

O&O software

O&O DiskImage 22

Premium Edition

Table of Contents

1 Introduction 4

2 Editions 6

3 Get started 8

3.1 System requirements 8

3.2 Install and activate 10

3.3 Quick start 12

3.4 Interface 14

4 Concepts 16

4.1 Backup types 16

4.2 Disks and file systems 18

5 Back up 20

5.1 Drive backup 20

5.2 Backup of changes 22

5.3 File backup 24

6 Restore 26

6.1 Restore drives 26

6.2 Restore the entire system 28

6.3 Restore files 30

6.4 Dissimilar hardware (M.I.R.) 31

6.5 BitLocker 34

7 Clone and recovery 36

7.1 Clone drives 36

7.2 Boot medium and O&O DiskImage ToGo 39

7.3 Load drivers 42

7.4 RecoveryPartition 44

8 Tasks and reports 46

8.1 Tasks 46

8.2 Manage tasks 49

8.3 Reports 51

9 Tools 53
9.1 Convert and merge backups 53
9.2 Virtual drives 55
9.3 Network drives and FTP 57
9.4 Backup information and validation 59
9.5 System tools 60
10 Reference 62
10.1 Program settings 62
10.2 Command line 65
10.3 Glossary 71
11 Troubleshooting 73
12 FAQ 76
13 Support and more from O&O 79

Introduction

This guide describes O&O DiskImage 22 in the Professional, Server and Enterprise Editions. They share the full interface with a start page, the **Drive backup**, **File backup** and **Tasks & Reports** areas and the **Tools** menu; the **Express View** reduces it to the most important functions.

If your window shows six tiles – **Back up your PC**, **Back up drives**, **Back up files**, **Restore backups**, **Duplicate drives** and **Tools** – you have the Premium Edition: use the manual of the Premium Edition. Editions compares the editions.

What you can do

- **Back up drives** as an image – individual drives, several partitions or the entire computer with the 1-Click backup – and **back up files** into file backups.
- **Back up changes** incrementally or differentially on the basis of an existing backup, and merge chains of change backups into a new full backup.
- **Automate** backups, duplications and other actions as **tasks** with schedules, user accounts, e-mail notifications and pre- and post-task commands.
- **Restore** drives, the entire system from the boot medium or the RecoveryPartition, individual files, and systems on dissimilar hardware with **M.I.R.**
- **Clone** disks and drives file-based or forensically.
- **Prepare recovery** with the boot medium, O&O DiskImage ToGo and the RecoveryPartition.
- **Use the tools** to convert, merge, validate and mount backups, connect network drives and FTP servers, change computer properties and check drives.
- **Script** backups and restores with the command line `oodicmdc.exe`.

Find a task

Goal	Page
Install, activate, update	Install and activate
First backup and restore	Quick start
Know the window, the Express View and the tray icon	Interface
Back up drives or the entire computer	Drive backup
Back up only changes	Backup of changes
Back up files and folders	File backup
Run backups automatically	Tasks
Restore a drive, the system or files	Restore drives, Restore the entire system, Restore files
Restore to another computer	Dissimilar hardware (M.I.R.)
Replace a disk	Clone drives
Prepare for a system that no longer starts	Boot medium and O&O DiskImage ToGo, RecoveryPartition
Look up a setting or a command	Program settings, Command line

License

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

Editions

O&O DiskImage 22 is available in several editions for desktop PCs and server environments. They share the backup engine and the backup formats, but differ in the supported systems, the functions and the interface.

Edition	For	Interface	Guide
Premium Edition	Home users with individual PCs: system backup, cloning and hardware-independent restore.	Tile interface	Manual of the Premium Edition
Professional Edition	Business customers with several desktops or workstations. All Premium functions plus management options, higher performance and optimized workstation compatibility. Not for server operating systems.	Full interface	This manual
Server Edition	Server systems. All Professional functions plus support for the common server operating systems, performance for large data volumes and extended network backup options.	Full interface	This manual
Enterprise Edition	Larger companies with extensive IT infrastructures: deployment on many systems with central management, flexible distribution and provisioning.	Full interface	This manual

Volume licenses deploy O&O DiskImage on several devices with central management, simplified deployment and a lower price per device. Contact the O&O sales team or an authorized O&O partner for advice.

Which edition do I have?

- The title bar of the application names the edition, for example **O&O DiskImage 22 Premium Edition**.
- The Premium Edition opens with six tiles – **Back up your PC**, **Back up drives**, **Back up files**, **Restore backups**, **Duplicate drives** and **Tools**.
- The Professional, Server and Enterprise Editions open the full interface with a start page, **Drive backup**, **File backup**, **Tasks & Reports** and the **Tools** menu, optionally reduced to the **Express View**.

What the editions have in common

- Backups in the O&O DiskImage format (`.omg` for drives, `.obk` for file backups in the full interface), optionally as VHD/VHDX.
- Full backups and backups of changes (incremental and differential), the backup technologies used sectors, forensic and direct forensic, compression, encryption and validation.

- Mounting backups as virtual drives, converting backups to VHDX, checking and repairing Windows.
- A recovery environment outside the running Windows: Fortress Mode and the startup medium in the Premium Edition, the boot medium, the RecoveryPartition and O&O DiskImage ToGo in the Professional / Server Edition.

Only in the Professional / Server Edition

- Scheduled **tasks** with notifications by e-mail, user accounts and pre- and post-task commands.
- The **command line** `oodicmdc.exe` for scripted backups, restores, conversions and duplications.
- **M.I.R.** (Machine Independent Restoration) for restoring a system to dissimilar hardware, and the **Change Computer Properties** tool.
- **Backups on FTP servers** and a password manager for network authentication.
- **Profiles** for backup, restore and copy options, **merging** backups and **splitting** backup files.
- The **Express View** as a reduced interface.

System requirements

The Professional, Server and Enterprise Editions run on 64-bit Windows systems. For current product information, see the O&O DiskImage product page.

Operating systems

Operating system	Professional Edition	Server Edition
Windows 11 (all editions)	Yes	Yes
Windows 10 (all editions)	Yes	Yes
Windows Server 2016	No	Yes
Windows Server 2019	No	Yes
Windows Server 2022	No	Yes
Windows Server 2025	No	Yes

The minimum requirements of the respective operating system apply; 64-bit support is required. The Enterprise Edition deploys the Professional and Server Editions on many systems.

Further requirements

Requirement	Details
Memory	Starting the PC from the boot medium requires at least 4 GB RAM.
Drivers	Keep the storage controller drivers of the operating system up to date; update them if in doubt.
Permissions	Local administrator rights, or equivalent permissions, for installation, configuration and activation. Domain administrators usually have sufficient rights.
Other backup software	No other backup or imaging software should run during the installation and use of O&O DiskImage, to avoid conflicts caused by parallel access to the drives.
RecoveryPartition	At least 3 GB of free space; as the default backup path at least 10 % of the disk, but no less than 25 GB. At most three primary partitions on MBR disks; no dynamic disks. See RecoveryPartition.

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

Supported file systems

File system	Use
FAT	One of the oldest file systems; still common on removable media because of its simplicity and compatibility.
FAT32	The extended FAT with larger files and volumes; older Windows systems and external drives.
NTFS	The preferred file system of modern Windows systems: large volumes, permissions, logging and recovery functions.
exFAT	Flash storage such as USB sticks and SD cards; large files and volumes, common in cameras and modern removable devices.

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

Next steps

- Install and activate
- Quick start

Install and activate

Check the system requirements before installing O&O DiskImage.

Install

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

No other backup or imaging software should run during the installation and use of O&O DiskImage; parallel access to the drives causes conflicts.

Enter the license

A valid license key activates the product. The registration wizard starts automatically on the first start of the program and whenever a license error is detected. The license key may also be called registration code, serial number or product ID.

1. Enter the license information you received with the purchase (download or boxed version).
2. Do not confuse letters and digits, and do not enter spaces.
3. Select **Next** to complete the registration, or **Cancel** to abort.

If the registration fails, contact O&O Software support. The license can also be entered from the command line with `/add license`; see Command line.

Trial period

O&O DiskImage can be tested free of charge for 30 days. The remaining trial period is shown each time the program starts. After the trial period, continued use requires a valid license.

Online registration

Registration gives you improved customer service, the recovery of lost license keys, information about products and updates, and discounted upgrades to new versions. A purchase in the O&O online shop registers the product automatically; with other purchase channels, the program asks after the license entry whether you want to register. The registration data can be entered or updated with the registration form on the O&O Software website.

Updates

O&O DiskImage checks automatically for available updates. To check manually, open **Tools > About O&O DiskImage**.

In a network environment, back up the authentication data of the password manager before a major update, so it can be restored afterwards.

Uninstall

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

Backup files are not deleted when the program is uninstalled.

Next steps

- Quick start
- Interface

Quick start

Create a backup first, then prepare a way to restore the system if Windows no longer starts.

Start O&O DiskImage

- Start O&O DiskImage from the desktop shortcut or from the Windows Start menu.
- The **Express View** offers the most important functions in a reduced interface; the **tray icon** in the notification area shows the status and gives quick access to common functions. See Interface.
- The integrated help opens with **F1** or from the **Help** menu.

Back up the entire computer

The **1-Click backup** backs up the entire computer – system partition, data and settings – with preset options: compression with **LZNT1** and the backup method **Backup of used sectors**. Store it on an external storage medium, for example a USB hard disk or a network share.

1. Start O&O DiskImage and select **Drive backup** on the start page.
2. In the Actions pane, select **Backup entire computer** (1-Click backup).
3. Check the suggested target path. The **[...]** button opens a folder dialog for another storage location.
4. Keep the backup name derived from the creation date, or enter your own.
5. Select **Start**.

The duration depends on the size of the disks and the speed of the target medium. If the target medium runs out of space, O&O DiskImage asks for an additional target path during the backup.

Back up individual drives

1. Select **Drive backup** on the start page.
2. In the drive list, enable the checkbox of each drive to back up.
3. Optionally open **Backup options**, or add the backup as a scheduled task.
4. Select **Start drive backup**.
5. Specify the target path – the suggested default path or a location of your own – and optionally a name for the backup.
6. Select **Start**.

See Drive backup for the options.

Restore a backup

1. Select **Drive restoration** on the start page.
2. Choose the backup under **Select image**, or browse to the backup file.
3. Enable the checkbox of each drive to restore and select the target drive.
4. Select **Start drive restoration** and follow the instructions.

The target drive is overwritten completely. To restore the system partition or the entire system, start the computer from the boot medium. See Restore drives and Restore the entire system.

Prepare for recovery

Create a boot medium with **Tools > Create Boot Medium**, or set up the RecoveryPartition, while the system still works, and test that the computer starts from it. See Boot medium and O&O DiskImage ToGo and RecoveryPartition.

Check regularly that the backup destinations have enough space and that the backups are intact; see Backup information and validation.

Interface

The full interface opens on the start page, from which the backup, restore, duplication and task areas are reached. The Express View reduces it to the most important functions, and the tray icon keeps the status visible in the Windows notification area.

Start page and areas

Area	Purpose
Drive backup	Back up individual drives, the entire computer (1-Click backup) and changes, add backups as tasks. See Drive backup.
File backup	Back up selected files and folders into file backups (`.obk`). See File backup.
Drive restoration and **File recovery**	Restore drives from an image or files from a file backup. See Restore drives and Restore files.
Drive duplication	Clone disks and drives. See Clone drives.
Tasks & Reports	Create, edit and run tasks, read reports. See Tasks.
Tools menu	Convert, merge, validate and mount backups, boot media, network drives, computer properties, drive check, command prompt. See Tools.
Program settings	Defaults for backups, restores, duplications, tasks, notifications and security. See Program settings.

The program settings determine which page opens at the program start; see General.

Drive list

The drive list shows the disks with their drives (partitions and volumes). Enable the checkbox of a drive to select it for a backup, restore or duplication. The **DiskView** shows the disks graphically with their partition layout and the free and used space; a click on a drive selects it.

The drive list of the Professional Edition and the view of the Server Edition differ slightly in their layout; the functions are identical. The program settings decide whether removable media, CD/DVD drives and drives that cannot be backed up are shown.

Express View

The **Express View** is a reduced interface for the most important functions. It creates backups, loads existing backups and performs restores with a few clicks; the full interface is available at any time.

Function	Purpose
Create Backup	Starts a backup of one or more drives.
Restore Backup	Starts the restore of an existing backup.
Read Backup Information	Shows the details of a backup file. The drop-down menu next to it mounts a drive of the backup as a virtual drive or unmounts it again.
Show Full View	Switches back to the full interface.
Open Help	Opens the integrated help.

The system partition cannot be restored while Windows is running; use the boot medium for that. See Restore the entire system.

Tray icon

After the installation, O&O DiskImage shows a tray icon in the notification area of the Windows taskbar. During an operation the icon is animated; when the program is idle, it is static.

The context menu of the icon opens the main application, cancels a running operation, hides the icon and disables the animation. Without administrator rights, the entry for starting the main application is unavailable. The menu also sets whether notifications about the progress of tasks and about changes of the O&O DiskImage service are shown.

- A right-click on the icon opens the **status window**, which shows whether an operation is running or the program is idle.
- If the tray icon was disabled permanently, it can be started again from the Windows Start menu: **O&O Software > O&O DiskImage > O&O DiskImage Tray**.

Backup types

A backup creates an image of drives or a container of files. This page explains the terms the guide uses for them.

Drives

A drive is a specifically assigned area on a disk; one physical disk can contain several drives. The term covers partitions, logical drives within extended partitions and volumes. A typical structure keeps the operating system and the applications on drive C: and the data – photos, documents, music – on drive D:, so system and data can be backed up separately.

Drive backup and file backup

Type	What it saves	Format
Drive backup	The used sectors or all sectors of a drive, including the file system, files and folders.	OMG (`.omg`)
File backup	Only the selected files and folders, as data sets.	OBK (`.obk`)

A drive backup is the basis for restoring a system; a file backup is the quick way to protect selected documents or projects. See Drive backup and File backup.

Backup files and formats

A backup consists of one or more files. If one medium is too small, the backup can be split across several media; number them, so they can be restored in the right order or serve as the base for incremental backups.

Format	Use
OMG	Backups of entire systems or individual drives. The native format with the full range of functions: backups of changes, encryption, recovery options and forensic methods.
OBK	File backups.
VHD	Virtual hard disk up to 2 TB; backed-up drives can be mounted.
VHDX	Virtual hard disk up to 64 TB, more robust against file corruption.

Create backups in the OMG format and convert them to VHD/VHDX when a virtual machine needs them. See Convert and merge backups.

Full backup and backup of changes

A **full backup** writes all selected data completely to the target medium. It is thorough and is the base for the subsequent backups.

A **backup of changes** saves only what changed since an earlier backup:

- A **differential backup** saves all differences since the last full backup.
- An **incremental backup** saves only the changes since the last backup – whether that was full, differential or incremental.

Both save storage space and time. The **base backup** is the starting point of a backup of changes: differential backups require a previous full backup, incremental backups use the last backup of any type as their reference. See Backup of changes.

Backup methods

Method	What is saved
Used sectors	Only the sectors that contain data. The standard method for intact file systems; the size of the backup roughly equals the used space plus metadata.
Forensic	Every sector of the drive, including unused and damaged areas; the backup is as large as the physical disk. For damaged file systems, data recovery and forensic analysis.
Direct forensic	Direct access to the physical disk, bypassing the file system driver.

A forensic backup is best created from the boot medium, so that Windows does not overwrite deleted data in the meantime. A drive with an unknown or unsupported file system is always backed up forensically. See Disks and file systems.

Disks and file systems

O&O DiskImage backs up the used sectors of the supported file systems and falls back to a forensic backup where it cannot read the file system.

Supported file systems

File system	Notes
FAT	Old and simple; still used on removable media.
FAT32	Larger files and volumes than FAT; older Windows systems and external drives.
NTFS	The preferred file system of modern Windows: large volumes, permissions, logging and recovery functions.
exFAT	Flash storage such as USB sticks and SD cards; large files and volumes.

If a volume uses an unknown or unsupported file system, O&O DiskImage backs up all of its sectors automatically – a forensic backup. To back up a supported drive forensically, choose the forensic method in the backup options instead of the backup of used sectors. See Backup types.

Dynamic disks and RAID

O&O DiskImage backs up dynamic disks and RAID systems within the capabilities that Windows provides. Because Windows does not guarantee that dynamic disks can be booted in every configuration, the duplication or restore of a system to or from dynamic disks cannot be guaranteed either.

Some functions exclude dynamic disks: a VHD/VHDX file can contain only one disk, so dynamic disks with spanned or mirrored partitions cannot be converted, and the RecoveryPartition cannot be created on a dynamic disk. When mounting a complete disk, spanned, striped, mirrored or RAID-5 volumes need all participating disks in the backup.

Disk signatures

When a second disk is the target of a duplication, O&O DiskImage changes the disk signature of the target. Two disks with the same signature connected at the same time cause system errors, conflicts in the disk management and boot problems. On basic disks, partitions are identified by the disk signature and the partition offset, so O&O DiskImage adjusts the registry entries for the drive letters accordingly.

Drive letters in the recovery environment

Under Windows PE – on the boot medium and in the RecoveryPartition – drive letters can differ from those in Windows: the usual drive C: may appear as drive D:. Identify drives by their name, size and content before restoring or duplicating. The RecoveryPartition is typically shown with the last available drive letter, often Z:.

BitLocker

BitLocker-encrypted drives can be backed up and restored; in the recovery environment they must be unlocked with the recovery key first, and the backup method decides whether the encryption survives a restore. See BitLocker.

Drive backup

Drive backup creates an image of one or more drives, or of the entire computer. Use it for the system backup and for the regular protection of data drives.

Back up individual drives

1. Select **Drive backup** on the start page.
2. In the drive list, enable the checkbox of each drive to back up. The **DiskView** shows the disks graphically with their partition layout and their free and used space; a click on a drive selects it.
3. Optionally open **Backup options** to adjust the settings, or add the backup as a recurring task with **Add as task**.
4. Select **Start drive backup**.
5. Specify the target path: the suggested default path, or a storage location of your own. The default path is set in the program settings.
6. Keep the backup name derived from the creation date, or enter your own. All information about the backup is stored with it and can be read later.
7. Select **Start**.

If the target medium runs out of space, O&O DiskImage asks for an additional target path during the backup.

Backing up the system drive and the data drives separately keeps the backups small and lets you restore a data drive without resetting the whole system.

Back up the entire computer (1-Click backup)

The **1-Click backup** creates a complete image of the computer: operating system, installed programs, settings and user data. Compression with **LZNT1** and the method **Backup of used sectors** are preset, so no configuration is needed. Store it on an external drive or a network share.

1. Select **Drive backup** on the start page.
2. Select **Backup entire computer** (in some views: **Back up everything**).
3. Check the suggested target path; the **[...]** button opens a folder dialog.
4. Keep the backup name derived from the creation date, or enter your own.
5. Select **Start**.

A full system backup takes some time, depending on the size of the disks and the speed of the target medium.

Backup options

Backup options holds the settings of the backup you are creating:

Option	Meaning
Backup method	Used sectors (standard), forensic or direct forensic. See Backup types.
Backup of changes	Creates an incremental or differential backup on the basis of an existing backup. See Backup of changes.
Compression	Reduces the size of the backup file.
Encryption	Protects the backup with a password.
Lock drive	Locks the source drive during the backup, so no changes are made to it. Without the lock, a snapshot keeps the backup consistent. See Clone drives for the details of locking.
Verify backup file for errors after creation	Validates the finished backup immediately. See Backup information and validation.

The defaults for new drive backups – preferred USB targets, automatic validation, overwriting without prompt – are set under **Program settings > Drive Backup**. See Program settings.

Profiles

Backup options can be saved as a profile and reused. Under the options, choose the **Current profile** – **Standard** or **User-defined** – save the current settings with **Save as...** under a name of your own, and edit or delete profiles with **Manage profiles**. The same applies to restore and copy options.

Recurring backups

To run a backup regularly, add it as a task: select the drives, adjust the options and select **Add as task**. The task assistant sets the schedule, the user account, the notification and the storage location. See Tasks.

Next steps

- Backup of changes – back up only what changed.
- Restore drives – restore the image.

Backup of changes

A **backup of changes** saves only the data that changed since an earlier backup. It needs less space and usually less time than a full backup, and it requires at least one existing full backup of the drives or folders.

How it works

The backup of changes is based on an existing backup, the **base backup** – a full backup, an incremental backup or a differential backup. O&O DiskImage compares every sector of the base backup with the corresponding sector of the current drive and stores only the sectors that changed. The comparison is thorough; it can take a little longer than a plain full backup, but reduces the storage requirement considerably.

- For an **incremental** backup, the last backup of any type is sufficient as the reference.
- For a **differential** backup, the last full backup is always required.

The option **Data comparison with checksums** is enabled by default. After each full backup, create no more than five to ten backups of changes before the next full backup; this keeps the chain reliable and the restore fast.

Back up drive changes

1. Make sure the computer can access the drive on which the base backup is stored.
2. Select **Backup of changes** on the start page.
3. In the file dialog, choose the base backup and select **Open**.
4. Keep the suggested target directory – ideally the folder of the base backup – or enter your own. The backup is named after the creation date; enter your own name if you prefer.
5. Optionally open **More options** for compression, encryption or the backup method.
6. Select **Start**.

Recurring backups of changes

A task creates differential or incremental backups automatically on the basis of an existing full backup:

1. Open **Drive backup** on the start page.
2. Select **Backup options**, enable **Backup of changes**, select the base backup and close the options.
3. Select **Add as task**.
4. Enter the task name and set the **schedule**.
5. Select the storage location of the backups.

The option **Use created backup as base backup for the next run** is enabled by default and creates **incremental** backups that build on the previous backup of changes. They are the most space-efficient, and the restore needs all backups since the last full backup. If you disable the option, every run creates a **differential** backup based on the last full backup: the backups are larger, but the restore needs only the full backup and the last differential backup.

If the full backup and the backups of changes are not stored in the same directory, clear **Suppress user prompts during execution** in the task, otherwise the task aborts when it cannot find the preceding backups. See Tasks.

Restore from a backup of changes

A restore needs the whole chain: the full backup, all preceding backups of changes and the backup with the desired state. Keep them together and available. Chains of backups of changes can be merged into a new full backup with **Tools > Merge Backup**; see Convert and merge backups.

Next steps

- File backup – backups of changes for files and folders.
- Restore drives

File backup

A file backup saves selected files and folders into a compressed file backup (`.obk`). Backing up entire drives remains the recommendation, so nothing important is left out; the file backup is the right choice for project folders, quick interim backups and the transfer of selected data. All file backup functions are under **File backup**.

Create a file backup

1. Select **File backup** on the start page. The file view takes a moment to load; the progress bar shows the status.
2. Navigate to the folder and enable the checkboxes of the files and folders to back up. Several items, and even an entire drive, can be selected.
3. Optionally select **Criteria** to include or exclude files by criteria, for example temporary files, certain file types or large files.
4. Select **Start File Backup**.
5. Check the suggested target directory and adjust it if necessary.
6. Optionally enter a name for the backup.
7. Select **Start**.

File Backup Options holds the advanced settings and adds the backup as a recurring task with **Add as task**. See Tasks.

File backup of changes

Like a drive backup, a file backup is either a full backup with all selected files, or a backup of changes with the files that were changed, deleted or added since the base backup – a previous full file backup or a previous file backup of changes.

1. Make sure the computer can access the base backup.
2. Select **File backup > File Backup of Changes** on the start page.
3. Select the base backup and select **Open**.
4. Choose the target directory – preferably the one of the base backup – and optionally a name.
5. Optionally open **Additional Options**.
6. Start the backup.

The comparison with the base backup takes more time than a full backup, but the backup needs considerably less space.

File backup options

File Operations > File Backup Options sets the defaults for every new file backup:

Setting	Meaning
Security	AES encryption with key lengths up to 256 bits. With encryption enabled, the backup asks for a password when it starts. An existing backup can be encrypted later with **Convert Backup File**.
Backup File > Backup Method	**Full Backup** (the recommended default) or **Backup of Changes** for repeated backups of the same folder structure.
Lock the source drive during backup	Locks the source drive, so no changes are made while it is backed up: the drive disappears from the File Explorer, programs accessing it are closed and nothing can be written to it. Off by default; without the lock, the snapshot cache or VSS captures changes.
Checksums	Stores checksums for incremental file backups, so unchanged files are identified reliably and follow-up backups are evaluated faster. Keep the option enabled when backups are stored in different directories.
File Size > Split backup into smaller backup files	Splits the backup automatically into files of the given maximum size, for example for CD/DVD storage. A backup can also be split afterwards with **Convert Backup File**.

Profiles

Save frequently used file backup options as a profile: open **File Backup Options**, select **Save As...**, enter a name and confirm. **Manage Profiles** edits or deletes profiles, and **Current Profile** switches between **Standard** and **Custom**.

Next steps

- Restore files – restore files from a file backup.
- Program settings – defaults for preferred USB targets, validation and overwriting.

Restore drives

A drive restore writes the drives of an image back to a disk. O&O DiskImage detects the type of the backup and the required parameters itself; in most cases no setting has to be changed.

Restore a drive

1. Select **Drive restoration** on the start page.
2. Under **Select image**, choose the backup. If the suggested entries are not the right ones, browse to the backup file (`.omg` , `.vhd` or `.vhdx`) and select **Open**.
3. All drives contained in the image are listed. Enable the checkbox of each drive to restore.
4. Select the **target drive** with its checkbox: an existing drive that is replaced, or a new target in unallocated space.
5. Optionally open **Restore options**.
6. Select **Start drive restoration**.

> **The target drive is overwritten**
>
> The selected target drive is overwritten completely. All data on it is lost and replaced by the data of the backup.

What a restore needs

- A backup that is spanned across several media needs all of these media.
- A backup of changes needs the whole chain: the full backup, all preceding backups of changes and the backup with the desired state. See Backup of changes.
- When an entire disk is restored to another disk sector by sector, the target must be at least as large as the original. A smaller target needs a file-based restore, see below.
- The system partition and the entire system can only be restored from the boot medium or the RecoveryPartition. See Restore the entire system.
- For a restore to another computer, see Dissimilar hardware (M.I.R.); for encrypted drives, see BitLocker.

Restore to a smaller disk

A drive can be restored or duplicated to a smaller target disk file by file:

1. Select the source, for example the system partition C:, and the smaller target disk.
2. Confirm with **Yes** when O&O DiskImage asks whether the boot partitions should be transferred as well.

3. O&O DiskImage recognizes that a sector-based 1:1 copy is not possible and offers **Sector-based** and **File-based**. Select **File-based**.
4. Define the size of the target partition and start the restore. The boot partitions are transferred completely.

If the source disk has several partitions, repeat the steps for each one and select the remaining free space of the target disk as its destination. The file-based restore uses the Volume Shadow Copy Service of Windows; if it causes problems, run the restore from the boot medium.

Restore options

Drive restoration > Restore options adapts the restore to your environment:

Option	Meaning
Security and data integrity	Checks of the data, for example the validation of the backup before the restore.
Behavior on unreadable sectors	What happens when a sector cannot be read.
Actions after the restore	Automatic actions once the restore is complete.
Advanced > Force write method	**Write to drive** writes through the file system driver and is the default for used sectors and forensic backups; **Write directly to disk** bypasses the driver and is the default for direct forensic backups. Forcing the direct method is required for encrypted disks, for drives that were backed up forensically and whenever the file system driver has to be bypassed.
Advanced > Explicitly overwrite unused sectors with 0	Overwrites the unused sectors of the target partition with zeros, so data remnants from before the restore cannot be recovered. Recommended for confidential data.

Like backup options, restore options can be saved as **profiles**: set the options, select **Save as**, enter a name and confirm; **Manage profiles** edits or deletes them, **Current profile** switches between **Standard** and **Custom**.

The defaults for new restores – validation before the restore and the double-click behavior in the drive list – are set under **Program settings > Drive Restore**. See Program settings.

Next steps

- Restore the entire system
- Restore files – when only files are needed.

Restore the entire system

The system partition cannot be overwritten while Windows is running. To restore it, or the entire computer, start O&O DiskImage from the boot medium or from the RecoveryPartition.

Before you start

- Create the boot medium while the system still works, or set up the RecoveryPartition. See Boot medium and O&O DiskImage ToGo and RecoveryPartition.
- Keep the backup with the system partition and all related drives available – on an external medium, a network share or the RecoveryPartition – together with the whole chain of a backup of changes.
- For a restore to a computer with different hardware, enable M.I.R. during the restore. See Dissimilar hardware (M.I.R.).
- For BitLocker-encrypted drives, have the recovery key ready. See BitLocker.

Restore the system from the boot medium

1. Start the computer from the boot medium, or from the RecoveryPartition. See Start from the medium.
2. Select **Restore** on the start page.
3. Select **Restore**, or use the browse button to navigate to the backup.
4. Select the backup file that contains the system partition and the related drives, and select **Open**.
5. All drives in the backup are listed. Enable the checkbox of each drive to restore – for a full system restore, all drives.
6. Select the **target drive** to which the backup is written.
7. Select **Start drive restoration**.
8. When the restore is complete, restart the computer as usual.

> **The target is overwritten**
>
> Restoring the system partition or the entire system overwrites all data on the target. Check the target carefully: under Windows PE, drive letters can differ from those in Windows – the usual drive C: may appear as drive D:.

After the restore

- Restart the computer and check that Windows starts. If a restored or duplicated system does not start, see the causes under Limitations of M.I.R..

- If the system was restored to another computer or deployed to several computers, change the computer name and the computer SID. See System tools.
- Recreate the boot medium after major Windows updates or an upgrade of O&O DiskImage, so it contains current drivers and components.

Next steps

- Restore drives – individual drives in the running Windows.
- Load drivers – if a disk or the network is missing in the recovery environment.

Restore files

File recovery restores individual files or complete directories from a file backup (`.obk`). Use it when only a few files are needed, when documents were deleted, when a project folder has to come back, or when restoring a whole drive would be too much.

Restore files from a file backup

Make sure the backup file is accessible – on an external drive, a network share or an internal disk.

1. Select **Start** and then **File Recovery**.
2. In the **Choose Backup** list, select the file backup. If it is not listed, browse the drives and select the OBK file manually.
3. If only certain files are needed, select them inside the backup.
4. Select the **Choose Target Directory** icon and choose one of the two options:

- **Restore to a new directory**: the files are restored to a new location; existing files are not overwritten.
- **Replace original data**: the files are restored to their original location; existing files are overwritten with the versions from the backup.

5. Select **Start**. The progress is shown, and the files are available as soon as the restore is complete.

The default behavior of the file restore dialog is set under **Program settings > File Restore**; see Program settings.

Copy files from an image

Files that are contained in a drive backup are reached by mounting the image as a virtual drive: the drives of the backup appear in Windows Explorer, and the files are copied like from any other drive. See Virtual drives.

Next steps

- File backup
- Restore drives

Dissimilar hardware (M.I.R.)

A backup of the system partition could traditionally only be restored to a computer whose hardware matched the original. With **M.I.R.** (Machine Independent Restoration), O&O DiskImage restores a backup – including the system partition – to computers with dissimilar hardware, and transfers complete system duplicates to other hardware platforms. M.I.R. replaces or re-integrates the key drivers, especially for mass storage and controllers, so Windows starts despite the changed hardware.

When to enable M.I.R.

Enable M.I.R. whenever the target hardware does not match the original environment or key components changed:

- a restore to a computer with different or newer hardware,
- the duplication or replication of a system to other machines,
- the replacement, removal or addition of mainboard, controllers or mass storage devices,
- the migration between physical systems and virtual machines (P2V and V2P),
- the replacement of faulty or incompatible drivers from the boot medium.

M.I.R. is enabled during the restore or duplication, before the operation completes; afterwards the adaptation runs automatically.

After deploying one Windows installation to several machines, change the computer name and the computer SID to avoid conflicts in workgroups and domains. See System tools.

Restore to dissimilar hardware

M.I.R. is available when the system partition is restored from a backup and when an entire system is duplicated; it does not matter whether the system partition is selected explicitly or an entire disk including the system partition.

1. Start the computer from the boot medium. See Boot medium and O&O DiskImage ToGo.
2. Select **Drive Restore** on the start page of the boot medium. O&O DiskImage suggests the location of the most recent backup.
3. If the suggested backup is not the right one, browse to the backup file and select **Open**.
4. Enable the checkbox of each drive to restore.
5. Select the target drive with its checkbox: an existing drive, or a new one in an unallocated area.
6. Open **More options** and enable **Adjust dissimilar hardware afterwards**.
7. Select **Start drive restore** and follow the dialogs. After a successful restore, restart the computer when prompted.

The target is overwritten

The selected target drive is overwritten completely; all data on it is replaced by the contents of the backup.

Limitations of M.I.R.

A restored or duplicated system can still fail to start although M.I.R. was enabled. The cause is usually an incomplete selection:

Cause	Effect
Not the entire disk was selected as the target, but a single partition, a volume or a free area.	System and boot information that exists only on the full disk is missing.
Delete layout was not selected when the target layout was created.	Partitions can be created at different offsets, so Windows no longer finds its boot areas.
Only individual source partitions were selected instead of the entire disk.	Boot areas such as the EFI partition, recovery partitions or the Windows boot manager are missing.
The bootable drive is attached to a controller that is not initialized at boot time, for example an internal drive on a USB controller.	Windows does not detect the drive in time during the boot.

To keep a restored system or duplicate bootable, always back up and restore or duplicate the **entire system disk**, not individual partitions.

Manual adjustment

If the system does not start as expected after the restore, or devices are not detected, adjust the hardware manually: restore or duplicate as usual, then open **Tools > Change Computer Properties** and supplement the missing adjustments. The adaptation of M.I.R. consists of three actions that can be enabled or disabled during a restore to dissimilar hardware:

Action	Meaning
Replace Hardware Abstraction Layer (HAL)	The HAL encapsulates architecture-specific functions such as interrupt controllers, multiprocessor communication and I/O interfaces, and is tightly bound to the hardware. After a change of mainboard or CPU it must be adapted so that Windows runs stably.
Adopt currently loaded device-control drivers	Integrates or replaces the device drivers, so Windows can access the new hardware after the restore.
Trigger operating system setup on next restart	Instructs Windows to run an internal setup routine on the next start, which registers new hardware and completes missing system information.

Next steps

- Restore the entire system
- Clone drives – duplicating a system to other hardware.

BitLocker

O&O DiskImage works with BitLocker-encrypted drives. In the recovery environment, an encrypted volume can only be accessed with the **BitLocker recovery key**; without it, Windows PE cannot decrypt the drive, and it can be neither backed up nor restored.

Restore an encrypted drive

The procedure depends on the backup method and on whether a single drive or the entire disk is restored.

Case	Procedure
The entire disk was encrypted and backed up as a whole	Restore the disk without entering the recovery key first. O&O DiskImage restores it to its original state, including all BitLocker metadata.
A single BitLocker volume is restored from a backup	Unlock the encrypted volume first from the command line: `manage-bde -unlock X: -RecoveryPassword YOUR-RECOVERY-KEY`, where `X:` is the drive letter and the recovery key follows `-RecoveryPassword`. The command only unlocks the drive; the restore follows as usual.

The backup method decides whether BitLocker stays active

Backup method	After the restore
Used sectors (the standard method)	The backup contains only the used data, not the encryption metadata. The restored drive is **no longer encrypted**; enable BitLocker again if needed. The right choice when BitLocker is not needed after the restore or the system is to be re-encrypted.
Direct forensic	The backup contains all sectors including the empty ones and the BitLocker metadata. The restored drive **stays encrypted** exactly as before. The right choice for a 1:1 restore of an encrypted system, for compliance or forensic images, and when the encryption must stay active without reinitialization.

Forensic backups are considerably larger, because unused areas are included as well. See Backup types.

Further notes

- Windows PE opens BitLocker volumes only with the recovery key, not with the normal user password.
- Windows PE does not use the TPM of the computer, so the recovery key is always required for TPM-bound drives.

- A BitLocker system restored from a forensic backup with M.I.R. stays encrypted even after a hardware change.
- A backed-up encrypted disk that is installed in another system needs the recovery key there as well.
- In the recovery environment, encrypted volumes are only usable after they have been unlocked. See Load drivers.

Clone drives

Cloning – in the interface **Drive duplication** – copies complete disks or individual drives directly to another disk, which can then replace the original. Backup and restore happen in one step, without a backup file; the source drives remain unchanged, because O&O DiskImage reads them only.

File-based or forensic

Method	Use
File-based cloning	Transfers all recognized data from the source to the target. Fast, efficient and sufficient for most cases.
Forensic cloning	Copies every sector of the source, whether used or not. Needed when the file system of the source is not supported, for data recovery, and whenever an exact bit-by-bit copy of all sectors is required. Considerably slower.

A clone needs more space than a backup, because it is not compressed; it cannot be compressed or encrypted, and there are no incremental or differential follow-up clones.

Duplicate a drive

1. Select **Drive duplication** in the quick access bar.
2. Enable the checkbox of the drive or disk to duplicate.
3. Under **Copy options**, set error handling, read method and drive locking if needed.
4. Select the target drive with its checkbox.
5. In the following dialog, optionally define under **Additional options** what happens after the duplication, for example a verification, a rescan or the automatic shutdown.
6. Select **Start**.

The duplicated data can later be copied back to another drive in the same way.

> **The target drive is overwritten**
>
> The selected target drive is overwritten completely; all data on it is lost. Use dedicated external or new drives as targets.

Notes for system partitions: adjust the properties of the target to its intended use and pay attention to bootability and partition types. When a second disk is the target, O&O DiskImage changes the disk signature of the target,

so that two disks with the same signature never run at the same time; see Disks and file systems. For a duplication to a computer with different hardware, enable M.I.R.; see Dissimilar hardware (M.I.R.).

Copy options

Drive duplication > Copy options controls the copy process in detail; the same options are available for restores.

Option	Meaning
Advanced > Ignore faulty sectors	**Abort on errors** stops the copy at the first faulty sector. **Continue and mark sector as empty** continues and writes faulty sectors as empty sectors, so all readable data is transferred – useful for damaged disks and data recovery.
Advanced > Read process > Lock drive	Locks the source drive during the copy: it is hidden from Explorer, cannot be written to, and programs accessing it are closed. Off by default, so you can keep working.
Read method	**Used sectors only** (fast; the standard for intact file systems), **Forensic** (all sectors) or **Direct forensic** (direct access to the physical disk, bypassing the file system driver). See Backup types.
Advanced > Force write method	**Write to drive** writes through the file system driver and is the default for used sectors and forensic; **Write directly to disk** bypasses the driver and is the default for direct forensic. Mandatory when encrypted drives are restored from a forensic backup.
Advanced > Explicitly overwrite unused sectors with 0	Overwrites unused sectors of the target with zeros, so deleted data in empty areas cannot be recovered – even with professional recovery software. For copies that must meet data protection requirements.

If the source drive is not locked, O&O DiskImage buffers changes in a cache of limited size; the cache status shows how much is left. A full cache lets changes reach the target directly, and the copy can become inconsistent – stop write-intensive processes such as a defragmentation during the copy. The system partition cannot be locked.

Profiles

Copy options can be saved and reused: under **Copy options**, choose the **Current profile** (**Standard** or **User-defined**), save the current settings with **Save as...**, and edit or delete profiles with **Manage profiles**. The defaults of the duplication dialog – whether non-cloneable drives are shown and what a double-click does – are set under **Program settings > Cloning**; see Program settings.

Next steps

- Restore drives – restoring from a backup instead.

- Boot medium and O&O DiskImage ToGo – duplicating the system disk from the recovery environment.

Boot medium and O&O DiskImage ToGo

A bootable medium starts the computer when Windows no longer boots and runs O&O DiskImage from a Windows PE environment with all of its functions, so backups can be restored from external storage or from the RecoveryPartition independently of the installed system. Create it while the system still works.

Create a boot medium

1. Open **Tools > Create Boot Medium**.
2. O&O DiskImage analyzes which creation methods are available: available options carry a green check mark, unavailable ones a cross. The most suitable **Windows PE base** is selected automatically; **Change** selects another one.
3. Choose the target: a **CD/DVD burner**, a **USB stick or removable drive**, or an **ISO file** for later burning or for virtual environments.
4. Select **Create**.

> **The target medium is erased**
>
> All data on the target medium is deleted during the creation. Because of a Windows limitation, at most 2 TB of the target drive are used; the rest stays unused.

Recreate the medium after major Windows updates or an upgrade of O&O DiskImage, so it contains current drivers and components. The medium can also be created from the command line; see Command line.

Windows PE base and drivers

The medium is built on the Windows Recovery Environment or – where that is not sufficient – on the Windows Assessment and Deployment Kit (ADK) or an earlier AIK. In the creation dialog, **download** opens the Microsoft download page of the ADK/AIK, and **package** starts a local ADK/AIK installation file. Windows 11 needs the ADK for Windows 11 with the WinPE add-on, Windows 10 the ADK 10.

Custom driver integration adds the drivers of a folder of your choice to the offline operating system of the medium, so storage controllers, network adapters and graphics drivers – including devices that are not Plug and Play – are available as soon as the environment starts. Drivers can also be loaded later in the running environment; see Load drivers.

O&O DiskImage ToGo

O&O DiskImage ToGo turns an external hard disk or a sufficiently large USB stick into a rescue boot medium **and** the preferred destination for system backups. As soon as the medium is connected, O&O DiskImage can

back up the system onto it; in an emergency, the computer starts from the same medium and restores the stored backup in a few steps.

1. Connect an external hard disk or USB stick with sufficient capacity.
2. Select the function for creating a bootable medium.
3. Select the connected drive as the target.
4. O&O DiskImage sets up the medium as a boot medium and marks it as the default backup path.

If no storage medium for backups exists yet, ToGo is the recommended solution. The RecoveryPartition offers a similar rescue environment on the internal disk; see RecoveryPartition.

Start from the medium

From CD/DVD

1. Set the computer to boot from the CD/DVD drive in the BIOS/UEFI setup; the documentation of the mainboard manufacturer describes how.
2. Insert the boot CD and restart the computer. Follow the prompt to boot from the CD.
3. In the system settings window, select the language and region.
4. Load additional drivers for devices that Windows PE has not found. See Load drivers.
5. Accept the license terms. O&O DiskImage starts.

From a USB stick

1. Open the boot menu while the computer starts, or change the boot order in the BIOS/UEFI setup.
2. Move the USB entry (removable devices) to the first position.
3. The computer starts O&O DiskImage from the stick.

The order chosen in the boot menu usually applies to the current start only. Some computers start a stick only from USB 2.0 ports, not from USB 3.0 ports. If the stick is not detected, recreate the medium – ideally directly with O&O DiskImage.

Notes before booting

- **Secure Boot** may have to be disabled so that the Windows PE medium starts.
- Start the computer in the same boot mode (UEFI or Legacy/CSM) in which the medium was created.
- Windows PE often uses the English (US) keyboard layout. Switch the layout in the start dialog before entering passwords or paths.
- If the backup is on a network share and Windows PE does not recognize the network adapter, load its driver.
- For BitLocker-protected drives, have the recovery key ready; encrypted volumes can only be used after they have been unlocked. See BitLocker.
- Drive letters can differ from those in Windows. Identify drives by their name, size and content.

Next steps

- Restore the entire system
- Dissimilar hardware (M.I.R.)

Load drivers

If a device – a hard disk, a RAID array, an NVMe controller or a network adapter – is not detected in the recovery environment of the boot medium, its driver is missing. Drivers can be loaded right after the start of the medium in the **O&O System Settings** dialog on the **Drivers** tab.

Typically affected are RAID and AHCI controllers, NVMe SSD controllers, special network adapters, USB controllers of modern mainboards and storage controllers in external enclosures.

Load a driver

1. Open the **Drivers** tab of the **O&O System Settings** dialog. It lists the devices that Windows PE detected and the devices without a driver.
2. Select the device for which a driver is to be loaded.
3. Select **Load**.
4. Select the driver – from a connected hard disk, a USB stick or the driver CD of the manufacturer. The boot CD can be removed from the drive to insert a driver CD.
5. Select **Open** to install the driver. A message reports the result.

If Windows PE asks for a restart after a driver was loaded, decline it and continue – the prompt is irrelevant when booting from a medium.

Notes

- **RAID systems** need the correct "F6 driver" or the Windows PE driver of the RAID controller (for example Intel RST, AMD RAID or LSI/Avago/Broadcom MegaRAID).
- **NVMe SSDs** need their driver with older PE versions, otherwise the SSD does not appear.
- **Encrypted drives** (BitLocker, VeraCrypt and others) are only supported in Windows PE after they have been unlocked or when compatible drivers are present. BitLocker volumes must be unlocked with the recovery key before a backup or restore. See BitLocker.

Prepare drivers in advance

Extra drivers are almost always needed on whitebox and server mainboards, on systems with hardware RAID, on notebooks with special I/O controllers, and wherever Windows PE cannot establish a network connection. To be ready for an emergency:

- copy the storage, network and chipset drivers of the computer to a USB stick in advance,
- store them in clearly labeled folders such as `\Storage`, `\Network`, `\NVMe` and `\RAID`,
- keep the stick connected when the boot medium starts.

If a drive or a RAID array is missing, the cause is in most cases a missing RAID, AHCI or NVMe driver, or a changed BIOS setting such as the RAID/IDE/AHCI mode. Drivers can also be integrated into the medium when it is created; see Boot medium and O&O DiskImage ToGo.

RecoveryPartition

The **O&O DiskImage RecoveryPartition** is a recovery environment installed next to Windows on the hard disk. It starts O&O DiskImage even when Windows no longer boots – without a separate boot medium, without preparation, and with direct access to the backups stored on the computer.

What it contains and when it helps

The RecoveryPartition is a standalone startup environment based on Windows PE with all O&O DiskImage components, the tools for backup and restore, drivers for the hardware detection, and access to internal and external drives, the network and the backup files. Once activated, it adds an entry to the Windows Boot Manager: at the start, you choose between **Start Windows** and **Start O&O DiskImage RecoveryPartition**.

Use it when Windows no longer starts, system files are damaged, a faulty or incompatible driver was installed, the system partition was destroyed or overwritten, malware or an update rendered the system unusable, or a system or drive restore should run without a USB stick or DVD. In the recovery environment, almost all tools are available: restoring system images, drives, partitions, files and folders, cloning, analyzing and validating images, access to network drives and external media, deleting and adjusting partitions, removing or resetting faulty drivers, and preparing M.I.R. restores.

Backups stored locally are detected automatically, so full and incremental backups can be restored quickly without additional media.

> **Note**
>
> The RecoveryPartition does not replace external backup media. If the disk fails or the hardware is defective, backups must exist on external media. Create a boot medium in addition to the RecoveryPartition. See Boot medium and O&O DiskImage ToGo.

Requirements

- At least 3 GB of free space; as the default backup path at least 10 % of the disk size, but no less than 25 GB.
- At most three primary partitions on MBR disks.
- No dynamic disks.

Create the RecoveryPartition

1. Select **Recovery Medium** on the start page.
2. Choose **Use existing partition** or **Create new partition**.

3. Select the disk and, if applicable, the partition to use.
4. Optionally define the RecoveryPartition as the default backup path; **Maximum size** adjusts its size.
5. Confirm with **OK**. The bootable image is generated.
6. Afterwards, create a full backup or a 1-Click backup – ideally directly onto the RecoveryPartition.

Start the RecoveryPartition

- Hold the Shift key and select **Restart** in the Start menu.
- Or open **Settings > Update & Security > Recovery > Advanced startup > Restart now**.
- If Windows detects system problems itself, choose **Advanced startup**, then **Troubleshoot > Advanced options > Startup Repair**.

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

Update or remove the RecoveryPartition

Under **Recovery Medium**:

- **Update** creates a new boot image after an update of O&O DiskImage; the backups on the partition remain intact.
- **Delete** removes the RecoveryPartition together with the backups stored on it and reactivates the Windows Recovery Environment.

> **Warning**
>
> Delete the RecoveryPartition only through O&O DiskImage. Deleting it manually, for example in the Disk Management, can cause system problems.

Tasks

The task assistant runs recurring backups and other actions according to a schedule, so the backup strategy works without manual intervention. **Start > Tasks & Reports** opens the overview of all configured tasks and all generated reports; a double-click edits a task or opens a report.

A task runs reliably only while its initial conditions remain stable: the paths and storage locations of the backups, the source and target drives, the drive names and the network access rights. If they change, the task can fail.

Add an action as a task

A task is created from an action in the main window – **Drive backup**, **File backup**, **Backup of changes** or **Duplicate**:

1. Select the drives or folders.
2. Adjust the backup options if needed – compression, encryption, method and so on.
3. Select **Add as task**.
4. In the task assistant, enter a name for the task. The name is only a label; several tasks may share it.
5. Configure the schedule, the notification and the backup options on the tabs of the assistant.

Run in **Tasks & Reports** starts a task immediately, after a safety prompt. A task can be **disabled** without deleting it; it stays stored and runs again once it is enabled.

Run task as user

Each task can run under a user account of your choice. The account determines the access to network drives, the e-mail notifications, the pre- and post-task commands and the required authentications. Without a user, the task runs under the **SYSTEM** account.

> **Warning**
>
> The SYSTEM account does not have access to all resources – in particular not to all network shares. Specify a user account for tasks that use the network.

Schedule

The **Schedule** tab sets when and how often the task runs:

Execution	Settings
One-time	Start date and start time.
Recurring	The weekdays, the start time, and the start and end date of the interval – for example every Tuesday at 21:00 for five weeks.

Notification by e-mail

The **Notification** tab sends an e-mail on successful execution, on errors or on warnings, to the recipient address you specify, optionally with a custom message text. The SMTP settings of the mail server must be configured first under **Program settings > Notification**; see Program settings.

Backup options of a task

The **Backup** tab sets the storage location and the file name of the backup, the backup type (full, changes, sector-based and so on), and compression and encryption.

The file name can be generated dynamically, by default for example `Backup_%Year%-%Month%-%Day%`. Variables such as `%Time%` or `%ComputerName%` avoid name collisions, especially with several backups per day.

The target path is taken from the program settings by default and can be set per task. If the base backup of an incremental task is moved, update its storage location in the task, otherwise the task cannot find it and fails.

Prompts, errors and actions after completion

Option	Behavior
Suppress user prompts during execution	Prompts such as "File already exists – overwrite?" are not shown; in doubtful cases the task aborts and logs the error. Needed for tasks that run unattended. Clear it when the full backup and the backups of changes are stored in different directories, otherwise the task aborts when it cannot find the preceding backups.
Abort on errors	Enabled: the task stops at the first error and runs no further step. Disabled: further steps run whenever possible, errors are logged.
Run after completing task	**Restart**, **Shut down** or **None** (default) – for example to shut down the computer after a nightly backup.

Pre- and post-task commands

Commands that run before or after the task automate additional actions: stopping and starting services (for example SQL or Exchange), running scripts, establishing network connections, deleting temporary files or

starting programs. Example:

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

The commands must be available on the system and run with the privileges of the configured user account; with the SYSTEM account, network access is not always possible.

Task information

The **Information** tab summarizes all settings of the task. It is for reading only.

Next steps

- Manage tasks – edit, check, delete, export and import tasks.
- Reports

Manage tasks

Tasks & Reports on the start page lists all configured tasks. Enable the checkbox of a task and choose the action.

Edit a task

1. Enable the checkbox of the task in the list.
2. Select **Edit**. The task assistant opens with the current settings.
3. Change what is needed: schedule, backup options, storage location, notifications, pre- and post-task commands or the user account.
4. Select **OK** to save the changes, or **Cancel** to discard them.

After changing critical parameters – the storage location of the backups or the source drives – check that the task still runs. For incremental tasks the relationship between the full backup and the backups of changes must remain intact, and after a change of the user account or the network paths, verify the authentication and the permissions.

Check a task

Check task verifies that the selected task has valid settings – that it is syntactically and logically executable on the local system.

Delete a task

Enable the checkbox of the task and select **Delete task**. The task is removed permanently; its backups stay on the disk.

Several tasks at once

Enable the checkboxes of several tasks to apply one of these actions to all of them:

Action	Purpose
Delete	Removes all selected tasks permanently.
Export	Saves the tasks to a file for other computers or for documentation.
Import	Loads previously exported tasks into the task list.

Export and import tasks

- **Export task**: enable the checkbox of the task and select **Export task**. Save the task file (`.xml`), for example to an external storage device, to reuse it on another computer.
- **Import task**: select **Import tasks**, choose the task file, and the task is added to the list.

Imported tasks are not enabled automatically. Check them and enable them by hand – especially when drive letters, paths or network conditions differ from the source computer.

Defaults

Program settings > Tasks and Reports sets whether a double-click starts a task or opens it for editing, and the storage locations of tasks and reports. See Program settings.

Reports

O&O DiskImage creates a status report for every action it performs. The reports are viewed and exported as XML files under **Tasks & Reports** on the start page; a double-click opens a report.

What a report contains

- the date and time of the execution,
- the type of action – backup, restore, clone, validation and so on,
- the settings and parameters used,
- the source and the target of the operation,
- success and error messages and warnings,
- a summary status indicator.

Reports help to trace operations, to find the source of an error and to handle support requests efficiently.

Which actions create reports

Program settings > Tasks and Reports sets for which actions reports are created, to reduce the storage usage. A report is always created when a scheduled task runs, regardless of that setting. The same page decides whether a double-click shows a report in O&O DiskImage or opens it in an external editor, and where reports are stored. See Program settings.

Notifications

Tasks can send their result by e-mail on success, on errors or on warnings. The SMTP server and the sender are configured under **Program settings > Notification**; a test e-mail from the settings checks the configuration. See Tasks.

The tray icon shows the progress of running operations and can show notifications about tasks and changes of the O&O DiskImage service; see Interface.

Contact support

If you contact O&O Software support, include:

- the version of O&O DiskImage (**Tools > About O&O DiskImage**) and the Windows version,
- the report of the failed operation,
- the type of source and destination – for example the system drive and a network share,

- whether the operation was started manually, as a task or from the command line,
- whether the problem occurred in Windows or in the recovery environment of the boot medium or the RecoveryPartition.

Convert and merge backups

The **Tools** menu converts, merges and processes existing backup files. Create backups in the native OMG format, which offers the full range of functions, and convert them when another format or other properties are needed.

Convert a backup

Convert Backup File changes the properties and the content of an existing OMG backup. A copy is always created; the original remains unchanged. You can:

- change the compression level,
- add or remove encryption,
- split the backup into several files of a fixed size,
- convert the backup into a VHD/VHDX file,
- remove drives from a backup or merge drives from several backups.

Create VHD/VHDX files

A backup converted to VHD or VHDX can be mounted as a virtual drive in Windows, booted as a virtual machine, tested without a restore, and analyzed after a failure or a malware attack.

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

Restrictions:

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

A converted virtual hard disk can be mounted as an additional drive in Windows, used as a virtual disk in Hyper-V or Virtual PC, used to verify that a backup can be restored, and booted to test a completed system state. Only backups of the same system boot successfully as VHD/VHDX, Windows 8.1 or newer is required, and changes made while running from the virtual disk affect the virtual disk – and the host system, if shared storage is used.

Merge backups

Tools > Convert Backup Files > Add merges individual backup files into a new backup: the drives are selected from several backup files and transferred into one backup. Only backup files of the same type can be merged – used sectors, forensic or direct forensic. Use it to consolidate backup sets or to reduce the number of archive files.

Merge backups of changes

A chain of backups of changes can be merged into a new full backup:

1. Make sure all backup files of the chain are available.
2. Select **Tools > Merge Backup**.
3. Select the backup files to merge.
4. Start the process.

The result is a new full backup; the older backups of changes can be deleted or archived, and the chain becomes easier to manage. Only consecutive backups of the same chain – with the same base backup – can be merged. See Backup of changes.

From the command line

Conversions can be scripted with `/convert image`; see Command line.

Virtual drives

A backup mounted as a virtual drive is browsed in the running Windows like any other drive – the way to copy individual files from an image without restoring it. ISO files can be mounted in the same way. Mounting needs a special O&O DiskImage driver; if it is not installed yet, the program says so and installs it on request.

Mount a backup as a virtual drive

1. Open the **Tools** tab and select **Mount**, or press **Ctrl+M**.
2. Select the backup file (`.omg`) that contains the drive. **Read backup information** shows the details of a backup if you are unsure.
3. All drives of the image are listed. Select the drive.
4. Choose a free drive letter, for example G:.
5. Select **Mount drive**. The virtual drive appears in Windows Explorer.

Copy files or folders from the drive, check or compare data, or browse the content. The mounted drive is read-only: nothing can be deleted, renamed or added inside the backup. Only the areas that the backup contains are accessible, updating the view can take a moment, and only backups that are available locally can be mounted – backups on network drives cannot.

Load whole disks

A backup also stores the layout of the disk: the partition table (MBR/GPT), extended boot sectors, the LDM database and other system areas. **Enable loading disk** loads this information too and presents the operating system with a virtual hard disk that reproduces the original layout – useful for recovering deleted or damaged data from a forensic backup.

Mounting a complete disk can fail to detect the partitions when the partition table is damaged or invalid, when an unsupported layout was used, when dynamic disks with spanned, striped, mirrored or RAID-5 volumes were backed up without all participating disks, or when the disk is encrypted.

Unmount a drive

1. Open the **Tools** tab and select **Unmount**.
2. Select the virtual drive and remove it with the corresponding button.

After a restart of Windows, mounted virtual drives are removed automatically.

Mount an ISO file

1. Open the **Tools** tab and select **Mount ISO file as drive**.
2. Select the ISO file (`.iso`).
3. Select **Mount ISO file**, and choose a drive letter if needed.
4. After a moment, the virtual drive appears in Windows Explorer. It is read-only.

To show the virtual CD/DVD drive in the drive list of O&O DiskImage too, enable **Include CD and DVD drives** under **Program settings > General** and **Show non-backupable drives** under **View**. The drive is removed automatically after a restart of Windows.

Limitations and notes

- **Remote Desktop**: in an RDP session, a new login may be needed before mounted drives are shown correctly.
- **VHD/VHDX**: when a VHD/VHDX file is mounted, Windows may report that the disk image could not be mounted or contains no recognizable partitions. The message can usually be ignored; the file is mounted correctly.
- **Access denied**: if files on the mounted drive cannot be opened, the cause is usually a different security ID (SID) – the files were created under another Windows installation or user account. If necessary, enable the **Administrator** account, which is disabled by default, and access the files with it; administrator rights allow far-reaching changes, so proceed carefully.

Mounting and unmounting can be scripted with `/mount image` and `/unmount image` ; see Command line.

Network drives and FTP

O&O DiskImage stores backups on network drives and FTP servers and restores from them. Connect the share, and store the credentials in the password manager so that backups in the background and tasks can authenticate.

Connect a network drive

1. Open the **Tools** menu and select **Connect Network Drive**.
2. Enter the path and, if required, the user name and the password.
3. Confirm. The network drive is available in O&O DiskImage like a local drive.

Tools > Disconnect Network Drive removes a connection: select the drive and disconnect it. Backups on network drives cannot be mounted as virtual drives; see Virtual drives.

Network authentication

Access to protected folders and network shares requires a user account with the matching permissions. The **password manager** of O&O DiskImage stores credentials once and uses them automatically whenever they are required – for backups on network paths and for backups loaded from there. The data is compressed, encrypted with AES and stored with a public/private key pair; the order of the records is randomized as well.

1. Open **Start > Program Settings > Security**.
2. If no password database exists yet, select **Create database**.
3. Assign a password for the database and confirm it. O&O DiskImage generates the key pair that protects the database and gives its service access, so backups can run in the background.
4. Select **Add** to create an authentication profile.
5. Under **Computer/Directory**, enter the network path, for example `\\ComputerName\Share` or `\\Domain\Share`. Only the computer name opens all shares of that computer with this user.
6. Enter the user name in the form `domain\user1` or `user1@domain`.
7. Enter the network password. The account needs sufficient permissions for the target directory.
8. Optionally add a description.

Afterwards, network shares are used like local storage locations for backups and restores. Back up the authentication data before a major update of O&O DiskImage, so it can be restored afterwards. **Reactivate** on the **Security** page shows all security prompts again that were disabled permanently.

Tasks that use the network must run under a user account with access to the share; the SYSTEM account does not have access to all shares. See Tasks.

FTP servers

Backups can be stored on and loaded from FTP servers; O&O DiskImage uses the passive FTP mode, which is more stable and firewall-friendly in most networks. The FTP access authenticates with the FTP user name and password, and it is identified by the prefix `ftp://`. O&O DiskImage matches the authentication data to the exact string of the configured network path, so enter the address exactly.

Use	Path format
Backup to an FTP server	`ftp://user@server/path` – the full FTP path including the user name, so the matching credentials are found.
Load a backup from an FTP server, for example in a file dialog	`ftp://user:password@server/` – afterwards, browse to the directory and select the backup like on a local drive.

When the credentials are stored correctly, the test of the authentication data succeeds, and the FTP location can be used as a regular backup target.

Backup information and validation

The functions for existing backup files are in the **Read or Validate Backups** section of the **Tools** menu. They apply to all backup types – OMG, OBK, VHD and VHDX.

Read backup information

1. Select **Read Backup Information**.
2. Choose the backup file (`.omg` or `.obk`).

The information shows the backup method, the creation date and time, the backup version, the number of drives or files, structural and file information, and the compression and encryption used. Use it to assess the structure and usability of a backup quickly, for example before mounting or converting it.

Validate a backup

Validate in the **Tools** menu checks the structural integrity of a backup file: that it is logically and technically correct, free of structural and internal errors, that it can be restored reliably in an emergency, and that encrypted or compressed backups are processed correctly. Decryption, decompression and the internal checksums are verified completely.

Let the validation run to the end. After **Skip** or **Cancel**, O&O DiskImage cannot guarantee that the backup was created correctly or can be restored without errors.

Typical reasons for a failed validation:

- errors during encryption or decryption – a wrong password or corrupted data,
- errors during compression or decompression,
- 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.

A backup that fails validation cannot be relied on: create a new backup and validate it, and keep an older validated backup until then.

Validate automatically

Program settings > Drive Backup and **File Backup** validate every new backup immediately after its creation, and **Drive Restore** validates a backup before every restore. See Program settings. From the command line, `/validate` checks a backup; see Command line.

System tools

Besides the backup functions, the **Tools** menu offers tools for the system: the boot medium and O&O DiskImage ToGo, the RecoveryPartition, the command prompt, the change of computer properties and the drive check. They serve disaster recovery, rollouts in networks and system diagnostics.

Change computer properties

Change Computer Properties adjusts the identity of a computer, in particular its **SID**. This is needed when a system image is deployed to several computers in the same network, when cloned systems with identical SIDs exist in one environment, and when authentication or security problems occur in workgroups. Every cloned system initially has the same SID.

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

1. Start the computer from the boot medium.
2. Select **Tools > Change Computer Properties**.
3. Load the inactive Windows system, usually `C:\Windows`.
4. Assign a new computer name.
5. Select **Change** to save the new identity, or **Close** to cancel.

The same dialog supplements the hardware adaptation of M.I.R. after a restore to dissimilar hardware; see Dissimilar hardware (M.I.R.).

Check a drive

Tools > Check Drive checks the structural integrity of the file system and the surface of the storage device, so impending data loss is detected early.

1. Start the **Check Drive** wizard.
2. Select the drive to check.
3. Start the analysis and follow the progress in the status display.
4. When the check is finished, all messages and errors found are listed.

Command prompt

Tools > Command Prompt opens a Windows command line window; the O&O DiskImage interface stays open in the background. The command line version of O&O DiskImage, `oodicmdc.exe`, runs backups, restores, conversions and duplications from there. See Command line.

Boot medium, ToGo and RecoveryPartition

The creation of the boot medium and of O&O DiskImage ToGo is described under Boot medium and O&O DiskImage ToGo, the RecoveryPartition under RecoveryPartition.

Program settings

Start > Program Settings adapts O&O DiskImage to your workflows and decides whether the settings are saved permanently and reused at the next start. When O&O DiskImage runs from the boot medium, the pages **General**, **Security** and **Notification** are not available; only the settings needed for recovery and system analysis are accessible there.

General

Setting	Meaning
Start page	The page that opens at the program start, for example the backup page if you back up regularly.
Appearance and behavior > Include removable drives	Whether USB sticks, external drives and memory cards appear in the drive list and are considered for backups and restores. Enable only the types you use, because many removable media are slow or only connected occasionally.
Include CD and DVD drives	Shows CD/DVD drives, for example a mounted ISO file, in the drive list.
Working directories	The default path for new backups, suggested for every new backup and changeable per backup, and the storage locations of tasks and reports.

Tasks and reports

Setting	Meaning
Report creation	For which actions reports are created. A report is always created for a scheduled task.
Behavior	Whether a double-click on a task starts it or opens it for editing, and whether a double-click on a report shows it in O&O DiskImage or opens it in an external editor.

File backup

Setting	Meaning
Prefer external USB drives as suggestions	Connected USB drives are suggested as targets for file backups.
Verify backup file for errors after creation	Every new file backup is validated immediately; this increases the duration a little.
Overwrite existing backup files without prompt	Suppresses the prompt when a backup file with the same name exists – for several automated backups per day that are named by date. Enable it only when older backups at that location are no longer needed.
Behavior	What a double-click on a file or folder in the file backup dialog does: open, select or add to the selection.

File restore

Setting	Meaning
Behavior	What a double-click on a drive in the file restore window does: open the drive, select it or set it as the target.

Notification

The SMTP access data of the mail server and the sender information for e-mail notifications of tasks. After they are saved, the task assistant offers the e-mail address as the recipient. The **Domain** field can hold the host name of the mail server instead of the local domain, so the SMTP dialog (EHLO/HELO) works with servers that enforce strict authentication. A test e-mail from the settings checks the configuration. See Tasks.

Cloning

Setting	Meaning
Show non-cloneable drives	Whether drives that cannot be duplicated – CD/DVD drives, empty floppy drives and other unsuitable devices – are shown in the duplication window.
Behavior	What a double-click on a drive in the duplication window does: select it, show its details or set it as the source.

Drive backup

Setting	Meaning
Prefer external USB drives as suggestions	Connected USB drives are suggested as targets when a destination path is selected.
Verify backup file for errors after creation	Every new drive backup is validated immediately after completion.
Overwrite existing backup files without prompt	Suppresses the prompt when a backup file with the same name exists; existing backups are replaced without confirmation.
Behavior for non-backupable drives	Whether drives that cannot be backed up are shown or hidden: empty card readers and floppy drives, the Microsoft Reserved Partition (MSR) on GPT disks, OEM partitions of manufacturers and internal system areas on basic disks.

Drive restore

Setting	Meaning
Validate backup before restore	The backup file is validated before every restore, so a damaged backup is noticed before the target is overwritten.
Behavior	What a double-click on a drive in the drive list does, for the drives in the backup and for the target drives: select, show details or assign as source or target.

Security

Setting	Meaning
Password database	The password manager with the credentials for network shares and FTP servers. See Network drives and FTP.
Reactivate	Shows all security prompts and confirmations again that were disabled permanently.

Tray icon

The context menu of the tray icon sets whether the icon is shown and animated and whether notifications about the progress of tasks and changes of the O&O DiskImage service appear. See Interface.

Command line

Besides the graphical interface, O&O DiskImage offers a command line version, `oodicmdc.exe`, that runs from the Windows command prompt. Open it with **Tools > Command Prompt**; the graphical interface stays open in the background. The typical path of the executable is `C:\Program Files\OO Software\DiskImage\oodicmdc.exe`.

Commands are called as `oodicmdc.exe <command> [subcommands] [parameters]`. Do not insert manual line breaks inside a command; the line breaks of the examples are formatting only. The integrated command line help lists all parameters.

Examples

```
oodicmdc.exe /create image /source S: /destination E:\Sample.omg
oodicmdc.exe /validate /source E:\Sample.omg
oodicmdc.exe /restore image /image E:\Sample.omg /source S: /destination T: /OverwriteTa
```

The first command creates a sector-based backup of drive S:, the second validates a backup file, the third restores S: from the backup to T: and overwrites the target.

Sources and destinations

A drive or disk is addressed in one of these formats:

Format	Example
Drive letter	`D:`
Volume GUID	`{xxxx-xxxx-xxxx-xxxx}`
Disk number	`DiskNo 0`
Offset of a volume on a disk	`1048576@1` (`Offset@DiskNo`)

/create image

Creates a sector-based backup (image).

Parameter	Meaning
`/source`	The drive or disk to back up, in one of the formats above.
`/destination`	Path and name of the backup file (optional).
`/password "…"`	Password for the encryption; enables the forced dismount if required (optional).
`/comment "…"`	Comment for the backup (optional).
`/exclude "…"`	Excludes objects by path or wildcard (optional).
`/type "…"`	`"used sector"` (default) or `"forensic"` (optional).
`/max <MB>`	Maximum size of a backup file in MB; larger backups are split (optional).
`/format "…"`	`"O&O DiskImage"` (default), `"VHD Format"` or `"VHDX Format"` (optional).
`/VirtualDiskType "…"`	`"dynamic hard disk"` (default) or `"fixed hard disk"` (optional).

/create image increment

Creates an incremental sector-based backup on the basis of an existing backup. It takes the parameters of `/create image` plus the parameters that identify the base backup and the incremental options.

/restore image

Restores a sector-based backup.

Parameter	Meaning
`/image "…"`	Path and name of the backup file.
`/source "…"`	The object in the backup: drive letter, `DiskNo X` or `Offset@DiskNo X@Y`.
`/destination "…"`	The target: drive letter, volume GUID, `DiskNo X` or `Offset@DiskNo X@Y` (optional).
`/DecryptPassword "…"`	Password of an encrypted backup (optional).
`/FillEmptyBlocksNull`	Fills empty sectors with zeros.
`/WriteHarddiskDrive`	Writes directly to the disk instead of through the volume.
`/CreateVolumeLikeSource`	Creates the target volume like the source volume without prompting.
`/IgnoreReadErrors`	Logs read errors instead of aborting.
`/SetBootPartitionBootable`	Marks a bootable partition as active.
`/ClearTargetDrive`	Clears the target layout without prompting.
`/OverwriteTargetData`	Overwrites data on the target without prompting.
`/IgnoreDataModification`	Reports data modifications but continues.

/convert image

Converts a sector-based backup to another format – for example VHD/VHDX – or to other properties.

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

/create backup

Creates a file-based backup (OBK).

Parameter	Meaning
`/source "…"`	File names with path, wildcards allowed, for example `C:\Data\*.docx`.
`/destination "…"`	Path and name of the backup.
`/password "…"`	Password for the encryption (optional).
`/dismount`	Forced dismount to protect against changes; the default is a VSS snapshot (optional).
`/comment "…"`	Comment (optional).
`/exclude "…"`	Exclusion filter (optional).
`/max <MB>`	Maximum size of a backup file (optional).
`/IgnoreReadErrors`	Ignores read errors (optional).

/restore backup

Restores a file-based backup.

Parameter	Meaning
`/source "…"`	Path and name of the backup.
`/destination "…"`	Target directory, full path.
`/DecryptPassword "…"`	Password of an encrypted backup.
`/IgnoreReadErrors`	Ignores read errors (optional).
`/OverwriteTargetData`	Overwrites the target without prompting (optional).
`/IgnoreDataModification`	Reports modifications but continues (optional).

/validate

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

Parameter	Meaning
`/source "…"`	Path and name of the backup.
`/DecryptPassword "…"`	Password of an encrypted backup (optional).
`/AllSplits`	Includes all parts of a split backup (optional).

/mount image

Mounts a sector-based backup as a virtual disk.

Parameter	Meaning
`/source "…"`	Drive letter or `DiskNo` of the virtual device.
`/image "…"`	Path and name of the backup file.
`/DecryptPassword "…"`	Password of an encrypted backup (optional).
`/driveletter X:`	The drive letter of the mounted volume.

/unmount image

Unmounts a mounted sector-based backup: `/source "…"` names the drive letter or `DiskNo` of the virtual disk.

/duplicate

Duplicates a drive or disk (clone).

Parameter	Meaning
`/source "…"`	The source: drive letter, volume GUID, `DiskNo X` or `Offset@DiskNo X@Y`.
`/destination "…"`	The target, in the same formats.
`/dismount`	Protection against changes with a VSS snapshot (optional).
`/exclude "…"`	Excludes contents (optional).
`/type "…"`	`"used sector"` (default) or `"forensic"` (optional).
Further options	`/FillEmptyBlocksNull`, `/WriteHarddiskDrive`, `/CreateVolumeLikeSource`, `/IgnoreReadErrors`, `/SetBootPartitionBootable`, `/ClearTargetDrive`, `/OverwriteTargetData` – as for `/restore image`.

/add license

Registers the product with `/name "…"`, `/company "…"` and `/serial "…"`.

/stop

Stops all running O&O DiskImage actions.

/creating bootable medium

Creates a bootable medium. The optional parameters `/recovery environment`, `/ADK`, `/AIK`, `/installation media`, `/boot device` and `/ISO path` determine which Windows components are used (Recovery Environment, ADK or AIK), which installation media, the target device (CD/DVD or USB) and the path of the ISO file to create. See Boot medium and O&O DiskImage ToGo.

/show volumes

Lists the volumes of the system with their drive letters, disk numbers and offsets in bytes. With `/image "…"`, it lists the volumes contained in a backup file.

Glossary

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

1-Click backup: The backup of the entire computer with preset options – compression LZNT1 and the backup of used sectors. See Drive backup.

Backup of changes: An incremental or differential backup that saves only what changed since the base backup. See Backup of changes.

Base backup: The backup on which a backup of changes is based: a full backup for differential backups, the last backup of any type for incremental backups.

Boot medium: A bootable CD/DVD, USB stick or ISO file with O&O DiskImage on a Windows PE base. It starts the computer when Windows no longer boots. See Boot medium and O&O DiskImage ToGo.

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

Direct forensic: The backup method that accesses the physical disk directly, bypassing the file system driver; preserves BitLocker metadata.

DiskView: The graphical overview of the disks with their partition layout and their free and used space in the drive backup.

Drive: A specifically assigned area on a disk – a partition, a logical drive in an extended partition or a volume. See Backup types.

Drive backup: An image of the used sectors or all sectors of a drive, stored in the OMG format.

Duplication: The direct copy of a disk or drive to another disk, without a backup file; also called cloning. See Clone drives.

Express View: The reduced interface with the functions Create Backup, Restore Backup and Read Backup Information. See Interface.

File backup: A backup of selected files and folders, stored in the OBK format. See File backup.

Forensic backup: Saves every sector of a drive, including unused and damaged areas; as large as the physical disk.

Full backup: Writes all selected data completely to the target medium; the base for subsequent backups of changes.

Incremental backup: Saves only the changes since the last backup – full, differential or incremental.

M.I.R.: Machine Independent Restoration – restores or duplicates a system to a computer with dissimilar hardware by adapting the hardware abstraction layer and the drivers. See Dissimilar hardware (M.I.R.).

OBK: The file format of file backups (`.obk`).

OMG: The native file format of drive backups (`.omg`) with the full range of functions.

oodicmdc.exe: The command line version of O&O DiskImage. See Command line.

Password manager: Stores the credentials for network shares and FTP servers in an encrypted database. See Network drives and FTP.

Profile: Saved backup, restore or copy options that can be reused under a name.

RecoveryPartition: A recovery environment on the internal disk that starts O&O DiskImage from the Windows Boot Manager and can hold backups. See RecoveryPartition.

Report: The record of an action with its time, parameters, source, target, messages and status. See Reports.

SID: The security identifier of a computer. Cloned systems share it until it is changed with **Change Computer Properties**. See System tools.

Task: A scheduled action – a backup, a backup of changes or a duplication – with a user account, notifications and optional pre- and post-task commands. See Tasks.

ToGo: O&O DiskImage ToGo – an external disk or USB stick that is both the boot medium and the preferred destination for system backups.

Tray icon: The icon in the Windows notification area that shows the status and offers quick access to the main functions.

Used sectors: The standard backup method; saves only the sectors that contain data.

Validation: Checks the structural integrity of a backup file. See Backup information and validation.

VHD / VHDX: Microsoft formats for virtual hard disks – up to 2 TB (VHD) and 64 TB (VHDX). Backups can be converted to them and mounted. See Convert and merge backups.

Virtual drive: A backup or ISO file mounted as a read-only drive in Windows. See Virtual drives.

Windows PE: The Windows Preinstallation Environment on which the boot medium and the RecoveryPartition are based.

Troubleshooting

A task does not run or aborts

A task runs only while its initial conditions remain stable. Check the paths and storage locations of the backups, the source and target drives, the drive names and the network access rights, and run **Check task** under **Tasks & Reports**.

A task that uses network shares must run under a user account with access to them; the SYSTEM account does not reach all shares. If the full backup and the backups of changes are in different directories, clear **Suppress user prompts during execution**, otherwise the task aborts when it cannot find the preceding backups. If the base backup was moved, update its location in the task. See Tasks and Manage tasks.

An imported task does not run

Imported tasks are not enabled automatically. Check them, adjust drive letters, paths and network conditions that differ from the source computer, and enable them. See Manage tasks.

No e-mail notifications arrive

Configure the SMTP access data and the sender under **Program settings > Notification** first and send a test e-mail. If the mail server enforces strict authentication, enter the host name of the mail server in the **Domain** field. Then select the recipient and the events in the task. See Program settings.

The target medium is too small

If the target runs out of space during a backup, O&O DiskImage asks for an additional target path. For a restore or duplication to a smaller disk, use the file-based method. See Restore drives.

The system partition cannot be restored

The system partition cannot be overwritten while Windows is running. Start the computer from the boot medium or the RecoveryPartition and restore from there. See Restore the entire system.

The restored or duplicated system does not start

The usual cause is an incomplete selection: not the entire disk was selected as the target, **Delete layout** was not selected when the target layout was created, only individual source partitions were selected instead of the entire disk, or the bootable drive hangs on a controller that is not initialized at boot time. Always back up and

restore or duplicate the entire system disk. For different hardware, enable **Adjust dissimilar hardware afterwards** (M.I.R.), and supplement the adaptation manually under **Tools > Change Computer Properties** if needed. See Dissimilar hardware (M.I.R.).

The computer does not start from the boot medium

Set the boot order in the BIOS/UEFI setup or in the boot menu so the medium starts first; the order chosen in the boot menu usually applies to the current start only. Disable **Secure Boot** if the Windows PE medium does not start, start in the same boot mode (UEFI or Legacy/CSM) in which the medium was created, and use a USB 2.0 port if the stick is not detected on a USB 3.0 port. If the medium is still not detected, recreate it. See Boot medium and O&O DiskImage ToGo.

A disk, a RAID array or the network is missing in the recovery environment

The driver of the storage controller, the NVMe SSD, the RAID controller or the network adapter is missing. Load it on the **Drivers** tab of the **O&O System Settings** dialog from a USB stick or a driver CD. In most cases the cause is a missing RAID, AHCI or NVMe driver, or a changed BIOS setting such as the RAID/IDE/AHCI mode. See Load drivers.

A BitLocker drive cannot be backed up or restored

In the recovery environment, an encrypted volume must be unlocked with the recovery key first – the user password and the TPM do not work there. A restored drive stays encrypted only when it was backed up with the direct forensic method; after a backup of used sectors it is no longer encrypted. See BitLocker.

The validation fails

Possible causes are a wrong password or corrupted data, errors during compression, backup files modified by the user or by other programs such as antivirus software, and defective storage media. A backup that fails validation cannot be relied on: create a new backup and validate it. Let every validation run to the end; after **Skip** or **Cancel** the result is not guaranteed. See Backup information and validation.

A backup cannot be mounted

Only backups that are available locally can be mounted; copy a backup from a network drive to a local disk first. Install the O&O DiskImage driver when the program asks for it. In a Remote Desktop session, log in again if mounted drives do not appear. If Windows reports that a VHD/VHDX file could not be mounted or contains no recognizable partitions, the message can usually be ignored. See Virtual drives.

Access denied on a mounted drive

The files were created under another Windows installation or user account, so their security IDs differ. If necessary, enable the **Administrator** account and access the files with it – carefully, because administrator rights allow far-reaching changes.

Two disks with the same signature

After a duplication, O&O DiskImage changes the disk signature of the target, so both disks can be connected at the same time. If a cloned system is deployed to several computers, change the computer name and the SID with **Tools > Change Computer Properties** from the boot medium. See System tools.

A backup of changes cannot be created or restored

A backup of changes needs its base backup: the last backup for incremental backups, the last full backup for differential backups. A restore needs the whole chain – the full backup and all backups of changes up to the desired state. Keep them together; merge a long chain into a new full backup with **Tools > Merge Backup**. See Backup of changes.

The copy becomes inconsistent during a duplication

If the source drive is not locked, O&O DiskImage buffers changes in a cache of limited size; when the cache is full, changes reach the target directly and the copy can become unusable. Lock the drive under **Copy options > Advanced > Read process**, or stop write-intensive processes such as a defragmentation during the copy. See Clone drives.

FAQ

Which editions does this guide cover?

The Professional, Server and Enterprise Editions with the full interface. The Premium Edition with the tile interface has its own guide. See Editions.

Which backup should I create first?

The 1-Click backup of the entire computer – **Drive backup > Backup entire computer** – onto an external drive or a network share. Then create a boot medium. See Quick start.

What is the difference between a drive backup and a file backup?

A drive backup is an image of a whole drive, stored as an OMG file, and the basis for restoring a system. A file backup contains only the selected files and folders, stored as an OBK file. See Backup types.

How do incremental and differential backups differ?

An incremental backup saves the changes since the last backup of any type, a differential backup the changes since the last full backup. A restore needs the full backup and – for incremental backups – all following backups of changes. See Backup of changes.

Can backups run automatically?

Yes. Select the action, adjust the options and select **Add as task**. The task assistant sets the schedule, the user account, the notifications and the actions after completion. See Tasks.

Why does a task that writes to a network share fail?

Without a user account, a task runs under the SYSTEM account, which does not reach all network shares. Run the task as a user with access to the share, and store the credentials in the password manager. See Network drives and FTP.

How do I restore the system partition?

Start the computer from the boot medium or the RecoveryPartition and restore from there; in the running Windows the system partition cannot be overwritten. See Restore the entire system.

Can I restore a system to a different computer?

Yes, with M.I.R.: enable **Adjust dissimilar hardware afterwards** in the restore options when restoring from the boot medium, and back up and restore the entire system disk. Change the computer name and the SID afterwards if the system is deployed several times. See Dissimilar hardware (M.I.R.).

Can I restore to a smaller disk?

Yes, file by file: O&O DiskImage offers the file-based method when a sector-based 1:1 copy does not fit, and you define the size of the target partition. See Restore drives.

Can I restore individual files from a drive backup?

Yes. Mount the backup as a virtual drive with **Tools > Mount** and copy the files in Windows Explorer. Files from a file backup are restored with **File Recovery**. See Virtual drives and Restore files.

Does a restored BitLocker drive stay encrypted?

Only when it was backed up with the direct forensic method. After a backup of used sectors, the restored drive is no longer encrypted. The recovery key is always required in the recovery environment. See BitLocker.

Can I use a backup in a virtual machine?

Yes. Convert the OMG backup to VHD or VHDX with **Tools > Convert Backup Files** and use the file in Hyper-V or Virtual PC. See Convert and merge backups.

Is there a command line?

Yes. `oodicmdc.exe` creates, restores, converts, validates, mounts and duplicates backups from the command prompt and from scripts. See Command line.

What is the difference between the boot medium, O&O DiskImage ToGo and the RecoveryPartition?

All three start O&O DiskImage without Windows. The boot medium is a CD/DVD, a USB stick or an ISO file; ToGo is an external disk that is boot medium and backup destination at once; the RecoveryPartition is a

recovery environment on the internal disk. The RecoveryPartition does not replace external backups. See Boot medium and O&O DiskImage ToGo and RecoveryPartition.

Support and more from O&O

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

Contact support

Open O&O Software support. Include:

- The version and edition of O&O DiskImage and the Windows version.
- The report of the failed operation.
- The type of source and destination.
- Whether the backup was started manually or by a task.
- Whether the problem occurred in Windows or after starting from the boot medium.

Add the report of the operation if support requests it. See Reports for where to find it, and Troubleshooting for common problems and their solutions.

Licensing and updates

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

More O&O products

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

See all O&O products.