

O&O software

O&O DiskImage 22

Premium Edition

Table of Contents

1 Introduction 3

2 Get started 5

2.1 System requirements 5

2.2 Install and activate 7

2.3 Quick start 8

2.4 The first backup 10

3 Concepts 13

3.1 Backup sources 13

3.2 Backup destinations 16

4 Back up 18

4.1 Backup options 18

4.2 Schedules and automation 21

4.3 File names and exclusions 23

5 Restore 24

5.1 Restore overview 24

5.2 Restore files 25

5.3 Restore drives 26

6 Clone and recovery 27

6.1 Duplicate drives 27

6.2 Fortress Mode and startup medium 29

7 Management 33

7.1 Manage backups 33

7.2 Reports and logs 35

7.3 Tools 37

8 Settings 42

9 Glossary 46

10 Troubleshooting 48

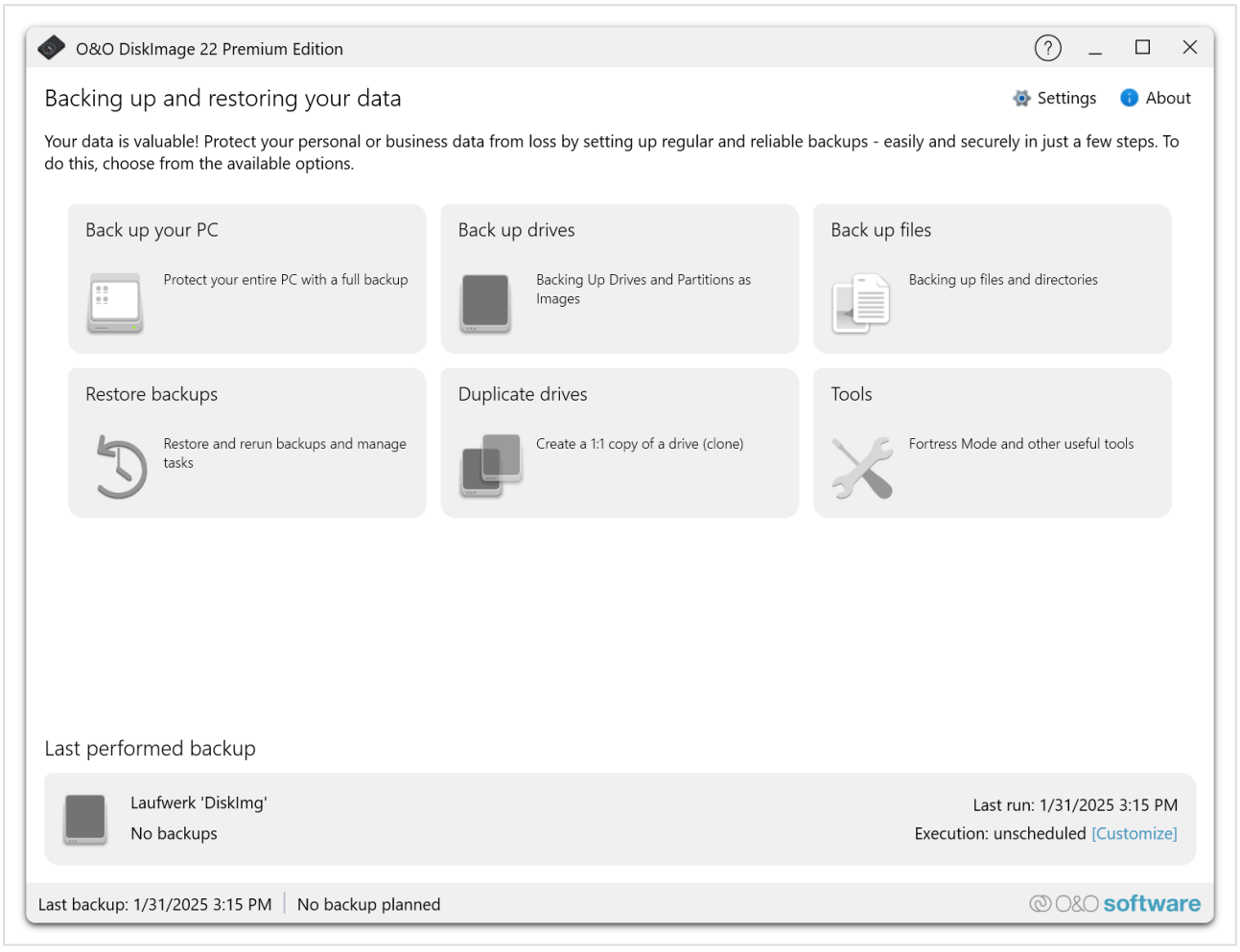
11 FAQ 51

12 Support and more from O&O 53

Introduction

This guide explains how to back up a Windows PC, restore data, duplicate drives, and prepare for recovery with **O&O DiskImage 22 Premium Edition**.

A backup is the insurance for your data: if a disk fails, malware strikes, or Windows no longer starts, you restore the PC from the backup instead of starting over. Back up regularly and keep the backups on a separate storage medium.



The start page offers the backup, restore and duplication functions and shows the last performed backup.

What you can do

- **Back up the entire PC**, selected drives and partitions, or individual files and folders.
- **Automate backups** with a schedule – once, hourly, daily, weekly or continuously – or start them when the backup drive is connected.
- **Choose a backup strategy**: a full backup followed by incremental or differential backups, or full backups only.

- **Restore** partitions, drives or whole disks from a backup, and copy individual files from a mounted backup.
- **Duplicate a drive** 1:1 when replacing or upgrading a disk.
- **Prepare recovery** with Fortress Mode and a startup medium, so the system can be restored even when Windows no longer starts.
- **Use the tools** to check, mount, convert and import backups, check and repair Windows, and connect network directories.

Where to start

Follow Quick start and The first backup for the first run. Then read Backup options and Schedules and automation to adjust ongoing protection.

Before you need to restore Windows, set up Fortress Mode and a startup medium.

Editions and license

This guide covers the Premium Edition for home users. The Professional, Server and Enterprise Editions add functions for business and server environments. They have a manual of their own: O&O DiskImage 22 Professional / Server.

O&O DiskImage is commercial software. You can try it during the trial period; continued use requires a valid license. See Install and activate.

System requirements

O&O DiskImage 22 backs up and restores Windows PCs. This page lists what the computer, the backup storage and the recovery options need. For current product information, see the O&O DiskImage product page.

Computer

Requirement	Minimum	Recommended
Operating system	Windows 10 (64-bit) or Windows 11 (64-bit)	Latest Windows updates installed
Memory	4 GB RAM	8 GB RAM or more
Disk space	500 MB for the installation, plus space for the data to back up or restore	Fast internal or external storage (for example an SSD) for backup and restore operations
Internet connection	Required for product activation, and for the recovery environment (Windows PE) – in particular for activation, updates and some recovery functions	–
Permissions	Local administrator rights for installation, configuration and activation	–

Dynamic disks are supported only as far as Windows supports them. Because Windows does not guarantee that dynamic disks can be booted in every configuration, the duplication or restore of a system to or from dynamic disks cannot be guaranteed either.

Supported file systems

File system	Use
NTFS	The standard file system of modern Windows versions, with access rights, compression, encryption and journaling.
FAT16 and FAT32	Older systems and removable media such as USB sticks and memory cards. Limited maximum file and partition sizes.
exFAT	High-capacity removable media and flash storage; manages very large files.
ReFS	Mainly server environments and critical applications; optimized for data integrity.

O&O DiskImage backs up the used sectors of all supported file systems. A partition with an unknown or unsupported file system is backed up forensically, that is, with all of its sectors. See Backup options.

Supported storage media

Storage medium	Notes
Internal hard disks (HDD/SSD)	All common internal disks, including RAID configurations.
External hard disks	Connected via USB, eSATA or Thunderbolt. Keeps the backup physically separate from the internal system disk.
USB sticks and memory cards	USB sticks, SD and microSD cards for portable backups.
Network storage (NAS)	Backups to NAS devices via SMB/CIFS.
Virtual hard disks	Backups in the VHD and VHDX formats for virtualized environments.

Store backups on a different physical disk from the data they protect. See Backup destinations.

Recovery

Option	Requirement
Fortress Mode	A working Windows Recovery Environment (WinRE) on the computer. O&O DiskImage checks it when you set up Fortress Mode.
Startup medium	A USB stick, a CD/DVD or an ISO file, and a PC that can boot from it. Booting the medium requires at least 4 GB RAM.
Drivers	Up-to-date storage controller drivers. The recovery environment can load additional drivers for RAID, NVMe or network controllers.

See Fortress Mode and startup medium.

Next steps

- Install and activate
- Quick start

Install and activate

Check the system requirements before installing O&O DiskImage 22. Product information is available on the O&O DiskImage product page.

Install

1. Download the setup file from the O&O Software website.
2. Run the setup file with administrator rights and follow the instructions of the setup.
3. Start **O&O DiskImage 22 Premium Edition**.

Trial and license

O&O DiskImage is commercial software. You can try it during the trial period; continued use requires a valid license.

Activating the license requires an active internet connection. The recovery environment of the startup medium also needs an internet connection, in particular for activation and updates.

After the installation

- Create the first backup. See Quick start.
- Open **Tools** and set up Fortress Mode or create a startup medium, so that you can restore the PC when Windows no longer starts.
- Check the defaults for new backups under **Settings**. See Settings.

Uninstall

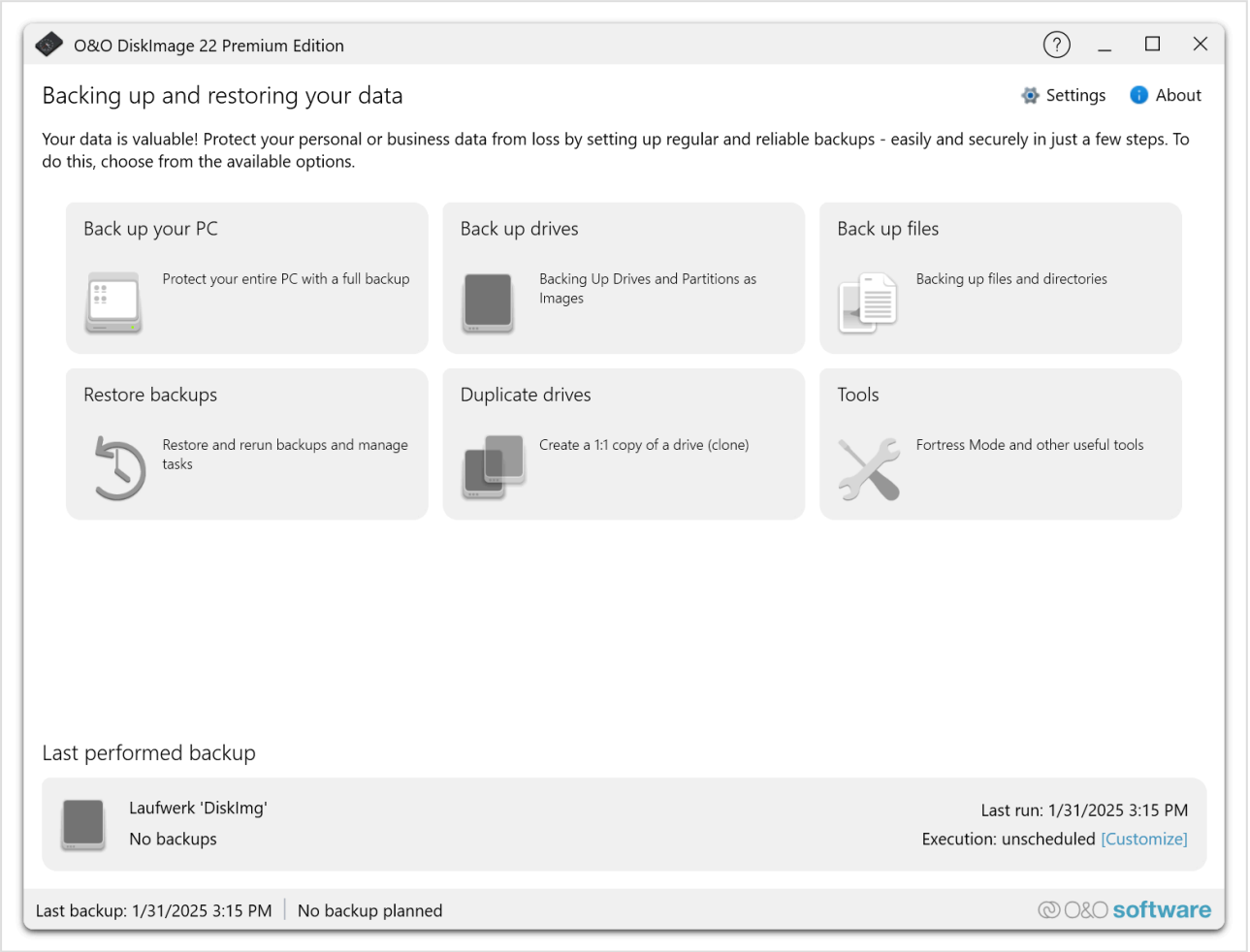
Open the Windows Control Panel, go to **Uninstall a program**, select O&O DiskImage and uninstall it. Backup files are not deleted when the application is uninstalled.

Next steps

- Quick start
- The first backup

Quick start

Create a backup first, then prepare a way to restore Windows if it can no longer start.



The start page offers the backup, restore and duplication functions; the lower part shows the last performed backup.

Before you start

Connect an external hard disk or prepare a network drive. An external storage medium is the recommended destination: a backup on the same disk as the data is lost together with it. Keep enough free space for the first full backup and the following backups.

Create the first backup

1. Open **O&O DiskImage 22 Premium Edition** and select **Back up your PC** on the start page.
2. Under **Description of the backup**, keep the name derived from the creation date or enter your own.

3. Check the **Destination file**. Use **Browse...** to select a folder on the external drive or network drive. A note below the field warns if the space on the target drive is expected to be insufficient.
4. Leave **Execution** on **Run Instantly**. To back up automatically later, select **Customize** – see Schedules and automation.
5. Select **Execute backup**. The backup can take some time, depending on the size of the drives.

The backup of the entire PC includes the system partition. It backs up only the used sectors and compresses the data, so the backup file is considerably smaller than the drives.

A practical starting point

Setting	Starting point
Scope	**Back up your PC**
Destination	External hard disk or network drive
Backup strategy	Full backup, then incremental backups (default)
Backup technology	Used sectors (default)
Compression	Lempel-Ziv (default)
Validation	Enable **Validate backup after completion** under **Settings > Validation**
Encryption	Enable **Encrypt backup with password** for backups on media that others can access

The defaults for new backups are set under **Settings**; see Backup options.

Prepare for recovery

Open **Tools** and set up **Fortress Mode**, or create a startup medium with **Creating a Startup Media**. Test that the PC starts from the medium and that the backup can be reached.

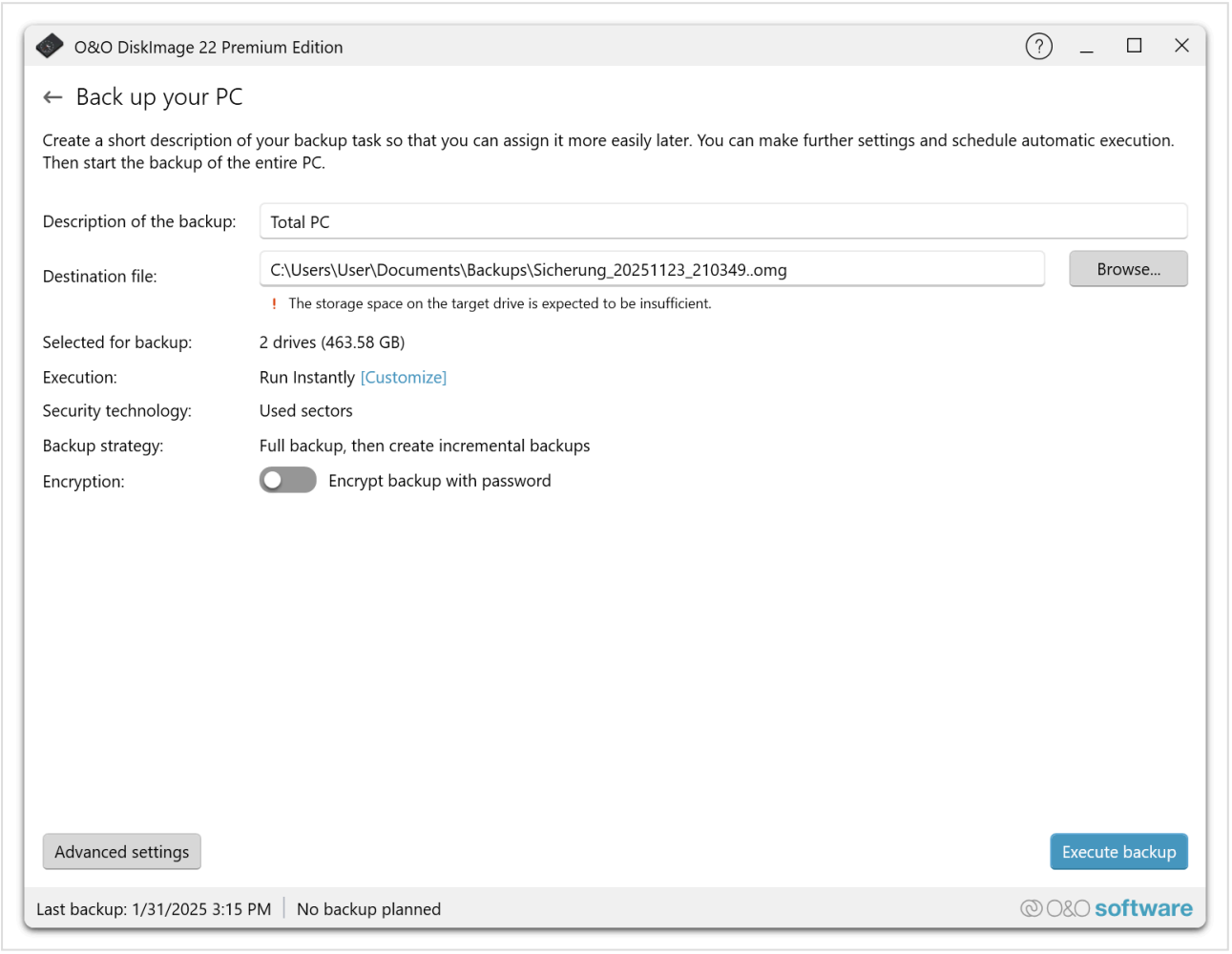
See Fortress Mode and startup medium.

Next steps

- The first backup explains the controls of the backup page.
- Manage backups shows how to rerun, move or delete backups.

The first backup

Every backup starts on the start page with one of three entries. The following backup page brings together the description, the destination file, the execution and the most important options.



The backup page summarizes the destination file, the execution and the options before the backup starts.

Choose what to back up

Entry on the start page	Use it for
Back up your PC	Windows, applications, settings and personal data – the entire PC including the system partition.
Back up drives	Images of selected drives or partitions.
Back up files	Selected files and folders, for example documents and photos.

For **Back up drives**, select the drives or partitions in the list and then select **Next**. Selecting a drive selects all of its partitions. For **Back up files**, navigate through the file system and select the files and folders.

See Backup sources for what each choice contains.

The backup page

Field	Meaning
Description of the backup	Name of the backup. By default it contains the creation date; enter a name that reflects the content if you prefer.
Destination file	Path and name of the backup file. **Browse...** opens a folder dialog. A note warns if the target drive is expected to run out of space.
Selected for backup	The number and size of the selected drives, or the selected files and folders.
Execution	**Run Instantly** by default. **Customize** opens the schedule. See Schedules and automation.
Security technology	The backup technology, by default **Used sectors**.
Backup strategy	The default strategy, for example **Full backup, then create incremental backups**.
Encryption	**Encrypt backup with password** protects the backup. Keep the password in a safe place: an encrypted backup cannot be restored without it.

Advanced settings opens the options of this backup, such as compression and backup technology. The defaults for all new backups are set under **Settings**. See Backup options.

Start and check the result

Select **Execute backup**. The duration depends on the size of the selected drives or files.

After completion, the start page shows the backup under **Last performed backup**, together with its execution setting. Open **Restore backups** and select **Show reports** to check the report of the backup. See Reports and

logs.

Next steps

- Schedules and automation – run the backup automatically.
- Manage backups – rerun, move or delete the backup.

Backup sources

A source is the data a backup protects. Choose **Back up your PC**, **Back up drives** or **Back up files** on the start page.

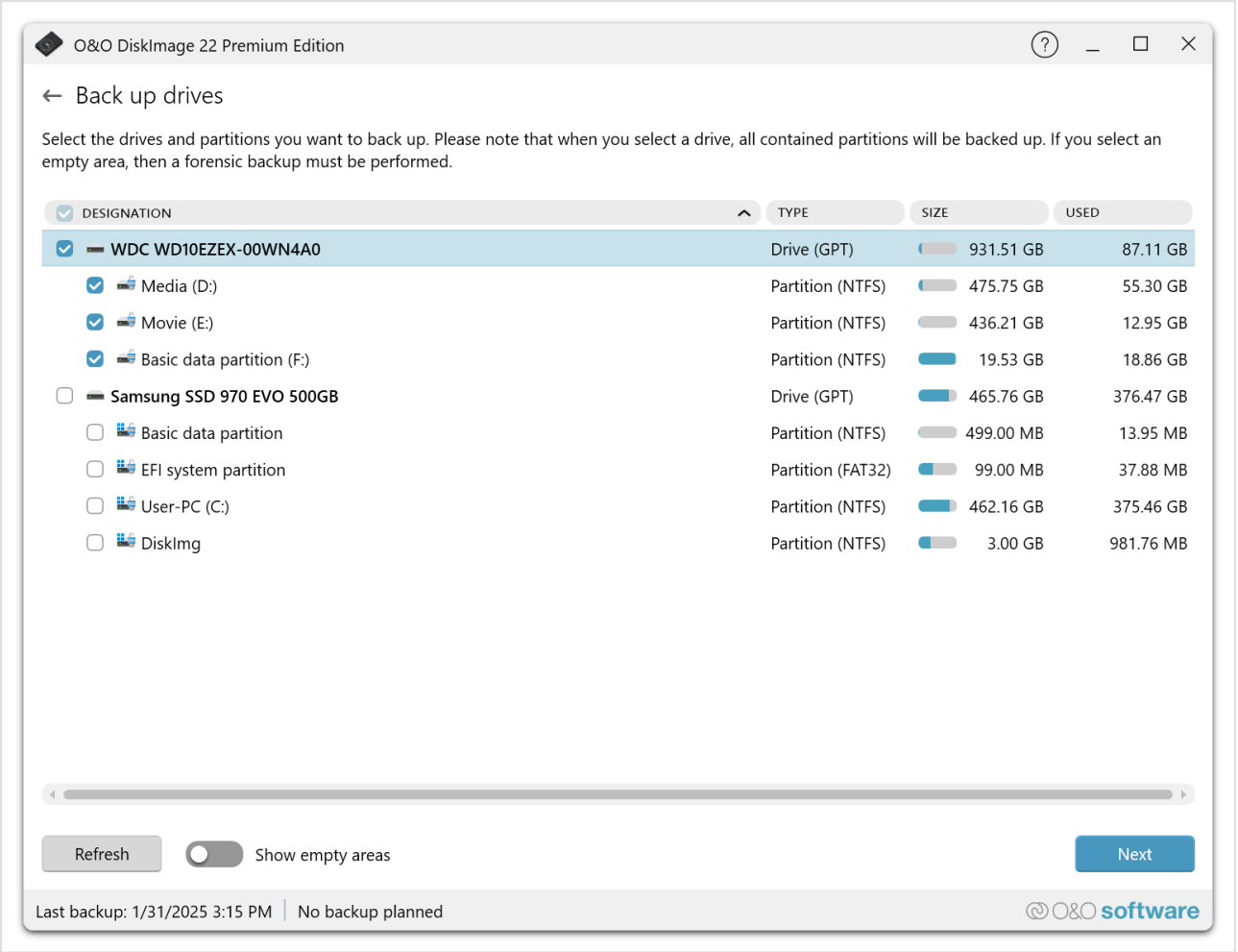
Entire PC

Back up your PC backs up the entire computer including the system partition – Windows, applications, settings and personal data. Use it as the starting point for system recovery and as the first backup of a new PC.

The backup uses the **Used sectors** technology, so only the parts of the disks that contain data are backed up, and compresses the data. See Backup options.

Drives and partitions

Back up drives creates an image of selected drives or partitions. Use it when you want to protect certain data or partitions rather than the whole system.



Select whole drives or individual partitions in the list; selecting a drive includes all of its partitions.

- Selecting a drive selects all of its partitions. The list shows the type, size and used space of every entry; **Refresh** reads the drives again.
- **Show empty areas** also lists unpartitioned areas. If you select an empty area, the backup must be a forensic backup, because there is no file system whose used sectors could be read.
- A partition with an unknown or unsupported file system is backed up forensically as well.

Files and folders

Back up files backs up selected files and folders, for example documents, photos or project folders, without creating an image of the whole drive. Navigate through the file system and select individual files or entire folders.

A file backup contains only the selected files. To restore Windows and the installed applications, you need a backup of the PC or of the system drive.

Exclusions

Files and folders on the **Exclusion** list under **Settings** are left out of every backup, for example temporary files or media that are already backed up elsewhere. See File names and exclusions.

Backup destinations

The destination is the folder in which O&O DiskImage stores the backup file. Choose a storage medium with enough space for the first full backup and the following backups.

Choose a destination

Store backups on a different physical disk from the data they protect. If the disk with the data fails, a backup on the same disk is lost with it. An external storage medium – a USB hard disk or a network drive – is the recommended destination.

On the backup page, the **Destination file** field shows the path and name of the backup file. **Browse...** opens a folder dialog. A note below the field warns if the space on the target drive is expected to be insufficient; choose another destination in that case.

Supported storage media

Storage medium	Use
Internal hard disks (HDD/SSD)	Local backups on a second internal disk, including RAID configurations.
External hard disks	USB, eSATA or Thunderbolt disks that keep the backup physically separate from the system disk.
USB sticks and memory cards	Portable backups of files and folders.
Network storage (NAS)	Central backups via SMB/CIFS. Connect the share first, see below.
Virtual hard disks	Backups in the VHD or VHDX format for virtualized environments.

Target folders

Under **Settings > Target folders**, specify the folders in which new backups are stored by default. You can enter several folders. O&O DiskImage uses them in descending order of their free space, so a new backup is stored where the most space is available.

- **Add** a folder, for example on a second storage medium.
- **Change** the path of a folder, for example after replacing a drive.
- **Remove** a folder that is no longer available or needed.

Check that the folders offer enough space and are permanently accessible. See Settings.

Network directories

To back up to a NAS or another network share, connect the directory first: open **Tools > Connect Network Directory**, enter the network path and, if required, the login credentials, and confirm. The share must remain accessible and must allow writing. See Tools.

Backups in network directories, on other PCs or on external drives that O&O DiskImage does not list can be added with **Import backups**. See Manage backups.

Backup options

The defaults for new backups are set under **Settings**; open them with **Settings** at the top right of the start page. **Advanced settings** on the backup page shows the options of the backup you are setting up.

Backup strategy

Strategy	What is stored	Files needed for a restore
Full backup, then create incremental backups	A full backup first; afterwards only the changes since the previous backup. Saves space and time.	The full backup and every incremental backup up to the selected one.
Full backup, then create differential backups	A full backup first; afterwards all changes since the last full backup.	The full backup and the selected differential backup.
Only create full backups	A complete copy of the selected data every time. Needs the most space.	That full backup alone.

Review the storage requirement and the efficiency of the chosen strategy from time to time and adjust it if needed.

Execution policy

The **Execution policy** determines after how many change backups – incremental or differential backups – a new full backup is created. This keeps the chain of change backups short, so a restore stays fast and simple.

Enable the option and specify the number of change backups after which a new full backup is created. Weigh the storage space of full backups against the speed and safety of a restore.

Backup technology

Technology	Meaning
Used sectors	Copies only the sectors of a drive that contain data. Saves space and time; the recommended method.
Forensic backup	Copies every sector of the drive, including unused areas with potentially recoverable data. Suitable for legal or investigative purposes.
Direct forensic backup	Creates an exact copy directly from the disk, so the original state is not changed. Available only in Fortress Mode.

Forensic backups need storage space for the full size of the backed-up drive. The direct forensic backup can only be performed in Fortress Mode; enable it under **Tools** before starting such a backup. See Fortress Mode and startup medium.

Compression method

Enable compression to reduce the size of the backup files. Without compression, the data is stored in its original size, which can be faster but needs more space.

Method	Meaning
Lempel-Ziv algorithm (default)	Balanced compression without a noticeable effect on the backup speed.
Lempel-Ziv algorithm (maximum)	Stronger compression that takes more time and reduces the file size further.
ZIP deflate compression	A common, widely supported compression method.
BZIP method (1K block size)	Efficient compression with a small block size; faster, but compresses less.
BZIP method (4K block size)	A balance between compression rate and speed.
BZIP method (9K block size)	The highest compression rate of the BZIP options, at the expense of speed.

Stronger compression lengthens the backup and uses more system resources.

Backup format

Format	Meaning
O&O DiskImage format	The recommended standard format. It allows all backup options and the restore with O&O DiskImage.
Virtual Hard Disk Format (VHD)	The Microsoft format for virtual hard disks, used by virtualization solutions.
Virtual Hard Disk Extended Format (VHDX)	The improved version of VHD with larger capacity and better performance.

> **Note**
>
> Backups in the VHD and VHDX formats cannot be restored with O&O DiskImage. They can only be mounted as virtual drives. Use the O&O DiskImage format for backups you want to restore.

Check that the chosen format is compatible with the systems on which you need to access the backup files.

Encryption

Encrypt backup with password on the backup page protects the backup with a password. Keep the password in a safe place: an encrypted backup cannot be restored without it.

Validation

Under **Settings > Validation**, enable **Validate backup after completion** to check every finished backup for integrity. The check reads the backup file and compares its structure with the expected data, so errors that occurred during the backup are found early.

Validation takes additional time, depending on the size and location of the backup file. Enable it at least for important backups. A backup can also be checked later with **Tools > Check backup**; see Tools.

Report

Under **Settings > Report**, enable **Create report** to record every backup operation with its time, the files involved, the space used and any errors. Reports help you to monitor backups and to analyze problems. See Reports and logs.

Schedules and automation

A backup runs immediately by default. The execution setting lets it run according to a schedule or as soon as the backup drive is connected (hotplug).

Open the execution settings

1. On the start page, select **Back up your PC**, **Back up drives** or **Back up files**.
2. On the backup page, **Execution** shows **Run Instantly**. Select **Customize**.
3. Choose the execution type and confirm.

The start page shows the execution of the last performed backup under **Last performed backup**, with a **Customize** link to change it. The status bar shows whether a backup is planned.

Execution options

Option	Behavior
Run backup immediately	The backup runs as soon as you select **Execute backup** and is not repeated automatically. Default.
Do not schedule automatic backup	The backup is only started manually.
Perform automatic backup according to a schedule	The backup runs regularly at the chosen interval.
Perform automatic backup when connecting a drive (Hotplug)	The backup starts as soon as the configured destination drive is connected.

Schedule

If you choose **Perform automatic backup according to a schedule**, the following intervals are available:

Interval	Behavior
Only once	Runs once at the specified time.
Hourly	Runs at a freely definable interval of hours.
Daily	Runs every day at the specified time.
Weekly	Runs on the selected weekdays at the specified time.
Continuous	Runs again after a waiting time that you define.

For **Continuous**, choose the **Waiting time until next backup**: 30 minutes, 1, 2, 4, 8 or 12 hours, 1 or 2 days, or 1, 2 or 4 weeks. The backup is run again whenever the waiting time has elapsed.

Backups when a drive is connected

With **Perform automatic backup when connecting a drive**, the backup starts as soon as the configured backup destination is connected, for example an external USB hard disk.

The **Execution delay** sets how long after the connection the backup starts: immediately, 5, 15 or 30 seconds, or 1, 5, 10, 15 or 30 minutes. A delay gives the drive time to initialize completely after it is connected.

Recommendation

Automatic execution keeps the backups current without manual intervention. For important data, set up a daily or continuous backup.

Keep the destination available at the planned time: a scheduled backup to an external drive or a network directory can only run while that destination is connected. See Troubleshooting.

File names and exclusions

Use the file name settings to keep backup files organized and the exclusion list to leave out data you do not need.

File names

Under **Settings > File names**, specify where new backup files are stored and how they are named:

Setting	Meaning
Storage path	The folder for the backup files: a local folder, a network path or an external drive.
File name	A fixed name, or a name with placeholders that is generated for every backup. Placeholders insert, for example, the current date, the time or a sequential number, so every backup file is identifiable.
Preview	Shows the resulting file name, so you can check that all placeholders are resolved as intended.

By default, the name contains the creation date. Backup files of the O&O DiskImage format have the extension `.omg`. On the backup page, **Destination file** shows the resulting path, and **Browse...** lets you choose another folder for that backup. See Backup destinations.

Exclusion

The **Exclusion** list under **Settings** excludes specific files and folders from every backup. Use it for temporary files, system cache files or media that are already backed up elsewhere, so backups stay small and contain only the data you need.

Add or remove entries

1. Open **Settings** and select **Exclusion**.
2. Select **+** and navigate to the file or folder to exclude.
3. Select the files or folders and confirm. They are added to the list and left out of future backups.
4. To remove an entry, select it in the list and select **−**.

An excluded folder is excluded with all of its contents. Excluded files are not contained in the backup and cannot be restored from it, so check carefully that no important data is excluded.

Restore overview

Select **Restore backups** on the start page to restore a backup or to manage the existing backups.

Find a backup

Restore backups lists the backups that O&O DiskImage knows. Select the backup in the list, or choose its file in the file dialog.

If a backup is not listed – for example a backup from another PC, on an external drive or in a network directory – add it with **Import backups**. See Manage backups. Keep the full backup and all change backups that belong to it available.

Choose a restore type

Goal	What to do
Restore partitions, drives or a whole disk	Restore the backup under **Restore backups**. See Restore drives.
Copy individual files from a backup	Mount the backup as a virtual drive with **Tools > Mount drives** and copy the files in Windows Explorer. See Restore files.
Restore the system partition or a locked drive	Start Fortress Mode under **Tools**; it allows full access to the entire system. See Fortress Mode and startup medium.
Restore a PC whose Windows no longer starts	Start the PC from the startup medium and restore the backup there.

Before you start

- Restoring a whole disk or the system partition overwrites all data on the target. Check that the target contains no data you still need.
- Keep the password of an encrypted backup available.
- Backups in the VHD or VHDX format cannot be restored with O&O DiskImage; they can only be mounted as virtual drives.
- Check the target disk carefully. In Fortress Mode and in the recovery environment of the startup medium, drive letters can differ from those in Windows.

Restore files

To get individual files or folders back, mount the backup as a virtual drive. Windows then shows the backup like a normal drive, and you copy the files you need.

Mount a backup

1. Open **Tools** on the start page and select **Mount drives**.
2. Select the backup file. If the backup is encrypted, enter its password.
3. Confirm. The drives of the backup appear with their own drive letters in Windows Explorer.
4. Copy the files and folders you need to the PC.

Use this to access files from a backup, to restore individual data, or to compare the content of a backup with the current state.

Backups in the VHD and VHDX formats can be mounted as well; mounting is the only way to access their content with O&O DiskImage.

Remove the virtual drive

When you no longer need the files, open **Tools** and select **Cancel integration**. The virtual drive disappears from the drive overview of Windows; the backup file itself is not changed.

Restore a file backup

A backup created with **Back up files** can also be restored as a whole: open **Restore backups**, select the file backup, specify what to restore and the destination, and follow the wizard. Restoring to the original location overwrites existing files; restore to a separate folder if you want to compare the files first.

Next steps

- Restore drives – restore partitions or whole disks.
- Manage backups – import, move or delete backups.

Restore drives

A drive restore writes the content of a backup to a partition, a drive or a whole disk. The existing data on the target is overwritten.

Restore a disk or partition

1. Select **Restore backups** on the start page.
2. Select the backup in the list, or choose its file in the file dialog.
3. Specify what to restore: the whole disk or individual partitions.
4. Select the target drive. It can be the original disk or a new or empty disk.
5. Start the restore and follow the steps of the wizard.

> **Data on the target is overwritten**
>
> Restoring a whole disk or the system partition overwrites all data on the target medium. Check that the target contains no data you still need.

Keep the full backup and all change backups that belong to the selected backup available. Backups in the VHD and VHDX formats cannot be restored; they can only be mounted. See Backup options.

Restore the system partition

The system drive is in use while Windows is running, so it cannot be overwritten in normal operation. Use **Fortress Mode** under **Tools**: it restarts the PC in a protected environment with full access to the entire system, including locked drives, and prevents running processes or malware from interfering with the restore.

If Windows no longer starts, start the PC from the startup medium and restore the backup from the recovery environment. Reconnect the backup storage there and keep the password of an encrypted backup available.

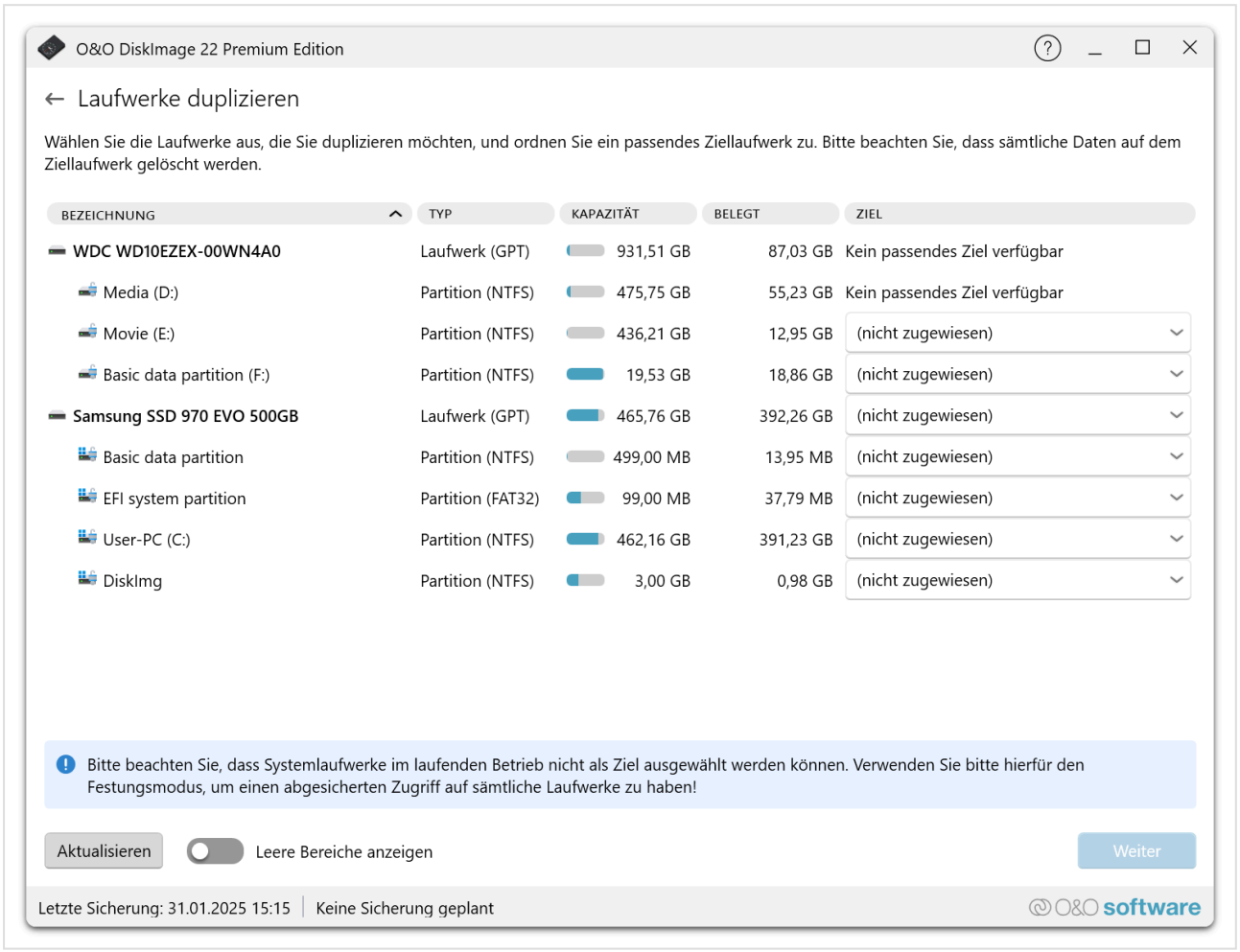
See Fortress Mode and startup medium.

After the restore

- Check the report of the restore and verify the restored data.
- After restoring Windows, restart the PC and check that it starts.
- If the PC has BitLocker-protected drives, have the recovery key ready: in the recovery environment, encrypted volumes can only be used after they have been unlocked.

Duplicate drives

Duplicate drives transfers an exact copy of a drive to another drive. Use it when you upgrade a hard disk or want a directly usable copy of a drive without storing a backup file.



Assign a target to the drive or partition to duplicate; the list shows the capacity and used space of every entry (German interface).

Duplicate a drive

1. Select **Duplicate drives** on the start page.
2. Select the source drive – the drive you want to duplicate.
3. Assign the target drive to which the data is transferred. The target must be at least as large as the source. If no suitable target is available, the list says so.
4. Check the selection and confirm that all data on the target drive will be deleted.
5. Start the duplication. It can take some time, depending on the size of the drives.

> **All data on the target drive is deleted**
>
> Duplicating a drive deletes all existing data on the target drive. Back up any data on the target you still need before you start.

Things to consider

- **Capacity of the target drive**: the target must be at least as large as the source drive.
- **System drives**: while Windows is running, the system drive cannot be selected as a target. Use Fortress Mode for protected access to all drives. See Fortress Mode and startup medium.
- **Avoid interruptions**: do not interrupt the duplication, otherwise the target drive can be left incomplete.
- **After the duplication**: check that the duplicated drive works and contains the expected data before you remove the original.

Next steps

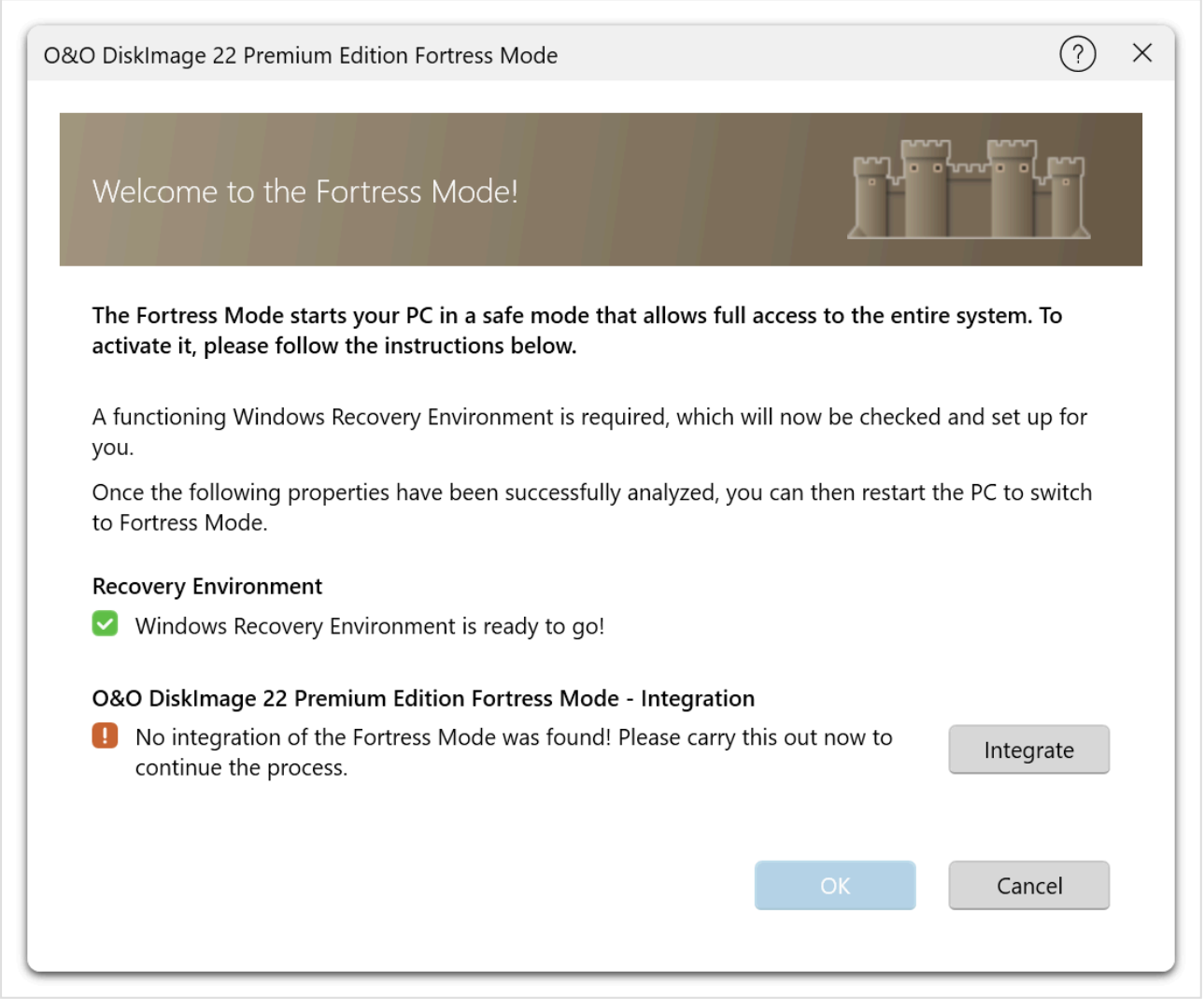
- Backup sources – when a backup file is the better choice.
- Restore drives – restore a drive from a backup instead.

Fortress Mode and startup medium

Both functions let you restore the PC outside the running Windows system: Fortress Mode restarts the installed PC in a protected environment, the startup medium starts a PC without a working operating system.

Fortress Mode

Fortress Mode starts the PC in a protected recovery environment with full access to the entire system. Use it to restore the system partition or locked drives, to duplicate to the system drive, and for direct forensic backups. Because Windows is not running, no running processes or malware can interfere with the operation.



The Fortress Mode dialog checks the Windows Recovery Environment and offers to integrate Fortress Mode.

Set up and start Fortress Mode

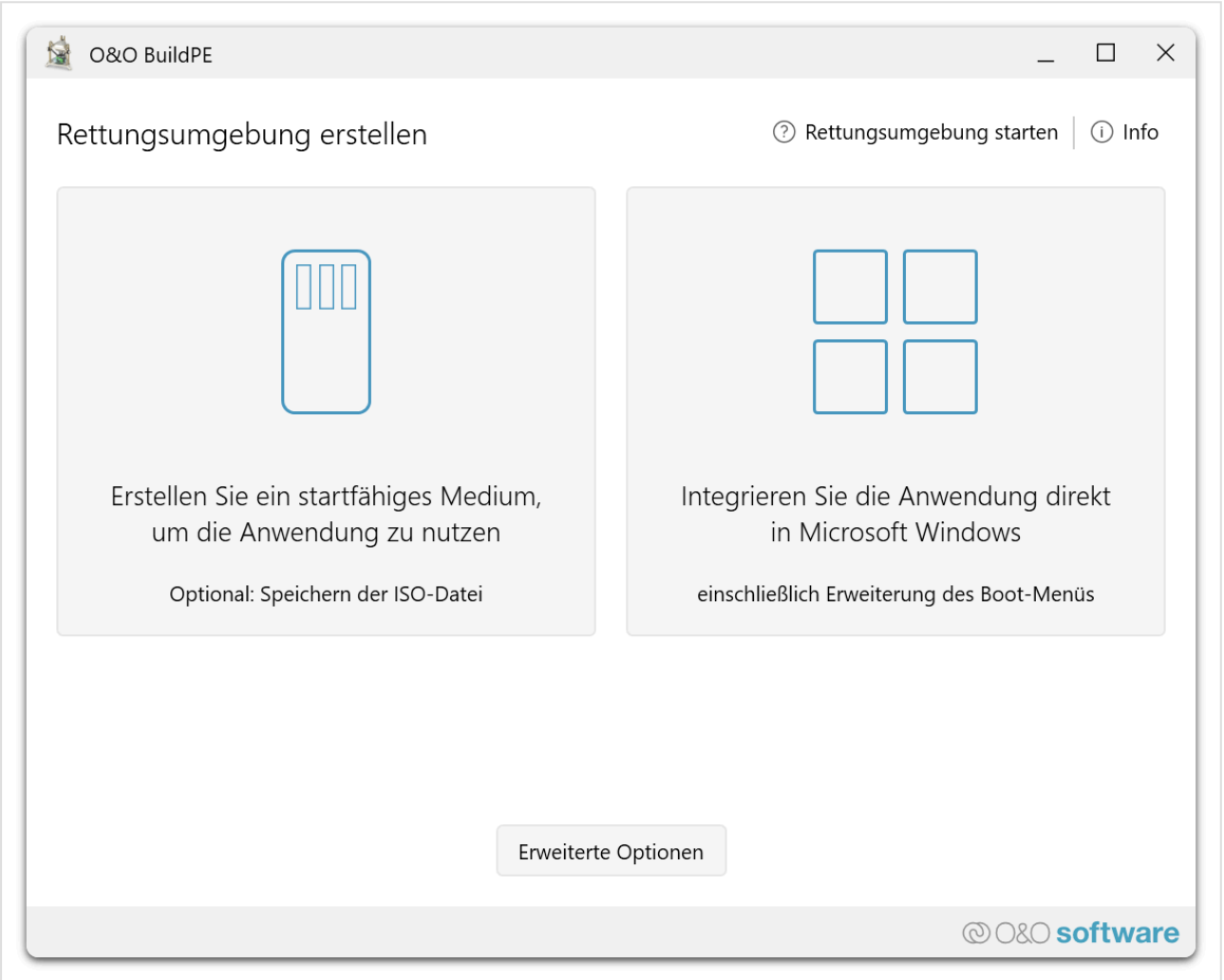
1. Open **Tools** on the start page and select **Fortress Mode**.

2. The dialog checks whether a working Windows Recovery Environment is available.
3. If Fortress Mode is not integrated yet, select **Integrate**.
4. Select **OK** and restart the PC to switch to Fortress Mode.

Set up Fortress Mode before you need it. It depends on a working Windows Recovery Environment (WinRE) on the local disk; if the system disk fails, you need the startup medium instead.

Startup medium

A startup medium starts a PC that has no working operating system and runs O&O DiskImage from a recovery environment based on Windows PE, so you can restore the whole computer or the system partition from a backup.



O&O BuildPE creates a bootable medium or integrates the recovery environment into the Windows boot menu (German interface).

Create a startup medium

1. Open **Tools** and select **Creating a Startup Media**. **O&O BuildPE** starts.
2. Choose one of the options:

- **Create a bootable medium to use the application**: creates a bootable USB stick, CD/DVD or ISO file. Optionally, save the ISO file for later use.
- **Integrate the application directly into Microsoft Windows**: adds the recovery environment to the Windows boot menu, so it can be started without an external medium.

3. Follow the steps of O&O BuildPE.

Advanced options offers the expert mode, a cleanup before the creation, the integration of O&O Syspectr, and the log files.

> **The medium is overwritten**
>
> The selected medium is completely overwritten. Back up any data on it first, and do not use the drive that holds your only backup.

Create the medium while the PC still works, and test that the PC starts from it and can reach the backup. Recreate the medium after major Windows updates or an upgrade of O&O DiskImage, so it contains current drivers and components.

Start the PC from the medium

1. Connect the USB stick or insert the CD/DVD and start the PC.
2. Open the boot menu of the PC, or change the boot order in the BIOS/UEFI setup, so the medium is started first. The documentation of the mainboard manufacturer describes how.
3. In the recovery environment, select the language and region, load additional drivers if a device is missing, and accept the license terms. O&O DiskImage starts.

Notes for the start:

- **Secure Boot** may have to be disabled so that the Windows PE medium can start.
- Start the PC in the same boot mode (UEFI or Legacy/CSM) in which the medium was created.
- Windows PE often uses the English (US) keyboard layout. Switch the layout in the start dialog before entering passwords or paths.
- Some PCs start a USB stick only from USB 2.0 ports. If the stick is not detected, use another port or recreate the medium.
- The boot order chosen in the boot menu usually applies to the current start only.

Work in the recovery environment

- If a hard disk, RAID array, NVMe controller or network adapter is not detected, its driver is missing. Load it in the **O&O System Settings** dialog on the **Drivers** tab from a USB stick or another drive. Copy the storage, network and chipset drivers of the PC to a USB stick in advance, so they are available in an emergency.
- If the backup is in a network directory, the network adapter must be recognized; load its driver if necessary.

- Have the recovery key of BitLocker-protected drives ready. Encrypted volumes can only be used after they have been unlocked.
- Drive letters can differ from those in Windows. Identify disks by their name, size and content before restoring.
- Keep the password of an encrypted backup available. The recovery environment needs an internet connection for activation and updates.

See Restore drives for the restore itself.

Manage backups

Restore backups on the start page is the central place for all existing backups. Besides the restore, it imports, moves, deletes and reruns backups and shows their reports.

The backup list

The list shows the backups that O&O DiskImage knows, with their name and the time of the last run. The start page also shows the last performed backup with its execution setting; **Customize** there changes the schedule. See Schedules and automation.

Import backups

Import backups adds existing backup files that O&O DiskImage has not detected automatically, for example:

- backups from other PCs,
- backups on external drives,
- backups in network directories.

Select the backup file; afterwards the backup is available for restore and management like any other. The same function is available under **Tools**. Keep the full backup and the change backups that belong to it together.

Move backups

Move backup transfers an existing backup file to another storage location, for example to a NAS, an external hard disk or a larger internal disk. O&O DiskImage updates its internal references, so the backup is still recognized afterwards.

Delete backups

Delete removes a backup that is no longer needed and frees its storage space. Select the backup in the list and select **Delete**.

> **Deleting is permanent**
>
> A deleted backup cannot be restored. Deleting a full backup also makes the incremental or differential backups that depend on it unusable.

Run a backup again

- **Run backup** creates a new backup with the settings stored in the backup file, for example the next incremental or differential backup of a strategy.
- **Run backup again** repeats a backup with exactly the same parameters as the original operation. Use it to update the same backup regularly.

Show reports

Show reports opens the reports of a backup: the time and duration, the parameters used, warnings or errors, validation results and the overall status. See Reports and logs.

Reports and logs

Reports record individual backup operations. Logs provide additional detail when a problem has to be analyzed.

Reports

When **Create report** is enabled under **Settings > Report**, O&O DiskImage records every backup operation. A report contains:

- the time and duration of the backup,
- the parameters used,
- the files involved and the storage space used,
- warnings or errors,
- the validation result, if validation is enabled,
- the overall status of the backup.

Open **Restore backups**, select the backup and select **Show reports** to read its reports. Use them to monitor backups, to document that they ran, and to find the cause of a problem.

Reports add a little administrative effort and storage space. Disable them only if you do not need the information.

Logs

Settings > Logging enables detailed logs of the backup operations. A log records the start and end time of a backup, the files involved, the size of the backup, and errors and warnings that occurred.

Logs help with three things:

- **Troubleshooting**: errors and warnings are recorded with their context, so the cause of a problem is easier to find.
- **Monitoring**: the logs show whether all planned backups ran as intended.
- **Documentation**: they are evidence that backups were performed, which some environments require.

Contact support

If you contact O&O Software support, include:

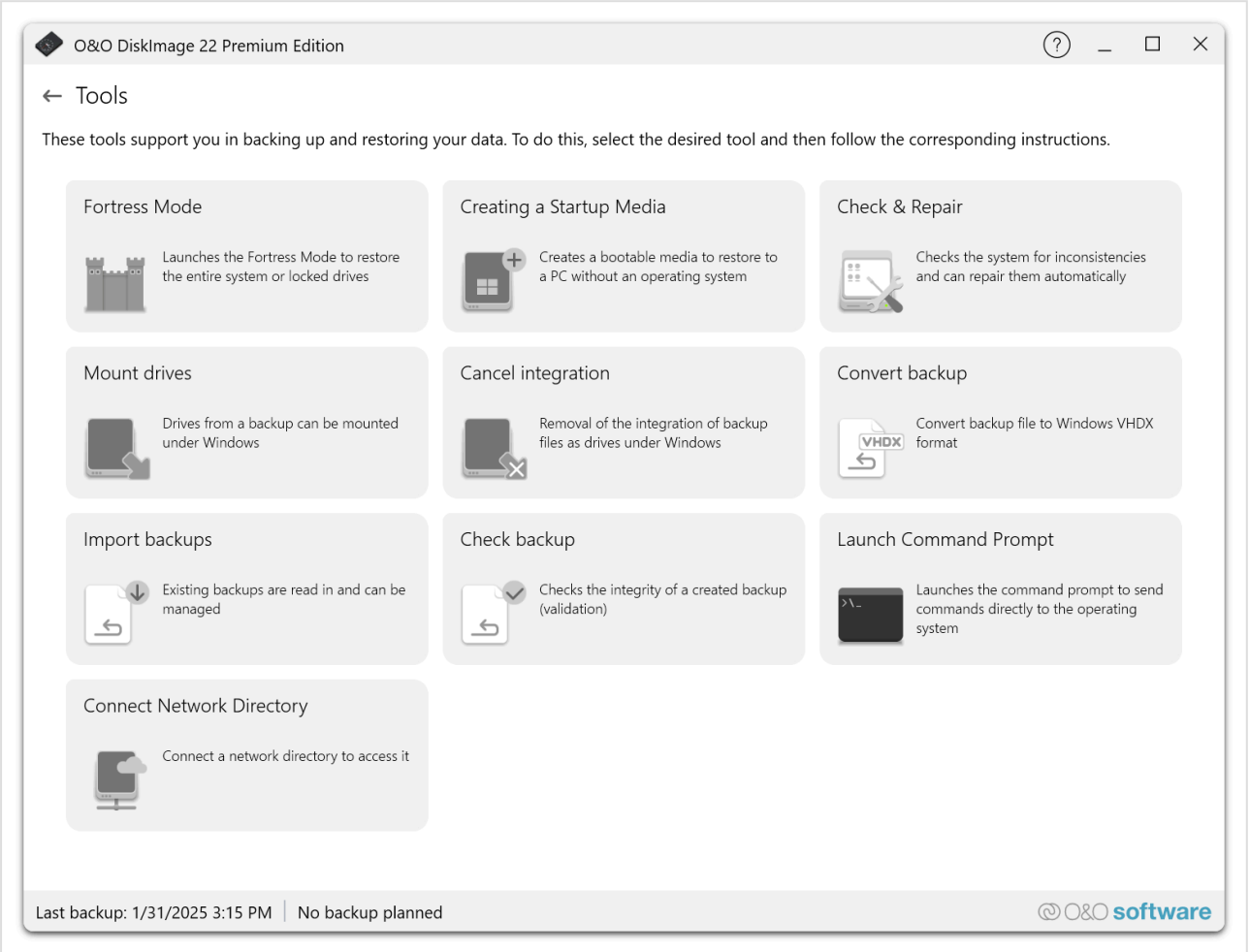
- the version of O&O DiskImage (**About** on the start page) and the Windows version,
- the report of the failed operation,
- the type of source and destination, for example the system drive and a USB disk,

- whether the backup was started manually, by schedule or when connecting the drive,
- whether the problem occurred in Windows, in Fortress Mode or in the recovery environment of the startup medium.

Add the logs if support requests them.

Tools

Select **Tools** on the start page. The tools support you in backing up and restoring data; select a tool and follow its instructions.



The Tools page groups the recovery, backup, system and network tools.

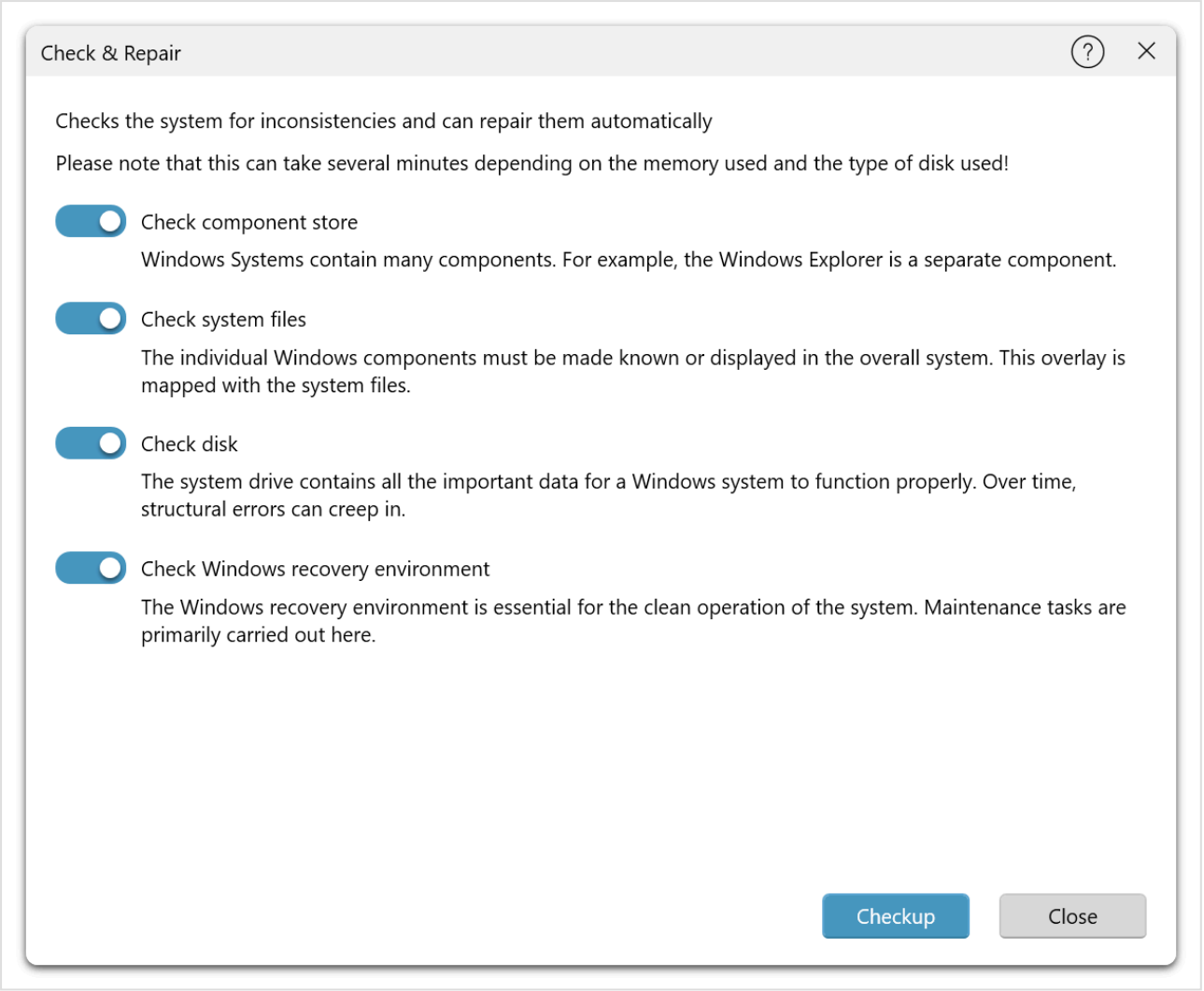
Tool	Purpose
Fortress Mode	Starts the protected recovery environment to restore the entire system or locked drives.
Creating a Startup Media	Creates a bootable medium to restore a PC without an operating system.
Check & Repair	Checks the Windows system for inconsistencies and repairs them.
Mount drives	Mounts the drives of a backup as drives in Windows.
Cancel integration	Removes mounted backup drives again.
Convert backup	Converts a backup file to the Windows VHDX format.
Import backups	Reads existing backups so that they can be managed.
Check backup	Checks the integrity of a created backup (validation).
Launch Command Prompt	Opens the command prompt to send commands directly to the operating system.
Connect Network Directory	Connects a network directory to access it.

Fortress Mode and startup medium

Fortress Mode and **Creating a Startup Media** prepare the recovery of the PC outside the running Windows system. See Fortress Mode and startup medium.

Check & Repair

Check & Repair checks the Windows system for inconsistencies and can repair them automatically. Depending on the amount of data and the type of disk, the check takes several minutes.



Choose what Check & Repair checks, then start the check with Checkup.

Option	What is checked
Check component store	The Windows component store, in which the components of Windows are kept.
Check system files	The protected system files; damaged files are repaired.
Check disk	The structure of the system drive, in which errors can creep in over time.
Check Windows recovery environment	Whether the Windows Recovery Environment works; Fortress Mode depends on it.

Enable the checks you need and select **Checkup**. Check & Repair checks Windows, not backup files; to check a backup, use **Check backup**.

Mount drives and cancel integration

Mount drives mounts a backup as a virtual drive in Windows, so you can copy files from the backup like from a normal drive, restore individual data, or compare the content of a backup. **Cancel integration** removes the virtual drive again without deleting any data. See Restore files.

Convert backup

Convert backup converts a backup file to the **VHDX** format of Windows. The result can be used as a virtual drive or in Hyper-V.

Import backups

Import backups reads existing backup files that are not registered in O&O DiskImage yet – backups from other PCs, older backups, or backups in network directories. Afterwards they are listed under **Restore backups**. See Manage backups.

Check backup

Check backup validates a backup file, so you know that it can be restored completely and without errors.

1. Open **Tools** and select **Check backup**.
2. Select the backup file to check.
3. Start the check.
4. Read the report that is shown when the check is finished.

The duration depends on the size and the storage location of the backup. To check every backup automatically after it is created, enable **Validate backup after completion** under **Settings > Validation**.

Launch Command Prompt

Launch Command Prompt opens the Windows command prompt, through which advanced commands can be sent directly to the operating system, for example:

- `chkdsk C: /f` – checks and repairs the file system of a drive
- `sfc /scannow` – checks and repairs protected system files
- `diskpart` – manages disks and partitions
- `ipconfig /all` – shows the network configuration

> **Warning**
>
> Some commands delete data or change system settings. Only run commands whose effect you know.

Connect Network Directory

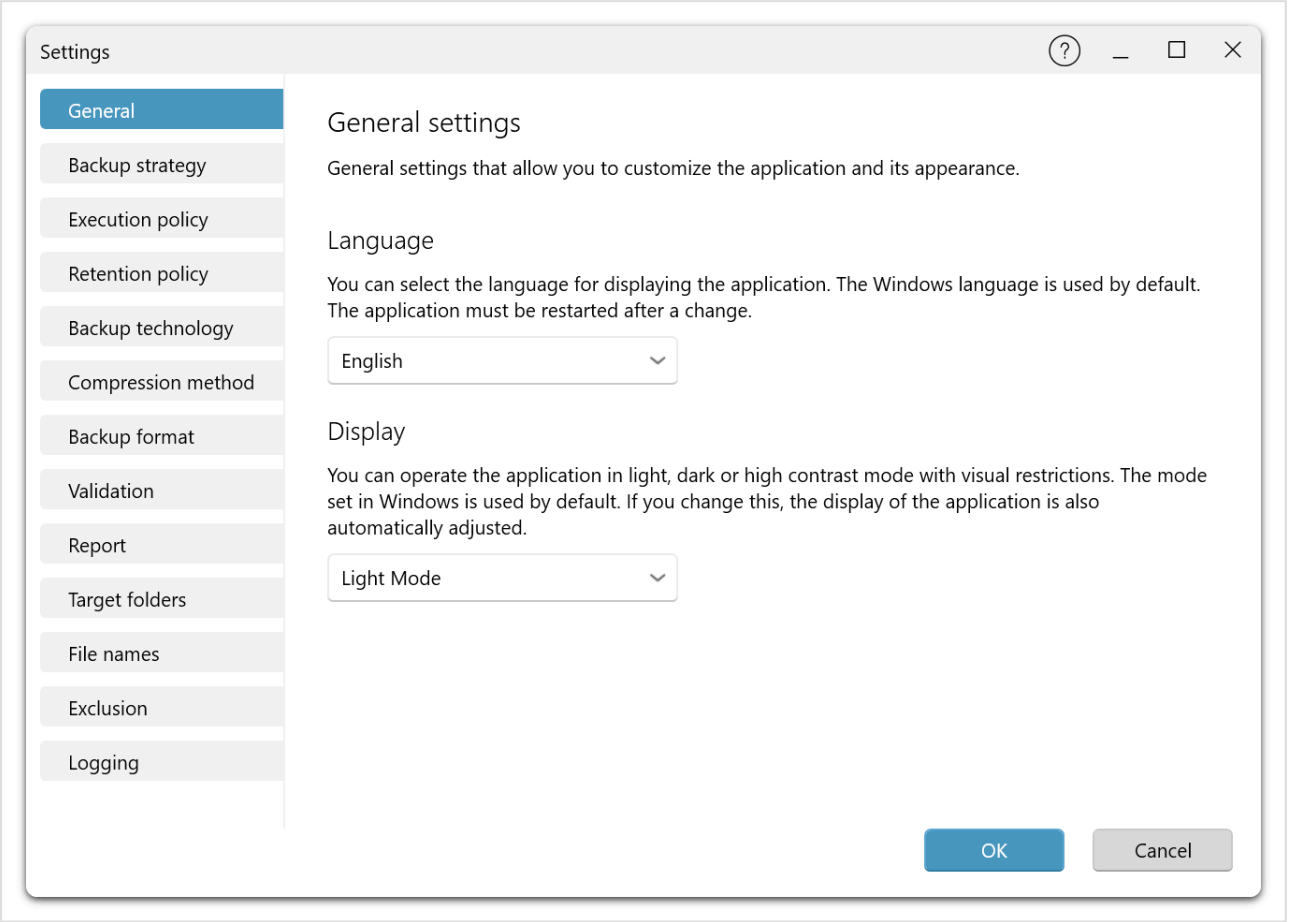
Connect Network Directory connects a shared network directory, for example on a NAS, so that backups can be stored there or read from there.

1. Open **Tools** and select **Connect Network Directory**.
2. Enter the network path and, if required, the login credentials.
3. Confirm the connection.

The network directory must remain accessible and must allow writing. See Backup destinations.

Settings

Open **Settings** at the top right of the start page. The settings are the defaults for new backups and the preferences of the application. Confirm the dialog with **OK** to save changes; **Cancel** discards them.



The General page sets the language and the display mode of the application.

Pages of the dialog

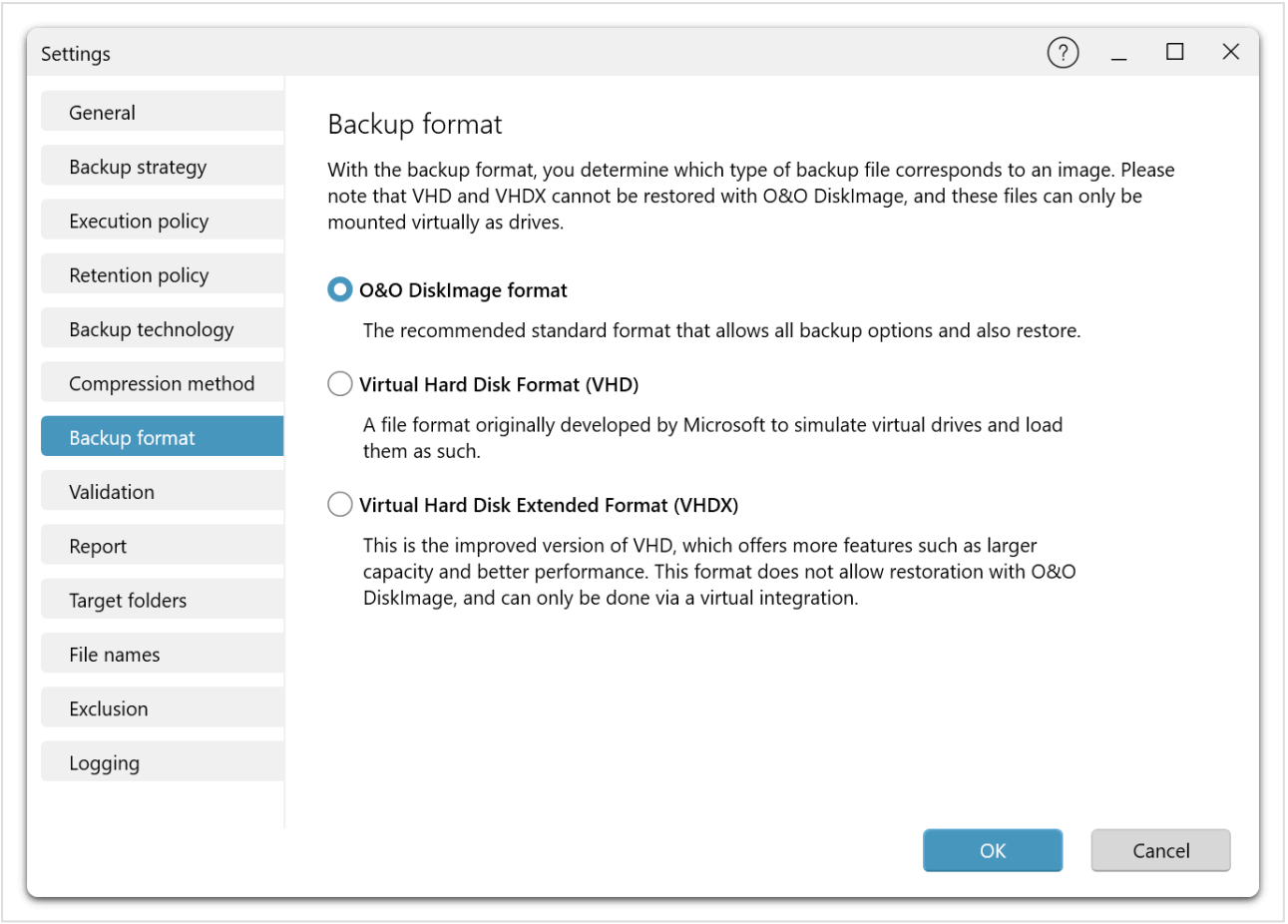
Page	Settings
General	Language of the user interface and display mode.
Backup strategy	Full backup followed by incremental or differential backups, or full backups only.
Execution policy	After how many change backups a new full backup is created.
Retention policy	Rules for how long backups are kept.
Backup technology	Used sectors, forensic backup or direct forensic backup.
Compression method	Whether and how backup files are compressed.
Backup format	O&O DiskImage format, VHD or VHDX.
Validation	Whether every backup is validated after completion.
Report	Whether a report is created for every backup.
Target folders	The folders in which new backups are stored.
File names	Storage path and file name of backup files, with placeholders.
Exclusion	Files and folders that are excluded from every backup.
Logging	Whether detailed logs of the backup operations are written.

General

Setting	Options	Default
Language	The languages of the user interface, among them German, English, French, Spanish, Italian, Russian, Japanese and Chinese. The application must be restarted after a change.	The Windows language
Display	**Light Mode**, dark mode or high contrast mode.	The mode set in Windows

Backup settings

The pages **Backup strategy**, **Execution policy**, **Backup technology**, **Compression method**, **Backup format**, **Validation** and **Report** hold the defaults for new backups. Their options are described under Backup options.



The Backup format page: only the O&O DiskImage format can be restored with O&O DiskImage; VHD and VHDX can only be mounted.

Page	Options	Default
Backup strategy	Full backup, then incremental backups; full backup, then differential backups; only full backups	Full backup, then incremental backups
Execution policy	Full backup after a chosen number of change backups: on or off, and the number	–
Backup technology	Used sectors; forensic backup; direct forensic backup (Fortress Mode only)	Used sectors
Compression method	Compression on or off; Lempel-Ziv (default or maximum), ZIP deflate, BZIP with 1K, 4K or 9K block size	Lempel-Ziv (default)
Backup format	O&O DiskImage format; VHD; VHDX	O&O DiskImage format
Validation	**Validate backup after completion** on or off	–
Report	**Create report** on or off	–

Storage settings

Page	Settings
Target folders	The folders for new backups. Several folders are used in descending order of their free space. Add, change or remove folders. See Backup destinations.
File names	**Storage path**, **File name** with placeholders, and the **Preview** of the resulting name. See File names and exclusions.
Exclusion	The list of excluded files and folders; **+** adds an entry, **−** removes it.

Logging

Logging writes detailed logs of the backup operations: start and end time, the files involved, the size of the backup, and errors and warnings. Enable it when a problem has to be analyzed or when support asks for logs. See Reports and logs.

About

About at the top right of the start page shows the version number of O&O DiskImage and the legal notices, including the license terms and the privacy policy.

Glossary

This glossary explains the terms used in this guide in alphabetical order.

Backup strategy: Determines whether a full backup is followed by incremental backups, by differential backups, or whether only full backups are created. See Backup options.

Change backup: An incremental or differential backup. It depends on the full backup and, for incremental backups, on the earlier change backups of the chain.

Check & Repair: A tool that checks the Windows component store, the system files, the system drive and the Windows Recovery Environment and repairs them where possible. It does not check backup files. See Tools.

Differential backup: Stores all changes since the last full backup. A restore needs the full backup and the selected differential backup.

Direct forensic backup: A forensic backup that reads the disk directly, so the original state is not changed. Only possible in Fortress Mode.

Duplicate drives: Transfers an exact copy of a drive to another drive, for example when replacing a disk. All data on the target drive is deleted. See Duplicate drives.

Execution policy: Determines after how many change backups a new full backup is created.

Exclusion: The list of files and folders that are left out of every backup. See File names and exclusions.

Forensic backup: Copies every sector of a drive, including unused areas, and therefore needs storage space for the full size of the drive.

Fortress Mode: A protected recovery environment in which the PC is restarted. It gives full access to the entire system, including locked drives and the system partition, and depends on a working Windows Recovery Environment. See Fortress Mode and startup medium.

Full backup: Stores all selected data and starts a new chain of backups.

Hotplug backup: A backup that starts automatically as soon as the configured backup drive is connected. See Schedules and automation.

Image: A backup of entire drives or partitions. An image can be restored or mounted as a virtual drive.

Incremental backup: Stores the changes since the previous backup. A restore needs the full backup and every incremental backup up to the selected one.

Mount: Makes the drives of a backup available as virtual drives in Windows, so their files can be copied. See Restore files.

O&O BuildPE: The program that creates the startup medium or integrates the recovery environment into the Windows boot menu.

O&O DiskImage format: The standard backup format with the file extension `.omg`. It supports all backup options and the restore with O&O DiskImage.

Report: The record of a backup operation with its time, duration, parameters, warnings and errors and its status. See Reports and logs.

Startup medium: A bootable USB stick, CD/DVD or ISO file with O&O DiskImage. It starts a PC without a working operating system and runs a recovery environment based on Windows PE.

Target folder: A folder in which new backups are stored by default. Several target folders are used in descending order of their free space.

Used sectors: The default backup technology. Copies only the sectors of a drive that contain data.

Validation: Checks a backup file for integrity, either automatically after every backup or later with **Check backup**.

VHD / VHDX: The Microsoft formats for virtual hard disks. O&O DiskImage can create and mount backups in these formats and convert backups to VHDX; it cannot restore them.

Windows PE: The Windows Preinstallation Environment, on which the recovery environment of the startup medium is based.

WinRE: The Windows Recovery Environment installed on the local disk. Fortress Mode depends on it.

Troubleshooting

The space on the target drive is insufficient

The backup page warns below **Destination file** when the target drive is expected to run out of space.

Choose a destination with more free space with **Browse...**, or add another folder under **Settings > Target folders**; new backups are stored in the folder with the most free space. A strategy with incremental backups and compression also reduces the space needed. See Backup destinations.

A scheduled backup did not run

Check the execution of the backup on the start page under **Last performed backup**: **Customize** shows whether a schedule or a hotplug backup is set, and the status bar shows whether a backup is planned.

A backup to an external drive or a network directory can only run while the destination is connected. Connect the drive or check the network connection, then run the backup manually with **Run backup** under **Restore backups**. See Schedules and automation.

A backup does not start when the drive is connected

Perform automatic backup when connecting a drive (Hotplug) must be selected in the execution settings, and the connected drive must be the destination drive of that backup. Wait for the configured **Execution delay** after connecting the drive. See Backups when a drive is connected.

The system drive cannot be restored or selected as a target

While Windows is running, the system drive is in use: it cannot be overwritten by a restore and cannot be selected as the target of a duplication. Start **Fortress Mode** under **Tools**, which gives protected access to all drives, or start the PC from the startup medium. See Fortress Mode and startup medium.

Fortress Mode cannot be set up

Fortress Mode needs a working Windows Recovery Environment. Run **Check & Repair** under **Tools** with **Check Windows recovery environment** enabled, then set up Fortress Mode again. If the recovery environment cannot be repaired, use the startup medium.

The PC does not start from the startup medium

- Change the boot order in the boot menu or in the BIOS/UEFI setup so that the medium is started first. The order chosen in the boot menu usually applies to the current start only.
- Disable **Secure Boot** if the Windows PE medium does not start.
- Start the PC in the same boot mode (UEFI or Legacy/CSM) in which the medium was created.
- Use a USB 2.0 port; some PCs do not start from USB 3.0 ports.
- If the medium is still not detected, recreate it with **Creating a Startup Media**.

A disk or the network is missing in the recovery environment

The driver of the storage controller, NVMe SSD, RAID array or network adapter is missing. Load it in the **O&O System Settings** dialog on the **Drivers** tab from a USB stick or another drive. In most cases a missing disk is caused by missing RAID, AHCI or NVMe drivers, or by changed BIOS settings such as the RAID/IDE/AHCI mode. See Work in the recovery environment.

A BitLocker-protected drive cannot be used in the recovery environment

Encrypted volumes can only be used after they have been unlocked. Unlock the drive with its BitLocker recovery key before backing up or restoring it.

A VHD or VHDX backup cannot be restored

Backups in the VHD and VHDX formats cannot be restored with O&O DiskImage. Mount the backup with **Tools > Mount drives** and copy the files you need. For backups you want to restore, use the O&O DiskImage format. See Backup options.

The backup had to be forensic

If an empty area of a drive is selected under **Back up drives**, or a partition has an unknown or unsupported file system, O&O DiskImage must back up all sectors instead of the used sectors. A forensic backup needs storage space for the full size of the drive. Deselect empty areas if you do not need them.

The validation reports errors

A backup that fails validation cannot be relied on. Check the source drive with **Check & Repair** or `chkdsk`, create a new backup and check it with **Check backup**. Keep an older, validated backup until the new one is checked. See Tools.

A backup is not listed

Backups from other PCs, on external drives or in network directories are added with **Import backups** under **Restore backups** or **Tools**. Connect the drive or network directory first. See Manage backups.

A password is not accepted

Enter the original password of the backup and check the capitalization and the keyboard layout – in the recovery environment the layout is often English (US). An encrypted backup cannot be restored without the correct password.

FAQ

Which edition does this guide cover?

This guide covers O&O DiskImage 22 Premium Edition for home users. The Professional, Server and Enterprise Editions add functions for business and server environments.

Which backup should I create first?

Start with **Back up your PC** and an external hard disk or network drive as the destination. Then set up Fortress Mode or create a startup medium. See Quick start.

What is the difference between full, incremental and differential backups?

A full backup stores all selected data. An incremental backup stores the changes since the previous backup, a differential backup the changes since the last full backup. The backup strategy under **Settings** combines them. See Backup options.

Can backups run automatically?

Yes. Select **Customize** next to **Execution** on the backup page and choose a schedule – once, hourly, daily, weekly or continuous – or a backup that starts when the backup drive is connected. See Schedules and automation.

Where should I store backups?

On a different physical disk from the data: an external USB hard disk or a network drive. Several default folders can be set under **Settings > Target folders**. See Backup destinations.

Can I restore individual files from a backup?

Yes. Mount the backup with **Tools > Mount drives** and copy the files in Windows Explorer; afterwards remove the drive with **Cancel integration**. See Restore files.

Can I restore a VHD or VHDX backup?

No. Backups in these formats can only be mounted as virtual drives. Use the O&O DiskImage format for backups you want to restore. See Backup options.

What is Fortress Mode?

A protected recovery environment in which the PC is restarted. It gives full access to the entire system, so the system partition and locked drives can be restored. Set it up under **Tools**. See Fortress Mode and startup medium.

Do I need a startup medium if Fortress Mode is set up?

Yes, as a precaution. Fortress Mode depends on the Windows Recovery Environment on the local disk. If that disk fails or Windows no longer starts, the startup medium starts the PC and O&O DiskImage.

Does Check & Repair fix damaged backup files?

No. It checks and repairs the Windows component store, the system files, the system drive and the Windows Recovery Environment. To check a backup file, use **Check backup**, and create a new backup if the check fails.

How do I know that a backup can be restored?

Enable **Validate backup after completion** under **Settings > Validation**, or check a backup later with **Tools > Check backup**. Test the startup medium once while the PC still works.

Can an encrypted backup be restored without the password?

No. Keep the password in a safe place, independently of the PC you may need to restore.

Support and more from O&O

O&O Software support helps with questions and problems concerning O&O DiskImage 22.

Contact support

Open O&O Software support. Include:

- The version of O&O DiskImage (**About** on the start page) and the Windows version.
- The report of the failed operation.
- The type of source and destination.
- Whether the backup was started manually, by schedule or when connecting the drive.
- Whether the problem occurred in Windows, in Fortress Mode or in the recovery environment of the startup medium.

Add logs if support requests them. See Reports and logs for how to enable logging, and Troubleshooting for common problems and their solutions.

Licensing and updates

O&O DiskImage is commercial software. You can try it during the trial period; continued use requires a valid license. Activation and installation are described under Install and activate. Product information is available on the O&O DiskImage product page.

More O&O products

Product	Purpose
O&O Syspectr	Remote monitoring and management of PCs and servers
O&O Defrag	Storage optimization for PCs and servers
O&O DiskRecovery	Recovery of deleted files and data from damaged file systems
O&O ShutUp10	Control of Windows privacy settings
O&O SafeErase	Secure, unrecoverable deletion of files and free space

See all O&O products.