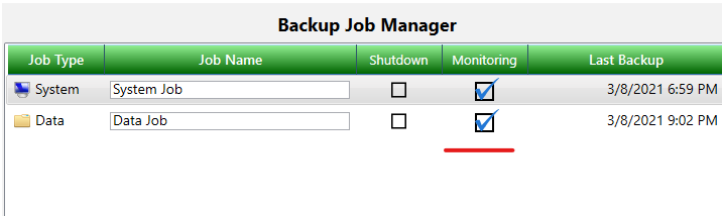
McAfee
https://service.mcafee.com/webcenter/portal/cp/home/articleview?locale=en-US&articleId=TS102056

For other antivirus solutions, see here:
https://www.scrapersnbots.com/software/troubleshooting/how-to-whitelist-software-in-antivirus-anti-virus-deletes-files-false-flagging.php

My PC is Running Slow

When you create a full-system mirror backup, the BounceBack Ultimate backup monitor will run continuously. This allows the software to track any changed files in the background. Since it is monitoring your entire system including the OS, this can become quite a busy task. This is complicated when antivirus or other applications continuously change logs or temporary files in the background. BounceBack Ultimate has identified and excluded many of these paths by default. It is possible that some of your applications are making these types of changes, which in turn causes your system to slowdown during the monitoring process. There are two methods to resolve this issue.

1. **Disable Backup Monitoring** – Choosing this option will cause BounceBack to not track file changes for a backup job. This results in losing the ability to perform incremental backups for that job. Many users may not need this option if they always perform full-system or full-data backups.



2. **Add Offending Paths to the Watcher Exclusion List –** For advanced users, BounceBack maintains a list of paths excluded from monitoring for incremental backups. This applies only to full-system backups. Paths to frequently changing folders such as browser temp and system cache folders are automatically excluded from incremental backups. You can determine which files and folders are causing issues by launching the following application: **C:\Program Files\CMS Products\BounceBack Ultimate\x64\WatcherExcluder.exe**

The items in the top panel are items that are frequently changing and being flagged for backup on your system. The items in the lower panel have been previously identified for exclusion from the background watcher and from your incremental backups. You can see the frequency of changed items in the upper panel, so you can add the worst offending items for exclusion below by clicking the checkbox, then clicking **Add Paths**. Make sure these are items that you do not want included during incremental backups. Also keep in mind that these items are not excluded during your full-system backups.

You can remove paths from the excluded list by selecting them, then clicking the **Remove Paths** button. Clicking the Reset Default button will reset to the original defaults created during the BounceBack installation.

NOTE: The preceding does not apply to image backups since incremental backups are not supported with image backups.