O&O software

O&O DiskImage

Inhaltsverzeichnis

About O&O DiskImage

Welcome, and thank you for choosing O&O DiskImage!

In today's digital world, protecting your data is more important than ever. A virus attack, hardware failure, or system crash can occur unexpectedly and put valuable data at risk. With O&O DiskImage, you have the optimal solution at hand to manage these risks effectively and keep your data safe.

Our tool supports not only the duplication and archiving of entire computers and individual drives, but also dynamic disks and RAID systems. Whether you want to create regular backups or full system images, O&O DiskImage can be flexibly adapted to your needs.

Benefit from advanced backup methods that can be individually configured to perfectly match your specific requirements. From complete 1:1 system copies to selective, custom backups – everything is possible. In addition, we offer numerous options for fine-tuning your backups to ensure maximum efficiency with minimal impact on your daily work.

In the following chapters of this help file, we guide you through the various features of O&O DiskImage, explain the basic steps, and provide tips on how to get the most out of the tool.

Enjoy the reliability and security that O&O DiskImage provides, and save valuable time – both at the office and at home. We are convinced that our product will become an essential part of your IT security strategy.

For more information and support, please visit our website:
https://www.oo-software.com

We wish you much success and security with O&O DiskImage.

Your O&O Software GmbH Team

General Definitions

To make working with O&O DiskImage easier, this chapter explains key terms you will encounter while using the program.

Drive / Partition

A drive is a specifically assigned area on a hard disk. A single physical disk can contain several drives. The term *drive* in this context covers partitions, logical drives within extended partitions, and volumes.

A typical structure for better organization might be:

- **Drive C:** Operating system and applications
- **Drive D:** Data such as photos, Office documents, music, etc.

This structure makes it easier to back up system and data separately.

Backup

A backup creates an *image* of your drives. It contains all information of the original and is stored in a special compressed file format that requires less disk space. Regular backups protect effectively against data loss. If the original data is damaged or lost, you can restore the state at the time of the backup with just a few clicks.

Difference Between File Backup and Drive Backup

- **File backup**
  Saves only files as data sets and stores them in OBK format (`.obk`).
- **Drive backup**
  Saves the used or all sectors of a drive, including the file system, files, and folders. The result is stored in OMG format (`.omg`).

Backup File

A backup consists of one or more files (`*.omg`). If the storage space of a single medium is not sufficient, the backup can be split across multiple media. These should be numbered to allow correct restoration or use as a base for incremental backups.

File Formats

O&O DiskImage uses and supports several file formats:

- **OMG:** Backups of entire systems or individual drives
- **OBK:** File backups
- **VHD:** Virtual hard disk, allows mounting of backed-up drives
- **VHDX:** Up to 64 TB capacity and more robust against file corruption (VHD: up to 2 TB)

Full Backup

A full backup writes all selected data completely and anew to the target medium. It is thorough because it creates a complete copy of the data.

Differential and Incremental Backups

After a full backup, changes can be backed up more efficiently:

- **Differential backup:** Saves all differences since the last full backup.

- **Incremental backup:** Saves only the changes since the last backup – regardless of whether it was full, differential, or incremental.

Both methods save disk space and time.

Base Backup

A base backup serves as the starting point for additional differential or incremental backups.

- Differential backups require a previous full backup.
- Incremental backups use the last backup (full, differential, or incremental) as their reference.

Installation, Licensing, and Uninstallation

Installation
Installing O&O DiskImage is straightforward and carried out as follows:

1. Start the computer on which you want to install O&O DiskImage.
2. Log in as a local administrator or with a user account that has equivalent rights.
3. Run the O&O DiskImage installation file that you downloaded from our website or received on CD/DVD.
4. Follow the instructions of the setup program.
5. Restart the computer if prompted.

Note: During installation and use of O&O DiskImage, no other backup or imaging software should be running, to avoid conflicts caused by parallel access to drives.

Entering the License
After installation or at a later time, you will need a valid license key to activate the product. The registration wizard starts automatically when you run the program for the first time or when a license error is detected.

Note: The license key may also be referred to as registration code, serial number, or product ID.

To activate your license:

1. Enter the license information you received when purchasing the product (download or boxed version).
2. Make sure not to confuse letters and numbers and do not enter spaces.
3. Click **Next** to complete registration, or **Cancel** to abort.

If you encounter problems, please contact our support.

Licensing Information
You can test O&O DiskImage free of charge for 30 days. The remaining trial period is displayed each time the program starts.

Online Registration
Registration offers you several advantages, including:

- Improved customer service
- Recovery of lost license keys
- Information about products and updates
- Discounted upgrades to new versions

How does online registration work?

- If you purchased the product via our online shop, registration is performed automatically.
- For other purchase channels, you will be asked after entering your license data whether you would like to register.

You can register or update your data using our *registration form*.

Uninstallation
To remove O&O DiskImage from your system:

1. Open the **Control Panel** and select **Programs** (or **Programs and Features / Software**, depending on Windows version).
2. Select **O&O DiskImage** from the list of installed programs and click **Change/Remove** or **Uninstall**.
3. Follow the instructions of the uninstall wizard.

Updates
O&O DiskImage automatically checks for available updates. You can also manually check for updates via:

- Menu **Tools → About O&O DiskImage**

Important: When using O&O DiskImage in a network environment, authentication data should be backed up before performing a **major update**, so that it can be restored afterwards.

System Requirements

Price
49.90 EUR incl. VAT

Basic Requirements

- The minimum system requirements of the respective operating system must be met.
- 64-bit support is required.
- Supported operating systems:
  - Windows® 10 (all editions)
  - Windows® 11 (all editions)
  - Windows® Server 2016 through Windows® Server 2025 (all editions)

Edition Compatibility

Operating System	Professional / Special Edition	Server Edition
Windows® 11	yes	yes
Windows® 10	yes	yes
Windows® Server 2016	no	yes
Windows® Server 2019	no	yes
Windows® Server 2022	no	yes
Windows® Server 2025	no	yes

Note:
Booting from the bootable medium requires **at least 4 GB RAM**.

Note:
Ensure that all storage controller drivers of your operating system are up to date. If in doubt, perform a driver update.

Note:
Dynamic disks are supported only within the capabilities provided by Microsoft Windows. Since Microsoft does not guarantee bootability of dynamic disks in every scenario, we cannot guarantee successful duplication or restoration of systems to/from dynamic disks.

Permissions
Local administrator rights or equivalent permissions are required for installation, configuration, and activation of O&O DiskImage.
Domain administrators usually have sufficient rights.

Differences Between the Various Editions

O&O DiskImage is designed for both desktop PCs and server environments, ensuring comprehensive data protection across different platforms. To support organizations of all sizes, we also offer volume-licensed packages at reduced prices—called **Combi Packs**.
For tailored advice, please contact our sales team: **sales@oo-software.com** or an authorized O&O partner.

Premium Edition
The Premium Edition is designed for home users. It offers all essential features for backing up individual PCs, including system backup, disk cloning, and hardware-independent restoration. It is ideal for classic desktop environments in private households.

Professional Edition
The Professional Edition is intended for business customers who manage multiple desktop or workstation systems. It offers all Premium Edition features along with enhancements for professional use—such as improved management options, higher performance, and optimized workstation compatibility.
This edition is **not** suitable for server operating systems.

Server Edition
The Server Edition includes all features of the Professional Edition and extends them with specialized capabilities for server environments. It supports all common server operating systems, optimized performance for large data volumes, enhanced network backup options, and additional functions required for professional server backups.

Enterprise Edition
The Enterprise Edition is designed for larger companies and extensive IT infrastructures. It enables the deployment of O&O DiskImage across many systems with centralized management, flexible distribution, and advanced provisioning features. It is the most comprehensive solution for complex, heterogeneous environments.

For companies with multiple installations
Volume licensing provides a cost-effective way to deploy O&O DiskImage across several devices. Benefits include:

- central management
- simplified deployment
- lower cost per device
- higher flexibility in larger environments

Supported File Systems

O&O DiskImage supports a wide range of commonly used file systems to ensure broad applicability across different storage devices. The most important supported file systems include:

File System	Description
FAT	One of the oldest file systems, developed for MS-DOS and early Windows versions. Still widely used for removable media due to its simplicity and compatibility.
FAT32	An extended version of FAT supporting larger files and volumes. Often used on older Windows systems and external drives. More efficient use of storage space than FAT.
NTFS	Introduced with Windows NT. Supports large volumes, permissions, logging, and recovery features. The preferred file system for modern Windows systems due to its stability and security features.
exFAT	Designed for flash storage such as USB sticks and SD cards. Supports large files and volumes more efficiently than FAT32. Commonly used in cameras, smartphones, and modern removable devices.

Note:
With O&O DiskImage, you can create backups of **used sectors** for all supported file systems.

If a volume or partition uses an **unknown or unsupported file system**, O&O DiskImage automatically performs a **forensic backup**, meaning **all sectors** are backed up.

To perform a forensic backup manually, choose the option for full sector backup (instead of used-sector backup) in the backup settings.

Quick Start

The Quick Start Guide for O&O DiskImage leads you through the essential steps—from launching the program to creating your first backup. After installation, a variety of features are available to reliably safeguard your data and restore it when needed.

Starting O&O DiskImage

- Start O&O DiskImage from the desktop shortcut or via the Windows Start Menu: *Start → O&O DiskImage*.
- For simplified operation, the **O&O DiskImage Express View** is available.
- The **tray icon** in the system tray provides quick access to status information and commonly used functions.

Creating a Backup

1. Open the main window of O&O DiskImage and select **Create Backup**.
2. Choose the drive or files you want to back up.
3. Select the storage location for the backup file, such as an external hard drive, network share, or cloud storage.
4. Start the process by clicking **Start**.
   The duration depends on data size and the speed of the storage medium used.

Restoring a Backup

1. Open the main window and select **Restore**.
2. Navigate to the desired backup file.
3. Choose the data or drives you wish to restore.
4. Click **Restore** and follow the on-screen instructions to safely recover your data.

Accessing the Help System
You can open the integrated help at any time via the **Help** menu or by pressing **F1**.

Note:
Ensure that your backup destinations provide enough storage space and are checked regularly to maintain the integrity of your backups.

Backing Up Individual Drives

With O&O DiskImage you can back up individual drives (partitions/volumes). This allows you to protect system and data drives separately. In the event of data loss, you only need to restore the affected data drive – without having to reset the entire system.

Creating a backup of one or more drives

1. On the start page, select **Drive backup**.
2. In the drive list, select one or more drives to be backed up by enabling the corresponding checkbox.
3. Optional: Under **Backup options** you can configure additional settings or schedule the backup as a recurring task.
4. Click **Start drive backup** to proceed to the next step.
5. Specify the target path where the backup will be stored.
   - You can use a suggested default path.
   - Alternatively, select a custom storage location.
   - A custom default path can be defined in the program settings.

6. By default, the backup is named according to the creation date.
    - You can assign a custom name at any time.
    - All relevant backup information is stored and can be retrieved later.
7. Click **Start** to create the backup.

Note:
If the available space on the target medium is not sufficient, O&O DiskImage will prompt you during the process to provide an additional target path.

Backing up individual drives (Server Edition)
The functionality is essentially identical to the Professional Edition, although the visual layout may differ.

Drive list
The drive list in the Professional Edition differs slightly from the view in the Server Edition. This difference is purely visual – the functionality is identical in both editions.

Full Computer Backup

The **1-Click backup** is the fastest and easiest way to back up your entire computer – including the system partition, data, and settings. This method is especially suitable for first-time backups or for users who want a complete backup quickly and without manual configuration.
For the 1-Click backup, compression (**LZNT1**) and backup method (**backup of used sectors**) are already optimally preset.

Note:
We recommend using an **external storage medium** as the target directory for the 1-Click backup, for example a USB hard drive or a network share.

How to create a 1-Click backup

1. Start O&O DiskImage and select **Drive backup** on the start page.
2. In the Actions pane, click **Backup entire computer** (1-Click backup).
3. Check the suggested target path and adjust it if necessary.
    - Use the **[…]** button to choose any storage location.
4. The backup is automatically named according to the creation date.
    - You can alternatively enter your own backup name.
5. Click **Start** to begin the backup process.

Note:
The duration of the backup depends on the size of your hard drive(s) and the speed of the target medium. A full system backup may therefore take some time.

Restoring the Entire Computer

To fully restore your entire computer or the system partition, you must start O&O DiskImage from a **bootable medium**. Follow the instructions in the chapter **Start directly from a bootable medium**.

Tip:
For restores to systems with **different hardware (M.I.R.)**, please also refer to the chapter **Restoring to different hardware**.

Procedure for a full system restore

1. Start O&O DiskImage directly from the **boot medium**.
2. On the start page, select **Restore**.

3. Click **Restore** or use the browser button to navigate to the location of your backup.
4. Select the backup file that contains the system partition and/or all related drives, then click **Open**.
5. All drives included in the backup are displayed in the list.
6. Enable the checkbox for each drive you want to restore.
    - For a full system restore, select **all drives**.
7. Select the **target drive** to which the backup data will be written.
8. Click **Start drive restoration** to begin the restore process.
9. After the restore is complete, you can restart your computer as usual.

Note:
Under Windows PE (from Windows Vista onward), drive letters may differ.
Example: Your usual **drive C:** may appear as **drive D:** under Windows PE.

Cloning Drives

Cloning is ideal if you want to replace an existing disk with a new one. In this process, backup and restore are combined into a single step. You can clone complete disks or individual drives (partitions/volumes) and then use them directly. The source drives remain unchanged.

File-based cloning
File-based cloning transfers all recognized data from the source to the target disk.
This method is fast, efficient, and sufficient for most scenarios.

Forensic cloning
Forensic cloning is recommended in the following cases:

- the file system of the source drive is not supported by O&O DiskImage
- data recovery is required
- an exact bit-by-bit copy of all sectors is needed

With forensic cloning, **every single sector** of the source drive is copied. This is highly accurate but requires significantly more time and processing power.

Functionality and characteristics

- No backup file is created during cloning.
- It produces a complete copy that can be used immediately as a replacement for the original disk.
- Both entire disks and individual partitions can be cloned.
- The source drives remain completely unchanged.

Important notes

- A cloned drive requires **significantly more storage space** than a backup.
- In contrast to backups, cloning does **not** support **compression or encryption**.
- There are **no incremental or differential follow-up clones**.

Restoring Drives

With O&O DiskImage you can restore one or more drives from an existing image. The following steps guide you through the complete restore process.

Restoring drives from an image

1. On the start page of O&O DiskImage, click **Drive restoration**.

2. In the dropdown under **Select image**, choose the desired image.
    - If the suggested images (*.obk) are not correct, browse your drives and manually select the path to the desired backup file.
3. Use the browse button to select the image file (*.omg,* .vhd or *.vhdx) and click **Open**.
4. All drives contained in the image are then displayed.
5. Select the drive you want to restore ("play back").
6. Select a **target drive** by enabling the corresponding checkbox.
    - You can replace an existing drive
    - or create a new target (e.g. in unallocated space).
7. Optional: Under **Restore options**, you can configure additional settings.
8. Click **Start drive restoration** to begin the restore process.

Important:
During restoration, the selected target drive is completely overwritten.
All data on this drive is irreversibly lost and replaced with the data from the backup.

Note:

- If your image is stored across **multiple media**, **all** of these media are required for restoration.
- For **incremental images**, O&O DiskImage requires all backups from the last **full image** up to the **last incremental image**.
- When restoring an entire disk, the target disk must have **at least the same capacity** as the original disk.
- To restore a **system partition or an entire system**, you must boot your computer from a **bootable O&O DiskImage medium**.
  See: *Start directly from a bootable medium*
- For restoring a system partition to **different hardware**, refer to: *Restoring to different hardware (M.I.R.)*.

O&O DiskImage RecoveryPartition

The **O&O DiskImage RecoveryPartition** is an integrated recovery environment stored directly on the computer. It allows you to start O&O DiskImage even if the Windows operating system no longer boots. This provides a particularly convenient and fast way to bring a defective system back to life – **without separate boot media**, **without complex preparation**, and **with direct access to your latest backups**.

What is the O&O DiskImage RecoveryPartition?
The RecoveryPartition is a standalone startup environment installed alongside Windows on the hard drive.
It is based on Windows PE and includes:

- all necessary O&O DiskImage components
- tools for backup and restore management
- drivers for hardware detection
- access to internal and external drives, networks, and backup files

This makes it a complete rescue system that is always ready to use in an emergency, without additional media.

When is the RecoveryPartition used?
The recovery environment is particularly useful when:

- Windows no longer starts
- critical system files are damaged
- faulty or incompatible drivers have been installed

- the system partition has been destroyed or overwritten
- malware or an update has rendered the system unusable
- you want to perform a system or drive restore without booting from USB/DVD

Advantages of the RecoveryPartition

- **Always available** – no dependency on USB sticks or DVDs
- **Fast startup directly via the boot menu**
- **Direct access to existing backups on the computer**
- **Full O&O DiskImage functionality**, including restore, cloning, and forensic analysis
- **Ideal for users without in-depth technical knowledge**
- **Perfect for laptops and devices without optical drives**
- **Stable and reliable**, even in severe system failures

How the RecoveryPartition boot works
Once activated, an additional entry is added to the Windows Boot Manager.
When the system starts, you can choose between:

- **Start Windows**
- **Start O&O DiskImage RecoveryPartition**

The latter loads the recovery environment and opens O&O DiskImage in rescue mode.

What can be done in the RecoveryPartition?
In the recovery environment, almost all tools available in normal operation can be used:

- Restore complete system images
- Restore individual drives and partitions
- Restore individual files and folders
- Clone drives
- Analyze and verify images
- Access network drives and externally connected media
- Delete and adjust partitions
- Remove or reset faulty drivers
- Prepare M.I.R. restores (hardware migration)

Integration of recent backups
If your backups are stored locally, the RecoveryPartition detects them automatically.
This enables:

- extremely fast restores
- access to full and incremental backups
- restores without additional media or downloads

Important note
The RecoveryPartition does **not** replace the use of external backup media.
In the event of a disk failure or complete hardware defect, backups must exist on external media.
For comprehensive protection, you should also create a **bootable medium** in addition to using the RecoveryPartition.

Backup of Changes

With **Backup of changes** you only back up the data that has changed since the last backup. This method is particularly efficient because it saves storage space and is usually faster than full backups.
However, it requires that **at least one full backup** of the relevant drives or directories already exists.

What is a backup of changes?
A backup of changes is based on an already existing backup – the so-called **base backup**. This can be:

- a **full backup**
- an **incremental backup**
- or a **differential backup**

O&O DiskImage compares the current state of the drive with the state of the base backup and stores only the changed sectors.

Backing up drive changes – step by step

1. Make sure your computer can access the drive on which the base backup is stored.
2. Start O&O DiskImage and select **Backup of changes** on the start page.
3. In the file selection dialog, choose the desired **base backup** and click **Open**.
4. Select the suggested target directory or enter your own storage location for the new backup.
    - The backup is automatically named according to the creation date.
    - Alternatively, you can specify your own name.
5. Under **More options** you can configure additional settings such as compression, encryption, or backup method.
6. Click **Start** to begin the backup of changes.

Note:
For a backup of changes, O&O DiskImage compares **every sector** of the existing backup with the corresponding sector of the current drive.
This method is thorough and stores only the data areas that have actually changed.
It may take a bit more time, but significantly reduces storage requirements compared to full backups.

Note:
The option **Data comparison with checksums** is enabled by default.

- For **incremental backups**, in principle the **last backup** is sufficient as the reference point.
- For **differential backups**, the last **full backup** is always required.

Backup Computer and Drives

Backing up your digital data is a crucial step in protecting yourself against data loss caused by hardware failure, software errors, accidental deletion, or cyberattacks. Under the **Drive backup** tab in O&O DiskImage you will find all the functions you need to reliably back up, duplicate, or restore individual drives, multiple partitions, or your entire system.

Overview of data protection features
The *Drive backup* chapter provides comprehensive guidance on creating and optimally using different types of backups, including:

- full system images (system backups)
- backup of individual drives or partitions
- backup of changed data only
- cloning of drives
- forensic backups
- advanced backup options such as compression, encryption, and scheduling

These tools enable flexible and powerful backup strategies for home users, businesses, and IT administrators.

Full system backups
With a full system backup you protect your entire computer – including operating system, applications, settings, and all files. This type of backup is ideal for complete system protection and forms the basis for disaster recovery or recovery after serious system failures.

Selective drive backups
You can selectively back up individual drives or partitions to regularly protect only specific data areas – for example important business documents, photos, or project files. This method saves time and storage space and is well suited for ongoing data protection strategies.

Advanced backup options
O&O DiskImage offers numerous additional options to fine-tune your backups to your needs, including:

- **Compression** to reduce storage usage
- **Encryption** to securely store sensitive data
- **Scheduling** for automated recurring backups
- **Backup methods** (full, differential, incremental)
- **Performance and security options** such as checksums, filters, or forensic procedures

This allows you to configure your backups to be both efficient **and** highly secure.

Suitable for beginners and professionals
Whether you are an experienced IT professional or a home user: the O&O DiskImage backup features are designed to be intuitive yet powerful enough to be used in complex IT environments.

This chapter helps you:

- choose the right backup strategy
- use the features effectively
- protect your data reliably in the long term

Copy Options

Under the **Copy process** settings you can define various options that influence the cloning (duplicating) of drives. These options are available via the **Computer and drives** action pane and allow precise control over the copy operation – from error handling and read methods to security and performance settings.

Ignore faulty sectors
Under **Drive duplication** ▯ **Copy options** ▯ **Advanced** you can define how O&O DiskImage should handle faulty sectors:

- **Abort on errors:**
  The copy process is aborted immediately when a faulty sector is encountered.
- **Continue and mark sector as empty:**
  The copy process continues despite errors. Faulty sectors are created as *empty sectors* in the copy.
  This allows all other readable data to be transferred correctly.

This setting is particularly useful for damaged disks or data recovery scenarios.

Lock drive
During the copy process you can lock the source drive to ensure that no changes are made to it.

- A locked drive:
  - is hidden from Explorer

  - can no longer be written to
  - automatically closes all applications that are accessing it
- By default, the drive is **not locked** so that you can continue working in parallel.

Enable this function under:
Drive duplication Copy options Advanced Read process.

If the drive is **not** locked, O&O DiskImage uses a **cache** to buffer temporary changes.

Important:
The cache is limited in size. The cache status display shows how much space is still available.

Warning:
If the cache becomes full, changes are written directly to the target drive.
 This can cause the copy to become **inconsistent or unusable**.

Note:

- The **system partition cannot be locked**.
- To prevent temporary files from being written to specific drives, set the registry value **NoSnapshotTmpFiles** (see chapter *Explanation of registry entries*).
- Stop write-intensive processes (e.g. defragmentation) to avoid cache overflows.

Set read method
Under **Drive duplication Copy options** you can define how data is read from the source drive. The methods correspond to the backup methods:

- **Used sectors only**
  (fast, efficient; standard method for intact file systems)
- **Forensic**
  (all sectors, regardless of content)
- **Direct forensic**
  (direct access to the physical disk, bypassing the file system driver)

These settings affect both the accuracy and the duration of the copy process.
For more details, see *Backup methods*.

Create profiles for duplication
You can save your individual copy options as profiles and reuse them at any time.

Under **Drive duplication Copy options** you have the following options:

- **Current profile:**
  - *Standard*
  - *User-defined*
- **Save as …**
  creates a new profile with your own name
- **Manage profiles:**
  Edit or delete existing profiles

This feature makes recurring cloning or duplication tasks much easier with a consistent configuration.

Force write method
Under **Computer and drives (Duplication) Options Advanced** you can define how data is written to the target medium:

- **Write to drive**
  - Default for “Used sectors only” and “Forensic”
  - Data is written via the operating system (file system driver)
- **Write directly to disk**
  - Default for “Direct forensic”
  - Bypasses the file system driver and writes directly to the physical disk
  - **Mandatory** when encrypted drives are restored from a forensic backup

To use this, enable:
Force write method and select the required method.

Overwrite unused sectors
Under **Advanced Explicitly overwrite unused sectors with 0** you can decide whether unused sectors should be overwritten with zeros during the copy process.

This ensures that:

- deleted data in empty areas **cannot be recovered**
- the copy contains no recoverable data remnants
- the copy is compliant with data protection requirements

Tip:
When you delete files normally in Windows, the data remains on the disk and can be recovered with special tools.
By overwriting with “0”, such recovery is **permanently prevented**, even with professional data recovery software.

Copy Process

When copying (duplicating) drives, you can replicate entire disks or individual partitions exactly. The created copy can then be used in place of the original disk—for example, when replacing a hard drive or SSD. The copy process combines backup and restoration into a single step and works **without creating classic backup files**.

The source drives remain unchanged because O&O DiskImage accesses them **read-only**.

Key characteristics of the copy process

- Copies contain **all data, structures, and partitions** of the original.
- **No backup files** (*.omg,* .vhd, *.vhdx*) are created.
- Required storage space is **significantly larger** than with backups because no compression is used.
- Copies **cannot** be compressed or encrypted.
- There are **no** incremental or differential copies as with backups.
- The source always remains intact; all changes are written exclusively to the target drive.

How to perform a duplication

1. In the quick access bar, select **Drive Duplication**.
2. Choose the drive or disk you want to duplicate by checking its selection box.
3. Under **Copy Options**, define additional settings (e.g., error handling, read method, drive locking).
4. Select the **target drive** by activating its checkbox.
5. Optionally, in the following dialog under **Additional Options**, you can define actions to run after duplication (e.g., verification, rescan, automatic shutdown).
6. Click **Start** to begin the copy process.
7. Once completed, you can also “copy back” the duplicated data to another drive as needed.

Important!

When copying a drive, the chosen **target drive is completely overwritten**.
All existing data on the target will be irretrievably lost and replaced with the data from the source.
Always use dedicated external or new drives for duplication tasks.

Note

Adjust the properties of the target drive according to the intended use.
When copying system partitions, pay special attention to **bootability** and **partition types**.

Note

If you use a second hard disk as the target, O&O DiskImage automatically changes the **disk signature** of the target.
This prevents having two disks with the same signature connected at the same time—an issue known to cause:

- system errors
- conflicts in disk management
- operating system boot problems

For **basic disks**, partitions are identified by a combination of disk signature and partition offset.
O&O DiskImage therefore adjusts the registry entries for drive letters accordingly.

Note

If you intend to copy a **system partition** to a PC with **different hardware**, please also refer to the chapter:
Restoring to Dissimilar Hardware (M.I.R.)
There you will find detailed information on driver adjustments, boot configuration, and hardware detection.

Backup

O&O DiskImage provides two primary types of backups: **full backups** and **backup of changes**.
Both methods can be performed either **file-based** or **forensically**, allowing you to choose the optimal balance of speed, storage efficiency, and precision.

Full Backup

A full backup contains all data of a drive or partition. It is often used as the base for subsequent backups.

There are two variants:

File-based Full Backup (Standard)

- Saves all detected data on the drive
- Required size roughly equals used space plus metadata
- Fast and ideal for most scenarios
- Sector-based backup is enabled by default

Forensic Full Backup

- Saves **every sector** of the disk, including unused and damaged areas
- Image size always equals the **physical size of the disk**
- Ideal for data loss, damaged file systems, or deep forensic analysis
- Recommended for data recovery cases

- Should be created using the **O&O DiskImage boot medium** to prevent Windows from overwriting deleted data
- See chapter *Create Boot Medium*

Backup of Changes

A backup of changes records only the data that changed since the previous backup.
This saves time and storage and is widely used in professional backup routines.

- Always requires an existing **full backup** or a previous **backup of changes**
- Stores only new, deleted, or modified data
- Backup size equals the changed sectors plus metadata
- Ideal for daily or frequent backups
- Highly efficient on running systems

Recommendation:
After each full backup, create **no more than five to ten** change backups before making a new full backup.
This keeps the backup chain reliable and shortens restore times.

Drive Backup
With O&O DiskImage you can back up individual drives or partitions. This allows you to protect system and data areas separately.

Procedure:

1. On the start page, select **Drive Backup**.
2. In the drive list, check the drives you want to back up.
3. Optional: Open **Backup options** or add the backup as a scheduled task.
4. Click **Start drive backup**.
5. Choose the target path or accept the suggested default path.
6. Optionally, specify a custom name for the backup.
7. Click **Start** to create the backup.

Note:
If the target medium does not have sufficient space, you will be prompted to specify an additional storage location.

DiskView (graphical drive overview)
The interactive DiskView shows:

- all detected disks
- their partition layout
- free and used space

Clicking a drive lets you select it directly for backup operations.

Task for differential and incremental backups
To run differential or incremental backups automatically, you need an existing **full backup** as a base.

To set up a backup task:

1. Open **Drive Backup** from the start page.
2. Click **Backup options** and enable **Backup of changes**.

3. Select the **base backup** and close the options.
4. Click **Add as task**.
5. Configure the task name and **schedule**.
6. Select the storage location for the backups.
7. The option **Use created backup as base backup for the next run** is enabled by default.
    - This creates **incremental** backups that always build on the last backup of changes.
    - Very space-efficient
    - For restore, **all** backups since the last full backup are required.

If you disable this option:

- Only **differential** backups are created.
- Each backup is based on the last **full backup**.
- For restore you only need:
    - the last differential backup
    - plus the corresponding full backup
- These backups are larger, but the restore is faster.

Note:
If full and subsequent backups are *not* stored in the same directory, the checkbox **Suppress user prompts during execution** must be **cleared**.
Otherwise the task will be aborted if preceding backups cannot be found.

Back up everything (1-Click Backup)
The **1-Click Backup** creates a complete system image, including:

- operating system
- installed programs
- settings
- user data

It is ideal for first-time users or for quickly creating a full system copy.
Compression (**LZNT1**) and the method **Backup of used sectors** are preconfigured.

Procedure:

1. Start O&O DiskImage and open **Drive Backup**.
2. Click **Back up everything**.
3. Check or change the target path.
4. Optionally specify a backup name.
5. Click **Start**.

Note:
Preferably store 1-Click Backups on **external drives** or network shares.

Backup of changes – step by step

1. Ensure the system has access to the base backup.
2. On the start page, select **Backup of changes**.
3. Open the base backup.

4. Select the target path (ideally in the same folder).
5. Optionally specify a name for the backup.
6. Optional: Open **Additional options**.
7. Click **Start**.

Note:
The option **Data comparison using checksums** is enabled by default and allows efficient verification of modified data.

Restore

Restoring backups in O&O DiskImage is automatically adapted to the type of backup used. In most cases you do not need to change any settings—O&O DiskImage detects the required parameters on its own.

If you want to restore a **backup of changes**, all associated backups must be available:

- the **full backup**,
- **all preceding backups of changes**,
- and the backup that contains the desired restore point.

This backup chain is required to correctly reconstruct the data state.

Drive restore (standard restore)
With drive restore, you can restore individual drives, multiple partitions, or entire disks from a backup.

Procedure:

1. On the start page of O&O DiskImage, click **Drive Restore**.
2. Under **Select backup**, choose the desired backup image.
    - If the proposed entries (*.omg,* .vhd, *.vhdx*) are not suitable, browse to the storage location manually.
3. Open the backup file via the browser dialog.
4. All drives contained in the backup are listed.
5. Check the drive you want to restore ("play back").
6. Select a **target drive** by ticking its checkbox.
    - You can overwrite an existing drive,
    - or create a new partition in unallocated space.
7. Optional: Open **Restore options** to configure additional settings.
8. Click **Start drive restore** to begin the restore.

Important:
The target drive is completely overwritten.
All existing data is irretrievably lost and replaced by the backed-up drive data.

Restore notes

- For backups that are **spanned across multiple media**, **all media** are required.
- For **incremental backups**, O&O DiskImage requires:
    - the **full backup**,
    - and **all following backups of changes** up to the last incremental backup.

- When restoring an **entire disk** to a different target disk, the target must have at least the **same capacity** (for sector-based restore).
  - Alternatively, a **file-based restore** can be used.
- To restore the **entire system** or the **system partition**, the computer must be started from the **O&O DiskImage boot medium**.
- For restores to different hardware, see the chapter **Restoring to Dissimilar Hardware (M.I.R.)**.

Restore / duplication to smaller disks
O&O DiskImage also allows you to restore or duplicate to a smaller target disk.

Requirements and procedure:

1. Select, for example, system partition **C:** as the source.
2. Select a **smaller target disk**.
3. O&O DiskImage asks whether the boot partitions should also be transferred confirm with **Yes**.
4. O&O DiskImage now recognizes that a sector-based 1:1 copy is not possible and offers two methods:
   - **Sector-based** (not possible if the target is too small)
   - **File-based** (recommended)
5. Select **File-based**.
6. In the next step, define the **target partition size**.
7. The process starts and the boot partitions are correctly and fully transferred.

If the source disk contains multiple partitions:

- Repeat the process for each additional partition.
- Each time, select the remaining free space on the target disk as the destination.

Note:
This process uses the **Microsoft Volume Shadow Copy Service (VSS)**.
If problems occur, the restore should be performed using the **O&O boot medium**.

Restore options
Under **Drive Restore Restore options** you can define additional settings, including:

- security options
- data integrity checks
- behavior on unreadable sectors
- automatic actions after the restore completes

These options allow you to adapt the restore process precisely to your environment or specific requirements.

Creating restore profiles
Under **Drive Restore Restore options**, you can manage profiles to execute recurring tasks quickly and consistently.

To create a profile:

1. Configure the desired restore options.
2. Click **Save as**.
3. Enter a profile name and confirm.
4. Under **Manage profiles**, you can edit or delete existing profiles.

In **Current profile** you can select:

- **Standard**, or
- **Custom**

Force write method
Under **Restore options Advanced**, you can define how data is written to the target:

- **Write to drive** (default for used sectors and forensic methods)
- **Write directly to disk** (default for Direct Forensic)

Forcing the low-level write method is required for:

- encrypted disks
- drives that were backed up forensically
- scenarios where the file system driver must be bypassed

Activate this by checking **Force write method** and selecting the desired option.

Overwrite unused sectors
Under **Restore options Advanced**, you can define whether unused sectors of the target partition should be explicitly overwritten with **zeroes** during restore.

Advantages:

- previously existing data remnants are *not* recoverable
- increases data privacy and security
- recommended for confidential or sensitive data

File Backup

In general, we recommend backing up entire partitions or disks to ensure that no important data is accidentally omitted. However, in some cases it is useful to back up **only specific files or folders**—for example, for project-related copies, quick interim backups, or transferring selected datasets.

All file-based backup functions can be found under the **Files** tab.

Backup

A file backup—just like a drive backup—can be created as either a **full backup** or a **backup of changes**:

- **Full Backup:**
  Contains all selected files and folders in their entirety.
- **Backup of Changes:**
  Contains only files that have been changed, deleted, or newly added since the base backup.
  A base backup can be:
  - a previous full file backup
  - a previous file backup of changes

This backup type is particularly space-efficient but requires an existing backup chain.

Performing a File Backup

If you want to back up only selected folders or files, use the file backup option:

1. On the O&O DiskImage start page, click **File Backup**.
   The file view may take a moment to load—the progress bar indicates the status.
2. Navigate to the desired folder.
3. Check the files/folders you want to include in the backup.
   - Multiple selections are possible.
   - You may also select an entire drive (all files will be included).
4. Click **Start File Backup**.
5. Check the proposed target directory and adjust it if necessary.
6. Optionally specify a name for the backup.
7. Click **Start**.

The result is a compressed **OBK** file (*.obk).

Selection Criteria

Before starting the file backup, you can include or exclude files based on specific criteria.
This is particularly useful when:

- excluding temporary files
- backing up only certain file types
- ignoring large files

Click **Criteria** to define the desired filters.

Tip:
Under **File Backup Options**, you can configure advanced settings or save the backup directly as a recurring scheduled task (**Add as task**).

Backup of Changes (File Backup)

Use this function to back up only files that have changed since the previous backup:

1. Ensure that your computer has access to the base backup.
2. On the start page, select **File Backup File Backup of Changes**.
3. Select the base backup and click **Open**.
4. Choose the target directory (preferably the same as the base backup).
5. Optionally specify a name for the backup.
6. Optional: Open **Additional Options**.
7. Start the process.

Note:
The backup of changes compares the data stored in the base backup with the current file system—file by file or sector by sector.
This may take more time but requires significantly less storage space.

File Backup Options

Under **File Operations File Backup Options**, you can define global default settings for every new file backup.

Encrypting File Backups

To protect sensitive data, O&O DiskImage supports **AES encryption** with key lengths up to **256 bits**.

To activate encryption:

1. Open **File Operations File Backup Options Security**.
2. Select the desired encryption level.
3. When starting the file backup, you will be prompted to enter a password.

You may also encrypt an existing backup afterward using **Convert Backup File**.

File Backup Method

Under **File Operations File Backup Options Backup File Backup Method**, choose the default method for future file backups:

- **Full Backup** (recommended default)
- **Backup of Changes**

For repeated backups of the same folder structure, the Backup of Changes significantly reduces storage needs.

Note:
The comparison process may take longer but is much more storage-efficient.

Advanced Settings – File Backup

Lock the Source Drive During Backup

To prevent changes during the backup process, you can lock the source drive.

Effects:

- The drive is hidden in File Explorer
- Programs accessing the drive are closed
- No write operations are possible during the backup

By default, locking is **not** enabled.
If locking is disabled, the snapshot cache or VSS uses temporary storage to capture changes.

Checksums for Identifying Unchanged Data For incremental file backups, checksums are stored by default. Benefits include:

- reliable identification of unchanged files
- faster evaluation during follow-up backups
- reduced storage needs for base backups

This option should remain enabled if backups are stored in different directories.

Splitting File Backups

Backups can be automatically split into multiple files—useful for CD/DVD storage or media with limited capacity.

- Under **File Size Split backup into smaller backup files**, specify the maximum file size.
- O&O DiskImage automatically creates multiple OBK files if the backup exceeds the limit.

A **post-processing split** is also possible via *Convert Backup File*.

Using Profiles for File Backups

Save frequently used settings as a profile:

1. Open **File Backup Options**.
2. Click **Save As…**.
3. Enter a profile name.
4. Under **Manage Profiles**, you can edit or delete profiles.

Under **Current Profile**, select:

- **Standard**, or
- **Custom**

This greatly speeds up recurring file backups.

File Recovery

File recovery allows you to restore individual files or complete directories from a previously created file backup (*.obk*). This method is ideal when:

- only a few files are needed quickly
- documents were accidentally deleted
- a project folder needs to be restored
- you want to avoid restoring an entire drive

Before starting, ensure that the backup file is accessible (e.g., an external drive, network share, or internal storage).

How to Restore Files

1. Click **Start** and select **File Recovery**.
2. In the **Choose Backup** dropdown list, select the desired OBK backup.
    - If it is not listed, browse your drives and select the OBK file manually.
3. Click the **Choose Target Directory** icon.
   You now have two options:
    - **Restore to a new directory**
      Files are restored to a new location without overwriting existing files.
    - **Replace original data**
      Files are restored to their original location;
      Existing files are overwritten with the versions from the backup.
4. Click **Start** to begin the recovery process.
   Progress will be shown, and files will be available immediately after completion.

Note:
If you only need specific files, you can select individual items inside the OBK before starting the restore.

Tools

The Tools menu provides a range of additional functions for processing, analyzing, and converting backup files. These options help you convert, merge, validate, or mount backups as virtual drives.

Convert

As a general rule, we recommend creating backups in the **native O&O DiskImage format (OMG)**. Only then is the full range of features available to you – including differential backups, encryption, recovery options, and forensic methods.

If you need another format, you can convert existing backups into different target types, for example into **VHD/VHDX files** for use with virtual machines.

In addition, this tool allows you to **merge backups of changes** and combine them into a single full backup – ideal for archiving or cleaning up older backup sets.

Backup File Conversion

With the **Convert** tool you can change the properties and contents of an existing backup (OMG).
Important: A **copy** of the backup is always created – the original file remains unchanged.

You can perform the following adjustments:

- Change the compression level
- Add or remove encryption
- Split the backup into multiple files of fixed size
- Convert the backup into a **VHD/VHDX file**
- Remove or merge drives contained within a backup

This tool gives you maximum flexibility when working with existing backup data.

Merging Backups

Under **Tools Convert Backup Files Add**, you can merge individual backup files into a new backup.

The following applies:

- Only **backup files of the same type** can be merged:
  - *Used sectors*
  - *Forensic*
  - *Direct forensic*
- The drives to be backed up are selected from multiple backup files and transferred into a new backup.

This is particularly useful for consolidating backup sets or reducing the number of archive files.

Working with Virtual Hard Disks (VHD/VHDX)

O&O DiskImage can convert backups (*.omg*) into **VHD** and **VHDX** formats.
This makes it possible to:

- mount the backup as a virtual drive in Windows
- boot it as a virtual machine
- test backups without performing a restore
- analyze system states after failures or malware attacks

To convert a backup:

1. Open **Tools → Convert Backup Files**.
2. Select an OMG backup file as the source.
3. Choose **Virtual Hard Disk (VHD/VHDX)** as the target format.
4. Click **Start**.

The following restrictions apply:

- Compression, encryption, and splitting are not available for VHD/VHDX targets.
- Only the **Used Sectors** and **Forensic** backup methods are supported.
- A file backup (OBK) **cannot** be converted to VHD/VHDX.
- A VHD/VHDX file can contain **only one disk**.
- Dynamic disks with spanned or mirrored partitions cannot be converted.

Merging Backups of Changes

If you have multiple backups that contain only changes, you can merge them into a new full backup.

Procedure:

1. Ensure that all backup files in the chain are available.
2. Click **Tools → Merge Backup**.
3. Select the backup files you want to merge.
4. Start the process.

After merging:

- A **new full backup** is created.
- Older change backups can be deleted or archived.
- The backup chain becomes much easier to manage.

Note:
Only **consecutive** backups from the same chain (identical base backup) can be merged.

Working with VHD/VHDX Files

Converted virtual hard disks can be used in many ways:

- They can be **mounted as additional drives** in Windows 8.1/10/11.
- They can be used as virtual disks in **Hyper-V or Virtual PC**.
- They are suitable for **verifying the recoverability** of a backup.
- They allow you to **boot a completed system state** for testing purposes.

Important notes:

- Only backups of the same system can be successfully booted as VHD/VHDX.
- A Windows operating system **from Windows 8.1 upwards** is required.
- Any changes made while running from the VHD/VHDX **directly affect the virtual disk**.
- If you boot from a VHD/VHDX and modify data that resides on shared disks, those changes may affect your host system, provided common storage is in use.

Network

O&O DiskImage allows you to store backups directly on network drives or restore backup files from the network. To use these functions, you must connect to the appropriate network share and, if necessary, authenticate on the network.

Connect Network Drive Via the Tools menu, you can connect a network drive to your system so that it can be used as a backup target or as a source for restores.

Procedure:

1. Open the **Tools** menu.
2. Select **Connect Network Drive**.
3. Enter the path, username, and password (if required).
4. Confirm your entries to connect the drive.

The network drive is then available in O&O DiskImage just like a local drive.

Disconnect Network Drive If you no longer need an existing connection, or want to disconnect it for security reasons:

1. Open the **Tools** menu.
2. Select **Disconnect Network Drive**.
3. Choose the desired drive and disconnect it.

Note:
To access network drives—for example, to store or restore backups—you may need to authenticate on the network.

For more details, see the chapter **Authenticating on the Network**.

Backup Files

All tools for managing existing backup files can be found in the **"Read or Validate Backups"** section. These functions can be applied to **all backup types**—regardless of whether they are OMG, OBK, VHD, or VHDX files.

Read Backup Information The **Read Backup Information** function displays detailed information about an existing backup file.

To use it:

1. Select **Read Backup Information**.
2. In the browser window, choose a backup file (*.omg* / .obk*).
3. You will then see, among other things:
    - the backup method used

- creation date and time
- backup version
- number of contained drives or files
- structural and file information
- compression and encryption used

This function is ideal for quickly assessing the structure and usability of a backup.

Validate Under **Tools**, you will find the **Validate** function, which checks the structural integrity of a backup file.

Validation ensures that:

- the backup file is logically and technically correct
- no structural or internal errors are present
- the file can be reliably restored in an emergency
- encrypted or compressed backups are processed correctly

During validation, decryption, decompression, and internal checksums are fully verified.

Typical reasons for failed validation include:

- Errors during **encryption or decryption** (wrong password, corrupted data)
- Errors during **compression or decompression** (issues in Windows APIs / drivers)
- Backup files modified by the user
- Manipulation by programs or drivers
  (for example, antivirus software blocking or changing the file)
- Damage caused by defective storage media or faulty hardware

Note:
Always allow the validation process to complete fully.
If you choose **"Skip"** or **"Cancel"**, O&O DiskImage cannot guarantee that:

- the backup was created correctly, or
- it can be restored without errors in an emergency.

A successful validation significantly increases the reliability of your entire backup strategy.

System

In addition to its backup features, O&O DiskImage provides a range of system tools that let you:

- create boot media (classic or as O&O DiskImage ToGo)
- control backup and restore processes via command line
- adjust computer properties (e.g. the SID)
- check drives for errors
- create and manage an O&O DiskImage RecoveryPartition

These features are especially useful in disaster recovery scenarios, rollout scenarios in networks, and for system diagnostics.

O&O DiskImage ToGo

O&O DiskImage ToGo turns an external hard drive or sufficiently large USB stick into both:

- a **rescue boot medium**, and
- the **preferred backup destination** for system backups.

As soon as the ToGo medium is connected, O&O DiskImage can automatically create a system backup onto it. In an emergency, you can boot directly from this medium and restore the stored backup in just a few steps – without having to look for a separate boot medium or backup storage.

How to create O&O DiskImage ToGo (short overview):

1. Connect an external hard drive or USB stick with sufficient capacity.
2. In the program, select the function to create a **bootable medium**.
3. Select the attached drive as the target.
4. O&O DiskImage configures this medium as a boot medium and marks it as the default backup path.

If you **have not yet set up any storage medium for your backups**, O&O DiskImage ToGo is a particularly recommended solution.

Create Boot Medium

A bootable O&O DiskImage medium (boot CD/DVD or USB stick) enables you to:

- start the computer when Windows no longer boots
- restore backups from external storage or from the RecoveryPartition
- perform restores independently of the running system

You create the boot medium via:
Tools Create Boot Medium

Process:

1. O&O DiskImage analyzes which **creation methods** for a boot medium are currently available.
    - Available options: marked with a green check mark
    - Unavailable options: marked with a cross
2. The most suitable **Windows PE base** is selected automatically (you can adjust it via **Change** if needed).
3. In the second step, choose the target:
    - **CD/DVD burner**
    - **USB stick / removable drive**
    - or **ISO file** (for later burning or for virtual environments)
4. Click **Create** to generate the bootable medium.

Note:
Due to Windows limitations, a maximum of **2 TB** of the target drive can be used for the boot medium. Any remaining space will not be used.
All data on the target medium will be **deleted** during creation.

Select Windows PE Base / Install ADK

To create the boot medium, O&O DiskImage uses the **Windows Recovery Environment** or – if that is not sufficient – the **Windows Assessment and Deployment Kit (ADK)** or earlier **AIK** variants.

In the boot medium creation dialog:

- Available creation methods are marked with a **green check**
- Unavailable variants are shown with a **cross**

Buttons:

- **download** – opens the corresponding Microsoft download page for ADK/AIK
- **package** – starts the local ADK/AIK installation file

Depending on your Windows version, you need:

- **Windows 11**: ADK for Windows 11 + WinPE add-on
- **Windows 10**: ADK 10
- **Windows 8.1**: ADK 8.1
- **Windows 8**: ADK 8.0

(The respective download links are available in Microsoft's online documentation.)

Custom Driver Integration

You can specify a folder containing drivers to be integrated into the offline operating system of the boot medium. This ensures that, for example:

- storage controllers
- network adapters
- graphics drivers

are available immediately when the boot environment starts – including for non–PnP-capable devices.

Command Prompt – Command Line

In addition to the graphical interface, O&O DiskImage offers a **command-line version** that is controlled via the Windows Command Prompt (cmd).

To open it:

1. In the program, go to **Tools → Command Prompt**.
2. A Windows command-line window appears.
3. The O&O DiskImage GUI remains open in the background.

Typical path of the executable:

```
C:\Program Files\OO Software\DiskImage\oodicmdc.exe
```

Examples:

- Sector-based backup of drive S:
  `oodicmdc.exe /create image /source S: /destination E:\Sample.omg`
- Validate a backup file:
  `oodicmdc.exe /validate /source E:\Sample.omg`
- Restore S: to T: (target drive will be overwritten):
  `oodicmdc.exe /restore image /image E:\Sample.omg /source S: /destination T: /OverwriteTargetData`

Note:
You must **not insert manual line breaks** inside a command in the command line. Line breaks in examples are for formatting only.

The command-line interface supports the following groups of commands, among others:

- **/create image** – create a sector-based backup (optionally incremental)
- **/restore image** – restore a sector-based backup
- **/convert image** – convert a backup (e.g. OMG → VHD/VHDX)
- **/create backup** – create a file-based backup
- **/restore backup** – restore a file-based backup

- **/validate** – validate a backup
- **/mount image / unmount image** – mount/unmount backups as virtual drives
- **/duplicate** – duplicate a drive or disk
- **/add license** – register the product
- **/stop** – stop running actions
- **/creating bootable medium** – create a bootable medium via command line
- **/show volumes** – list volumes and their properties

A complete parameter reference can be found in the technical documentation and in the integrated command-line help.

Supported Commands and Parameters

The O&O DiskImage command-line interface supports the following commands. Commands are generally called as:

`oodicmdc.exe <command> [subcommands] [parameters]`

/create image
Creates a **sector-based backup** (image).

Key parameters:

- `/source`
  Source selection – one of the following formats:
  - drive letter, e.g. `D:`
  - volume GUID, e.g. `{xxxx-xxxx-xxxx-xxxx}`
  - `DiskNo X` (disk number, e.g. `DiskNo 0`)
  - `Offset@DiskNo X@Y` (offset of a volume on a disk, e.g. `1048576@1`)
- `/destination` (optional)
  Path and name of the backup file.
- `/password "…"` (optional)
  Password for automatic encryption (also enables “force dismount” if required).
- `/comment "…"` (optional)
  Comment for the backup.
- `/exclude "…"` (optional)
  Exclude specific objects (path/wildcards).
- `/type "…"` (optional)
  Backup type:
  - `"used sector"` (default)
  - `"forensic"`
- `/max <MB>` (optional)
  Maximum file size of the backup in MB (splitting occurs automatically above this).
- `/format "…"` (optional)
  Backup file format:
  - `"O&O DiskImage"` (default)
  - `"VHD Format"`
  - `"VHDX Format"`

- `/VirtualDiskType "…"` (optional)
  Virtual hard disk type:
  - `"dynamic hard disk"` (default)
  - `"fixed hard disk"`

/create image increment
Creates an **incremental sector-based backup** based on an existing backup.

(Uses the same fundamental parameters as `/create image`, plus parameters identifying the base backup and incremental-specific options.)

/restore image
Restores a **sector-based backup**.

Key parameters:

- `/image "…"`
  Path and name of the backup file.
- `/source "…"`
  Source object from the backup:
  - drive letter, e.g. `D:`
  - `DiskNo X`
  - `Offset@DiskNo X@Y`
- `/destination "…"` (optional)
  Target for the restore:
  - drive letter, e.g. `D:`
  - volume GUID `{…}`
  - `DiskNo X`
  - `Offset@DiskNo X@Y`
- `/DecryptPassword "…"` (optional)
  Password for encrypted backups.
- `/FillEmptyBlocksNull` (optional)
  Fill empty sectors with `0`.
- `/WriteHarddiskDrive` (optional)
  Write directly to the disk instead of via the volume.
- `/CreateVolumeLikeSource` (optional)
  Create the target volume like the source volume without prompting.
- `/IgnoreReadErrors` (optional)
  Ignore read errors (log them but do not abort).
- `/SetBootPartitionBootable` (optional)
  Automatically mark a bootable partition as active.
- `/ClearTargetDrive` (optional)
  Clear the target layout without prompting.
- `/OverwriteTargetData` (optional)
  Overwrite data on the target without prompting.
- `/IgnoreDataModification` (optional)
  Report data modifications but do not abort the process.

/convert image
Converts a **sector-based backup** to another format (e.g. VHD/VHDX) or with other properties.

Key parameters:

- `/image "…"`
  Path and name of the source backup.
- `/source "…"`
  Source selection (drive letter or `DiskNo`).
- `/DecryptPassword "…"`
  Password for encrypted backups.
- `/destination "…"`
  Path and name of the target backup.
- `/destinationPassword "…"` (optional)
  Password for the new (target) backup.
- `/comment "…"` (optional)
  Comment.
- `/max <MB>` (optional)
  Maximum size of the target file.
- `/format "…"` (optional)
  `"O&O DiskImage"`, `"VHD Format"`, or `"VHDX Format"`.
- `/VirtualDiskType "…"` (optional)
  `"dynamic hard disk"` (default) or `"fixed hard disk"`.

/create backup
Creates a **file-based backup** (OBK).

Key parameters:

- `/source "…"`
  File name including path and/or wildcards (e.g. `C:\Data\*.docx`).
- `/destination "…"`
  Backup path/backup name.
- `/password "…"` (optional)
  Password for encryption.
- `/dismount` (optional)
  “Force dismount” – unmounting to protect against changes (default is VSS/snapshot).
- `/comment "…"` (optional)
  Comment.
- `/exclude "…"` (optional)
  Exclusion filter.
- `/max <MB>` (optional)
  Maximum size of the backup file.
- `/IgnoreReadErrors` (optional)
  Ignore read errors.

/restore backup
Restores a **file-based backup**.

Key parameters:

- `/source "…"`
  Backup path/backup name.
- `/destination "…"`
  Target directory (full path).
- `/DecryptPassword "…"`
  Password for encrypted backups.
- `/IgnoreReadErrors` (optional)
  Ignore read errors.
- `/OverwriteTargetData` (optional)
  Overwrite target without prompting.
- `/IgnoreDataModification` (optional)
  Report modifications but continue the process.

/validate
Checks the **integrity** of a sector- or file-based backup.

Key parameters:

- `/source "…"`
  Backup path/backup name.
- `/DecryptPassword "…"` (optional)
  Password for encrypted backups.
- `/AllSplits` (optional)
  Include all parts (splits) of a split backup.

/mount image
Mounts a sector-based backup as a **virtual disk**.

Key parameters:

- `/source "…"`
  Drive letter or `DiskNo` of the virtual device.
- `/image "…"`
  Path and name of the backup file.
- `/DecryptPassword "…"` (optional)
  Password for encrypted backups.
- `/driveletter X:`
  Drive letter to assign to the mounted volume.

/unmount image
Unmounts a previously mounted sector-based backup.

- `/source "…"`
  Drive letter or `DiskNo` of the virtual disk.

/duplicate
Duplicates a drive or disk (clone function).

Key parameters:

- `/source "…"`
  Source selection:

  - drive letter, e.g. `D:`
  - volume GUID `{…}`
  - `DiskNo X`
  - `Offset@DiskNo X@Y`
- `/dismount` (optional)
  Protection against changes (VSS/snapshot).
- `/exclude "…"` (optional)
  Exclude specific contents.
- `/type "…"` (optional)
  `"used sector"` or `"forensic"` (default: `used sector`).
- `/destination "…"`
  Target selection, in the same formats as `/source`.
- Additional optional parameters:
  - `/FillEmptyBlocksNull`
  - `/WriteHarddiskDrive`
  - `/CreateVolumeLikeSource`
  - `/IgnoreReadErrors`
  - `/SetBootPartitionBootable`
  - `/ClearTargetDrive`
  - `/OverwriteTargetData`

/add license
Registers the product.

Parameters:

- `/name "…"` – your name
- `/company "…"` – your company
- `/serial "…"` – serial number

/stop
Stops all currently running O&O DiskImage actions.

/creating bootable medium
Creates a **bootable medium** from the command line.

Optional parameters:

- `/recovery environment`
- `/ADK`
- `/AIK`
- `/installation media`
- `/boot device`
- `/ISO path`

These determine:

- which Windows components are used (Recovery Environment, ADK, AIK)
- which installation media is used
- the target device (CD/DVD/USB)
- the path of the ISO file to be created

/show volumes
Displays information about volumes.

- Without additional parameters: lists the system's volumes.
- With `/image "…"`: shows volumes contained in a backup file.

The output includes, among other things:

- drive letters
- disk number (DiskNo)
- offset in bytes

Change Computer Properties

This function lets you adjust the **identity of a computer**, especially the **computer SID**. This is important when:

- a system image is deployed to multiple computers on the same network
- cloned systems with identical SIDs exist in the same environment
- authentication or security issues occur in workgroups

Each cloned system initially has the same SID, which can negatively affect security and device management. O&O DiskImage therefore includes a tool to change this identity.

Important notes:

- The SID can **only be changed** when O&O DiskImage is started **from the boot medium** (not in a running Windows system).
- If errors occur while changing the SID, the registry hives **SECURITY** and **SAM** should be reset.

Procedure:

1. Boot the computer from the O&O DiskImage boot medium.
2. In the program, select **Tools → Change Computer Properties**.
3. Load the **inactive Windows system** (usually `C:\Windows`).
4. Assign a **new computer name**.
5. Click **Change** to save the new identity, or **Close** to cancel.

Check Drive

Via **Tools → Check Drive**, you can have O&O DiskImage check:

- the **structural integrity of the file system**, and
- the **surface of the storage device**

This helps you detect impending data loss at an early stage.

Process:

1. Start the **Check Drive (CheckDisk)** wizard.
2. Select the drive to be checked.

3. Start the analysis.
4. Monitor the progress in the status display.
5. Once finished, all messages and any errors found are listed.

O&O DiskImage RecoveryPartition

The **O&O DiskImage RecoveryPartition** is a special recovery partition that contains:

- a **bootable O&O DiskImage environment**, and
- optionally backups stored directly on this partition

If Windows no longer starts, the O&O DiskImage boot environment is automatically loaded from this partition, allowing you to restore:

- backups from external media, or
- backups from the RecoveryPartition itself.

System requirements (excerpt):

- At least **3 GB** of free space
- If used as the standard backup path: at least **10% of the disk size**, but a minimum of **25 GB**
- A maximum of **3 primary partitions** for MBR layouts
- **No support for dynamic disks**

Creating a RecoveryPartition (short overview):

1. On the start page, click **Recovery Medium**.
2. Choose:
    - **Use existing partition**, or
    - **Create new partition**
3. Select the disk and, if applicable, the partition to be used.
4. Optionally define the RecoveryPartition as the **standard backup path** (size can be adjusted using *Maximum size*).
5. Confirm with **OK** – the bootable image will be generated.
6. Afterwards, it is recommended to create a full or 1-Click backup, ideally directly onto the RecoveryPartition.

Booting from the RecoveryPartition (examples):

- Hold the Shift key and click **Restart** in the Start menu.
- Go to **Settings** → **Update & Security** → **Recovery** → **Advanced startup** → **Restart now**.
- If system problems are detected automatically: choose **Advanced startup**, then **Troubleshoot** → **Advanced options** → **Startup Repair**.

After booting, the RecoveryPartition is typically shown in O&O DiskImage with the last available drive letter (often "Z:").

Update or Remove the RecoveryPartition:

Via **Recovery Medium**, you can:

- **Update** – create a new boot image after an O&O DiskImage update; backups on the partition remain intact.
- **Delete** – remove the RecoveryPartition and the backups stored on it; the Windows Recovery Environment is reactivated.

Warning:
Always delete the O&O DiskImage RecoveryPartition **via O&O DiskImage itself**. Deleting it manually (e.g. via Disk Management) can cause system issues.

Virtual Drives

Virtual drives are useful in many situations – for example, when you only need individual files from a backup without restoring the entire image. O&O DiskImage lets you mount backups and ISO files as virtual drives and browse them directly in a running Windows system.

Note:
In many cases, a special O&O DiskImage driver is required to mount backups. If it is not yet installed, the program will notify you and allow you to install it directly.

Mounting a Backup as a Virtual Drive

You can mount drives from a backup file (*.omg) as additional drives in Windows Explorer. This allows you to:

- copy individual files or folders from the backup
- check or compare data
- browse the contents without restoring the image

You **cannot modify** the mounted virtual drive (no deleting, renaming or adding files inside the backup).

To mount a backup:

1. In the menu bar, open the **Tools** tab and select **Mount** (or press **Ctrl+M**).
2. In the dialog, select the backup file (*.omg) that contains the drive you want to load.
    - If you are unsure, you can use **Read backup information** to display details about the backup.
3. After selecting the backup, all drives contained in the image are listed.
4. Select the desired drive.
5. Choose a free **drive letter** (for example, G:).
6. Click **Mount drive**.
7. The virtual drive now appears as a regular drive in Windows Explorer.

Note:

- You can only access areas that are actually contained in the backup.
- Updating the view may take a moment.
- Backups can only be mounted if they are **available locally**. Backups stored on network drives cannot be mounted as virtual drives.

Enable Loading of Disks

In addition to the actual data, a backup also stores information about the disk layout, for example:

- partition table (MBR/GPT)
- extended boot sectors
- LDM database (Logical Disk Management)
- other system areas

With the **Enable loading disk** option you can also load this information and present the operating system with a "virtual hard disk" that reproduces the original layout.

This is especially useful if you want to recover deleted or damaged data from a **forensic backup**.

Note – possible detection issues with entire disks

When mounting a complete disk, detection problems may occur if:

- the partition table is damaged or invalid
- an unsupported layout was used (for example GPT under older systems)
- dynamic disks with spanned, striped, mirrored or RAID-5 volumes were backed up without including all participating disks
- the disk is encrypted

Unmounting a Mounted Drive

If you no longer need a virtual drive, you can remove it again:

1. In the **Tools** tab, select **Unmount**.
2. In the dialog, select the desired virtual drive.
3. Remove it using the corresponding button.

Tip:
After restarting Windows, mounted virtual drives are automatically removed from the drive list.

Technical Limitations

Please note the following:

- **Remote Desktop Connection:**
  When working via RDP, you may need to **log in again** for mounted drives to be displayed correctly.
- **Windows XP 32-bit:**
  Mounting backups larger than **2 TB** is not supported under 32-bit Windows XP.
- **VHD/VHDX mounting:**
  When mounting VHD/VHDX files, Windows may display an error message stating that the disk image could not be mounted or contains no recognizable partitions.
  In this context, this message can usually be **ignored** – the file will still be mounted correctly.

Note on Permissions (SID Issues)

If messages such as "Access denied" appear when accessing files on the mounted drive, this may be due to different **Security IDs (SIDs)** – for example, if the files were created under a previous Windows installation or with a different user account.

Solution:
If necessary, enable the **"Administrator"** account (which is disabled by default) and access the files using this account. Proceed carefully, as working with administrator rights allows far-reaching changes to the system.

Mounting an ISO File

O&O DiskImage can also mount **ISO files** as virtual drives. This lets you browse the contents of an ISO file and copy files from it to existing drives. You cannot modify the mounted ISO drive itself.

To mount an ISO file:

1. In the **Tools** tab, select **Mount ISO file as drive**.
2. Select the desired ISO file (*.iso).
3. Click **Mount ISO file**.
4. If needed, choose a specific drive letter.

5. After a short time, the virtual drive appears in Windows Explorer.

Tip:
To have the virtual CD/DVD drive also shown in the O&O DiskImage drive list:

- in **Program settings** → **General**, enable **Include CD and DVD drives**, and
- under **View**, enable **Show non-backupable drives**.

Note:
After restarting Windows, this virtual drive is also removed automatically.

Tasks and Reports

The task assistant in O&O DiskImage allows you to run recurring backups or other automated processes according to a defined schedule. This lets you fully automate your backup strategy – ideal for regular backups that should run reliably without manual intervention.

Via **Start** → **Tasks & Reports** you open a central overview of all configured tasks and all generated reports. A double-click lets you edit tasks or view reports.

Important:
For a recurring task to work reliably, all initial conditions must remain stable, for example:

- paths and storage locations of backups
- available source and target drives
- drive names
- network access rights

If these conditions change, a task may no longer run successfully.

Tasks

Run Tasks

Click **Start** → **Tasks & Reports** to start or edit an existing task.
Use the **Run** function to start a task immediately – after a safety prompt.

Add as Task – General

Before you can create a task, you must first select an action in the main window, for example:

- **Drive backup**
- **File backup**
- **Backup of changes**
- **Duplicate (clone)**

Then:

1. Select the desired drives or folders.
2. Optionally adjust the backup options (compression, encryption, method, etc.).
3. Click **Add as task**.
4. In the task assistant, enter a name for the task.
5. Configure schedule, notifications and backup options.

Note:
The task name is only a label – multiple tasks may use the same name.

Task Enabled / Disabled

If you temporarily **do not want a task to run**, you can disable it without deleting it.
The task remains stored, but will only be executed again after it is re-enabled.

Run Task as User

For each task you can define a user account under whose privileges the task will run. This affects:

- access to network drives
- e-mail notifications
- pre- and post-processing commands
- required authentications

If no user is specified, the task runs under the **SYSTEM** account.

Warning:
The SYSTEM account does *not* have access to all resources – especially not to all network shares.

Set Schedule

In the **Schedule** tab you define when and how often a task should run.

 One-time execution

- start date
- start time

 Recurring execution

For weekly or periodic execution you can set:

- selected weekdays
- start time
- start and end date of the interval
  (for example, every Tuesday at 21:00 for 5 weeks)

Notification by e-mail

In the **Notification** tab you can configure whether you want to receive an e-mail:

- on successful execution
- on errors
- on warnings

Specify the recipient address and optionally a custom message text.

Important:
In **Program settings Notifications**, the SMTP settings of your mail server must be configured beforehand.

Backup – Options

On the **Backup** tab you configure:

- storage location of the backup file

- file name (can also be generated dynamically)
- backup type (full, changes, sector-based, etc.)
- compression and encryption

Dynamically generated file names

By default, for example:

`Backup_%Year%-%Month%-%Day%`

Additional variables such as `%Time%` or `%ComputerName%` are useful to avoid collisions – especially with multiple backups per day.

Suppress User Prompts During Execution

If this option is enabled:

- prompts (for example "File already exists – overwrite?") are **not** displayed
- the task aborts automatically in doubtful cases
- errors are logged

This is especially important for tasks that are intended to run unattended.

Abort on Errors

If enabled:

- the entire task is aborted when the first error occurs
- no further step is executed

If disabled:

- further steps are processed whenever possible
- errors are only logged

Run After Completing Task

You can define automatic actions after the task completes:

- **Restart**
- **Shut down**
- **None** (default)

This is useful for nightly backups where the computer should automatically shut down afterwards.

Special Notes for Backup Tasks

Target Path

- Taken from program settings by default
- Can be set manually per task

Example for Incremental Backups

If the *base backup* is moved, the new storage location must be updated in the task assistant.
Otherwise the task cannot find the base backup and will fail.

Pre- and Post-Task Commands

With this feature you can automate additional actions, for example:

- stop services (e.g. SQL, Exchange)
- run custom scripts
- establish network connections
- delete temporary files
- start user-defined programs

Examples

```
net stop MSSQLSERVER net start "My Custom Database Service"
```

Notes:

- Commands must be available on the system.
- Commands are executed with the privileges of the configured user account.
- When using the SYSTEM account, network access is not always possible.

Task Information

On the final **Information** tab, all settings of the task are listed in a clear summary.
This page is for information only – changes cannot be made here.

Edit Task

To modify an existing task, first open **Tasks & Reports** on the O&O DiskImage start page. There you will see a list of all configured tasks.

Edit Task – Step by Step

1. **Select task**
   In the task list, check the box next to the task you want to edit.
2. **Open Edit**
   Click the **Edit** icon.
   The task assistant opens with all current settings of the task.
3. **Adjust settings**
   Make the desired changes.
   You can edit all parts of the task, for example:
   - schedule
   - backup options
   - storage location
   - notifications
   - pre- / post-processing commands
   - user account for execution
4. **Save changes**
   Click **OK** to apply the changes.
   If you do not want to save any changes, click **Cancel**.

Manage Multiple Tasks at Once

For certain administrative actions you can select multiple tasks at the same time. Simply check all tasks you want to edit.

The following functions can be applied to multiple tasks at once:

- **Delete**
  Permanently removes all selected tasks.
- **Export**
  Saves tasks to a file so they can be imported on other computers or used for documentation.
- **Import**
  Loads previously exported tasks and adds them to the task list.

Note:
Imported tasks are not activated automatically. After importing, they may need to be checked and enabled manually – especially if drive letters, paths or network conditions differ.

Important Notes on Editing Tasks

- If you change critical parameters, such as the backup storage location or the source drives, the task may no longer be able to run successfully.
- For incremental backup tasks in particular, the relationships between full and subsequent backups must remain correct.
- If the user account or network paths have changed, always verify authentication and permissions.

Delete Task

To delete a task, go to the O&O DiskImage start page and select **Tasks & Reports**.

Then check the box next to the task you want to delete and click **Delete task**.

Check Task

To check whether a task has valid settings – i.e. whether it is syntactically and logically executable on a local system – go to the O&O DiskImage start page and select **Tasks & Reports**.

Then check the box next to the task you want to validate and click **Check task**.

Task Files

Import Task
To import a task, go to the O&O DiskImage start page, select **Tasks & Reports** and open the **Import tasks** function. In the dialog, select the desired task file – it will then be added to the task list.

Export Task
To export a task, go to the O&O DiskImage start page and select **Tasks & Reports**.
In the task list, check the box next to the task you want to export and click **Export task**.
Save the task file (*.xml), for example, to an external storage device so that it can be reused on another computer (see **Import task**).

Reports

A status report is automatically created for every action carried out by O&O DiskImage. These reports can be viewed and exported as XML files from the start page under **Tasks & Reports**.

A report includes, among other things:

- date and time of execution
- type of action (backup, restore, clone, validation, etc.)
- settings and parameters used
- source and target of the operation performed
- success or error messages as well as warnings
- a summary status indicator

Reports are particularly helpful for tracing processes, identifying sources of errors or handling support requests efficiently.

Program Settings

Under **Start Program Settings** you can configure O&O DiskImage to suit your needs and workflows. Here you can also define whether your custom settings should be saved permanently and automatically reused the next time the program starts.

In addition to general behavior options, you can adjust security-related settings and notification options, depending on the edition and environment in which you are using O&O DiskImage.

Note:
If you start O&O DiskImage directly from a boot medium, the tabs **General**, **Security** and **E-Mail Notification** are not available. In the bootable environment, only those settings are accessible that are necessary for recovery and system analysis.

General – Change Defaults

In the **General** section of the program settings you can define basic behavior and display options for O&O DiskImage. These settings are designed to simplify your daily work and align the program start with your preferred routines.

Set Start Page
You can specify which program page is displayed when O&O DiskImage starts. For example, if you regularly perform backups, you can set the *Backup* page to appear by default at program start.

Include Removable Drives
Under *Appearance and behavior* you can define whether removable media such as USB sticks, external drives or memory cards are displayed in the drive list and taken into account for backup or restore operations.
Because many removable media are significantly slower or only used occasionally, it is recommended that you enable only those types you actually intend to use for backups or restores.

Default Storage Locations
Under *Working directories* you can set the default path where new backups will be stored. This target path is automatically suggested for every new backup and can be overridden individually as needed.

You can also define the storage locations for **tasks** and **reports** here. This lets you keep all automatically executed processes and their logs centrally organized and easy to find.

Tasks and Reports

If you want to adjust defaults for tasks and reports, open the **Tasks and Reports** section in the program settings. Here you can configure both report creation and the behavior when interacting with tasks and reports.

Report Creation
O&O DiskImage can create reports for all program activities. These contain detailed information about the process, status and possible errors of an operation.
To reduce storage usage, you can specify for which actions reports should be generated. Regardless of these settings, a report is always created when a scheduled task is executed – even if reports for other actions have been disabled.

Behavior
To streamline your workflow, you can define what happens when you double-click an entry. This applies to both tasks and reports:

- For tasks, you can choose whether a double-click should start the task or open it for editing.
- For reports, you can decide whether a double-click should display the report directly in O&O DiskImage or open it in an external editor.

These options help you tailor O&O DiskImage to your preferred way of working.

File Backup

Under **File Backup** in the program settings you can define various backup-specific options that improve both convenience and security for file backups.

Prefer External USB Drives as Suggestions
If you enable this option, externally connected USB drives are automatically suggested as preferred targets for file backups. This is particularly useful if you regularly store your backups on portable media or want a clear separation between system and backup data.

Verify Backup File for Errors After Creation
With this setting you can specify that every newly created backup file should be automatically validated immediately after creation. This ensures that the backup is error-free and fully restorable. It improves data security but may slightly increase the total duration of the backup process.

Overwrite Existing Backup Files Without Prompt
If you enable this option, the safety prompt for overwriting existing backup files with the same name is suppressed. This is especially useful when multiple automated backups per day are created and named by date.
Only activate this option if you are certain older backups in that location are no longer needed.

Behavior on Double-Click
Under *Behavior* you can define what happens when you double-click a file or folder in the file backup dialog.
Using the drop-down, you can decide, for example, whether a folder should be opened, selected, or directly added to the backup selection.
This lets you fine-tune the interface to match your personal working style.

File Restore

Under **File Restore** in the program settings you can define how O&O DiskImage should behave when restoring files and folders. These defaults are particularly useful if you frequently restore individual files from backups.

Behavior on Double-Click
You can decide what action should be triggered when you double-click a drive in the *File Restore* action window. Depending on your choice, the double-click can, for example, open a drive, select it or set it directly as the target for the restore.
This allows for a more efficient, workflow-oriented operation.

Notification Settings

For O&O DiskImage to notify you via e-mail about the progress or result of a task, you must first enter the access data for your SMTP server and the sender information. These settings are configured under **Notification** in the program settings.

Once all required information has been entered and saved, you can select your e-mail address as the recipient in the task assistant and enable notifications for specific events. Only then will e-mails be sent correctly during or after execution of a task.

Tip:
The *Domain* field does not necessarily have to contain your local network domain. Instead, you can enter the hostname of your mail server. This ensures that the SMTP dialog (EHLO/HELO) works correctly – especially with servers that enforce strict authentication requirements.

To verify your configuration, you can send a test e-mail directly from the program settings and check whether it is delivered successfully.

Drive Duplication

If you want to adjust defaults for drive duplication, open the **Cloning** section in the program settings. Here you can define how O&O DiskImage presents the available drives in the cloning dialog and how the program behaves when drives are selected.

Show Non-Cloneable Drives
You can configure whether drives that cannot be duplicated – for example CD/DVD drives, empty floppy drives or other unsuitable devices – are shown by default in the *Cloning* action window.
Displaying such drives can be useful if you want a complete overview of all devices, but they are not relevant for the actual duplication process.

Behavior on Double-Click
You can define what happens when you double-click a drive in the *Cloning* action window. Depending on the setting, the double-click can, for example, select the drive, show details or set it directly as the source for the cloning process.
This option helps you tailor the cloning dialog to your working habits for more efficient operation.

Drive Backup

Under **Drive Backup** in the program settings you can define backup-related defaults that make your drive backups more convenient and efficient.

Prefer External USB Drives as Suggestions
If you enable this option, O&O DiskImage will automatically suggest attached USB drives as preferred targets when selecting a destination path. This is especially useful if you regularly store drive backups on external media.

Verify Backup File for Errors After Creation
This setting ensures that each new drive backup is automatically validated immediately after completion. This checks whether the backup file is error-free and fully restorable. While this increases data safety, it may also extend the overall backup time.

Overwrite Existing Backup Files Without Prompt
When this option is enabled, the confirmation prompt for overwriting backup files with the same name is suppressed. This is particularly helpful when regular automated backups are created using date-based naming.
Use this option with care, as existing backups will be replaced without additional confirmation.

Behavior for Non-Backupable Drives
Under *Behavior* you can decide whether non-backupable drives should be shown or hidden in the user interface.
These include, among others:

- empty card readers or floppy drives
- the *Microsoft Reserved Partition* (MSR) on GPT disks

- OEM/manufacturer partitions (e.g. on Dell or IBM systems)
- internal system areas on basic disks

Hiding such drives provides a clearer view and makes it easier to select relevant backup sources.

Drive Restore

Under **Drive Restore** in the program settings, you can define how O&O DiskImage behaves when restoring drives. These presets are particularly useful for recurring or automated restore processes.

Validate backup before restore
You can configure O&O DiskImage to automatically validate the backup file before every restore. This ensures that the backup is intact and fully restorable before the actual process begins. This check increases data security but may also extend the total duration of the restore operation.

Behavior on double-click
Under *Behavior*, you can define what happens when you double-click a drive in the drive list – both for drives contained in the backup and for existing target drives.
Depending on the setting, a double-click can select the drive, show its details, or assign it directly as source or target for the restore operation. This allows faster and more intuitive handling of the restore view.

Security – Network Authentication

To authenticate locally or on the network – for example, to access protected folders or network drives – you must log in with your user account. A user account generally consists of a user name and the corresponding password and has specific sharing and access permissions.
In the context of O&O DiskImage, this particularly applies to storing backups on network paths or loading backups that are stored there.

To make authentication more convenient and automated, O&O DiskImage provides a **password manager**. Here you can store credentials once, which the program will then use automatically whenever required.

Reset security prompts to default
Many security warnings and confirmation dialogs in the program can be disabled permanently. If you want all security prompts to appear again as they did at first program start, you can reset them in the program settings under **Security** by clicking *Reactivate*.

Explanation: Password Manager
The password manager stores your authentication data securely and in encrypted form. The data is compressed, encrypted using the AES method, and then saved. In addition, the order of the records is randomized to further increase security.

For encryption, a pair of keys is used: a public and a private key:

- The public key is stored in the registry:
  `HKEY_LOCAL_MACHINE\Software\O&O\O&O DiskImage7`
  (Note: This key must have a value; an empty entry is not accepted.)
- The private key has a default size of 64 bytes.

Important!
Changes to the Windows registry can cause serious system problems. Only make changes if you are familiar with the registry. Be sure to create a backup of your important data with O&O DiskImage beforehand.

Note:
After making changes in the registry, the database must be reloaded. An overview of the registry entries can be found in the next chapter.

Authenticate on the network
To configure network authentication, proceed as follows:

1. Open **Start** → **Program Settings** → **Security**.
2. If no password database exists yet, click *Create database*.

3. Assign a password for the database and confirm it.
   This password is stored in encrypted form. O&O DiskImage additionally generates an internal key pair (public/private key) to protect the database.
   The O&O DiskImage service also automatically receives access, so that backups can be created in the background.
4. In the security dialog, click **Add** to create a new authentication profile.
5. Under *Computer/Directory*, enter the network path, e.g.:
   `\\ComputerName\Share` or `\\Domain\Share`
   You can also enter only the computer name if all shares on that computer should be opened with this user.
6. Enter the user name in the correct format, e.g.:
   `domain\user1` or `user1@domain`.
7. Enter the appropriate network password.
   Make sure that this user account has sufficient permissions to access the target directory.
8. Optionally, add a description for the stored credentials.

Once this setup is complete, you can use network shares like local storage locations – both for backups and restores.

Security – Using FTP with O&O DiskImage

O&O DiskImage supports the use of FTP servers for storing and loading backups. Only **passive FTP mode** (Passive Mode) is used, as this mode is more stable and firewall-friendly in most network environments.

To store backups on an FTP server, you must authenticate with your FTP user account. This account consists of an FTP user name and the associated FTP password.
It is important that FTP access is clearly identified as such – this is always done using the **"ftp://"** prefix.

When determining the required authentication information, O&O DiskImage uses the exact string of the configured network path. Therefore, make sure you enter the address correctly.

If all details are stored correctly, the test of the authentication information should succeed and the FTP location can be used as a regular backup target.

Specifying the FTP path for backups
For backup operations, O&O DiskImage must be given the full FTP path, including user name.
The format is:

`ftp://user@server/path`

Based on the user name and server, the program can uniquely assign the appropriate authentication information.

Selecting a backup from an FTP server
If you want to load a backup from an FTP server – for example via an open-file dialog – you must enter user name and password to access the directory.

Use the following format to browse the FTP storage:

`ftp://user:password@server/`

Once login is successful, you can browse to the desired directory and select the backup as if it were stored on a local drive.

Tray Icon

After installation, O&O DiskImage displays a **tray icon** in the notification area of the Windows taskbar by default. This icon shows you at all times whether the program is active. During an ongoing operation, an animation is displayed; when idle, the icon remains static.

The tray icon's context menu gives you quick access to important O&O DiskImage functions, including:

- opening the main application

- canceling a running operation
- hiding the tray icon
- disabling the animation

If you do not have administrator rights, the option to start the main application in the context menu is grayed out.

You can also configure whether notifications about task progress or changes to the O&O DiskImage service should be displayed.

Tip:
If you have permanently disabled the tray icon, you can re-enable it at any time via:
Start → All Programs → O&O Software → O&O DiskImage → O&O DiskImage Tray.

Show status window
By right-clicking the tray icon, you can open the **status window**, which shows the current state of the program. From the display you can immediately see whether an action is running or O&O DiskImage is idle.

Restore on Dissimilar Hardware

Traditionally, it was only possible to restore a system partition backup on a computer whose hardware largely or completely matched that of the original system. The same applied when cloning a machine: the target computer's hardware had to be nearly identical. As a result, typical use cases were mostly limited to backing up and restoring the same device.

With the **M.I.R. feature (Machine Independent Restoration)**, O&O DiskImage now allows you to restore a backup – including the system partition – on computers with dissimilar hardware. Likewise, complete system duplicates can be transferred to different hardware platforms.
M.I.R. ensures that key drivers – especially for mass storage and controllers – are automatically replaced or re-integrated so that Windows can successfully start despite changed hardware.

When M.I.R. should be enabled
M.I.R. is required or recommended whenever the target hardware configuration does not match the original environment, or when key components have changed:

- restoring a system to a computer with different or newer hardware
- duplicating or replicating a system to other machines
- replacing, removing or adding key hardware components such as mainboard, controllers or mass storage devices
- migrating from physical systems to virtual machines (P2V) or vice versa (V2P)
- replacing faulty or incompatible drivers using the bootable medium

M.I.R. is enabled as part of the restore process and automatically performs all necessary adjustments to keep the system bootable.

Note:
If you duplicate a system or deploy an existing Windows installation to multiple machines, you should change the **computer name** and the **computer SID** after the restore. This prevents conflicts in network environments, especially when accessing shares or during authentication in workgroups or domains.

Automatic Restore with M.I.R.

The M.I.R. (Machine Independent Restoration) feature in O&O DiskImage is available both when restoring the system partition from a backup and when duplicating an entire system. It does not matter whether you select the system partition explicitly or restore an entire disk including the system partition.
The only important point is that you **enable M.I.R. before the restore or duplication operation is completed**. After that, the automatic adaptation takes care of all further required adjustments.

Procedure for restoring to dissimilar hardware (example: restore from a backup)

To restore a system partition or an entire system to dissimilar hardware, proceed as follows:

1. **Start from the boot medium**
   Boot your computer using the O&O DiskImage boot medium.
   Follow the instructions in the chapter *Start directly from a bootable medium*.
2. **Open Drive Restore**
   On the start page of the boot medium, click **Drive Restore**.
   O&O DiskImage automatically suggests the location of the most recently created backup.
3. **Select the backup file**
   If the suggested backup is not the correct one, browse your drives and select the desired backup file.
   Then click **Open**.
4. **Select drives**
   Once the backup is loaded, all contained drives are listed.
   Check the box for the drive you want to restore.
5. **Define target drive**
   Select the target by checking the corresponding box.
   You can overwrite an existing drive or create a new one in an unallocated area.
6. **Enable M.I.R.**
   Open **More options** and enable the setting **Adjust dissimilar hardware afterwards**.
   This option ensures that system-relevant drivers are automatically adapted to the new hardware.
7. **Start restore**
   Click **Start drive restore** and follow the subsequent dialogs.
   After the restore completes successfully, you will be prompted to restart the computer.

Important:
During the restore, the selected target drive is completely overwritten. All existing data is lost and replaced by the contents of the backup.

Limitations of M.I.R.

Under certain circumstances, a restored or duplicated system may still fail to boot or show malfunctions during startup, even when M.I.R. has been enabled. This is usually caused by incomplete or unsuitable restore/duplication parameters. The following scenarios can lead to boot problems:

The entire disk was not selected as the target.
If only a single partition, a volume or a free area is selected, important system and boot information that exists only on the full disk may be missing.

"Delete layout" was not selected when creating the target layout.
In this case, partitions may be created at different offsets, which can cause Windows to no longer find its boot areas correctly.

Only individual source partitions were selected instead of the entire disk.
As a result, critical boot areas such as EFI partitions, recovery partitions or the Windows boot manager may be missing.

The bootable drive is attached to a controller that is not initialized at boot time.
For example, an internal drive attached via a USB controller (not a USB stick!) may not be detected in time by Windows during boot. In such cases, the startup process can fail.

Note:
If error messages appear during the boot process, you will find detailed assistance in the chapter *Help with error messages during boot*.

Note:
To ensure that a restored system or duplicate is reliably bootable, you should always back up and restore or duplicate the **entire system disk**, not just individual partitions.

Manual Adjustment

In addition to automatic adaptation via M.I.R., you can perform **manual adjustments** to the changed hardware after a restore or duplication. This is especially recommended if the system does not start as expected after the restore, or if certain devices are not detected correctly.

First, carry out the restore or duplication of the system partition or the entire computer as usual.
Afterwards, open the **Change Computer Properties** dialog in O&O DiskImage via *Tools* → *Change Computer Properties*.
There you can intervene manually and supplement any missing hardware adjustments.

The adaptations performed by M.I.R. are based on three actions that can be enabled or disabled during restoration to dissimilar hardware:

Replace Hardware Abstraction Layer (HAL)
Windows uses a Hardware Abstraction Layer (HAL) to support different hardware platforms. It encapsulates architecture-specific functions such as interrupt controllers, multiprocessor communication, or I/O interfaces from the core operating system.
In a running Windows system, the HAL is tightly bound to the existing hardware. If the hardware is changed (e.g. mainboard or CPU replacement), the HAL must be adapted so that Windows can continue to operate stably and without errors. M.I.R. performs this replacement automatically, provided the option has been enabled.

Adopt currently loaded device-control drivers
Device drivers form the communication interface between the hardware abstraction layer and the end devices. For Windows to access new hardware after a hardware change, the required drivers must be installed correctly.
M.I.R. enables the automatic integration or replacement of these drivers so that, after a restore, the system remains bootable and can use the new hardware.

Trigger operating system setup on next restart
This action instructs the Windows operating system to run an internal setup routine on the next startup. This allows incomplete system information to be supplemented, new hardware to be registered, and missing configurations to be updated.
This step helps ensure that Windows starts correctly even after extensive hardware changes and automatically adapts itself to the new environment.

Booting from Media

When you run O&O DiskImage directly from a bootable medium such as a CD, DVD, or USB stick, all functions are available without restriction.

The bootable medium contains Windows PE and is ideal, for example, for restoring your entire computer or the system partition when you have previously created a corresponding backup. You can use the bootable medium with O&O DiskImage even if your Windows can no longer start due to a software error.

Important Notes Before Booting

- **Secure Boot** may need to be disabled depending on system configuration so that the Windows PE medium can start.
- The system should be started in the appropriate **boot mode (UEFI or Legacy/CSM)** – ideally the same mode in which the boot medium was created.
- Windows PE often uses the **English (US) keyboard layout** by default. If necessary, switch to German in the startup dialog before entering passwords or paths.
- If your backup is located on a network share and Windows PE does not recognize the network adapter, you can add additional network drivers using **Load Drivers**.
- For **BitLocker-protected drives**, have the recovery key ready. In the boot environment, encrypted volumes can only be used after they have been unlocked.

Booting from CD/DVD

1. Make sure your system is configured to boot from the CD. You can set this in the BIOS/UEFI. For details, refer to your motherboard manufacturer's documentation.
2. Insert the O&O DiskImage boot CD into your computer's CD/DVD drive.
3. Restart the computer and follow the prompt to boot from CD.
4. A window with system settings will appear. Select language and region.
5. In the next step, you can load additional drivers for devices for which Windows PE has not yet found a driver (see chapter *Load Drivers*).
6. After accepting the license terms, O&O DiskImage is started.

Booting from USB Stick

To boot from a USB stick, you generally need to change the boot order in your computer's boot menu. Alternatively, you can adjust the settings directly in the BIOS/UEFI. For more details, consult your motherboard manufacturer's documentation.

1. Open the boot menu while the computer is starting.
2. Change the order in the menu so that the USB entry (Removable Devices) is listed first.
3. The computer will then recognize the USB stick as a boot medium and start O&O DiskImage from it.

Notes:

- The boot order set in the boot menu is usually only valid for the current startup. You may need to repeat this step the next time you boot.
- On some systems, a stick will only boot from **USB 2.0 ports**, not from USB 3.0 ports.
- If the stick is not detected, recreate the boot medium – ideally directly using O&O DiskImage.

Tip:
If you purchased O&O DiskImage online, refer to the chapter *Create Boot Medium* for how to create your own bootable medium.

Additional Notes on Restore

- If you want to perform a restore on a device with dissimilar hardware, please refer to the chapter *Restoring on Dissimilar Hardware (M.I.R.)*.
- In the O&O DiskImage Special Edition, the boot CD for running without an installed operating system is **not included**.

Recommendation:
Recreate the boot medium after major Windows updates or O&O version upgrades to ensure that you always have up-to-date drivers and components available.

Load Drivers

If, when using the boot medium under Windows PE, a device such as a hard disk, RAID array, NVMe controller, or network adapter is not detected automatically, the necessary driver may be missing. This particularly affects:

- RAID or AHCI controllers
- NVMe SSD controllers (especially with older PE versions)
- special network adapters (Intel PRO/10G, Realtek, server adapters, etc.)

- USB controllers on modern mainboards
- storage controllers in external enclosures

Drivers can be loaded directly after launching the boot CD via the **O&O System Settings** dialog on the **Drivers** tab.

Loading Drivers – Procedure

1. Open the **Drivers** tab in the *O&O System Settings* dialog.
   All devices automatically detected by Windows PE, as well as devices without an installed driver, are displayed.
2. Select a device for which you want to load a driver.
3. Click **Load**.
4. Select the desired driver – for example, from a connected hard disk, a USB stick, or a manufacturer's driver CD*.
5. Click **Open** to install the driver.
6. A program message will then indicate the result of the installation.

Notes

- You can remove the boot CD from the drive in order to insert a manufacturer's driver CD.
- If you load an additional driver under Windows PE, Windows PE may display a restart prompt.
  This prompt is irrelevant when booting from CD – decline it and continue.
- **Encrypted drives** (BitLocker, VeraCrypt, etc.) are only supported in Windows PE after unlocking or if compatible drivers are present. BitLocker-protected volumes must be unlocked using the BitLocker recovery key before backup or restore.
- **RAID systems:**
  It is important to use the correct "F6 driver" or the appropriate Windows PE driver of the RAID controller (e.g. Intel RST, AMD RAID, LSI/Avago/Broadcom MegaRAID).
- **NVMe SSDs:**
  With older PE versions (e.g. based on Windows 7/8), NVMe drivers must be loaded manually so that the SSD appears.

Additional Helpful Information

When you almost always need extra drivers

- Whitebox or server mainboards (Supermicro, Dell, Fujitsu, HP, etc.)
- Systems with hardware RAID
- Notebooks with special I/O controllers
- Systems where Windows PE cannot establish a network connection

Recommended preparation To ensure a successful restore in an emergency, it is recommended to:

- copy all relevant drivers (storage, network, chipset)
  in advance to a USB stick
- store them in clearly labeled folders, e.g.:
  `\Storage`, `\Network`, `\NVMe`, `\RAID`, etc.
- have this stick connected when starting the boot medium

Typical source of errors If a drive is missing or a RAID array is not shown, in **over 80%** of all cases the cause is:

- missing RAID or AHCI drivers
- missing NVMe drivers
- BIOS settings changed (e.g. RAID/IDE/AHCI mode)

BitLocker

O&O DiskImage supports working with BitLocker-encrypted drives. To access encrypted volumes, the **BitLocker recovery key** is currently required. Without this key, Windows PE cannot decrypt the drive and it cannot be backed up or restored.

Restoring BitLocker-Encrypted Drives

The procedure depends crucially on **which backup method was used** and **whether you are restoring a single drive or the entire disk**.

Restoring a Fully Encrypted Disk If the entire disk was **encrypted and backed up as a whole**, the restore can be performed **without entering** the BitLocker recovery key beforehand.
O&O DiskImage restores the disk to its original state – including all BitLocker metadata.

Restoring a Single BitLocker Volume If you want to restore a **single drive** from a backup, you must first have access to the encrypted volume.
Do this via the command line:

```
manage-bde -unlock X: -RecoveryPassword YOUR-RECOVERY-KEY
```

- *X* is the drive letter.
- After *RecoveryPassword* you must enter the full recovery key.

Note:
This command only unlocks the drive – it is made accessible in decrypted form, but not restored.

Important: The Backup Method Determines Whether BitLocker Remains Active After Restore

The BitLocker status of a drive **directly depends on the backup type**:

1. Used Sectors (standard method)

- Encryption metadata is *not* backed up.
- The backup contains only the used data, not the physical BitLocker structure.
- After the restore, the drive is **no longer encrypted**.
- BitLocker would need to be enabled again if required.

This method is correct if BitLocker is **not needed** after the restore or if you intend to re-encrypt the system.

2. Direct Forensic

- All sectors – **including empty sectors** and BitLocker metadata – are backed up.
- This preserves not only the file structure but also BitLocker in full.
- After the restore, the drive remains **encrypted**, exactly as in the original state.

This is the recommended method if:

- a BitLocker-encrypted system is to be restored **1:1**
- you need an image for compliance or forensic purposes
- encryption should remain active without reinitialization

Warning:
Forensic backups are significantly larger because unused areas are also included.

Additional Useful Notes

- **BitLocker in Windows PE:**
  Windows PE can only open BitLocker volumes using the recovery key, not with normal user passwords.
- **TPM-bound drives:**
  Since Windows PE does not use your computer's TPM, the recovery key is *always* required.
- **Automatic restore in M.I.R. mode:**
  If a BitLocker system is restored from a forensic backup, BitLocker remains active even after a hardware change.
- **BitLocker and moving a disk:**
  If a backed-up encrypted disk is installed in another system, the recovery key is also required there.

Using the Express View

The Express View provides a particularly simple and intuitive user interface for the most important functions of O&O DiskImage. It allows you to create backups, load existing backups, or perform restores with just a few clicks. You can switch to the full user interface at any time if required.

Tip:
If you want to hide certain functions from users, you can disable them via the registry entry **ExpressFlags**. For more information, see the chapter *Explanation of Registry Entries*.

Note:
The system partition cannot be restored while Windows is running. For this, use the O&O DiskImage boot medium and run the program directly from there.

Express View – Functions

1. **Create Backup**
   Starts a backup of one or more drives.
2. **Restore Backup**
   Starts the restore process for a previously created backup.
3. **Read Backup Information**
   Displays detailed information about a backup file.
   Via the drop-down menu (small arrow on the right), you can also mount a drive from a backup as a virtual drive or unmount it again.
4. **Show Full View**
   Switches from Express View back to the full O&O DiskImage user interface.
5. **Open Help**
   Opens the integrated help for O&O DiskImage.