



© O&O software

O&O DiskImage

Table of Contents

1 Introduction	3
2 Getting Started	5
2.1 Quick Start	5
2.2 Your First Backup	7
3 Core Concepts	9
3.1 Backup Sources	9
3.2 Backup Destinations	11
4 Backup Deep Dive	13
4.1 Backup Options	13
4.2 Schedules And Automation	16
4.3 File Names And Exclusions	18
5 Restore	20
5.1 Restore Overview	20
5.2 Restore Files	21
5.3 Restore Drives	22
6 Clone And Recovery	23
6.1 Clone Drives	23
6.2 Rescue Media And Fortress Mode	24
7 Management	25
7.1 Backup Sets And Tasks	25
7.2 Reports And Logs	27
7.3 Tools	29
8 Settings	32
8.1 Settings Reference	32
9 Troubleshooting	35
9.1 Common Issues	35
10 FAQ	37
11 Development	40
11.1 Online Documentation	40

O&O DiskImage 23 Premium Edition User's Guide

Welcome to the user's guide for **O&O DiskImage 23 Premium Edition**. This guide explains how to create backups, restore data, clone drives, prepare recovery options, and tune the application for reliable day-to-day protection.

O&O DiskImage Premium is the modern O&O DiskImage application for Windows PCs. It is built around a guided workflow: choose what to protect, choose where to store it, adjust the options that matter, and then run the backup now or automatically later.

Premium Edition only

O&O DiskImage 23 is documented here as a Premium Edition product. There is no separate Free Edition in this guide.

What You Can Do

- **Back up your entire PC** so Windows, programs, settings, and personal data can be restored after a failure.
- **Create images of drives and partitions** for system migration, targeted protection, or recovery of a specific volume.
- **Back up files and folders** when you only need selected data and want smaller, faster backup runs.
- **Restore drives, partitions, and files** from available backup sets.
- **Clone disks** to move to a larger or faster SSD or create a direct 1:1 replacement drive.
- **Schedule backups** once, daily, weekly, hourly, continuously, or when a USB backup drive is connected.
- **Use backup destinations** such as local folders, USB drives, NAS shares, WebDAV destinations, and S3-compatible storage.
- **Generate reports and logs** so you can verify completed operations and diagnose problems.
- **Prepare recovery access** with Fortress Mode or bootable recovery media.

How This Guide Is Organized

Start with **Getting Started** if you want the shortest path to your first backup. Use **Backup Deep Dive** when you want to understand backup strategies, image formats, compression, validation, retention, encryption, schedules, and naming templates.

Experienced users can jump directly to the settings reference or the schedule deep dive. New users should read the quick start and first backup pages first; they explain the core terms used throughout the rest of the

guide.

Quick Start

This page gives you the shortest reliable path to your first O&O DiskImage backup.

Before You Start

Prepare a backup destination that is separate from the data you are protecting. Good choices are an external USB drive, a NAS share, WebDAV storage, or S3-compatible object storage. A second folder on the same system drive is convenient for testing but not safe as a real disaster-recovery destination.

Also keep the computer connected to power for large backups. Drive images can take time, especially the first full backup.

Create Your First Backup

1. Open **O&O DiskImage 23 Premium Edition**.
2. Choose **Back up your PC** for complete system protection.
3. Review the selected source. For a full PC backup, O&O DiskImage includes Windows, applications, settings, and personal data.
4. Choose a backup destination.
5. On the options page, decide whether to run the backup now, schedule it, encrypt it with a password, or open advanced settings.
6. Select **Start backup**.
7. After completion, open **Reports** and verify that the run completed successfully.

Recommended First Setup

Setting	Recommendation
Backup type	Back up your PC
Destination	External drive or NAS
Backup strategy	Incremental
Backup technology	Used sectors
Backup format	O&O DiskImage format
Compression	On, standard
Reports	On
Validation	On for important backups, with enough time reserved

What To Do Next

After the first backup, configure a schedule. Daily or weekly is enough for many PCs. Hourly or continuous schedules are better suited to small, frequently changing, business-critical data.

Then prepare a recovery path. Use **Fortress Mode** for recovery built into the local PC, or create bootable rescue media for recovery from a USB stick or ISO image.

Your First Backup

O&O DiskImage uses guided backup workflows. The exact pages depend on the source you choose, but every backup follows the same idea: select the source, select the destination, adjust options, confirm the summary, and run.

Choose A Backup Source

Choice	Use it when
Back up your PC	You want complete protection for the current computer.
Back up drives	You want to image selected drives or partitions.
Back up files	You want to protect selected folders and files without imaging an entire drive.

New users should usually begin with **Back up your PC**. It gives you the broadest recovery option after a system failure.

Choose A Destination

The destination is where backup data is stored. O&O DiskImage can use local folders, removable drives, NAS or network shares, WebDAV destinations, and S3-compatible storage.

If you select a network share, enter credentials when prompted. O&O DiskImage stores them securely through Windows Credential Manager so scheduled backups can reach the destination later.

Review The Options Page

The options page shows a recap of the backup and several option groups:

- **Run on a schedule:** create an automatic time-based schedule.
- **Run when the backup drive is connected:** available for removable or USB destinations and mutually exclusive with time-based schedules.
- **Encrypt backup with password:** protect the backup from unauthorized access.
- **Advanced settings:** open backup strategy, compression, validation, retention, reports, file names, and exclusions.

Confirm And Start

The final summary shows what will be backed up, where it will be stored, when it will run, and which protection options are active. Select **Start backup** to begin.

During the backup, the progress view shows the current action, overall progress, source, destination, and status. When the operation finishes, O&O DiskImage can generate a report that records the result.

Verify The Result

Open **Reports** after your first backup. A successful report confirms that the backup ran and gives you useful information about source, destination, backup type, duration, data volume, warnings, and errors.

Backup Sources

A backup source is the data O&O DiskImage protects. Choosing the right source is the first major decision in every backup plan.

Full PC Backup

Back up your PC captures the complete computer: Windows, installed programs, settings, and personal data. This is the recommended starting point because it gives you the broadest restore path after disk failure, system corruption, or a failed update.

Use it for:

- First-time protection of a PC.
- Disaster recovery.
- Rebuilding the same computer after a failed system drive.
- Creating a baseline before major Windows or hardware changes.

Drive And Partition Images

Back up drives creates images of selected drives or partitions. It is useful when you want precise control over what is imaged, for example only the system partition, a data volume, or an external disk.

Drive and partition images are sector-based. Depending on the backup technology, they can contain only used sectors or a bit-precise copy of all sectors.

File And Folder Backups

Back up files protects selected directories and files. It is usually smaller and faster than a full drive image and is a good fit for documents, project folders, media collections, or other user data.

File backups support exclusions so temporary files, system files, previous backup files, and other unnecessary data can be skipped.

Default Exclusions

O&O DiskImage excludes common temporary and system-specific files by default, including paging and hibernation files, system volume information, temporary files, and backup container formats such as O&O DiskImage, VHD, and VHDX files. These exclusions avoid unnecessary data and prevent backups from recursively containing previous backups.

You can adjust exclusions in **Settings > Exclusion** or from advanced backup settings.

Backup Destinations

A backup destination is where O&O DiskImage stores backup data. The destination should be reliable, large enough, and preferably separate from the source computer.

Supported Destination Types

Destination	Description
Local folder	A folder on an internal, external, or removable drive.
USB drive	A removable drive detected by O&O DiskImage; useful for hotplug backups.
NAS / network share	A UNC path such as <code>\\server\share</code> , with optional stored credentials.
WebDAV	A WebDAV server with authentication and optional SSL/TLS.
S3-compatible storage	Object storage such as AWS S3, MinIO, or compatible services.

Primary Destination

When multiple destinations are configured, one can be set as the primary destination. O&O DiskImage displays destination availability, free space, total size, and backup usage where that information is available.

Network Credentials

NAS, WebDAV, and S3 destinations may require credentials. O&O DiskImage stores secrets through Windows Credential Manager, encrypted by Windows, instead of writing passwords into ordinary configuration files.

Use **Test connection** after entering remote destination settings. It checks whether the destination can be reached and reports common problems such as authentication failure, unreachable host, timeout, certificate issues, or missing S3 bucket.

USB Drive Detection

For local and removable destinations, O&O DiskImage can detect USB drives and present them as selectable destinations. Hotplug backups use enhanced drive matching where possible. Instead of relying only on a drive letter, O&O DiskImage can compare serial number, volume label, size, and model.

Destination Advice

- Use a destination with enough space for the first full backup and several later backup runs.
- Do not keep the only backup on the same disk you are protecting.
- For ransomware resilience, disconnect USB backup drives when not in use or use storage with independent access controls.
- For scheduled NAS backups, test credentials after setup and after password changes.

Backup Options

Backup options control how O&O DiskImage stores data, how much space it uses, whether the result is checked, and how long old backup runs are kept.

Backup Strategy

Strategy	What it does	Best for
Full	Stores all selected data every time.	Standalone archive points and simple retention.
Incremental	Creates a full backup first, then stores changes since the last backup run.	Regular automatic protection with efficient storage use.
Differential	Stores changes since the last full backup.	Easier chains than incremental, with more storage use.

Incremental is the default strategy and is usually the best balance of speed and storage. Differential backups can be easier to manage because each differential depends on the full backup rather than the immediately previous change backup. Full backups are simplest but require the most storage.

Execution Policy

The execution policy can create a new full backup after a configured number of change backups. This reduces the risk of very long incremental or differential chains and makes restore points easier to manage over time.

Backup Technology

Technology	Meaning
Used sectors	Backs up only sectors that contain data. This is recommended for normal use.
Forensic	Creates a bit-precise copy of the entire source, including empty sectors.
Direct forensic	Creates an exact copy directly from the data carrier and is intended for Fortress Mode scenarios.

Forensic backups require storage close to the full size of the source, not just the used data size.

Backup Format

Format	Notes
O&O DiskImage format	Recommended standard format. Supports all normal backup and restore options.
VHD	Microsoft virtual hard disk format. Useful for virtual mounting, with limited O&O DiskImage restore options.
VHDX	Newer Microsoft virtual disk format with larger capacity and better virtual disk features.

When you create VHD or VHDX files, Windows may automatically mount or display them during backup. That is normal and does not affect the backup.

Compression

Compression is enabled by default. The standard Lempel-Ziv option is optimized for performance and is the best general-purpose choice.

Available compression methods include:

- **Lempel-Ziv standard:** fast, lossless, moderate space savings.
- **Lempel-Ziv maximum:** stronger compression with more processing time.
- **ZIP deflate:** efficient for file backups; image backups fall back to Lempel-Ziv standard where required.
- **BZIP 1K, 4K, 9K block sizes:** increasing compression strength with increasing processing time.

VHD and VHDX backups do not use compression.

Encryption

Enable **Encrypt backup with password** to protect backup contents from unauthorized access. O&O DiskImage requires the original password when restoring or opening encrypted backups.

Store the password in a password manager or another secure place. O&O DiskImage cannot restore an encrypted backup without it.

Validation

Validation checks the backup file after completion for structural integrity. It adds time to the backup run but is valuable for important backups and new destinations.

Recovery partitions can have special characteristics that may cause validation to fail even when the backup itself is usable. The **Skip validation for recovery partitions** setting skips validation for backups that contain recovery partitions while leaving the backup unchanged.

Retention Policy

The retention policy defines how many backup runs are kept. When the limit is reached, O&O DiskImage deletes the oldest eligible backup run.

Retention is intentionally cautious with incremental chains. Deleting a backup that later incremental backups depend on would break the chain, so retention may be disabled or limited depending on the strategy.

Schedules And Automation

Schedules let O&O DiskImage run backup sets automatically.

Schedule Types

Type	Behavior
Once	Runs one time at the selected date and time.
Daily	Runs every N days at the selected time.
Weekly	Runs on selected weekdays at the selected time.
Hourly	Runs every N hours, starting at the selected time.
Continuous	Starts another backup after the previous one completes and the interval has passed.
Hotplug	Runs when the configured backup drive becomes available.

Time-based schedules and hotplug schedules are mutually exclusive for a backup set. Enabling hotplug replaces the time schedule for that set.

Hourly Backups

Hourly backups are useful when data changes often and the acceptable data-loss window is short. Choose a start time and an interval, such as every 1, 2, 4, or 8 hours.

Use incremental backups for hourly schedules unless you have a specific reason to create full backups. Full hourly backups can fill storage quickly.

Continuous Backups

Continuous backups are the most aggressive schedule type. After one run finishes, O&O DiskImage waits for the configured interval and then starts again.

Use continuous backups only when the source data is important enough to justify the extra load. Good candidates are small, frequently changing, business-critical datasets. Avoid continuous full-system backups on ordinary workstations unless you have tested performance and storage impact.

Hotplug Backups

Hotplug backups run when the backup drive is connected. They are useful for users who store backups on an external USB drive and do not want to keep that drive attached all the time.

O&O DiskImage can identify the expected drive by drive letter, serial number, volume name, size, and model. If only a drive letter is available, it falls back to letter-based matching. After a successful hotplug backup, the stored drive identity can be updated.

Hotplug options include:

- A start delay after the drive is detected.
- A next-run delay to avoid running the same backup repeatedly when the drive is reconnected too soon.

Missed And Overlapping Runs

O&O DiskImage is designed to avoid parallel executions of the same backup set. If a scheduled run is due while a previous run is still active, the new run is queued rather than started in parallel.

Large backups can run for hours. Do not shorten intervals until you know how long a normal run takes on your hardware and destination.

Schedule Advice

- Use **daily** for frequently used work PCs.
- Use **weekly** for less active systems.
- Use **hourly** for active business data.
- Use **continuous** only for carefully selected critical workloads.
- Use **hotplug** when backups should run only when a removable backup drive is connected.

File Names And Exclusions

O&O DiskImage lets you control how backup files are named and which files or folders are skipped.

File Name Templates

File name templates generate backup paths and file names automatically. The default pattern uses placeholders such as year, month, day, hour, minute, second, user name, computer name, and file extension.

Use templates to:

- Keep backup files sorted by date.
- Include the computer name when several PCs write to the same destination.
- Separate backup sets into predictable folders.
- Standardize naming across scheduled backups.

Example pattern:

```
Backup_{Year}{Month}{Day}_{Hours}{Minutes}{Seconds}{Extension}
```

Storage Path Templates

The storage path can also contain placeholders. A typical default is based on the selected default destination and a `Backups` folder.

Keep paths short and predictable, especially for NAS destinations. Very deep folder structures are harder to browse and troubleshoot.

Exclusions

Exclusions remove unnecessary or unsafe data from backups. O&O DiskImage includes predefined exclusions for temporary files, paging and hibernation files, system volume information, and backup container files.

You can add:

- A full file path.
- A folder path.
- A wildcard pattern such as `*.tmp`.
- A path fragment surrounded by backslashes, such as `\System Volume Information\`.

Best Practices

- Keep default exclusions unless you have a specific recovery requirement.
- Exclude application caches and temporary build folders from file backups.
- Do not exclude system folders from full PC or drive images unless instructed by support.
- Avoid storing backup files inside a folder that is itself selected for backup.

Restore Overview

Restore brings data back from a backup. O&O DiskImage supports restoring files and directories, restoring entire drives or partitions, and mounting supported image backups as read-only drives.

Restore Entry Points

Use **Manage backups** or **Restore backups** to select an existing backup set. Backups on disconnected storage can still appear so you know which restore points exist; connect the storage before starting the restore.

For each backup set, O&O DiskImage can show backup files, reports, metadata, backup type, creation date, source computer, user, dependency information, and file path.

Restore Types

Restore type	Use it when
Restore files and directories	You need selected files or folders from a file backup.
Restore entire drives from backup	You need to overwrite a drive or partition with data from an image.
Mount backup as drive	You want read-only access to image contents in Windows Explorer.
Full system restore	Windows or the system disk must be restored from a recovery environment.

Safety Before Restore

Drive and partition restore operations overwrite the selected target. Always confirm that the target is the correct drive or partition. O&O DiskImage shows the selected targets in the wizard summary and asks for confirmation before destructive operations.

For full system recovery, start from Fortress Mode or bootable rescue media so locked system volumes can be restored safely.

Restore Files

File restore is the safest restore workflow because it does not overwrite an entire drive. You can restore all files from a file backup or choose individual directories and files.

Restore A File Backup

1. Open **Manage backups** or **Restore backups**.
2. Select the backup set.
3. Choose **Restore files and directories**.
4. Select the backup run to restore from.
5. Choose whether to restore all data or select directories and files.
6. Select the target folder.
7. Start the restore.

Large backups may take time and memory to load when browsing the file tree. If you only need a few files from a large image backup, mounting the backup as a drive can be faster.

Restore Target Folder

For file restore, the target is a folder. You can restore to the original location when appropriate or to a separate folder if you want to compare files first.

If the selected target path is invalid or has too little free space, O&O DiskImage warns before starting.

Encrypted Backups

If the backup is encrypted, select **Enter password** and provide the password used when the backup was created. Without the correct password, the restore cannot continue.

Restore Drives

Drive restore writes image data back to a drive or partition. This is a powerful and destructive operation: the selected target can be overwritten.

Restore A Drive Or Partition

1. Open **Restore backups**.
2. Select the image backup set.
3. Choose **Restore entire drives from backup**.
4. Select the backup run.
5. Map the source drive or partition from the image to the target drive or partition.
6. Review the summary carefully.
7. Confirm the warning and start the restore.

Target Size Checks

O&O DiskImage checks whether the selected target has enough space. For partition restore, the target must fit the used data plus filesystem overhead. A target can sometimes be smaller than the original partition if the used data fits, but it cannot be too small.

Mount Instead Of Restore

If you only need to inspect an image or copy a few files, use **Mount backup as drive**. Mounted backups are available read-only in Windows, so you can browse them with Windows Explorer without overwriting a target disk.

After Restore

After restoring a system volume, reboot and verify Windows starts correctly. After restoring a data volume, confirm that files and applications see the restored data as expected.

Clone Drives

Cloning creates a 1:1 copy from a source disk to a target disk. It is most often used when moving from an old drive to a larger or faster SSD.

When To Clone

Use cloning when:

- You are replacing a disk and want the target to be immediately bootable.
- You want a direct disk-to-disk migration.
- You do not need a stored backup history for this operation.

Use a backup instead when you want multiple restore points, off-disk protection, or a reusable disaster-recovery archive.

Clone Workflow

1. Choose **Clone drives**.
2. Select the source drive.
3. Select the target drive.
4. Review the target layout.
5. Confirm the warning that target data will be overwritten.
6. Start disk cloning.

Safety Rules

- Never select the same physical disk as both source and target.
- Use a target disk that is at least large enough for the source data and desired layout.
- Disconnect unnecessary external disks if that makes target selection clearer.
- After cloning a system disk, shut down before removing or replacing drives.

Clone Technology

Clone operations use the configured image technology, such as used sectors or forensic sector copying. Used sectors is the normal choice. Forensic clone modes are slower and require enough target capacity for all sectors, including empty areas.

Rescue Media And Fortress Mode

Recovery preparation matters before a failure happens. O&O DiskImage provides recovery options for situations where normal Windows can no longer start.

Fortress Mode

Fortress Mode installs O&O DiskImage into the local Windows Recovery Environment. It is the fastest recovery option for the same PC because no separate USB stick is required.

Use Fortress Mode when:

- You want recovery built into the current computer.
- You need to restore the system drive even when Windows will not boot.
- You prefer not to depend on removable recovery media.

Fortress Mode depends on Windows Recovery Environment being available and enabled.

Bootable Rescue Media

Bootable rescue media starts O&O DiskImage outside the installed Windows environment. Use it when:

- The local recovery environment is unavailable.
- You need a USB stick or ISO that can be used on another PC.
- You are preparing for disk replacement or severe system failure.

Keep rescue media in a safe place and test that the computer can boot from it before you need it.

Recovery Checklist

- Create at least one full PC backup.
- Store the backup on external or network storage.
- Configure Fortress Mode or create rescue media.
- Confirm you know how to access firmware boot options if using USB media.
- Keep backup passwords available for encrypted backups.

Backup Sets And Tasks

O&O DiskImage separates restore-focused backup management from task-focused backup management.

Restore View

The restore view shows backup sets with backup files available for restore. Backups stored on disconnected destinations can remain visible so you can identify the storage you need to reconnect.

Use this view to:

- Restore files and directories.
- Restore drives or partitions.
- Mount a backup as a drive.
- Inspect backup metadata.
- Import existing backups.

Tasks View

The tasks view shows configured backup sets as runnable tasks. It includes backup sets that have never run or do not currently have backup files.

Use this view to:

- Run a backup again.
- Change a schedule.
- Rename a backup set.
- Delete a backup task.
- Review whether a task is manual, scheduled, or automatic.

Deleting Backups

Deleting backup files is permanent. If a backup chain uses incremental backups, deleting a required earlier file can make later restore points unusable. Use O&O DiskImage's delete workflow instead of removing files manually in Explorer.

Deleting a task does not necessarily remove all backup data and reports. O&O DiskImage can keep restore information available even when a task is removed from the task list.

Importing Existing Backups

If you have backups on external storage or from another PC, import them from the restore view. O&O DiskImage reads the backup metadata and adds them to the manageable backup list.

Reports And Logs

Reports and logs help you prove that backups ran and understand what happened when something goes wrong.

Reports

Reports are created automatically after backup, restore, and clone operations when report generation is enabled. A report contains the source, destination, data volume, duration, result, and any warnings or errors.

The **Reports** tab lets you:

- View report details.
- Open a report in the default text editor.
- Save a report as another file.
- Delete report files.
- Filter or review recent reports.

Reports remain useful even after the original task changes because they describe what the operation actually did.

Report Status

Status	Meaning
Successful	The operation completed without reported issues.
Completed with warnings	The operation completed, but one or more warnings should be reviewed.
Failed	The operation did not complete successfully.
Cancelled	The operation was stopped before completion.

Logs

Application logging records relevant events locally. Engine logging records lower-level disk imaging engine activity and is primarily intended for support diagnostics.

Enable logging only when needed or when support asks for it. Engine logging may require restarting the application before it takes effect.

What To Send To Support

When asking for help, include:

- Product version.
- Windows version.
- Backup source and destination type.
- The latest report for the failed operation.
- Application or engine logs if requested.
- Whether the operation was manual, scheduled, hotplug, or continuous.

Tools

The **Tools** page collects the utility features of O&O DiskImage that sit outside the guided backup, restore, and clone workflows. Tools are grouped by purpose so related actions stay together.

Screenshot pending

 The Tools page with its grouped tool cards

Placeholder image. Capture instructions are listed in [help/SCREENSHOTS.md](#) ([tools-overview.png](#)).

Tool Groups

Group	Tools
Backup Utilities	Validate a backup, Check and repair a backup, Import existing backups.
Virtual Disks	Mount a backup as a drive, Unmount a mounted backup, Convert to virtual disk, Create image from disk, Restore image to disk.
Network	Connect a network drive.
System	Open a command prompt.

Some tools are only available in the full (non-trial) product. Selecting a trial-gated tool opens an information dialog instead of running the tool.

Backup Utilities

Validate A Backup

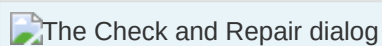
Validation checks a backup file for structural integrity after the fact, independently of the validation option used during a backup run. Use it when you want to confirm that an older backup on disk is still readable before you rely on it for a restore.

Check And Repair

Check and repair scans a backup file for damage and attempts to repair recoverable problems. Use it when a backup fails to open or validate, for example after a storage error or an interrupted transfer.

Check and repair works on the backup container. It cannot recover data that was never written or that was lost when the underlying storage failed. Keep a second backup copy for important data so a single damaged file is never your only restore point.

Screenshot pending



Placeholder image. Capture instructions are listed in `help/SCREENSHOTS.md` (`check-and-repair-dialog.png`).

Import Existing Backups

Import reads the metadata of a backup file that O&O DiskImage does not currently track — for example a backup created on another PC or found on reconnected external storage — and adds it to the manageable backup list so it can be restored. See Backup Sets And Tasks for how imported backups appear afterwards.

Virtual Disks

Mount Backup As Drive

Mounting makes the contents of a supported image backup available read-only in Windows Explorer, without restoring anything. It is the fastest way to copy a few files out of a large image backup. Mounted backups cannot be changed; they are for read access only.

Unmount Backup

Unmounting removes a previously mounted backup drive from Windows. Unmount backups you no longer need so the assigned drive letters are released.

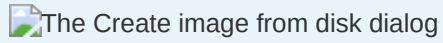
Convert To Virtual Disk

Conversion turns an O&O DiskImage backup into a Microsoft virtual disk file (VHD or VHDX) for use with virtualization tools or Windows' built-in virtual disk features. Virtual disk formats support fewer O&O DiskImage options than the native format.

Create Image From Disk

Creates an image directly from a selected disk or partition as a one-off operation, without configuring a reusable backup set. Use it for a quick ad-hoc image when you do not need a scheduled or managed backup.

Screenshot pending



Placeholder image. Capture instructions are listed in `help/SCREENSHOTS.md` (`create-image-from-disk-dialog.png`).

Restore Image To Disk

Writes an existing image back to a selected disk or partition as a one-off operation. This is a destructive action: the selected target is overwritten. Confirm the target carefully. For guided, managed restores use the Restore workflow instead.

Network

Connect Network Drive

Maps a network share to a drive letter so it can be used as a backup source or destination. Enter the UNC path and, if required, credentials. O&O DiskImage stores network secrets through Windows Credential Manager. See Backup Destinations for guidance on network destinations.

System

Command Prompt

Opens a Windows command prompt. This is intended for advanced diagnostics and support scenarios.

Settings Reference

The Settings dialog controls defaults for newly created backup sets and maintenance options for the application.

General

Controls language and application appearance. The application can follow the system theme or use a light, dark, or high-contrast mode.

Backup Strategy

Sets the default strategy for new backups:

- Full backup only.
- Full backup followed by incremental backups.
- Differential backups.

Existing backup sets keep their own settings unless you explicitly change them.

Execution Policy

Controls when a new full backup is created after a number of change backups. This is useful for limiting long dependency chains.

Retention Policy

Defines the maximum number of backup runs to keep. If disabled, backups are limited by available destination space. Retention is restricted for strategies where deleting a file would break the backup chain.

Backup Technology

Controls image creation technology:

- Used sectors.
- Forensic.
- Direct forensic.

Used sectors is recommended for normal backups.

Compression Method

Controls whether compression is enabled and which compression method is used. Standard Lempel-Ziv is the recommended default. Maximum and BZIP methods can save more space but take more time.

Backup Format

Controls the image file format:

- O&O DiskImage format.
- VHD.
- VHDX.

Use O&O DiskImage format for normal backup and restore workflows.

Validation

Controls whether backup files are checked after creation and whether validation is skipped for recovery partitions.

Report

Controls whether reports are generated for backup, restore, and clone operations.

Backup Destinations

Backup destinations are managed in the destination dialog. Supported types include local folders, USB drives, NAS or network shares, WebDAV, and S3-compatible storage.

File Names

Controls default storage paths and file name templates. Placeholders can insert date, time, user name, computer name, weekday, calendar week, default path, and extension.

Exclusion

Controls excluded files and folders. Use this for temporary files, caches, and data that should not be included in file backups.

Logging

Enables application logging. Use this when diagnosing problems.

Advanced

Contains support and maintenance options such as engine logging, re-reading backup information on the next start, and resetting user settings. Some advanced changes require restarting the application.

Common Issues

A Backup Destination Is Not Reachable

Check that the drive is connected, the network path is available, and credentials are current. For NAS destinations, use **Test connection** and confirm the UNC path, username, and password.

For S3 or WebDAV destinations, check the URL, SSL/TLS setting, bucket or base path, and authentication data.

A Scheduled Backup Did Not Run

Check the backup set in **Tasks**, then review the latest report. Confirm the PC was powered on, the destination was available, and the schedule is still active.

If the backup uses a network destination, confirm credentials are stored. If it uses a USB destination, confirm the expected drive is connected.

A Hotplug Backup Did Not Start

Connect the correct drive and wait for the configured start delay. If the drive was reformatted, relabeled, or replaced, manually run the backup once so O&O DiskImage can update the stored drive identity.

If multiple drives use the same drive letter, O&O DiskImage may reject the wrong drive when serial number, size, label, or model do not match.

A Backup Is Slow

Large first backups are expected to take longer. Performance depends on source disk speed, destination speed, compression method, validation, encryption, and network bandwidth.

To improve performance:

- Use incremental backups after the first full backup.
- Use standard compression instead of maximum compression.
- Schedule backups outside working hours.
- Use a faster USB, NAS, or network connection.
- Disable validation only if you understand the tradeoff.

Restore Target Is Too Small

Choose a larger target or reduce the restore scope. For partition restore, the target must fit the used data plus filesystem overhead.

Password Is Not Accepted

Encrypted backups require the exact original password. Check keyboard layout, capitalization, and whether the password was changed in your password manager. O&O DiskImage cannot restore encrypted data without the correct password.

Reports Are Missing

Confirm report generation is enabled in **Settings > Report**. If report files were deleted manually or from the Reports tab, existing backups remain but those specific reports are gone. Future operations will create new reports.

Frequently Asked Questions

General

Is there a Free Edition of O&O DiskImage 23?

No. This guide covers **O&O DiskImage 23 Premium Edition**. It does not describe a separate Free Edition.

Which backup should I create first?

For most users, the first backup should be **Back up your PC**. It protects the operating system, installed applications, settings, and personal data. After that, you can add more focused drive or file backups if you need them.

What is the difference between a backup set and a backup run?

A **backup set** is the stored configuration and history for a backup task. A **backup run** is one execution of that set. For example, a weekly PC backup is one backup set; each weekly result is a backup run in that set.

Where should I store backups?

Use storage that is separate from the source data. A USB drive, NAS share, WebDAV destination, or S3-compatible storage is safer than another folder on the same internal disk. If the system disk fails, a backup stored on that same disk may be lost with it.

Backup Options

Should I use full, incremental, or differential backups?

Use **incremental** for regular protection because it creates one full backup first and then stores only changes. Use **differential** when you want each change backup to depend only on the last full backup. Use **full** when each backup must stand on its own and storage space is less important.

Why is used-sectors imaging recommended?

Used-sectors imaging backs up only the sectors that contain data. It is usually much smaller and faster than a forensic image. Use forensic options only when you need a bit-precise copy of the entire source, including empty sectors.

Can encrypted backups be restored without the password?

No. If you set a password, keep it in a safe place. Without that password, the backup cannot be restored.

Why are VHD and VHDX options limited?

VHD and VHDX are virtual disk formats. They are useful when you want Windows or virtualization tools to mount a backup as a virtual disk, but they do not support all O&O DiskImage options. The O&O DiskImage format is the recommended format for normal backup and restore workflows.

Scheduling

Can O&O DiskImage run backups automatically?

Yes. A backup set can run once, daily, weekly, hourly, continuously, or when the configured backup drive is connected.

What does continuous backup mean?

Continuous backup starts another backup after the previous one completes and the configured interval has passed. It can be useful for very active critical data, but it can also consume storage, CPU, disk I/O, and network bandwidth quickly.

What is hotplug backup?

Hotplug backup starts when the configured USB or removable backup drive becomes available. O&O DiskImage stores more than just the drive letter when possible, including drive identity information such as serial number, label, size, and model, so the wrong drive is less likely to trigger the backup.

Restore And Recovery

Can I restore only one file?

Yes. For file backups, you can restore the entire backup or select individual directories and files. For image backups, you can mount supported backup files as read-only drives and copy out files with Windows Explorer.

Can I restore to a smaller partition?

A restore target must have enough room for the used data plus required filesystem overhead. O&O DiskImage checks target size before restore and warns when the target is too small.

What is Fortress Mode?

Fortress Mode installs O&O DiskImage into the local Windows Recovery Environment. It lets you start recovery on the same PC even if normal Windows no longer starts, without requiring a separate USB recovery drive.

Troubleshooting

A scheduled backup did not run. What should I check?

Confirm that the PC was available, the destination was reachable, credentials were stored for network destinations, and the backup set still exists. Then open **Reports** to check the last result and enable logging if support needs more detail.

My NAS backup asks for credentials.

Enter the username and password for the network share in the backup options or destination settings. Credentials are stored through Windows Credential Manager so scheduled and manual backups can access the share after reboot.

The backup drive is full.

Review retention policy, reduce backup frequency, switch from full to incremental backups where appropriate, or use a larger destination. Do not delete random files from an incremental chain unless you are sure no later backups depend on them.

Online Documentation

This documentation is built with Docusaurus and lives in `docusaurus/oodipe` .

Structure

Folder	Purpose
<code>docs/getting-started</code>	Onboarding and first-backup guidance.
<code>docs/core-concepts</code>	Sources, destinations, and terminology.
<code>docs/backups</code>	Backup options, schedules, naming, and exclusions.
<code>docs/restore</code>	File, drive, partition, and image restore workflows.
<code>docs/clone-and-recovery</code>	Cloning, rescue media, and Fortress Mode.
<code>docs/management</code>	Backup sets, tasks, reports, and logs.
<code>docs/settings</code>	Settings reference.
<code>docs/troubleshooting</code>	Common issues and diagnosis.

Terminology

Use the same terms as the application:

- **Backup** for file-level protection.
- **Image** for drive or partition imaging.
- **Destination** for storage where backups are saved.
- **Target** for drives, partitions, or folders that receive restored or cloned data.
- **Backup set** for a stored backup configuration and its history.
- **Backup run** for one execution of a backup set.

Local Development

From `docusaurus/oodipe` :

```
npm install  
npm start
```

Build the static site with:

```
npm run build
```

Generate the PDF manual with:

```
npm run build:pdf
```