



Hard Disk Manager 18

Quick Start Guide



Paragon Technologie GmbH
Software Development Company
Leo-Wohleb-Straße 8
79098 Freiburg, Germany

Contacts

Tel. +49 (0) 761 59018201
Fax +49 (0) 761 59018130
www.paragon-software.com

CONTENTS

- 1. Introduction 3
 - 1.1 About Quick Start Guide 3
- 2. About The Program 4
 - 2.1 Overview 4
 - 2.2 System Requirements 4
 - 2.3 Pre-Installation Checklist 4
- 3. Installation and First Start 5
 - 3.1 Setup Wizard 5
 - 3.2 First Start 6
 - 3.3 Screen Elements 9
- 4. Essential Preparation 11
 - 4.1 Create Recovery Media 11
- 5. Key Features 13
 - 5.1 Backup 13
 - 5.1.1 Backup Overview 13
 - 5.1.2 Local Backup 14
 - 5.1.3 Backup To Cloud 19
 - 5.1.3.1 S3 Compatible 20
 - 5.1.3.2 Azure 21
 - 5.2 Recovery 25
 - 5.2.1 Recovery Overview 25
 - 5.2.2 Bare-Metal Recovery 26
 - 5.2.3 Import Backups 37
 - 5.2.4 Recover Individual Files and Folders 40
 - 5.3 Disk and Partition Management 44
- 6. Notifications and Reports 45
- 7. Support and Legal Notices 53
 - 7.1 Support 53
 - 7.2 Copyright and Legal Notices 54

1. INTRODUCTION

1.1 About Quick Start Guide

This Quick Start Guide is intended to ensure a smooth introduction to using Hard Disk Manager and contains brief descriptions of the key program features.

For a detailed description of all program features, refer to the User Manual.

2. ABOUT THE PROGRAM

2.1 Overview

Hard Disk Manager is the ultimate tool for keeping hard disks and personal data safe. The solution is designed to tackle common and advanced problems you might face while using a PC. Hard Disk Manager version raises the bar for data and system portability and delivers advanced control over disks, partitions, volumes, and file system structures.

2.2 System Requirements

- **Processor:** 1 GHz or faster 64-bit (x64 or Arm64) processor
- **Memory:** 4 GB+ RAM
- **Operating System:** Windows 11 Arm64 editions, Windows 10 x64 (1809 and newer), Windows 11 x64; for server versions: x64 Windows Servers 2016, 2019, 2022, 2025
- **Network:** Firewall ports to be opened: Inbound and Outbound TCP 80, 443
- **Peripherals:** Keyboard and mouse

During the installation, 1.2 GB of available disk space is required.

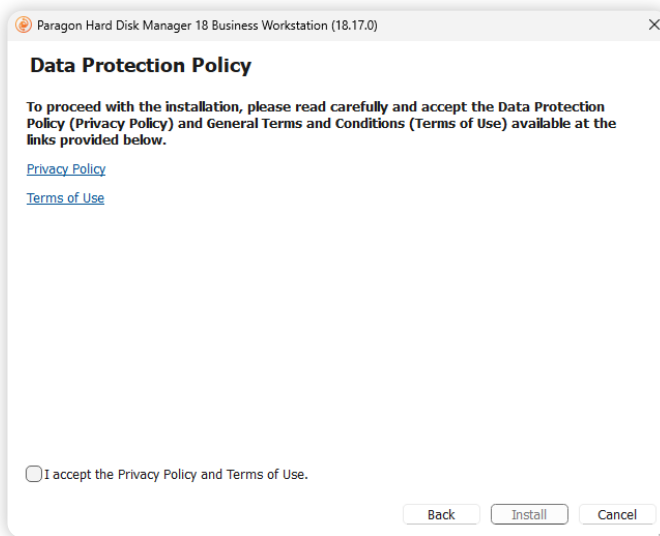
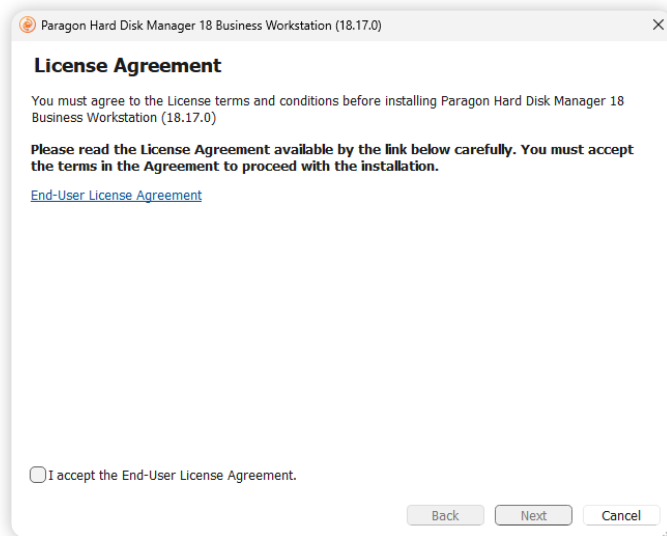
2.3 Pre-Installation Checklist

- **Admin Rights:** Verify you have local administrative privileges before starting.
- **Prior Versions:** Completely uninstall any older versions of the program.

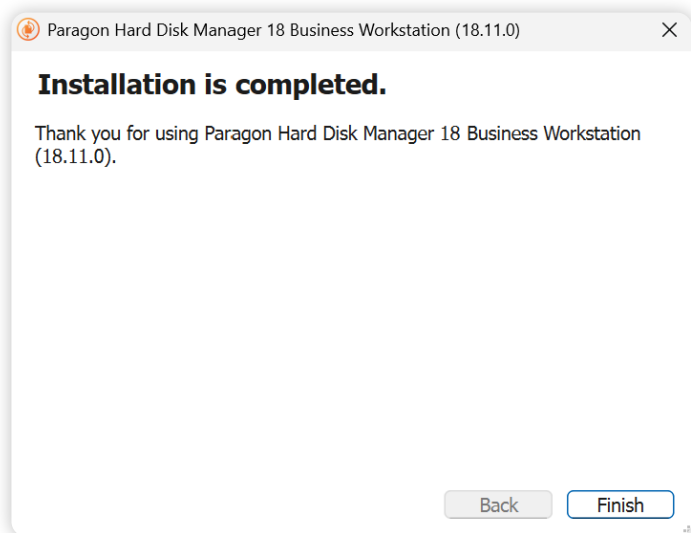
3. INSTALLATION AND FIRST START

3.1 Setup Wizard

1. Double-click the installation file to start.
2. Please read the **License Agreement for Paragon Software Products** as well as the **Privacy Policy** and the **Terms of Use** carefully and agree to them in order to proceed with the installation.



3. The final page indicates the completion of the installation process. Click **Finish** to close the Wizard.

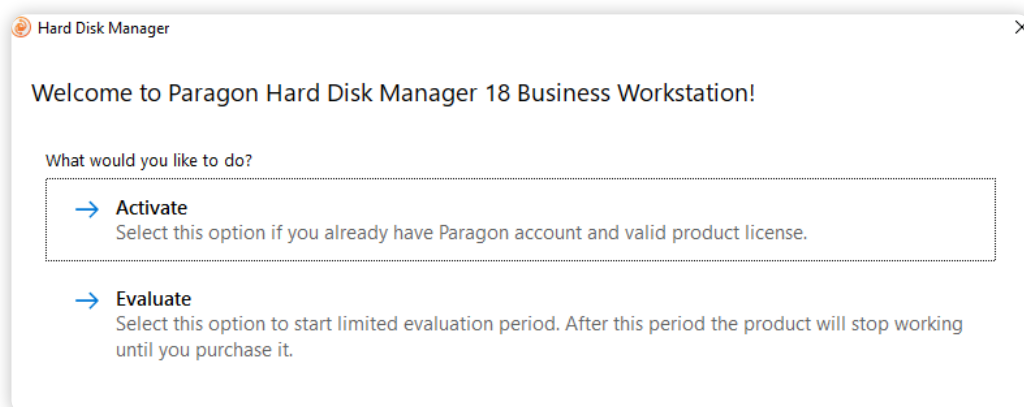


3.2 First Start

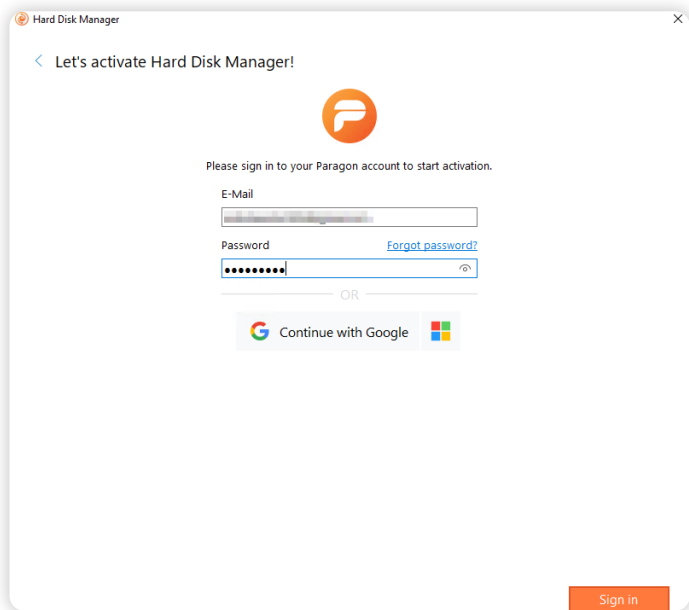
Once you have installed the program, the Hard Disk Manager icon will appear on your desktop:



1. Double-click the icon to launch the program. A welcome window will appear.
2. Proceed as follows:
 - If you have a valid Paragon account, select **Activate** and use the credentials that you have received by e-mail from your software vendor.



Sign in to your Paragon account to activate your license. Use the e-mail that you specified during the purchasing process and the password that you created when confirming your email. Click **Sign in**.



Hard Disk Manager

< Let's activate Hard Disk Manager!



Please sign in to your Paragon account to start activation.

E-Mail

Password [Forgot password?](#)

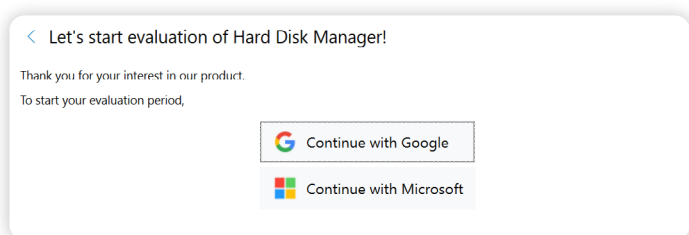
OR

 Continue with Google 

Sign in

Depending on your purchase method, you might need to visit the [Paragon Licensing center](#), create an account, and enter the coupon serial number in order to register your product. Detailed instructions will be provided by our sales department by email after the purchase.

- If you have downloaded the trial version, select **Evaluate** and use your own credentials to start the evaluation period. Use your Google or Microsoft credentials to continue.



< Let's start evaluation of Hard Disk Manager!

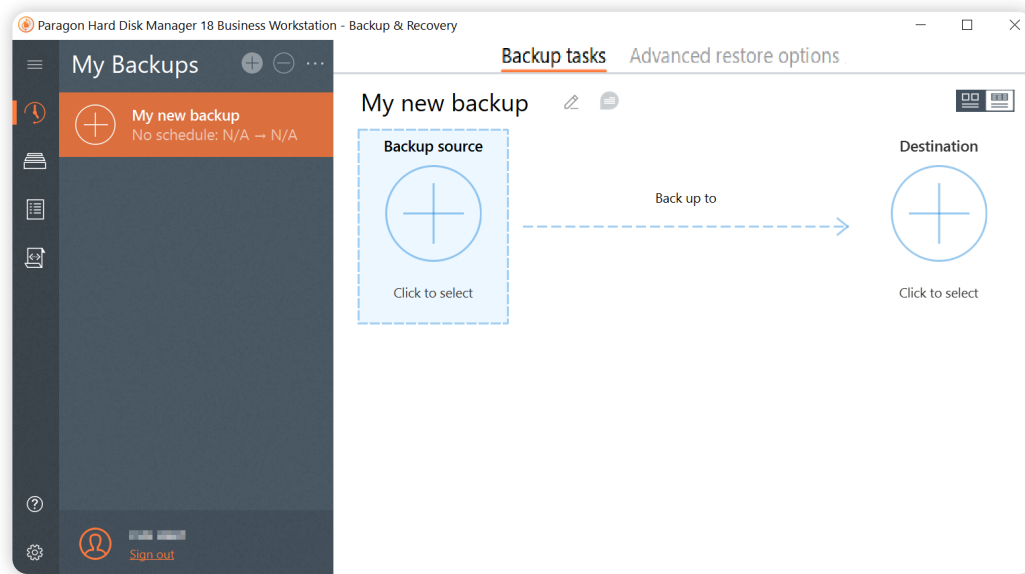
Thank you for your interest in our product.
To start your evaluation period,

 Continue with Google

 Continue with Microsoft

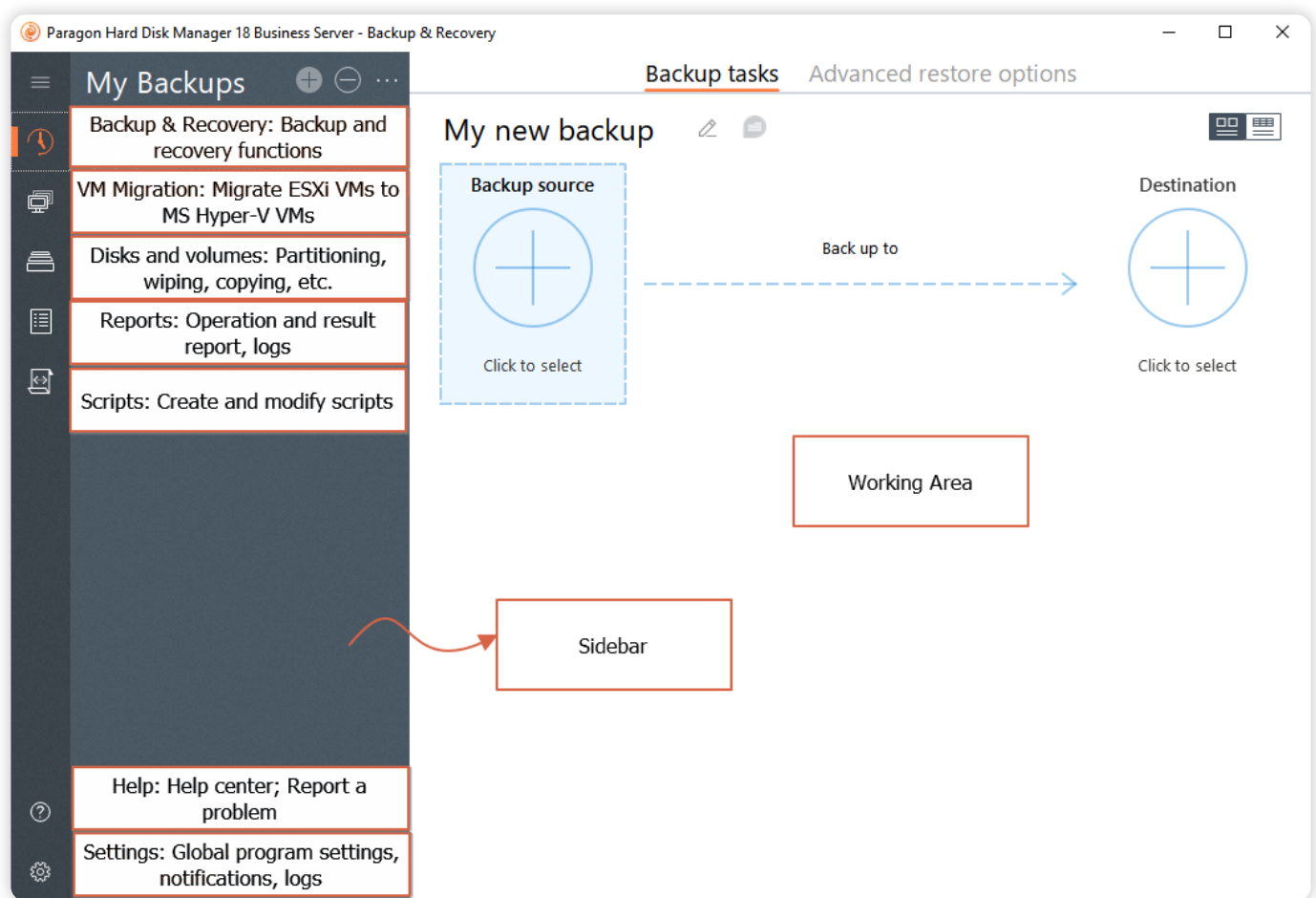
Hard Disk Manager doesn't access or store your password locally. Authentication happens entirely on Paragon's secure servers.

3. The main program window will open. You can now use all the features of the program.



3.3 Screen Elements

Main User Interface Elements



Some features might be missing depending on your specific product edition.

Paragon Hard Disk Manager 18 Business Server contains all available features, while other editions have fewer options. Please note that this information describes the current state of the product and may change in the future.

The main interface window contains the following elements:

- **Sidebar:** Provides quick access to the various features of the program.
- **Working area:** Displays the main content, tools, and controls for the currently selected feature.

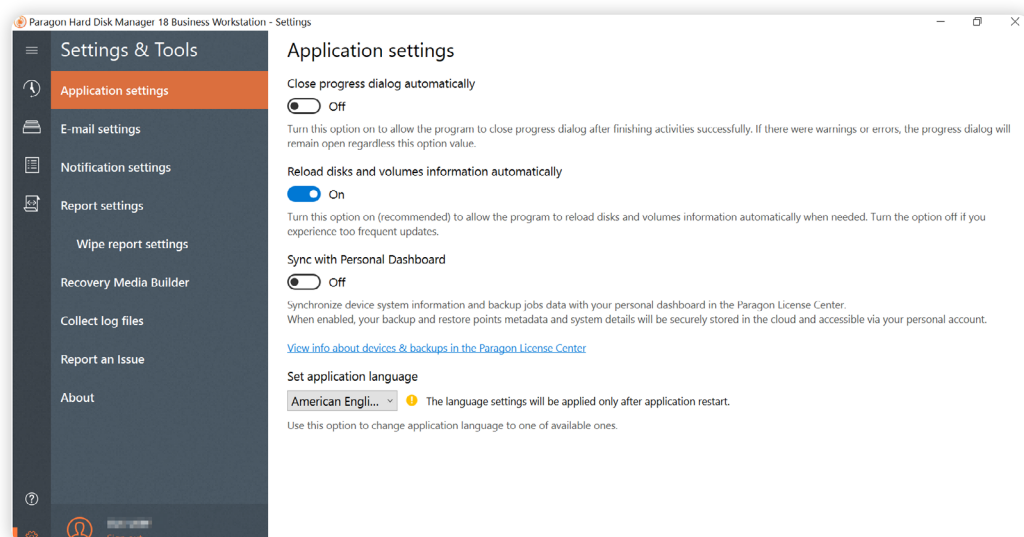
Additional User Interface Elements

The following icons are available next to the section title at the top:

+	Add	Add a new entry (Backup & Recovery, VM Migration, Scripts tabs)
—	Remove	Remove the selected entry. You will be prompted to delete either the database record only or all associated backups and scripts.
...	More actions	Backup & Recovery tab: Restore from PBF, Import backup Disks and volumes tab: Connect virtual disk, Find and copy OS, Copy files and folders, Refresh

Settings

The bottom of the sidebar features the **Settings**  menu for configuring application parameters.



4. ESSENTIAL PREPARATION

4.1 Create Recovery Media

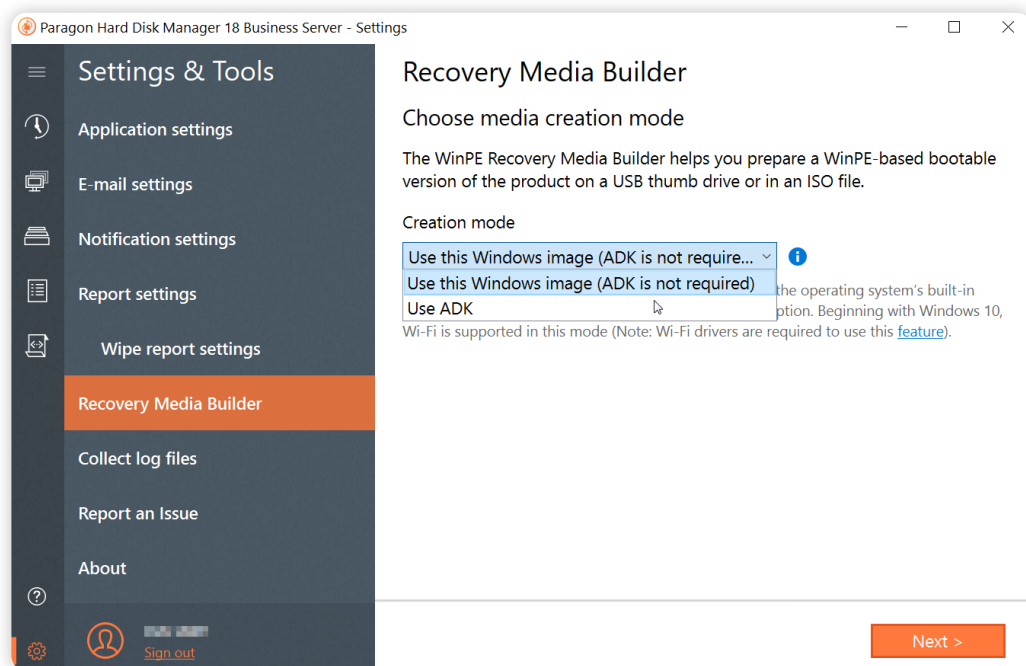
Recovery media is essential for recovering your computer, restoring your data from backups, and fixing system errors if your Windows operating system fails to boot.

Hard Disk Manager builds its recovery media on top of the Microsoft Windows Preinstallation Environment (WinPE). Since our software integrates directly into this Microsoft-provided base, the overall capabilities and performance of the recovery environment depend entirely on the specific WinPE version used.

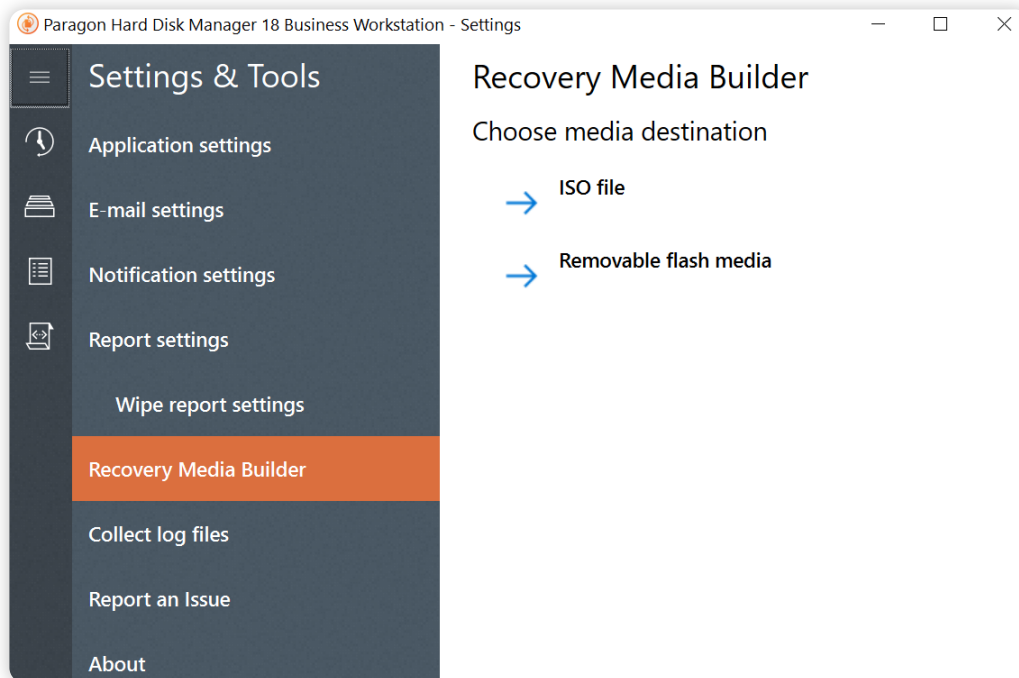
To open the step-by-step creation wizard, go to the sidebar and select **Settings** ⚙️ > **Recovery Media Builder**.

Please note the following when working with the wizard:

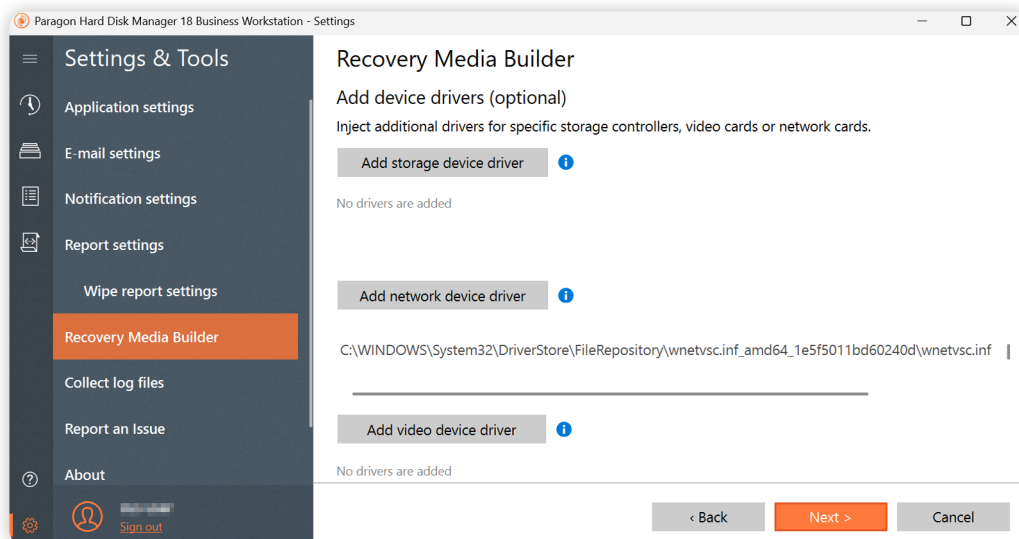
- **Windows ADK Requirements:** Installing the Windows Assessment and Deployment Kit (ADK) is optional. The wizard can automatically build the rescue environment using the local WIM image from the system's Windows Recovery Environment (WinRE). However, if the local WIM image is missing, if you intend to create an ISO file, or if you prefer a newer WinPE system as your base, select the **Use ADK** option.



- **Output formats:** The recovery media can be written directly to a **Removable flash media** or saved as an **ISO file** (for later burning to a CD/DVD).



- **Wi-Fi support:** To access Wi-Fi networks within the recovery environment, you must run Windows 10 or 11 and select the **Use this Windows image (ADK is not required)** option.
- **Advanced customization:** You can customize your recovery media during creation by adding hardware drivers, configuring network profiles, and mapping network drives.



For more information on the rescue media, refer to our [Knowledge base](#).

5. KEY FEATURES

5.1 Backup

5.1.1 Backup Overview

A backup is an image (compressed backup archive) of individual files, specific volumes, or an entire hard drive. It is created and stored on an independent medium to ensure quick recovery in the event of data loss, corruption, or system failure.

Supported Backup Scenarios

- **System Protection:** Creating a full system backup to ensure quick recovery after a crash or virus infection.
- **Bare-Metal Preparation:** Generating a comprehensive disk archive to deploy your entire environment onto a blank drive.
- **Migration Planning:** Cloning or backing up your current hard drive to easily move the system to a larger or new disk.

Backup Execution Methods

- **On-Demand (Manual) Backup:** You start the backup process manually before performing risky system updates or partitioning operations.
- **Scheduled (Automated) Backup:** The program runs automatically as a background system service according to your predefined daily, weekly, or monthly plan.

Available Backup Options

Depending on what you want to protect, you can choose from various backup sources:

- **Entire Computer:** The program copies everything, including your operating system, programs, settings, and all connected hard drives.
- **Disks and Volumes:** You can choose to back up only specific hard drives or separate partitions to save storage space.
- **Files and Folders:** You can select only specific files or folders to protect your active work documents.
- **Hyper-V Backup:** You can back up the selected virtual machine along with its configurations, checkpoints, and virtual hard disks.

Backup Synchronization

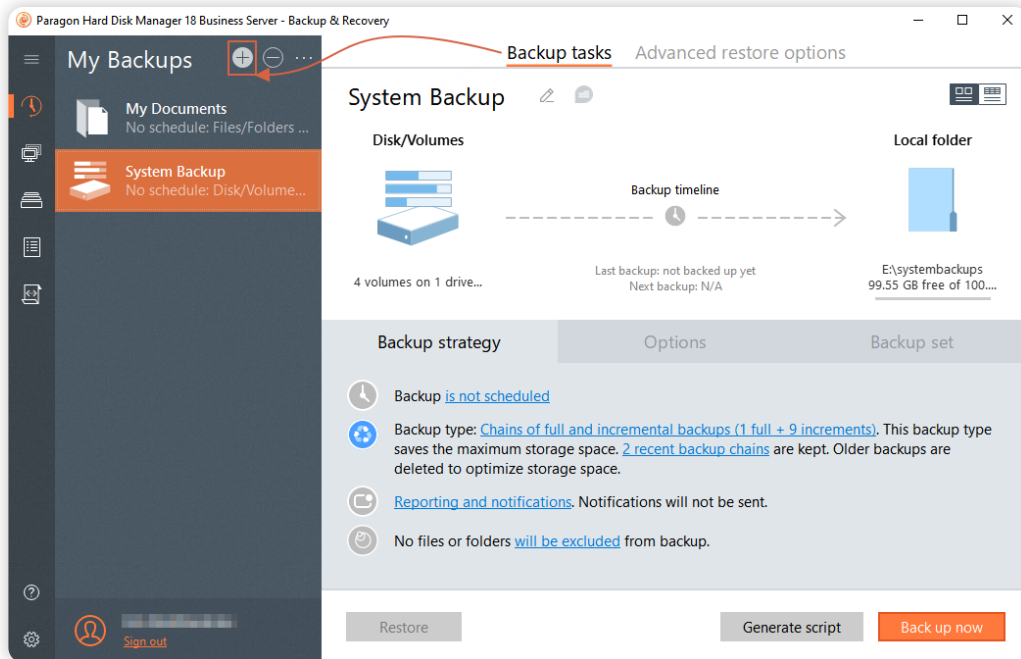
You can synchronize device system information and backup jobs data with your personal dashboard in the Paragon Licensing Center. Your backup and restore points metadata and system details will be securely stored in the cloud and accessible via your personal account.

5.1.2 Local Backup

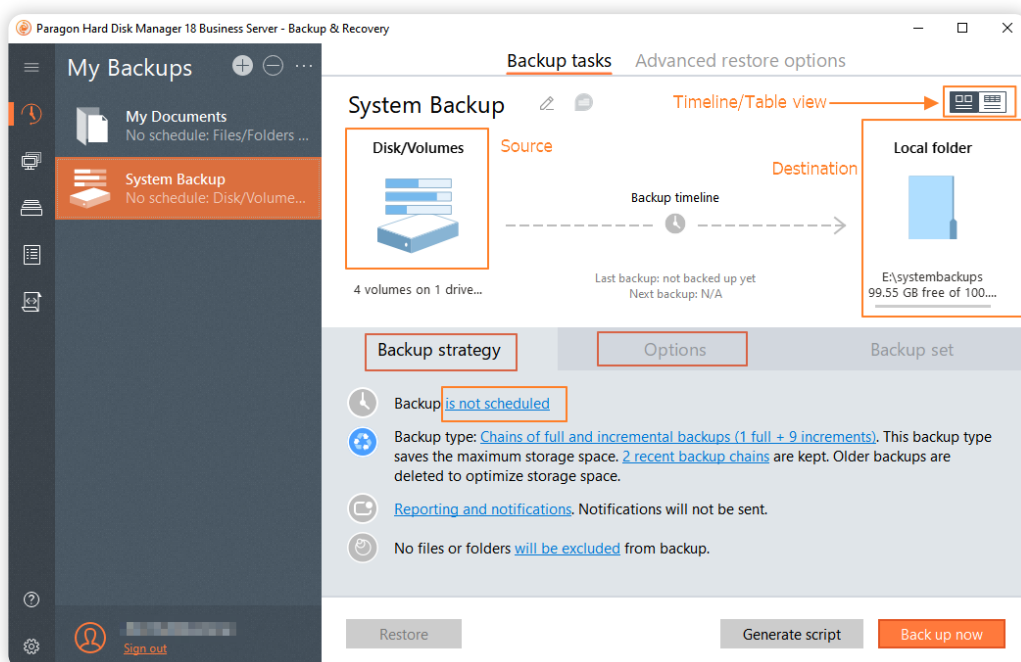
Backup Logic

Every single backup created by a backup task is saved as an individual restore point.

If your backup tasks require different source data, target destinations, or custom settings, use the + button to set up a separate backup job for each configuration.



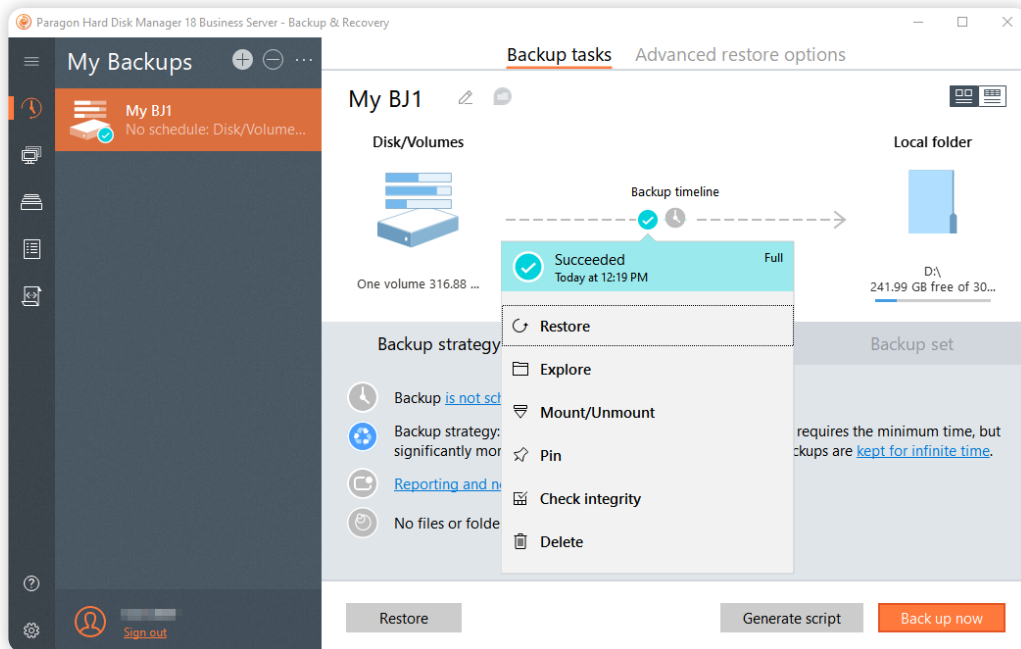
A standard backup job contains your selected source and target, execution schedule, backup type, and cleanup (retention) settings. For further customization, navigate to **Options** to configure password protection, container file format, compression levels, and other advanced parameters.



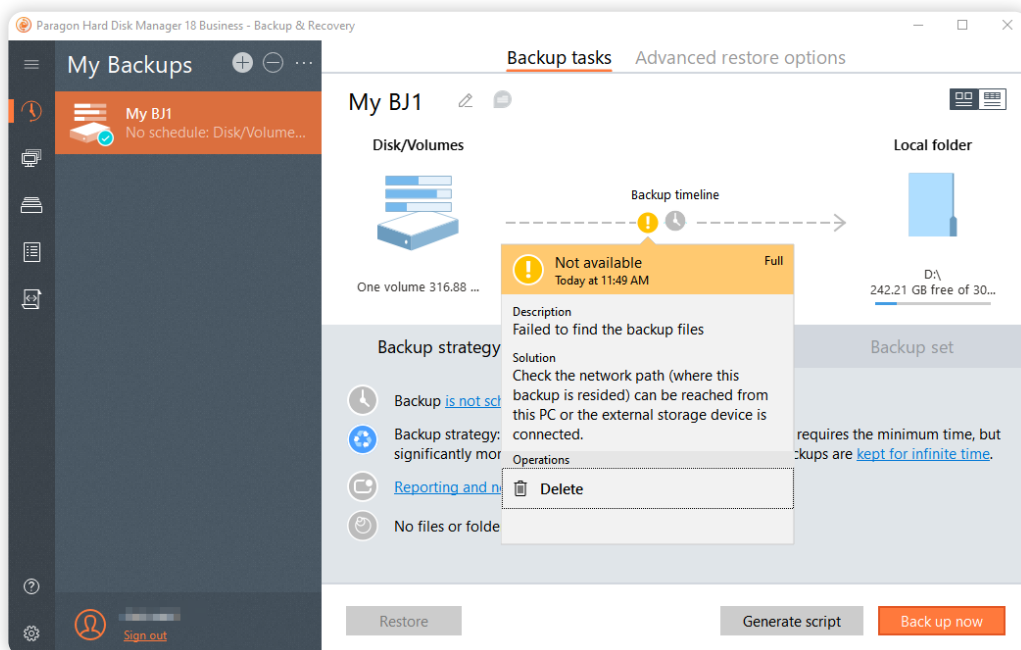
Backup Management and Restore Points

All backup jobs are managed and tracked through the archive database. Each completed backup is recorded as a restore point on the timeline, color-coded as follows:

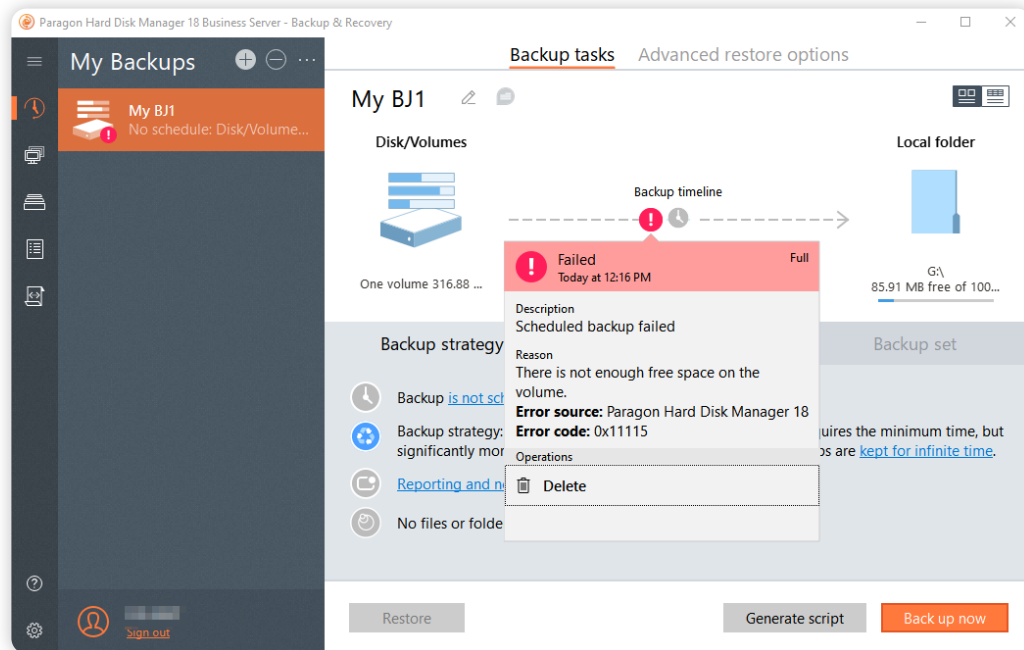
- **Turquoise line:** The restore point is intact, verified, and ready for recovery.



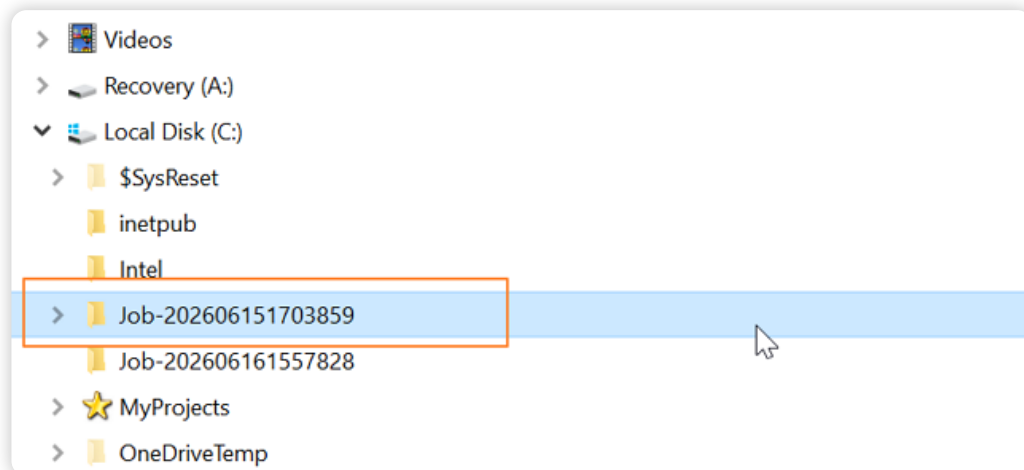
- **Yellow line:** The restore point is currently inaccessible (e.g., the external drive is disconnected or missing a drive letter).



- **Red line:** An error occurred during the backup process. Point to the line to view the specific error message.



The backup job stores all results in a single directory (including any subdirectories) on the selected target drive.



Create a Backup Job

To set up a scheduled or one-time backup, follow these steps:

1. On the sidebar, go to **Backup & Recovery** section.
2. Click **+** to start a new backup or continue with the currently open job template.
3. Configure the backup parameters: **Backup Source** and **Destination**.

Please note that these parameters are mandatory. If they are not specified, the backup job cannot be started, and creating an additional backup template will be unavailable.

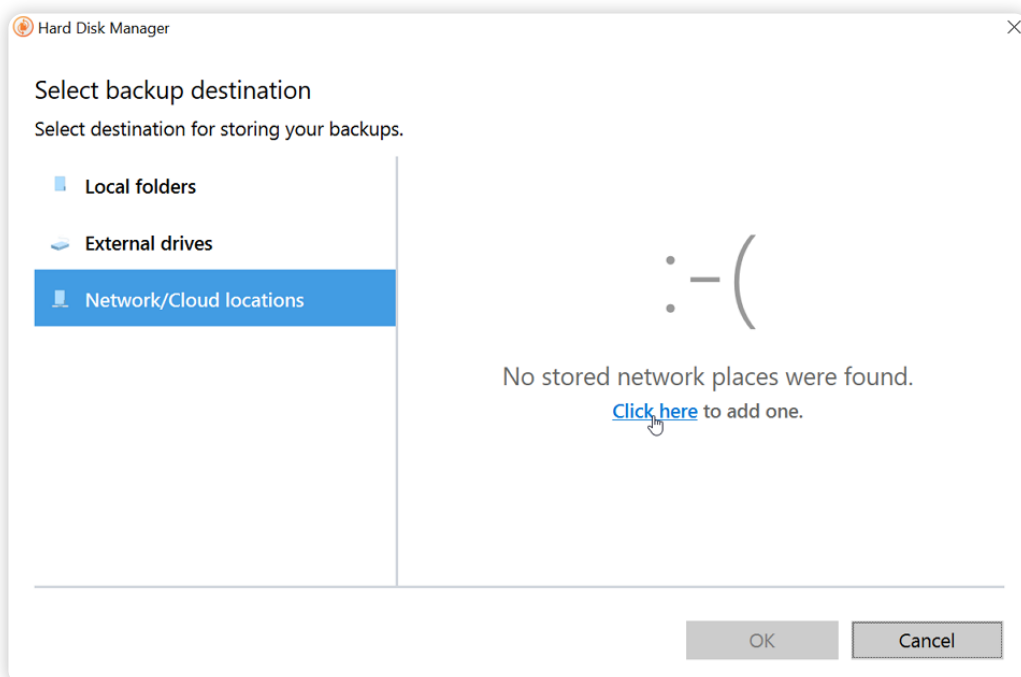
4. Customize the default properties in the **Backup Strategy** and **Options** sections.

Any subsequent modifications or additional settings are updated instantly without the need to click the **Save** button. If you accidentally close the application before specifying both the source and destination, your draft will be preserved and will automatically reload upon the next application launch.

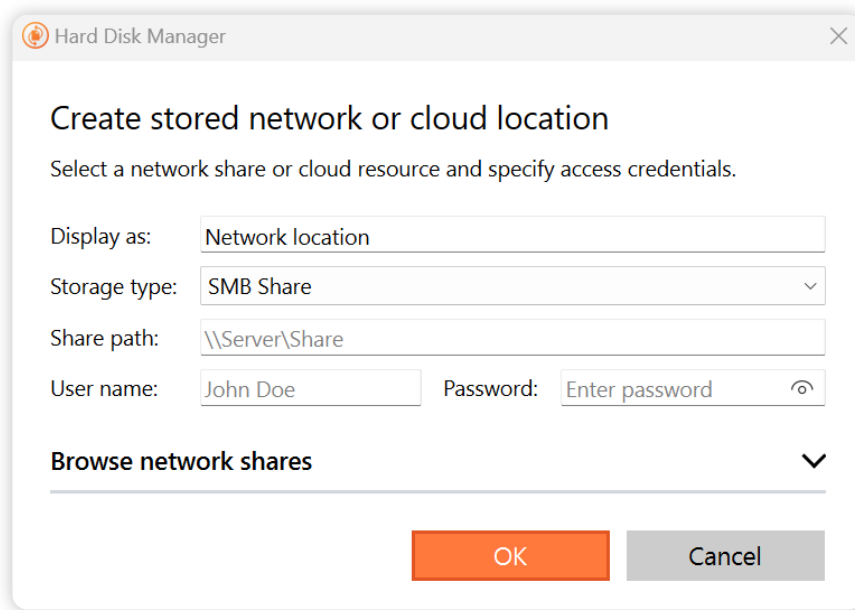
Configure Backup to SMB Share

If you want to store your backups to SMB shares, Paragon Hard Disk Manager allows users to securely backup files and folders over the network.

1. On the sidebar, go to **Backup & Recovery**.
2. Select the backup job or create a new one.
3. Click on the **Destination** menu. The **Select backup destination** window will open.
4. Select **Network/Cloud locations**. In the right part of the opened window, click on the **Click here** link to add a network location.



5. In the window that opens, configure the following parameters:



Hard Disk Manager

Create stored network or cloud location

Select a network share or cloud resource and specify access credentials.

Display as:

Storage type:

Share path:

User name: Password:

Browse network shares

- **Display as:** Specify the desired network location name.
- **Storage type:** Select **SMB Share** from the list with available options (**SMB Share**, **Amazon S3 Compatible**, **Azure**).
- **Share path:** Specify the path to the location where you want to store your backups.

Do not map the SMB share as a network drive letter (e.g., Z:\). The Hard Disk Manager backup service often runs under a separate Windows user account. Since mapped drive letters are unique to each user profile, the backup process will not be able to detect or access the drive, causing the backup task to fail. Instead, specify the storage destination using a direct network path (e.g., \\ServerName\ShareName)

- **User name** and **Password:** Specify your access credentials.

Click on the arrow to the right of the **Browse network shares** menu to view the available network paths and shared folders. To collapse this menu, click **Hide network shares browser**.

6. Click **OK** to apply your changes.

5.1.3 Backup To Cloud

The cloud storage integration feature allows you to store your Hard Disk Manager backups of entire disks, individual volumes/partitions, and specific files or folders directly in cloud object storage.

Supported Cloud Services

- **Public Cloud Providers:** Azure Blob Storage, Amazon S3, Wasabi, and other S3-compatible services.
- **Private Cloud Storage:** In-house S3-compatible systems.

Data Security and Reliability

Both Azure and S3-compatible protocols automatically verify data integrity during upload and download. This ensures your backups remain safe, complete, and protected against data corruption.

Limitations

- **Azure User Delegation SAS Authorization:** Not supported (designed for short-term interactions and is unsuitable for long-term backup operations).
- **Microsoft Entra ID Authorization:** Currently not supported. Compatibility is under development for future releases.

Important Considerations

Ensure your computer's clock is accurately synced before using S3 and Azure. Any time zone is acceptable, but the absolute offset must be under 10 minutes.

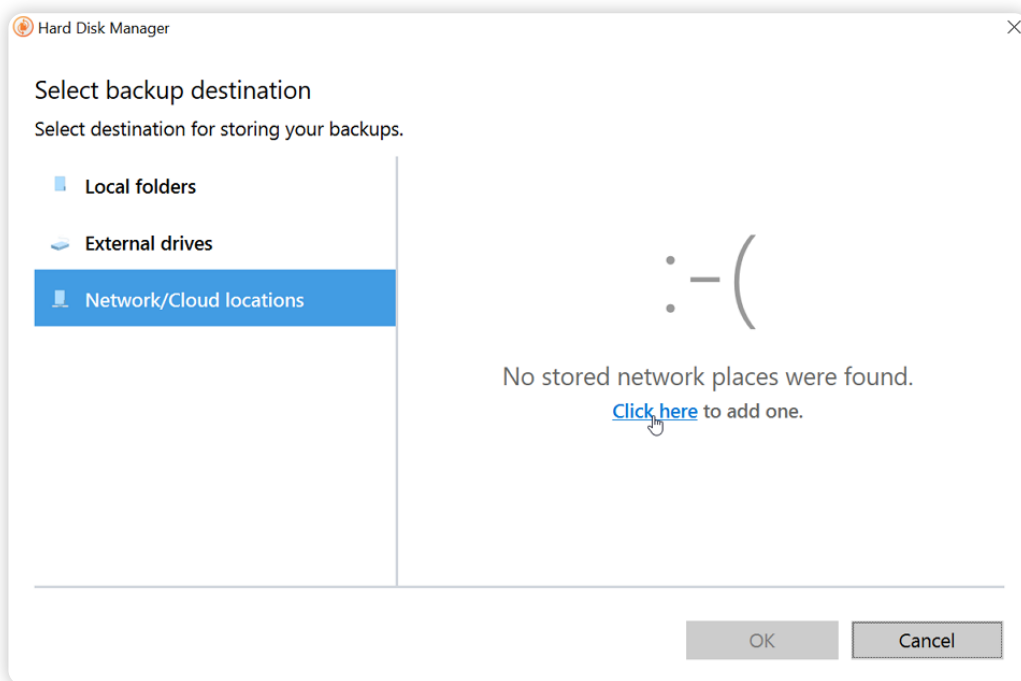
Recommended Settings

We recommend enabling backup encryption (password protection) and selecting the optimal compression level in the backup job settings.

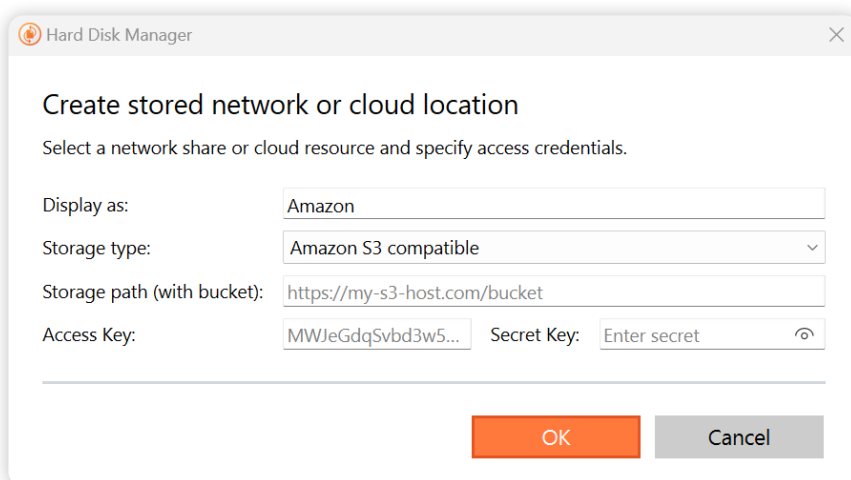
5.1.3.1 S3 Compatible

Configure Cloud Storage

1. On the sidebar, go to **Backup & Recovery**.
2. Select the backup or create a new one.
3. Click on the **Destination** menu. The **Select backup destination** window will open.
4. Select **Network/Cloud locations**. In the right part of the opened window, click on the **Click here** link to add a network or cloud location.



5. In the window that opens, configure the following parameters:



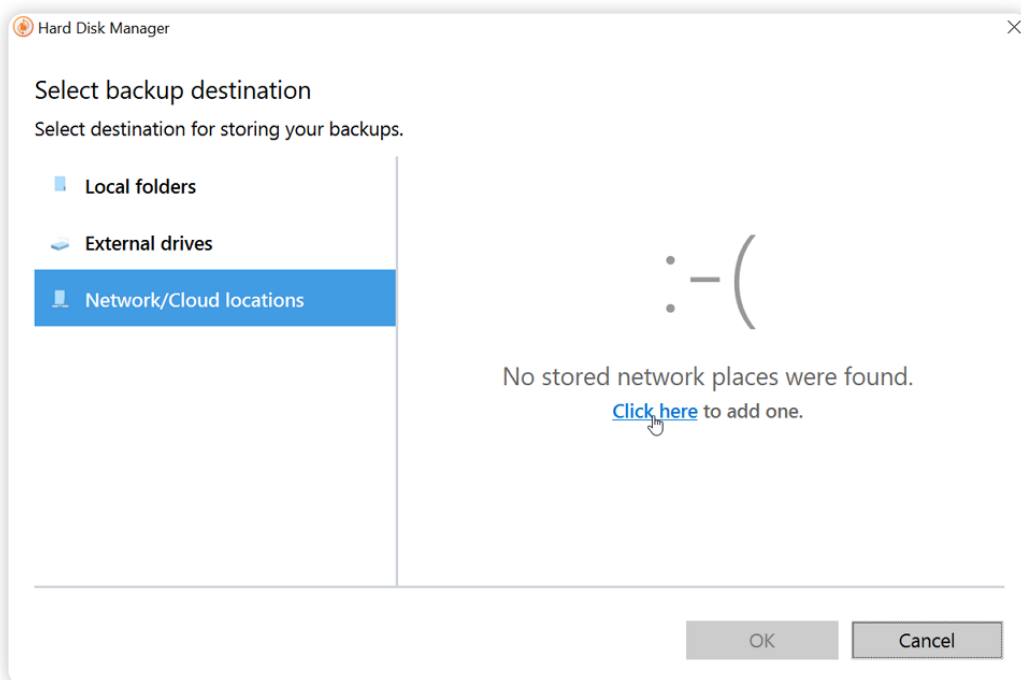
- **Display as:** Specify the desired cloud location name.

- **Storage type:** Select **Amazon S3 Compatible** from the list with available options (**SMB Share, Amazon S3 Compatible, Azure**).
 - **Storage path (with bucket):** Enter the full host path, including the bucket name and the port number (if required, not mandatory): **http(s)://<hosting_address>:<port>/<bucket_name>**. Do not select or manually specify subfolders inside the bucket path. We strongly recommend creating a separate, dedicated bucket exclusively for Hard Disk Manager backups.
 - **Access Key and Secret Key:** Enter your credentials to authenticate and grant access to the storage. Both the **Access Key** and **Secret Key** can be modified at any time within the existing network location properties.
6. Click **OK** to apply your changes.

5.1.3.2 Azure

Configure Azure Storage

1. On the sidebar, go to **Backup & Recovery**.
2. Select the backup or create a new one.
3. Click on the **Destination** menu. The **Select backup destination** window will open.
4. Select **Network/Cloud locations**. In the right part of the opened window, click on the **Click here** link to add a network or cloud location.



5. In the window that opens, configure the following parameters:

Hard Disk Manager

Create stored network or cloud location

Select a network share or cloud resource and specify access credentials.

Display as:

Storage type:

Generated Blob SAS URL:

i Please use Azure Storage Browser to acquire Generated Blob SAS URL and copy it to clipboard.

OK **Cancel**

- **Display as:** Specify the desired cloud location name.
- **Storage type:** Select **Azure** from the list with available options (**SMB Share**, **Amazon S3 Compatible**, **Azure**).
- **Generated Blob SAS URL:** Enter the secure Azure URL that contains both the storage destination address and its embedded access token. You can easily replace an expired or active service SAS token with a new one at any time within the network location properties.

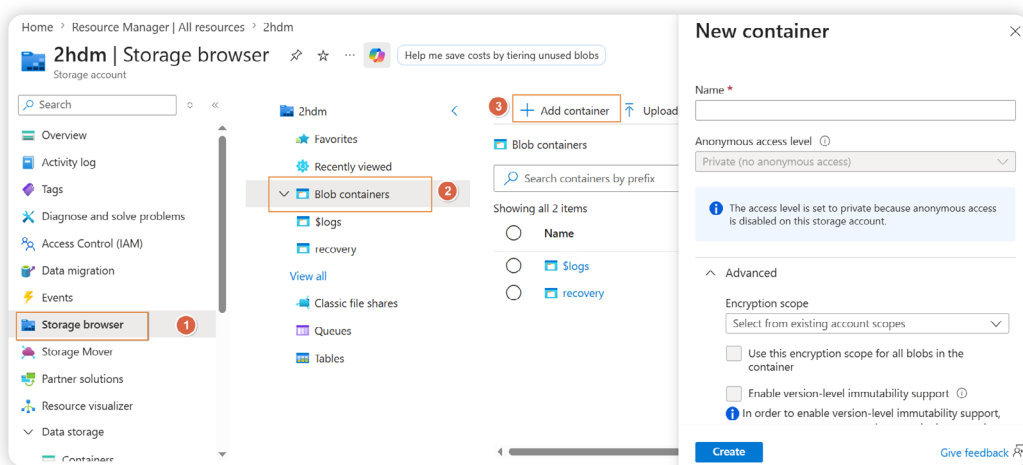
For more information on how to obtain **Generated Blob SAS URL**, see [Generate Blob SAS URL](#).

6. Click **OK** to apply your changes.

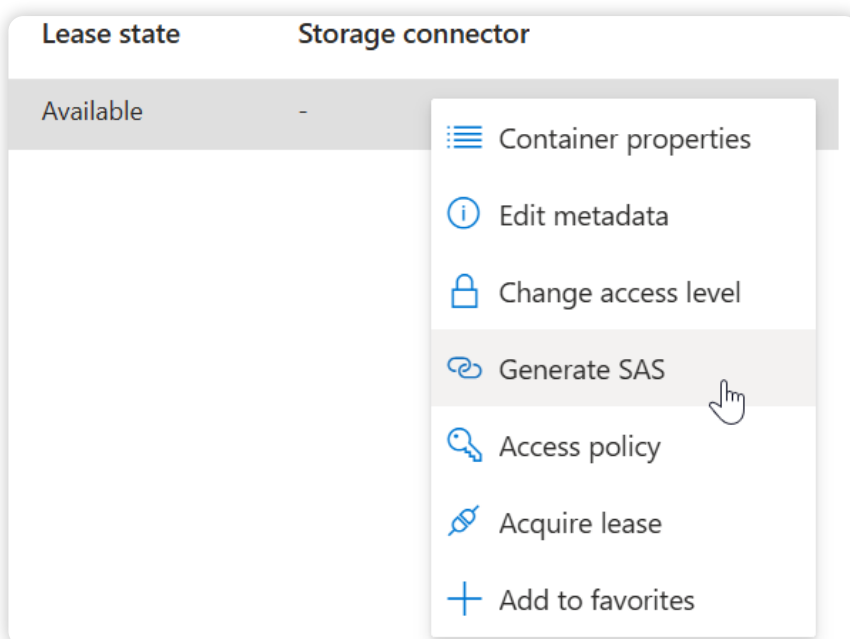
Generate Blob SAS URL

A Blob SAS URL is a secure, temporary link that provides restricted access to a specific Azure Storage blob without exposing your master account keys. To obtain this link, do the following:

1. Go to the [Azure portal](#) and log in using your credentials.
2. Select your storage account. To do this, in the left navigation menu select **Storage accounts**. A list of available storage accounts will open in the workspace to the right. To create a new storage account, on the top toolbar, click **Create**.
3. On the sidebar of the selected storage account, select **Storage browser > Blob containers**. In the top menu, click **Add container**. In the **New container** window that opens, fill in the container name in lowercase letters and select the encryption scope.



4. In the row of the blob container, select the last column on the right and click **Context menu**. In the menu that opens, select **Generate SAS**.



5. In the window that opens, fill the desired parameters and click **Generate SAS token and URL**.

Generate SAS

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage container. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. [Learn more about creating an account SAS](#)

Signing method
☒ Account key ☐ User delegation key

Signing key ⓘ
Key 1

Stored access policy
None

Permissions * ⓘ
Read

Start and expiry date/time ⓘ
Start
06/30/2026 4:20:26 PM
(UTC+03:00) --- Current Time Zone ---

Allowed IP addresses ⓘ
for example, 168.1.5.65 or 168.1.5.65-168.1....

Allowed protocols ⓘ
☒ HTTPS only ☐ HTTPS and HTTP

Generate SAS token and URL

Please note that the generated SAS token must explicitly include the following access permissions:

- Read
- Add
- Create
- Write
- Delete
- List

6. Once the button is clicked, 2 blob SAS elements will appear on the screen:

Blob SAS token ⓘ

sp=r&st=2026-06-30T13:20:26Z&se=2026-06-30T21:35:26Z&spr=https&sv=2026-0...

Blob SAS URL

https://2hdm.blob.core.windows.net/recovery?sp=r&st=2026-06-30T13:20:26Z&se=...

Copy the information from the **Blob SAS URL** and use it to configure the Azure storage.

5.2 Recovery

5.2.1 Recovery Overview

Data recovery is the process of reinstating backed-up data to its original or alternative location.

Supported recovery scenarios:

- Restoring a system after a crash or virus infection.
- Performing a bare-metal recovery to a blank drive.
- Moving the system to a larger or new hard disk.

For restoring a specific restore point, regardless of the type of backup source chosen (entire computer, disks/drives, files, and folders), three restoration options are available:

- **As a whole disk:** The target drive is completely overwritten (even if only part of a disk was backed up).
- **Partition by partition:** You can individually decide which partition will be restored and to which suitable location (free space or in place of an existing partition).
- **Individual files and folders to an existing partition:** When recovering individual files and folders to an existing partition, using simpler native alternatives like the Browse function or revealing the data via the **Show** or **Hide** in Explorer command is generally more efficient than executing a standard full restore operation.

Please note that in order to facilitate restoration, Hard Disk Manager automatically searches for the appropriate scenario (disk or partition restoration) and selects suitable backups and targets for the restoration.

When restoring regular system backups, the wizard typically suggests the **Partition by Partition** restoration option.

5.2.2 Bare-Metal Recovery

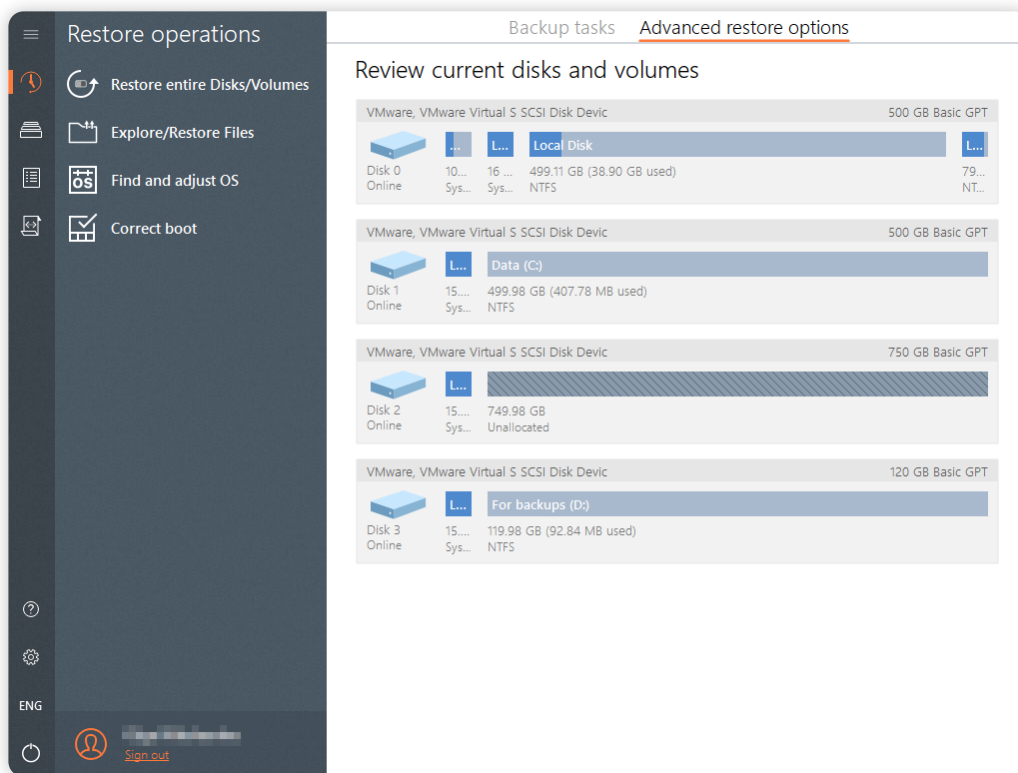
Bare-Metal Recovery (BMR) is a data restoration process where a computer system is restored from a backup onto a completely blank hard drive or new hardware that has no pre-installed operating system, software, or drivers.

To perform a bare-metal recovery, you can use either a USB flash drive or an ISO file generated by the [recovery media](#) builder. The recovery media allows you to boot your PC to restore data from an existing backup, secure important files, or rectify boot errors when the Windows OS fails to start.

To perform the recovery, proceed as follows:

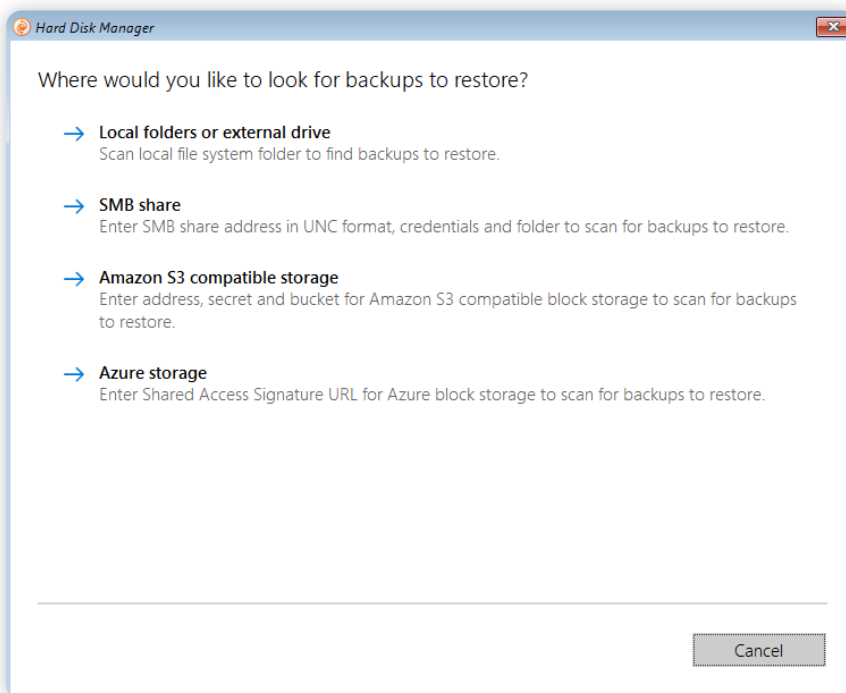
1. Start up the computer from the prepared [recovery media](#).
2. The **Restore operations** window will open with the **Advanced restore options** tab available for review. Select **Restore entire Disks/Volumes**.

WinPE media



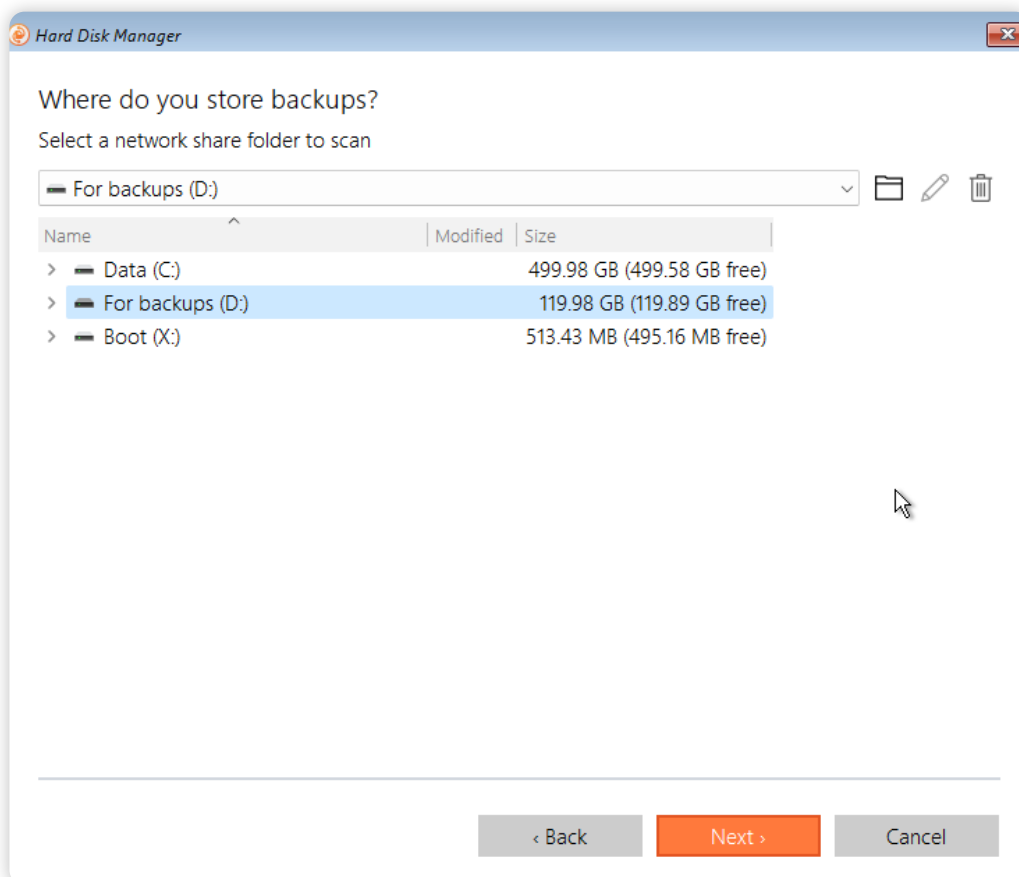
Selecting **Explore/Restore files** will allow restoring files from local folders, external drives or SMB share.

3. In the next window, select where the backups that you would like to restore are located.

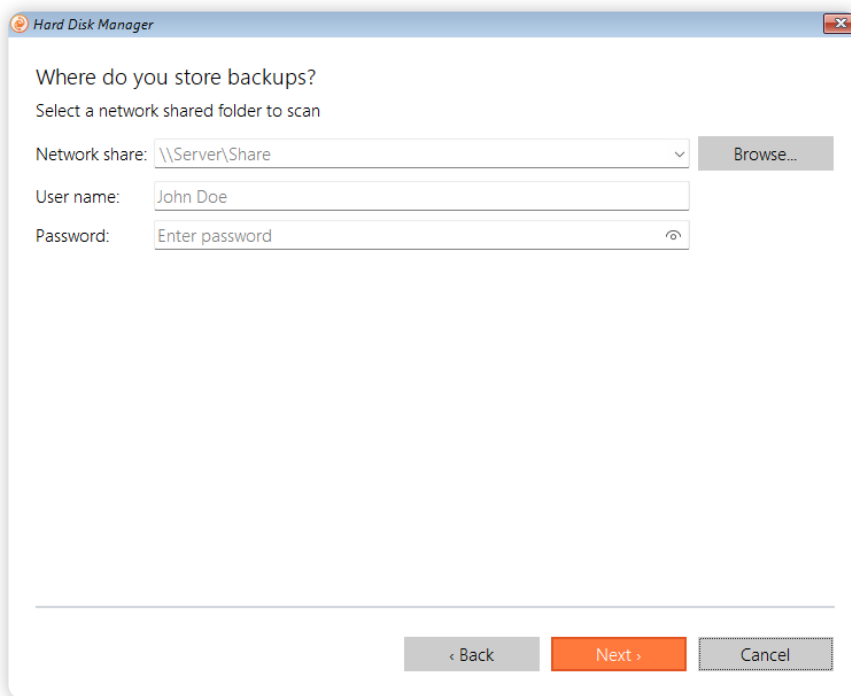


Select the desired option and proceed as follows:

- **Local folders or external drive**: Select where you store your backups and click **Next**.



- **SMB share:** Fill in the required data and click Next.



Hard Disk Manager

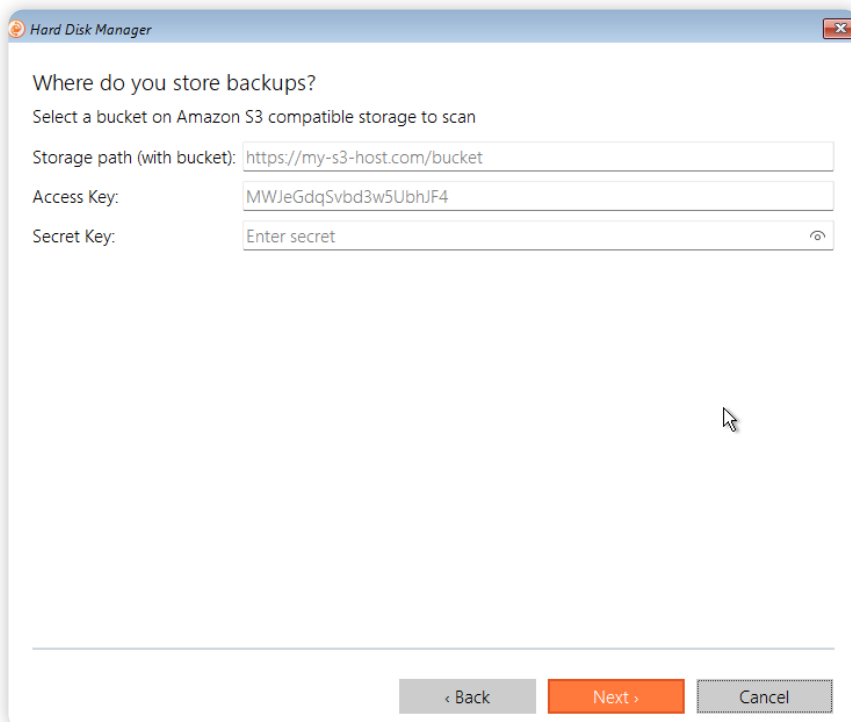
Where do you store backups?
Select a network shared folder to scan

Network share:

User name:

Password:

- **Amazon S3 compatible storage:** Fill in the required data and click Next. For more information on configuring the S3 storage, see [S3](#).



Hard Disk Manager

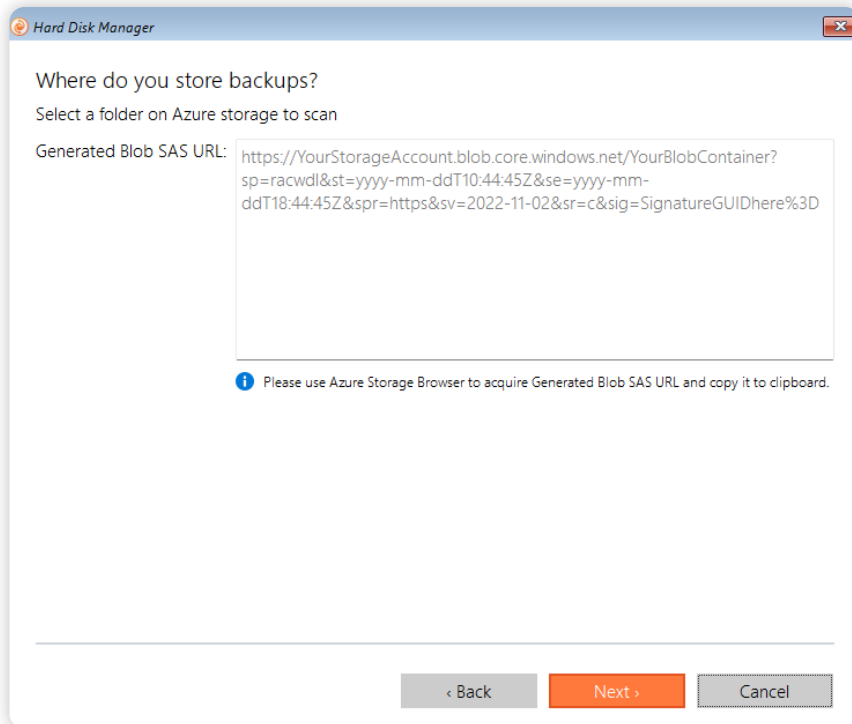
Where do you store backups?
Select a bucket on Amazon S3 compatible storage to scan

Storage path (with bucket):

Access Key:

Secret Key:

- **Azure storage:** Fill in the required data and click Next. For more information on Generated Blob SAS URL, see [Generate Blob SAS URL](#).



Hard Disk Manager

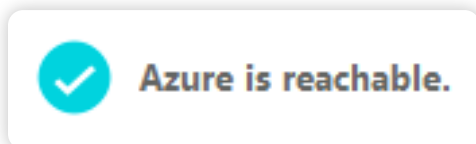
Where do you store backups?
Select a folder on Azure storage to scan

Generated Blob SAS URL: `https://YourStorageAccount.blob.core.windows.net/YourBlobContainer?sp=racwdl&st=yyyy-mm-ddT10:44:45Z&se=yyyy-mm-ddT18:44:45Z&spr=https&sv=2022-11-02&sr=c&sig=SignatureGUIDhere%3D`

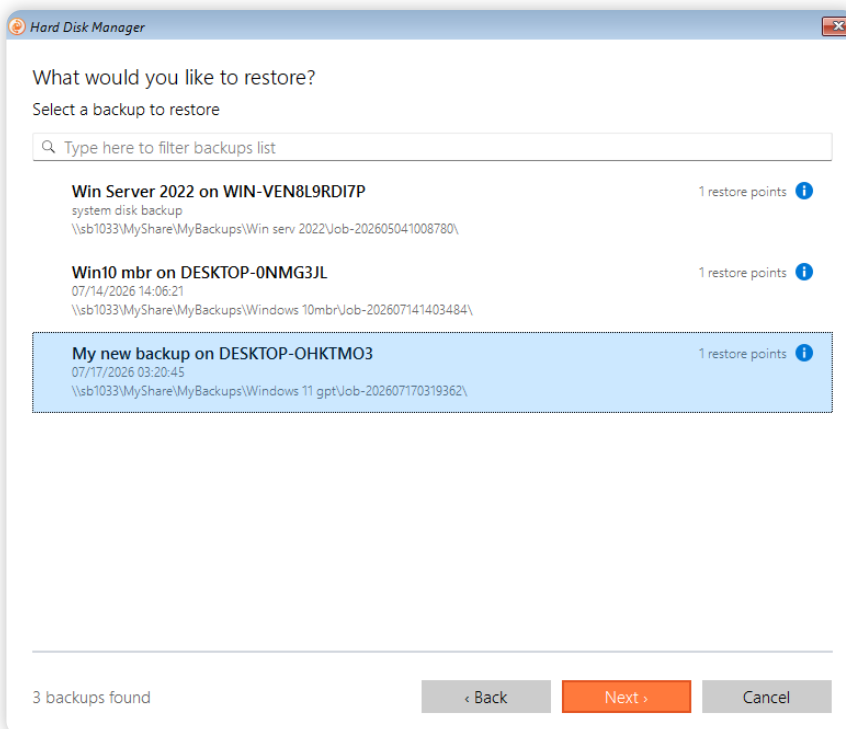
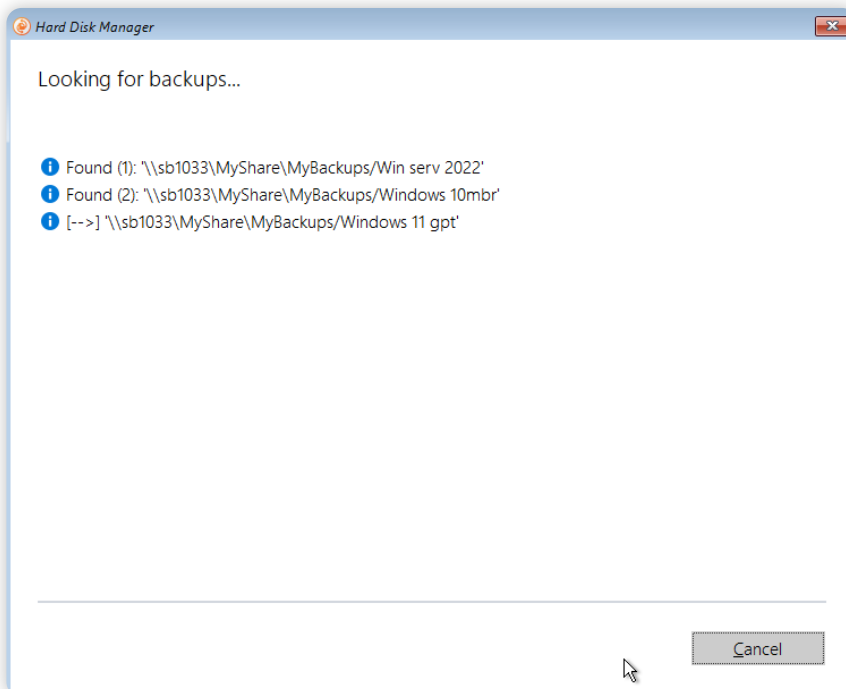
 Please use Azure Storage Browser to acquire Generated Blob SAS URL and copy it to clipboard.

[< Back](#) [Next >](#) [Cancel](#)

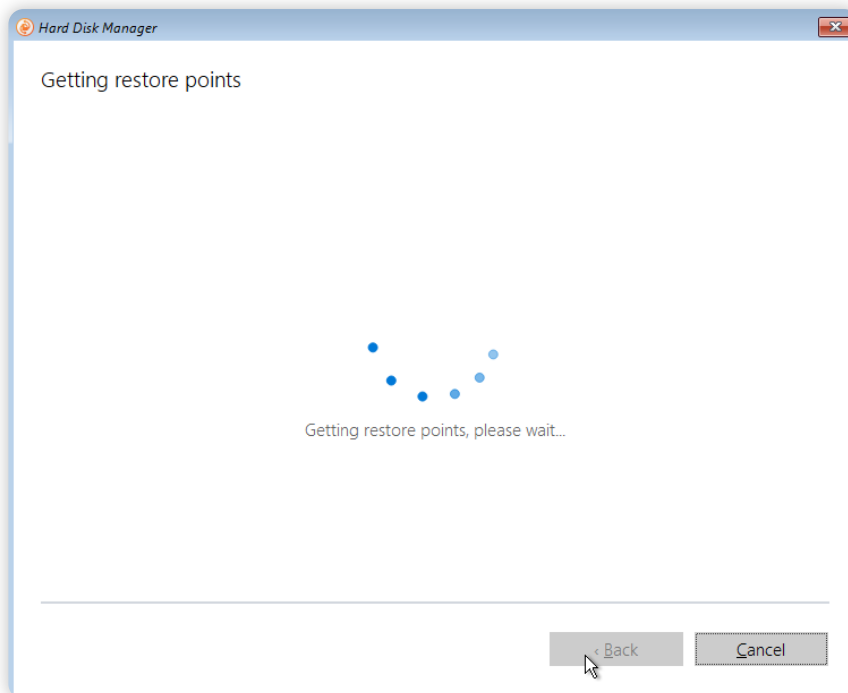
Before starting a recovery from Azure Blob Storage, Hard Disk Manager verifies source availability so you do not waste time entering credentials for an offline repository:



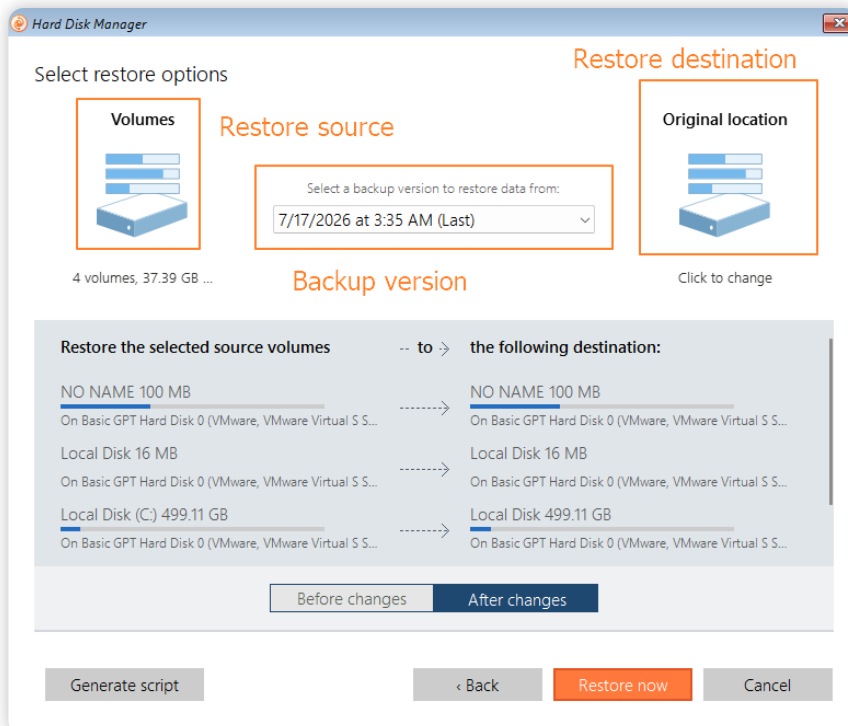
4. Hard Disk Manager will perform the backup search and suggest the backups to choose from. Click **Next** to continue.

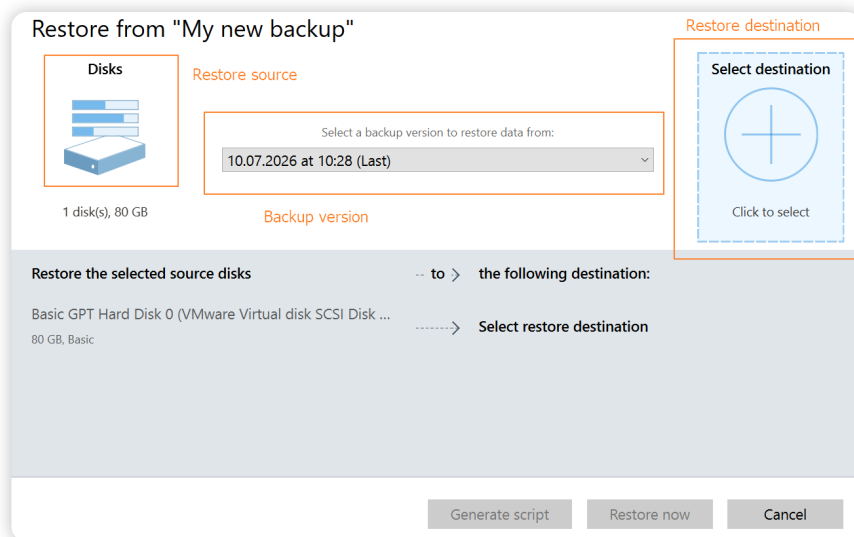


5. Hard Disk Manager will get the available restore points.



6. Select the desired backup version from the drop-down list in the middle. Review the current restore settings in the gray area and, if needed, change the restore source and destination by clicking on the source and destination icons.





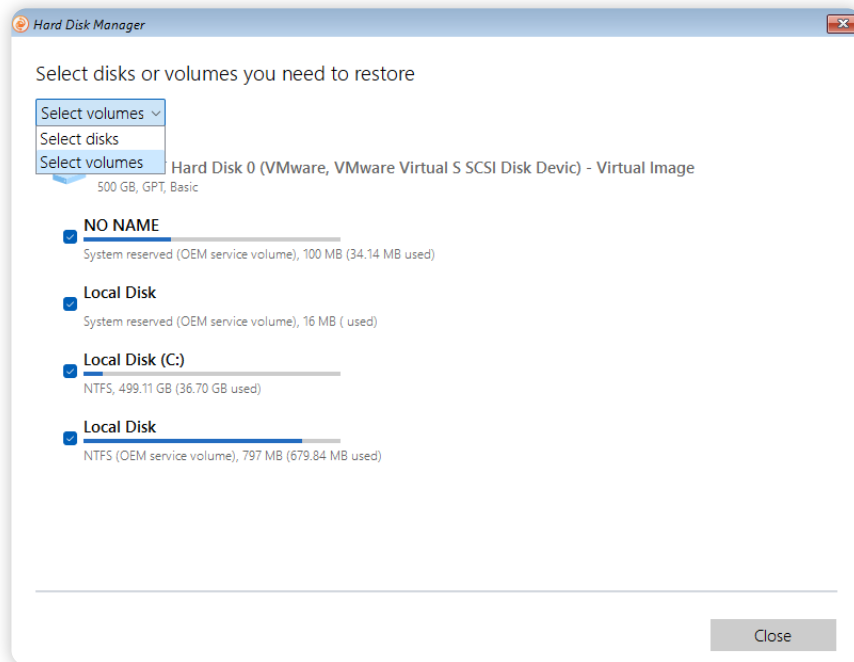
If Hard Disk Manager displays **Original location** as the destination, the restore will be applied at the **volume** level. This means the software detects the original drive with its existing partition structure intact. It will only overwrite the specific partitions included in your backup, leaving other volumes untouched.

If Hard Disk Manager prompts you to **Select destination**, the data is being restored to a different location than the original source. In this scenario, the software will perform a disk-level restore.

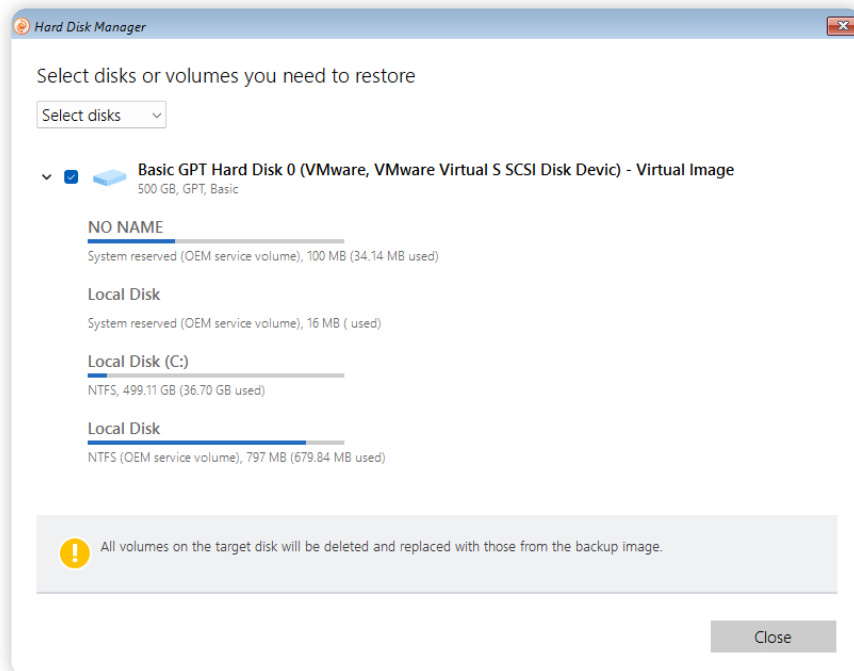
Warning: This action will completely wipe and destroy all existing data on the target drive.

Please note that these restore options are customizable; you can manually select a different restore method than the one recommended by Hard Disk Manager. However, we highly recommend stick to the suggested scenario unless you fully understand the reasons for changing it and the potential consequences.

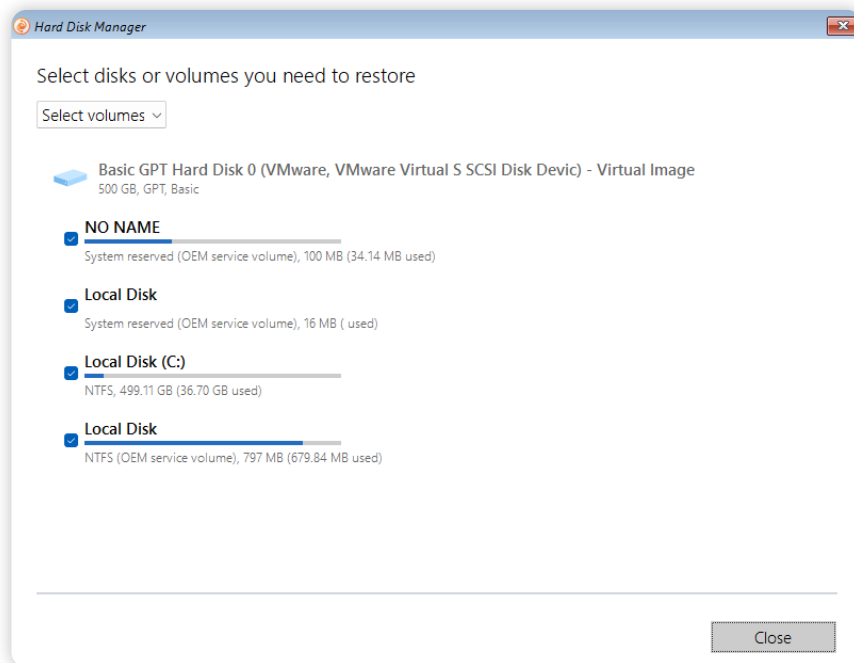
Clicking on the restore source will open the window where you can select disks or volumes to be restored.



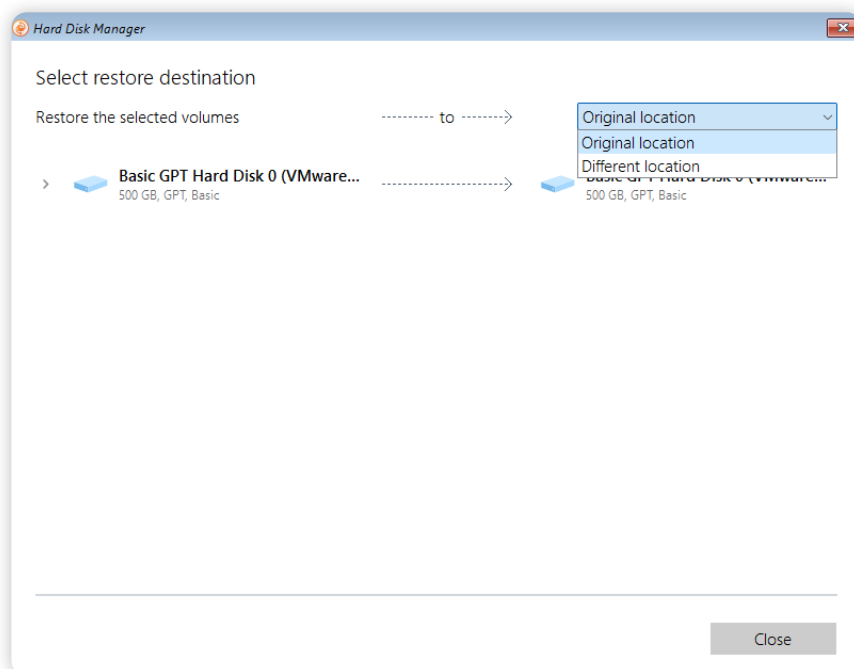
Disks selected



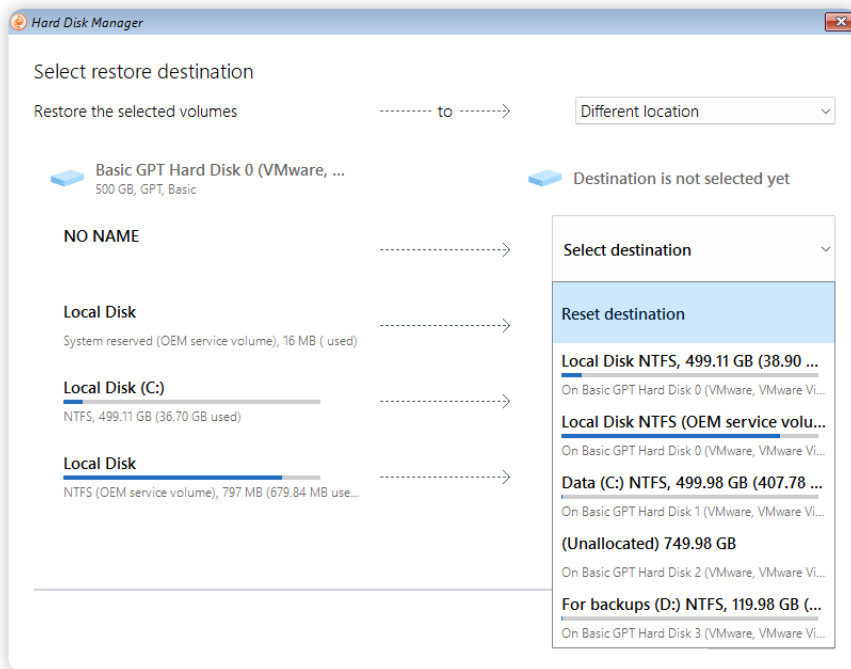
Volumes selected



Clicking on the **Original location** will open the window where the location can be selected.

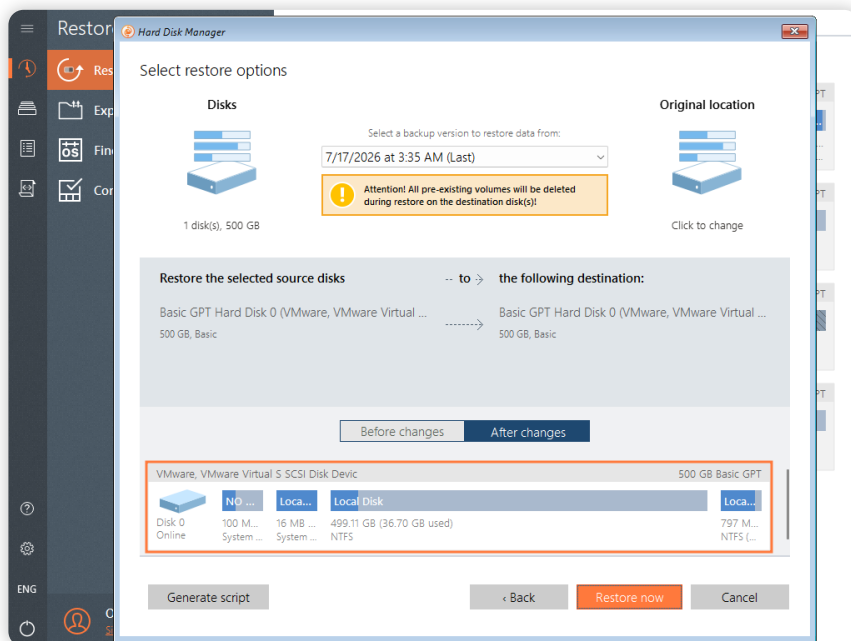


If you select **Different location**, a list of possible options will open.



7. Review your selection in the workspace by clicking **Before changes** or **After changes**.

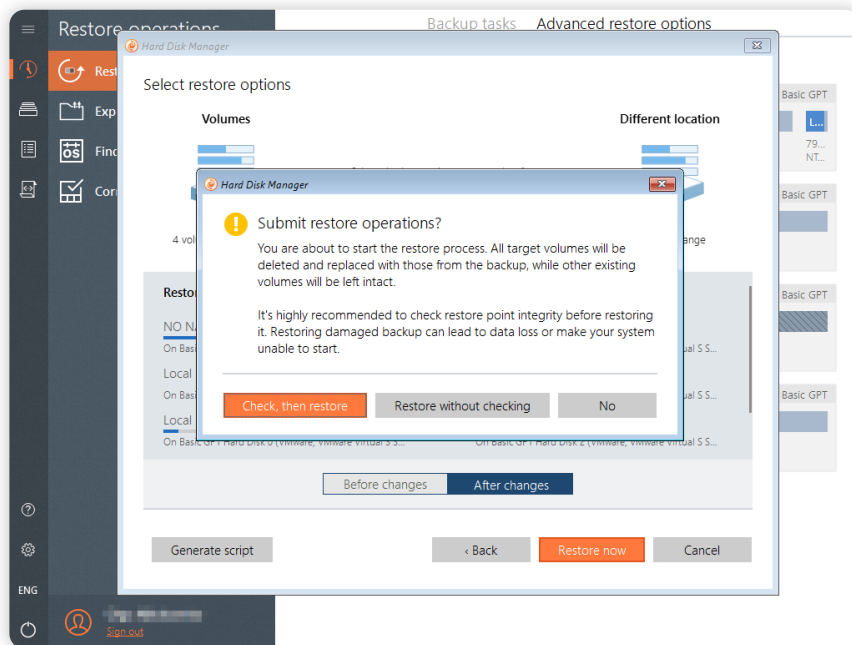
8. Click one of the buttons to continue:



- **Generate script:** Select this advanced feature to generate a script based on the specified restore operations. If you choose to create a script, the configured restore task will be canceled. For more information on scripts, refer to the User Manual.
- **Restore now:** Click this button to start the restore process.

- **Cancel:** Cancel the current recovery.

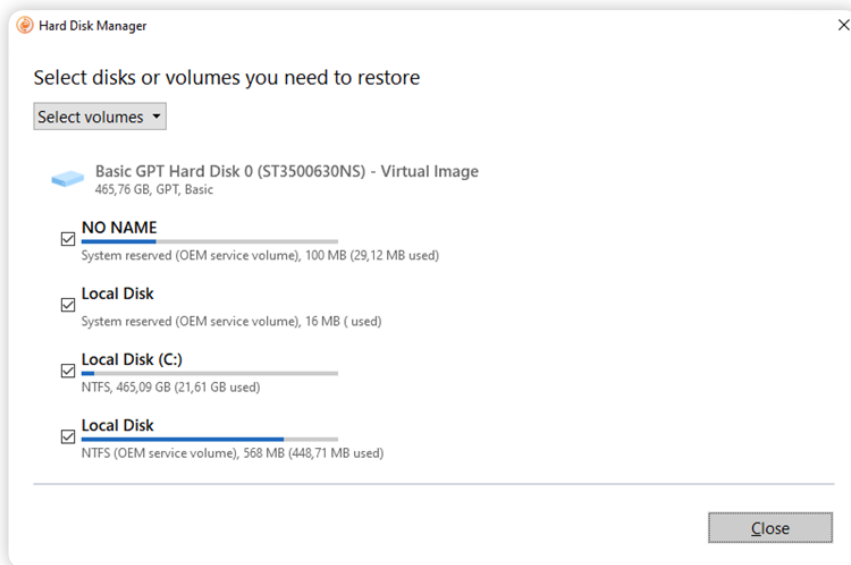
Selecting the **Restore now** option will prompt you to confirm the operation. You will also be asked to verify the integrity of the selected restore point (recommended). If you are confident the archive is intact, you can skip this verification and select **Restore without checking**.



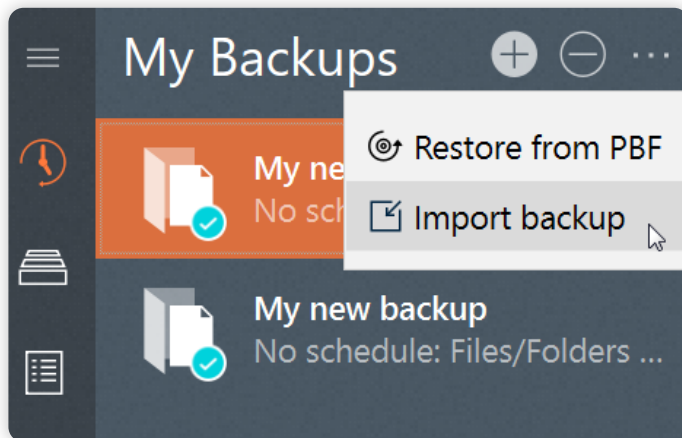
9. Apply the operation and wait for the system recovery process to complete.
10. Once finished, restart your computer and unplug the recovery media (unplug the USB drive or disconnect the ISO image).

5.2.3 Import Backups

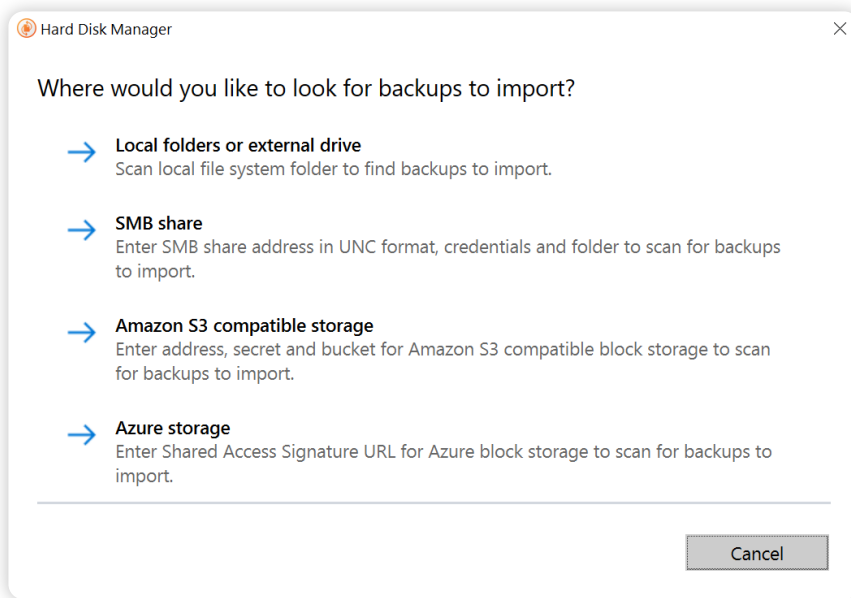
Backups are stored as archives in an archive database. If a backup archive is missing from the database, you can still recover your data using the **Import backup** feature.



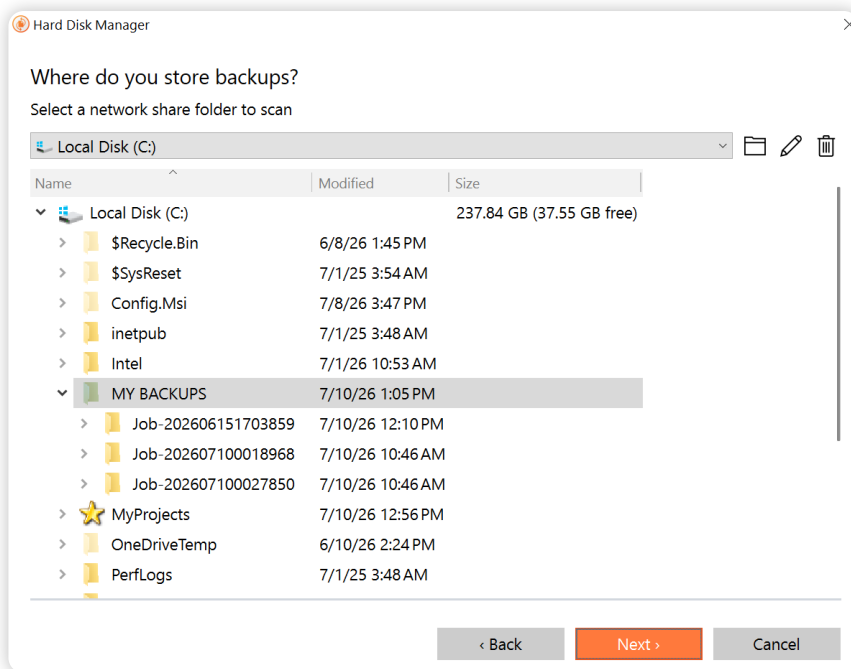
1. On the sidebar, go to **Backup & Recovery**.
2. In the top left corner, next to **My Backups**, click **More actions > Import backup**.



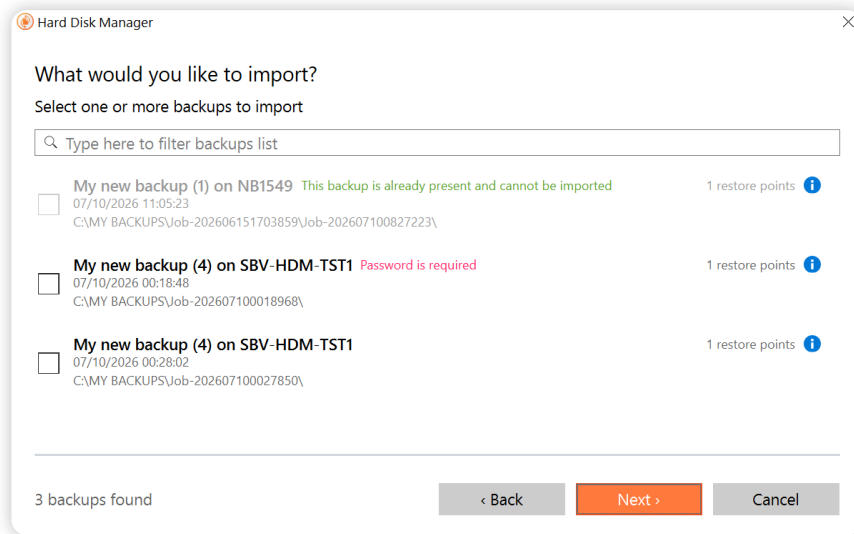
3. Select the path to the backup which needs to be recovered.



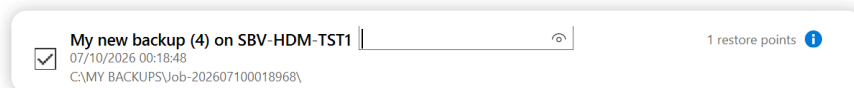
4. Select the folder where you store backups. Click **Next** to make the program select the backups available for export.



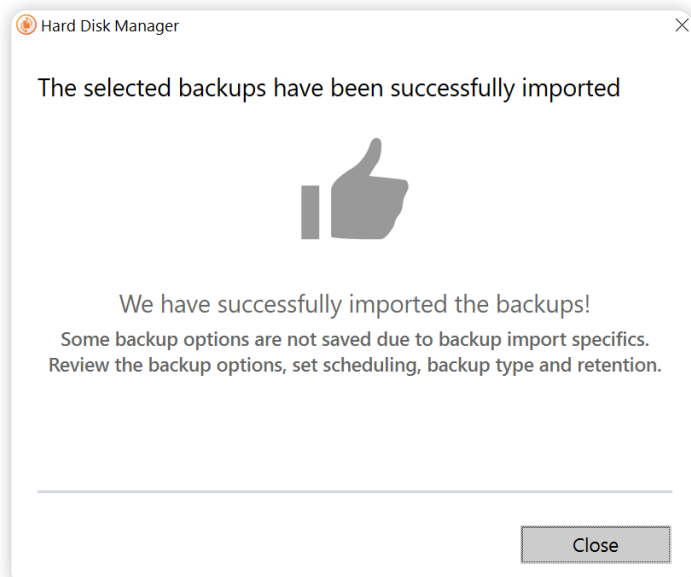
5. The list of backups will be displayed. Select the backup(s) that you want to import and click **Next**.



Please note that before handling password-protected backups you will need to enter the password.



6. If the import is successful, the corresponding message will appear on the screen.



Please check the imported backups to make sure all the settings are in order.
The imported backup will appear in the list of backups on the sidebar to the right.

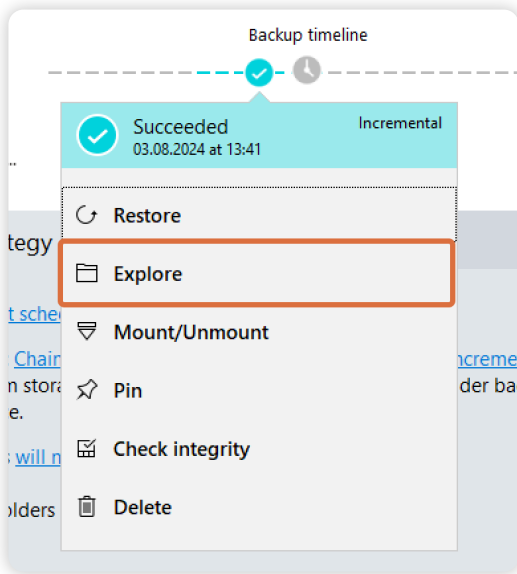
5.2.4 Recover Individual Files and Folders

When recovering individual files and folders to an existing partition, using simpler native alternatives like the **Browse** function or revealing the data via the **Show** or **Hide** commands in File Explorer is generally more efficient than executing a standard full restore operation.

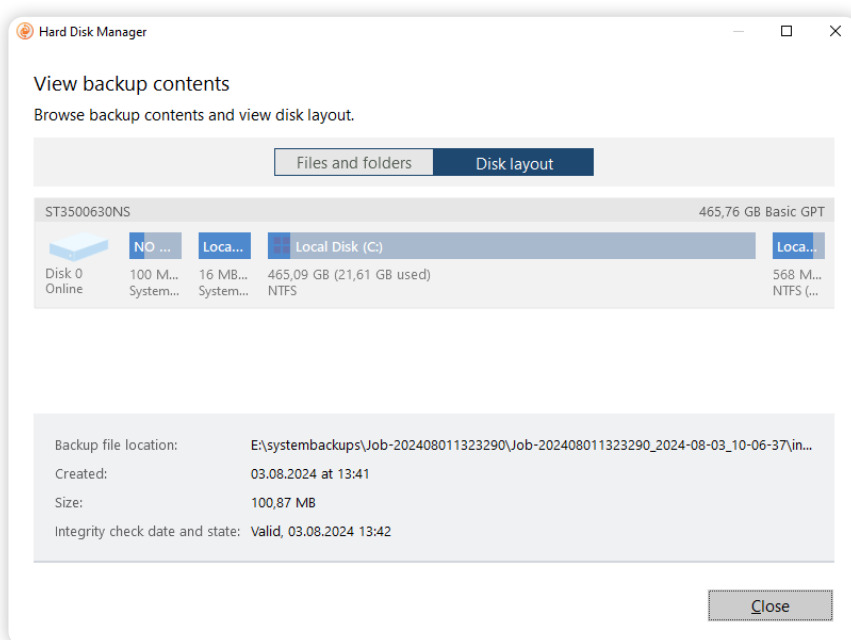
Hard Disk Manager allows you to recover individual files and folders by exporting them or mounting the backup image. This eliminates the need to run the full-scale restore wizard for minor data recovery.

Export Files and Folders

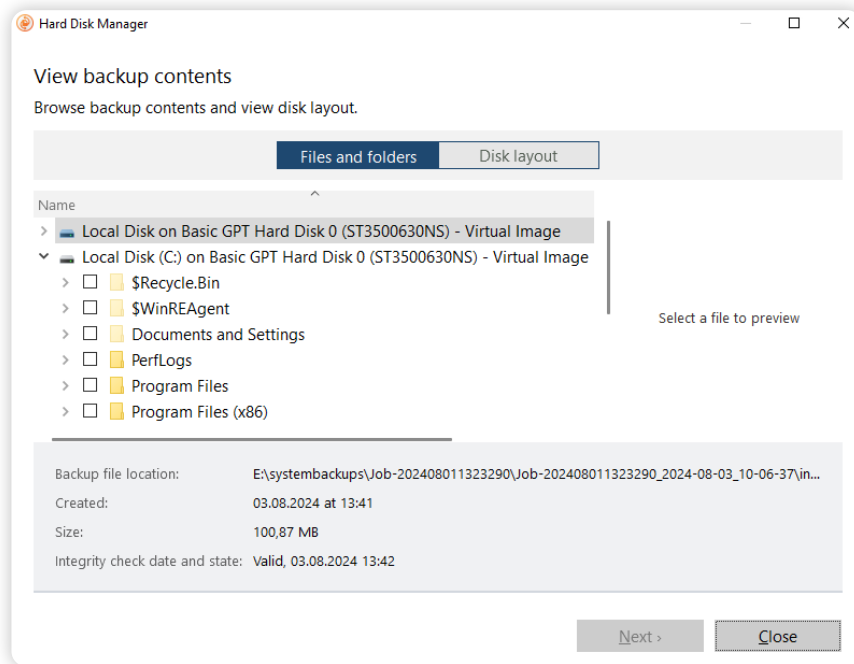
1. Select a backup job, click on a restore point in the timeline view, and then choose **Explore**.



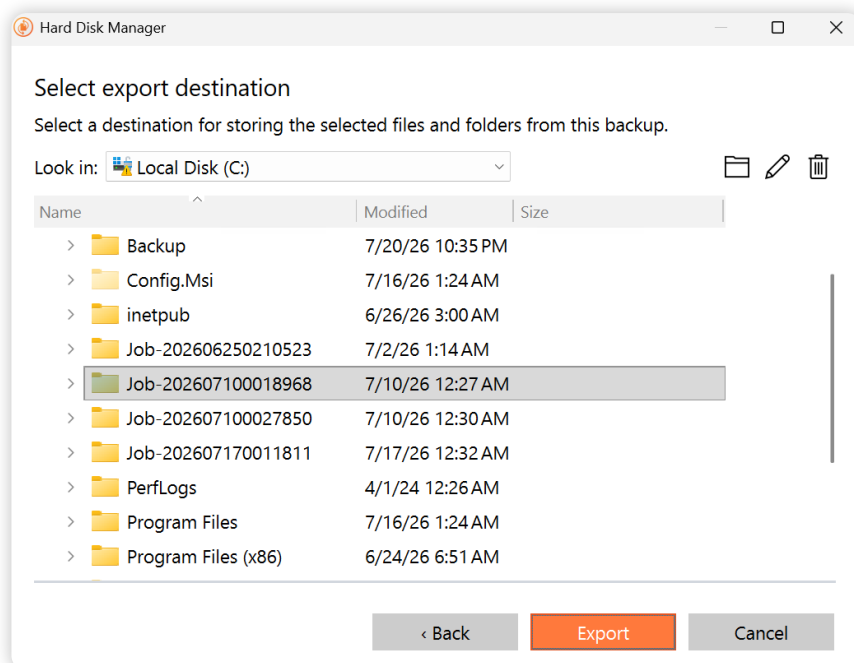
2. For partition and disk backups, the **Disk layout** view will appear first.



3. Select the drive from which you want to export files by switching to the **Files and folders** view and navigating to the target path.



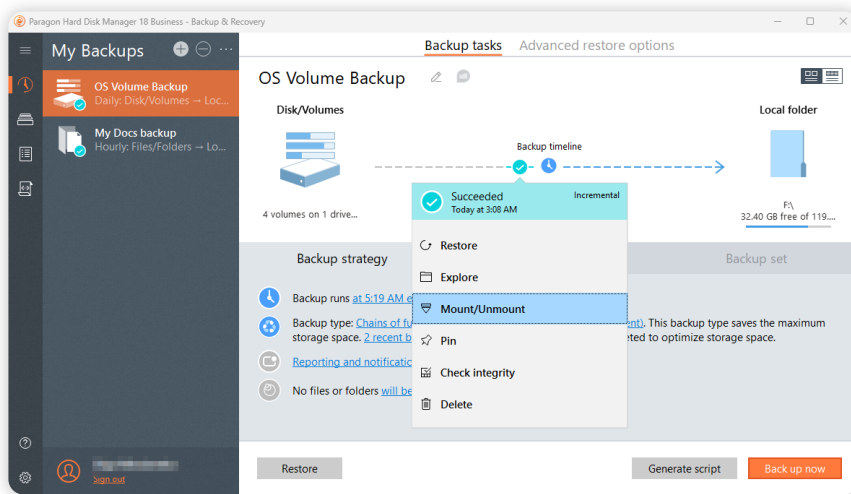
4. Select the files and folders to be exported using the checkboxes, then choose the destination location.
5. Click **Export** to export files and folders to the desired location.



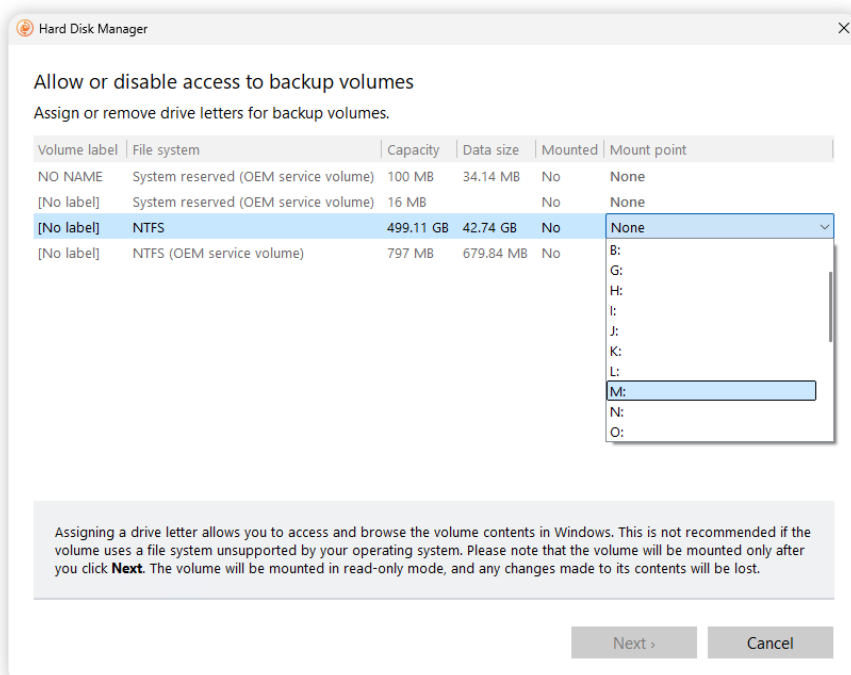
Mounting Backup Image

You can assign a drive letter to any partition inside an existing backup image. This mounts the partition in the system, allowing you to easily browse its contents and copy the required information using standard Windows tools. This is the easiest way to copy individual files from a backup to another location.

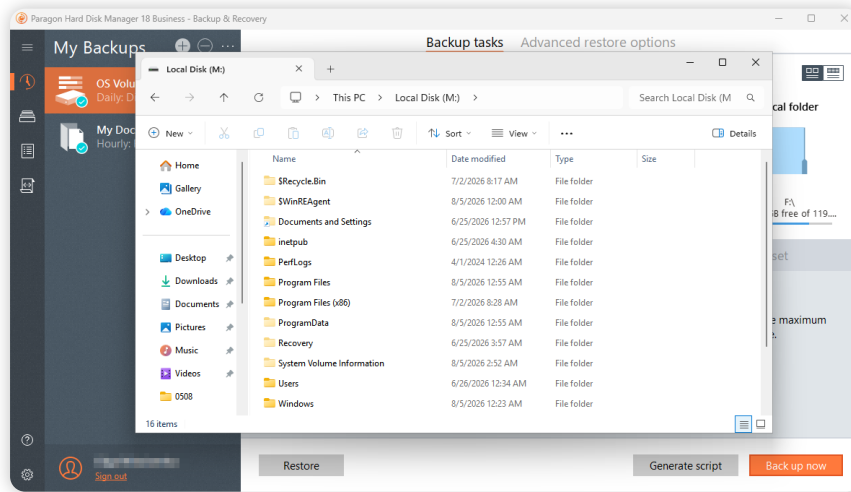
1. On the sidebar, go to **Backup & Recovery**.
2. In the **My Backups** list, select the desired backup from which you want to recover the data.
3. In the backup job working area to the right, right-click on the backup timeline (the turquoise line) to select the desired restore point. In the window that opens, select **Mount/Unmount**.



4. In the window that opens, you can view the contents of the selected backup image. Select the partition you want to mount, then choose an available drive letter from the list to assign to it. Click **Next** to confirm.



5. Once mounted, you can treat the backup partition as you would any other Windows volume (browse, retrieve files, modify files).

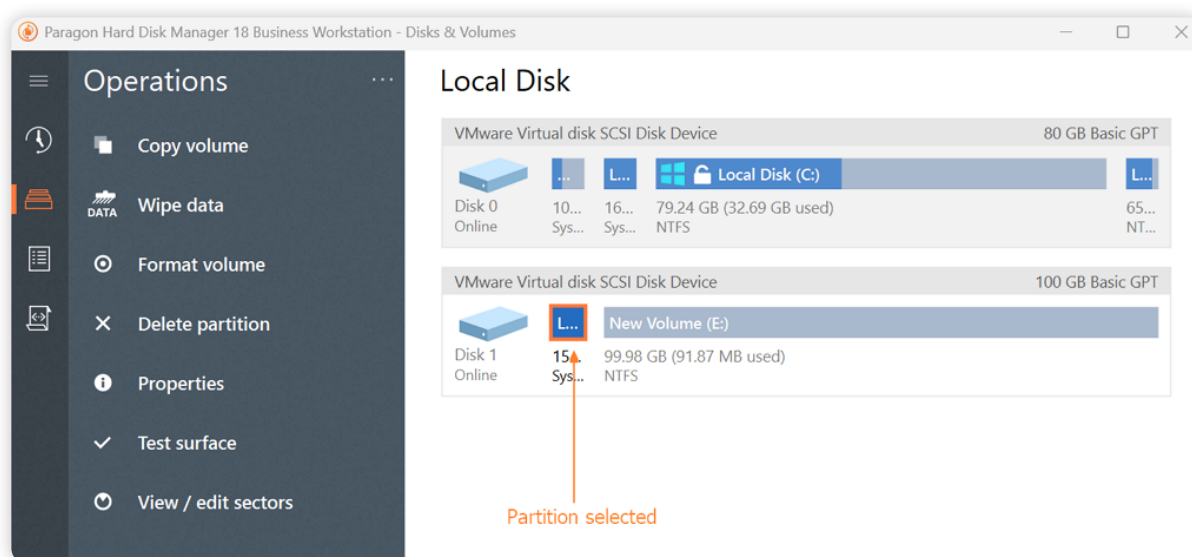
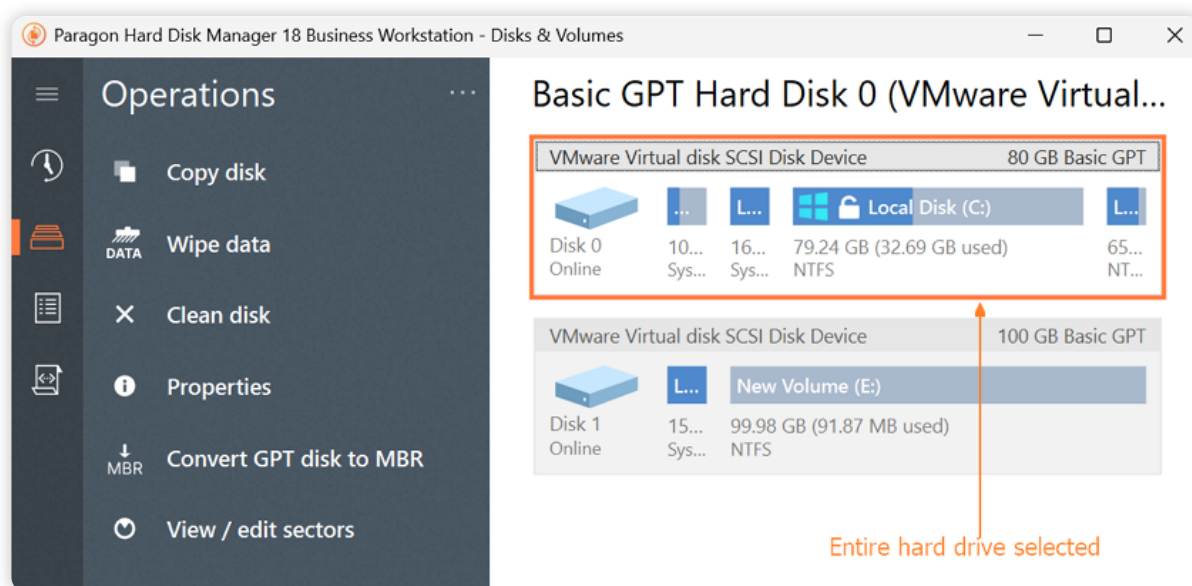


If you have selected a bootable partition, a warning message will appear.

Once mounted, you can open, copy, and edit files on this virtual drive. However, the source backup archive is protected and remains read-only. This means any changes you make are temporary and will be deleted when you unmount the drive. To keep your work, copy the edited files to your local PC before unmounting.

5.3 Disk and Partition Management

When you click on an item (disk or partition) under the **Disks & Volumes** tab in the main window, all the functions or operations that can be performed on this item will appear on the left side in the sidebar:



If certain volume operations are unavailable, the drive or partition is likely protected by BitLocker. To modify these partitions, you must fully decrypt the drive rather than just unlocking it. Once the changes are complete, BitLocker can be re-enabled. For step-by-step instructions, see our knowledge base article on [BitLocker Drive Encryption \(BDE\) Support](#).

For a detailed description of all disk and partition operations, please refer to our User Manual.

6. NOTIFICATIONS AND REPORTS

Overview

Hard Disk Manager allows you to receive notifications and reports.

Automated e-mail **notifications** keep you updated on all program tasks. Hard Disk Manager acts as a built-in e-mail client (similar to Outlook or Thunderbird) and connects directly to your SMTP server. To enable this feature, first configure your global e-mail settings and enable notifications for individual tasks.

You can also receive backup success and failure **notifications** from no-reply@paragon-software.com when you choose to synchronize device system information and backup jobs with your personal dashboard in the Paragon Licensing Center.

Automatically created **reports** provide detailed information for all backup and wipe operations. These summaries can be edited, printed, e-mailed, or saved in text, PDF, or HTML formats for future reference.

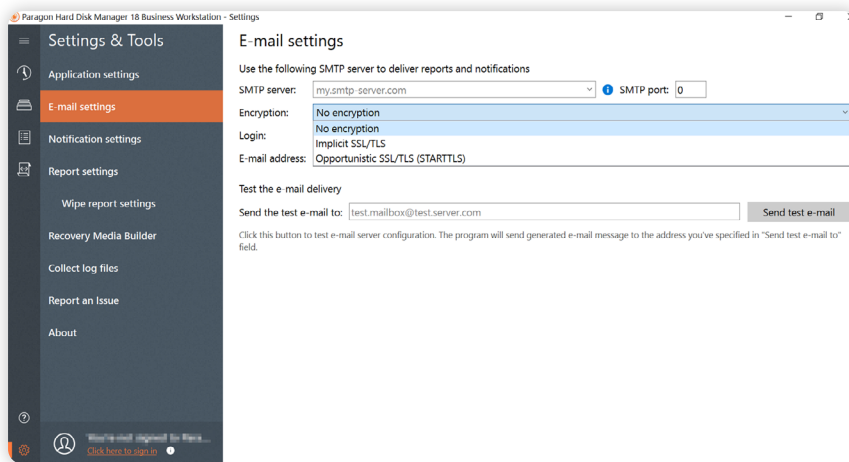
Configure E-mail Settings

To receive the reports and notifications, configure your e-mail preferences.

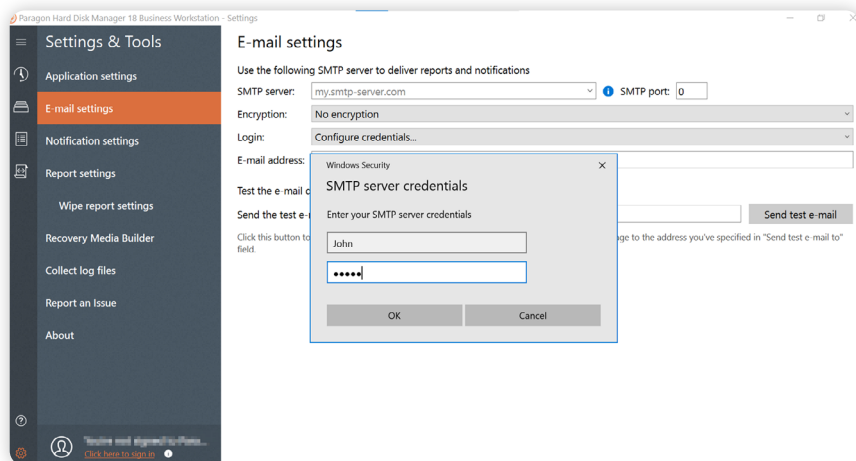
1. On the Sidebar, go to **Settings** ⚙️ > **E-mail settings** to configure the SMTP server through which the messages will be sent.

You can enter the address of your own private SMTP server or use one of the well-known services on the web.

2. Enter the address of the SMTP server or select one of the suggested options: **Gmail**, **Outlook.com**, **Yahoo**, or **AOL**. Select the port.
3. Select the type of encryption from the drop-down list:



4. Enter the login credentials for the user account:



Web mail providers often limit daily e-mail volumes and enforce strict security. For example, when using Google services, you must enable 2-Step Verification and use an **App Password** instead of your regular account password. Check your e-mail provider's help center for detailed instructions.

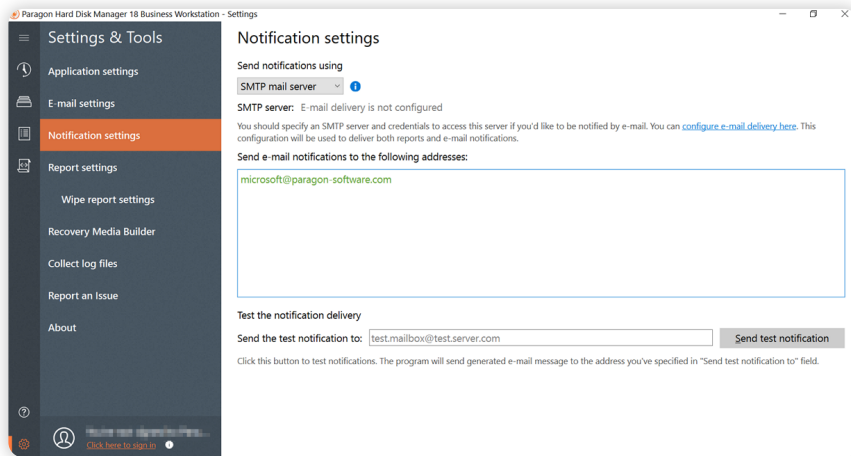
5. Test the success of the SMTP server configuration by clicking the **Send test e-mail button**.

The settings remain saved even after restarting the program or the computer, but they may be lost after certain Windows updates.

Notification Settings

The settings stored in this section serve as default values for all operations within the **Backup & Recovery** and **Disks and Volumes** sidebar elements, provided the notification function is activated there (see [Enabling Notification Function](#)). For each individual operation, you only need to specify whether all operations or only failed ones should be reported.

To apply the new SMTP configuration to your notification tasks, close and restart Hard Disk Manager.

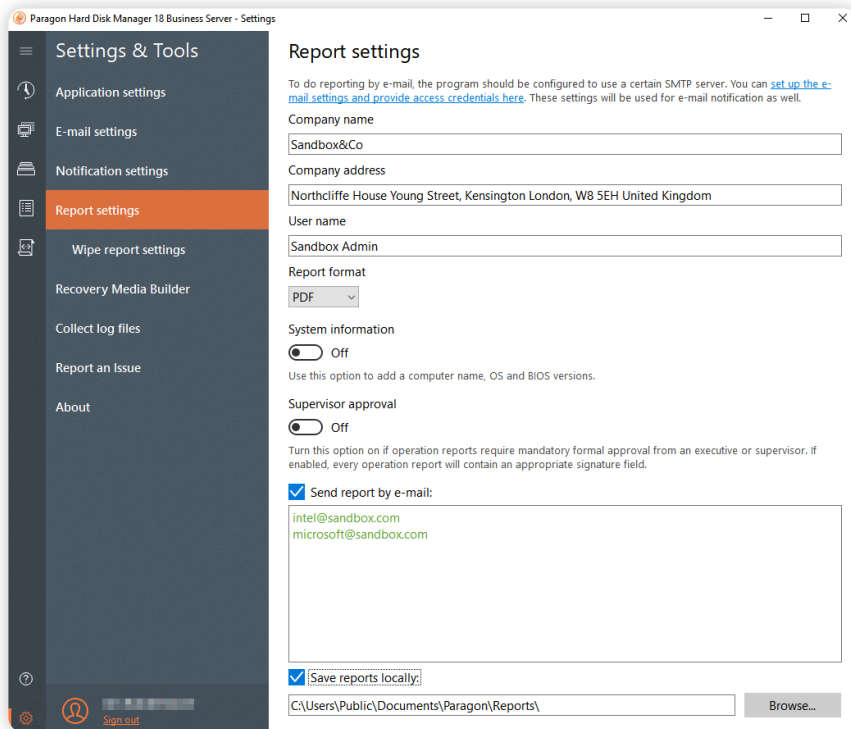


Send a test notification to confirm successful configuration. This also helps you verify if the recipient's spam filter requires a whitelist exception.

Report Creation Settings

The settings stored here apply by default to all automated operation and result reports, which you can access via the sidebar > **Reports**.

1. On the sidebar, go to **Settings** ⚙️ > **Report settings**. Enter the company name, company address, user name, and report format.

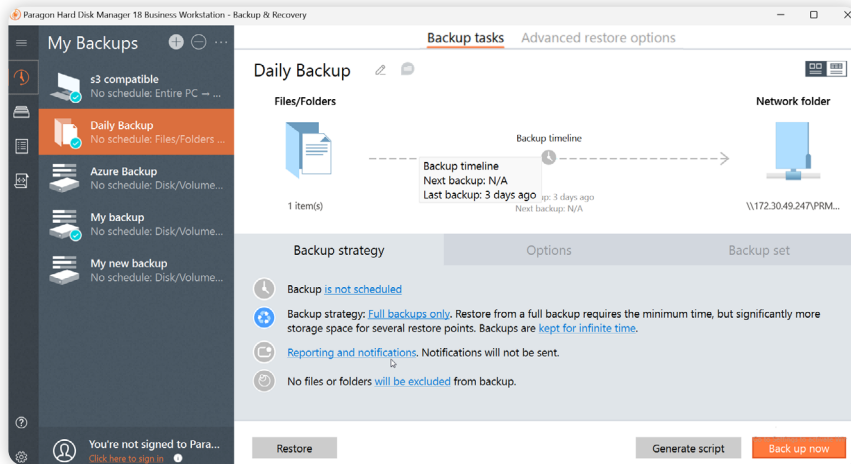


2. Choose the additional report parameters: **Report format**, **System information**, **Supervisor approval**.
3. Enter the e-mail addresses to receive the reports. Syntactically correct e-mail addresses will appear in green.
Please note that you need to configure the SMTP settings in the [E-mail settings](#) to receive the reports.
4. Select the **Save reports locally** option and specify the saving path or clear this option.

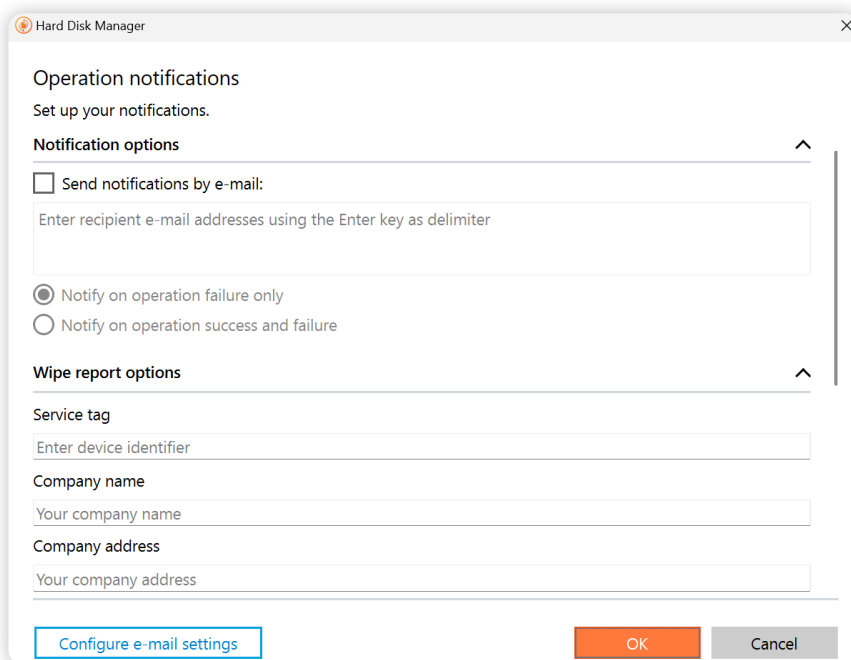
If you need to configure wipe report parameters, they are also available in the **Settings** ⚙️ > **Report settings** > **Wipe report settings**.

Enabling Notification Function

1. On the sidebar, go to **Backup & Recovery**.
2. To the right, under **My Backups**, select the backup you want to receive the notifications about, go to the **Backup strategy** tab and click **Reporting and notifications** in the backup work area.



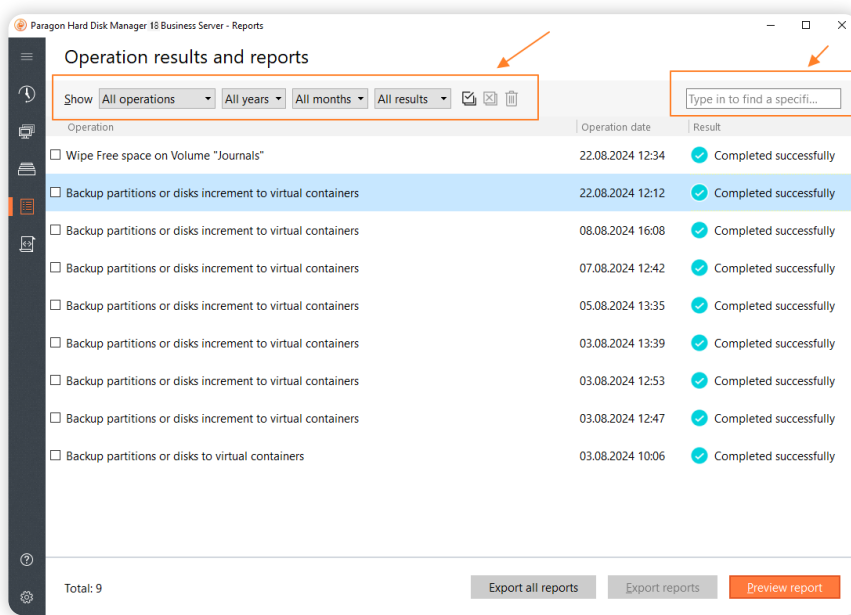
3. In the window that opens, select the operation notification options and click **OK**.



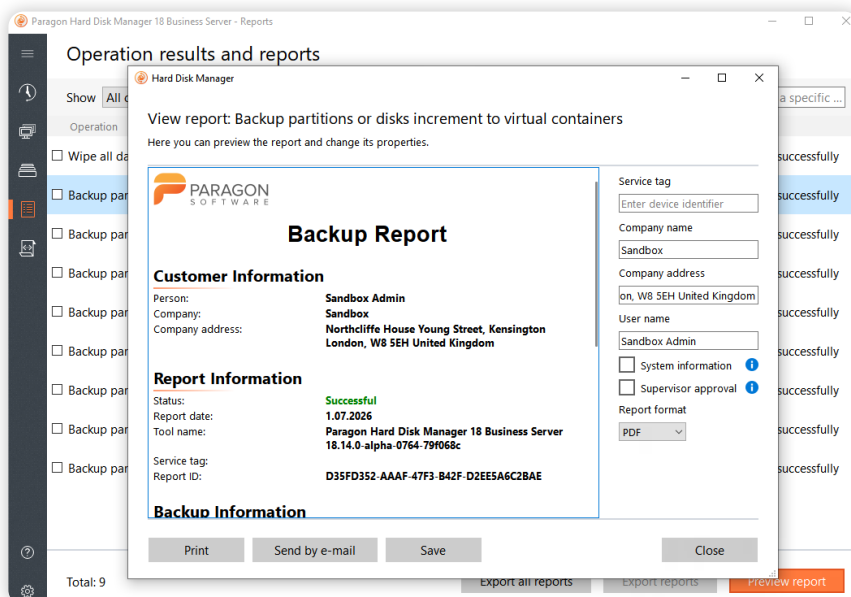
Operation and Result Reports

To see the results of the performed operations and the reports, use the **Operation results and reports** section.

1. On the sidebar, go to **Reports**.
2. In the **Operation results and reports**, select the desired report by checking the corresponding box or by double-clicking the report. You can customize the display of the reports by using the drop-down lists above the list of operations (Show **All operations**, **Backup operations**, **Wipe operations**, **All years**, **Current year**, **All months**, **All results**, **Succeeded**, **Canceled**, **Failed**) or typing in the desired operation type in the respective field.



3. Click **Preview report** to see the future report. The preview is customizable: you can add information and modify the layout.



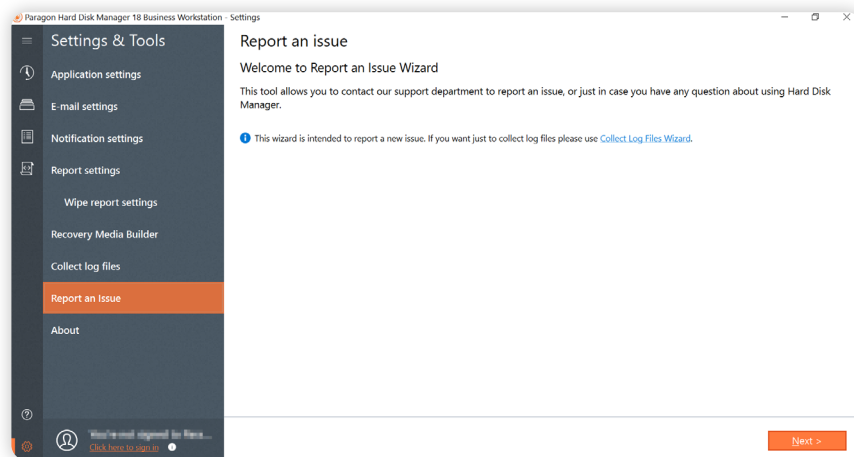
4. Select **Export all reports** to export all available reports in the operation list or **Export reports** to export the selected reports.
5. Do one of the following: print the report, send it by e-mail, save it or close the preview window.

7. SUPPORT AND LEGAL NOTICES

7.1 Support

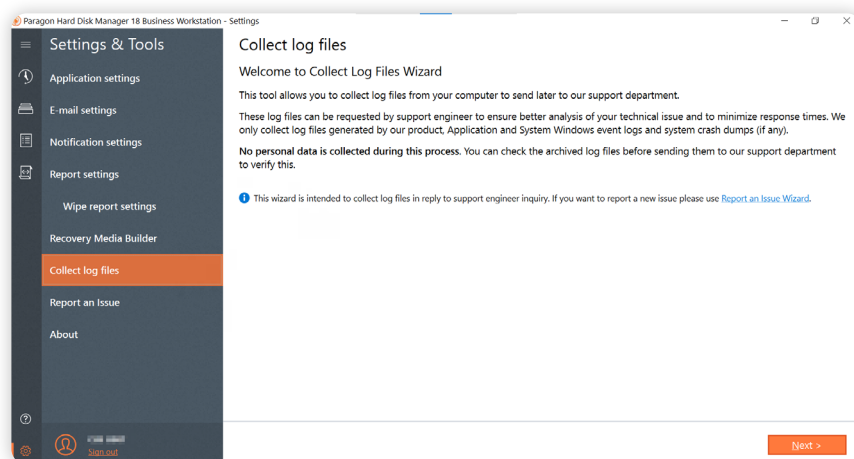
To contact our support, do one of the following:

- Go to **Settings** ⚙️ > **Report an Issue**. The **Report an Issue Wizard** will guide you through the process.



Note: Including log files in your support request allows our technical support team to provide a faster and more accurate solution.

To collect log files, go to **Settings** ⚙️ > **Collect log files**. Use the **Collect Log Files Wizard** to get the archived log file.



- Send an e-mail to support@paragon-software.com.
- Submit your [support request](#) via the website.

You can also refer to our [Knowledge base](#) to find out more about our products.

7.2 Copyright and Legal Notices

All rights reserved. No part of this manual may be processed, reproduced, or distributed in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, or by any data storage and retrieval systems—without the prior written permission of Paragon Software.

- **Trademarks:** All product names and services mentioned in this document may be registered trademarks or protected trademarks of their respective owners. The publisher and author make no claim to these trademarks.
- **Disclaimer of Liability:** Although this manual has been prepared with the utmost care, the publisher and author assume no responsibility for errors, omissions, or damage resulting from the use of the information contained herein or from the use of the associated software and source codes. Under no circumstances shall the publisher or author be liable for any loss of revenue, profits, data, or for direct, indirect, incidental, or consequential damages.