

O&O software

O&O DiskImage

Table of Contents

1 Introduction 4

2 Get started 5

2.1 System requirements 5

2.2 Install and activate 7

2.3 Quick start 9

2.4 The first backup 11

3 Concepts 14

3.1 Backup sources 14

3.2 Backup destinations 17

4 Back up 20

4.1 Backup options 20

4.2 Schedules and automation 23

4.3 File names and exclusions 25

4.4 Second copy 26

5 Restore 28

5.1 Restore overview 28

5.2 Restore files 31

5.3 Restore drives 33

6 Clone and recovery 36

6.1 Clone drives 36

6.2 Rescue media and recovery environment 38

7 Management 41

7.1 Backup plans and saved backups 41

7.2 Reports and logs 44

7.3 Tools 46

8 Settings 55

9 Glossary 59

10 Troubleshooting 61

11 FAQ 64

12 Support and more from O&O 66

Introduction

This guide explains how to back up a Windows PC, restore data, clone disks, and prepare for recovery with **O&O DiskImage 23 Premium Edition**.

Start by choosing what to protect, where to store the backup, and when it should run. A backup plan keeps those choices together with the history and other options.

What you can do

- **Back up an entire PC**, selected drives and partitions, or individual files and folders.
- **Keep a backup history** with daily, weekly, and monthly restore points, or custom retention rules.
- **Keep a second copy** on another drive, a network share, S3-compatible storage, or WebDAV.
- **Automate backups** with one-time, daily, weekly, monthly, hourly, continuous, or drive-triggered schedules.
- **Restore files, partitions, or whole disks**, including from an available second copy.
- **Work with virtual disks**, including VHD/VHDX backups and supported Hyper-V checkpoints.
- **Clone a disk** when replacing or migrating a drive.
- **Prepare recovery access** using the local recovery environment or bootable startup media.
- **Review reports and notifications** to check completed operations and diagnose failures.

Where to start

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

Before you need to restore Windows, prepare and test the recovery environment or startup media.

This guide covers the Premium Edition. The trial identifies restricted tools on the relevant pages and provides links to purchase or activate a license.

System requirements

O&O DiskImage 23 backs up and restores Windows PCs. This page lists what the computer, the backup storage, and the recovery options need. For the supported Windows versions, see the O&O DiskImage product page.

Computer

Requirement	Details
Operating system	Windows. O&O DiskImage backs up the running Windows system, its applications, settings, and personal data.
Background service	Installed with the application. It runs schedules, second copies, and email notifications. Application and service versions must be compatible; otherwise schedules are suspended.
Notification-area application	Needed for drive-triggered backups. It also lets administrators start plans or cancel operations without opening an elevated main window.
Power	Connect a portable PC to power for backups. The computer is kept awake during backups and transfers.
Wake timers	Allowed in the active Windows power plan if a schedule should wake the computer from sleep.

Backup storage

Requirement	Details
Separate disk	An external drive, a USB drive, or a network share (NAS). Store backups on a different physical disk from the data they protect; the Windows disk is not suggested as a destination.
Free space	Enough for the initial full backup, the history, and temporary space during later runs. Forensic backups need space for the full source size.
Network share	A UNC path with a valid server and share name, credentials, and write permissions.
VHD/VHDX backups	Source volumes available for exclusive access and a destination on another physical disk.

Second copy

A second copy needs another physical disk or a remote destination:

- **Network share**: UNC path, credentials, and write permissions.
- **S3-compatible storage**: endpoint, bucket, region, access keys, and any path prefix.
- **WebDAV**: server address, folder, and credentials.

Uploads use the computer's proxy settings through the background service. Use HTTPS for transfers over the internet.

Recovery

Option	Requirement
Local recovery environment	A working local Windows Recovery Environment (WinRE) on the computer.
Startup media	A USB device that may be formatted, or an ISO file. The computer must be able to boot from the medium.
License verification	Internet access if the recovery environment needs to verify the license; a wired network connection is recommended.

See Rescue media and recovery environment.

Next steps

- Install and activate
- Quick start

Install and activate

Check the system requirements before installing O&O DiskImage 23. Product information is available on the O&O DiskImage product page.

Installed components

Component	Purpose
Application	Sets up backup plans, restores, clones, tools, and settings.
Background service	Runs time-based schedules, second copies, cleanup of old versions, and email notifications, even when the main window is closed.
Notification-area application	Shows progress, starts plans, cancels operations, and detects drives for drive-triggered backups.

After installing, open **Recovery** and prepare the local recovery environment or startup media before you need them. See Rescue media and recovery environment.

Trial and license

The trial restricts some features, for example cloning and some tools. The affected pages explain the restriction and provide links to purchase a license or activate one.

To activate O&O DiskImage, select the activation link on one of these pages. Unmounting backups remains available in the trial.

In the recovery environment, license verification may need internet access. Use a wired network connection where possible.

After an update

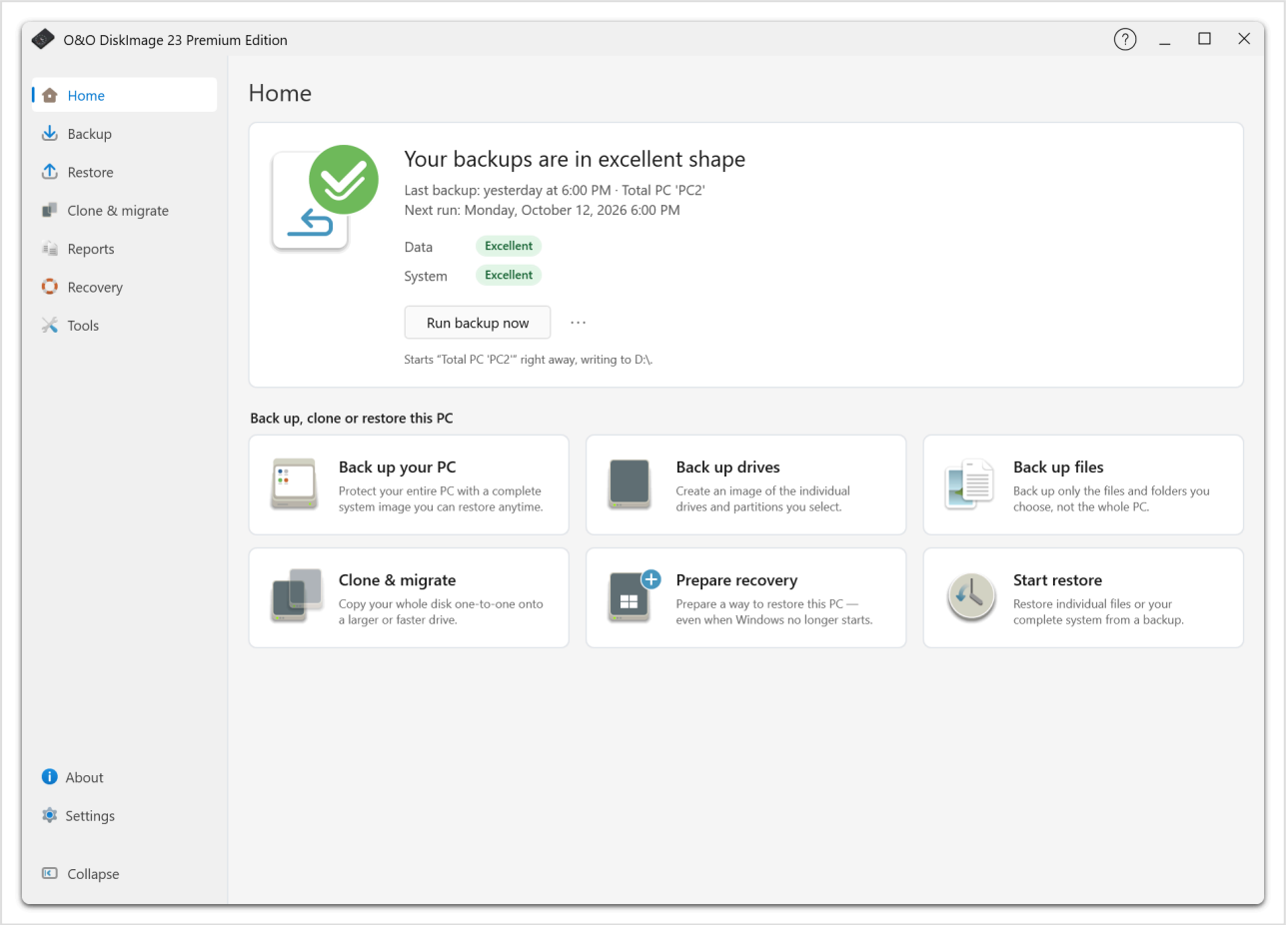
- If the application and the background service versions are incompatible, schedules are suspended and the application shows update guidance. Until the service is updated, a manual backup can run in the application where available.
- If the application reports that the service version cannot upload to S3 or WebDAV, update the service.
- Open **Recovery** and check the status. Rebuild the local recovery environment if the page reports that it is outdated.
- Existing plans keep their retention rules until you change them.

Next steps

- Quick start
- The first backup

Quick start

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



Home shows the backup status and actions for backup, cloning, and recovery.

Before you start

Connect an external backup drive or prepare a network share. Keep enough space for the initial full backup and later versions, and connect a portable PC to power.

Create the first backup

1. Open **O&O DiskImage 23 Premium Edition**.
2. Choose **Backup > Entire PC**.
3. Review **What** and choose the destination under **Where**.
4. Review **When**. Automatic backup is enabled by default: on connection for an external drive, or daily at 18:00 for other destinations.

5. Open **More options** to review history, encryption, and validation. Set a password now if you need encryption.
6. Choose to run the first backup now and select **Start backup**.
7. Open **Reports** after completion and check the result and any second-copy warnings.

A practical starting point

Setting	Starting point
Scope	Entire PC
Destination	External drive or NAS
History	One month, if the storage estimate fits
Method	Automatic
Format and technology	O&O DiskImage format, used sectors
Compression	Standard Lempel-Ziv
Validation	Enabled
Second copy	Another disk or a remote destination

You can adjust the plan later. See The first backup for the available controls.

Prepare for recovery

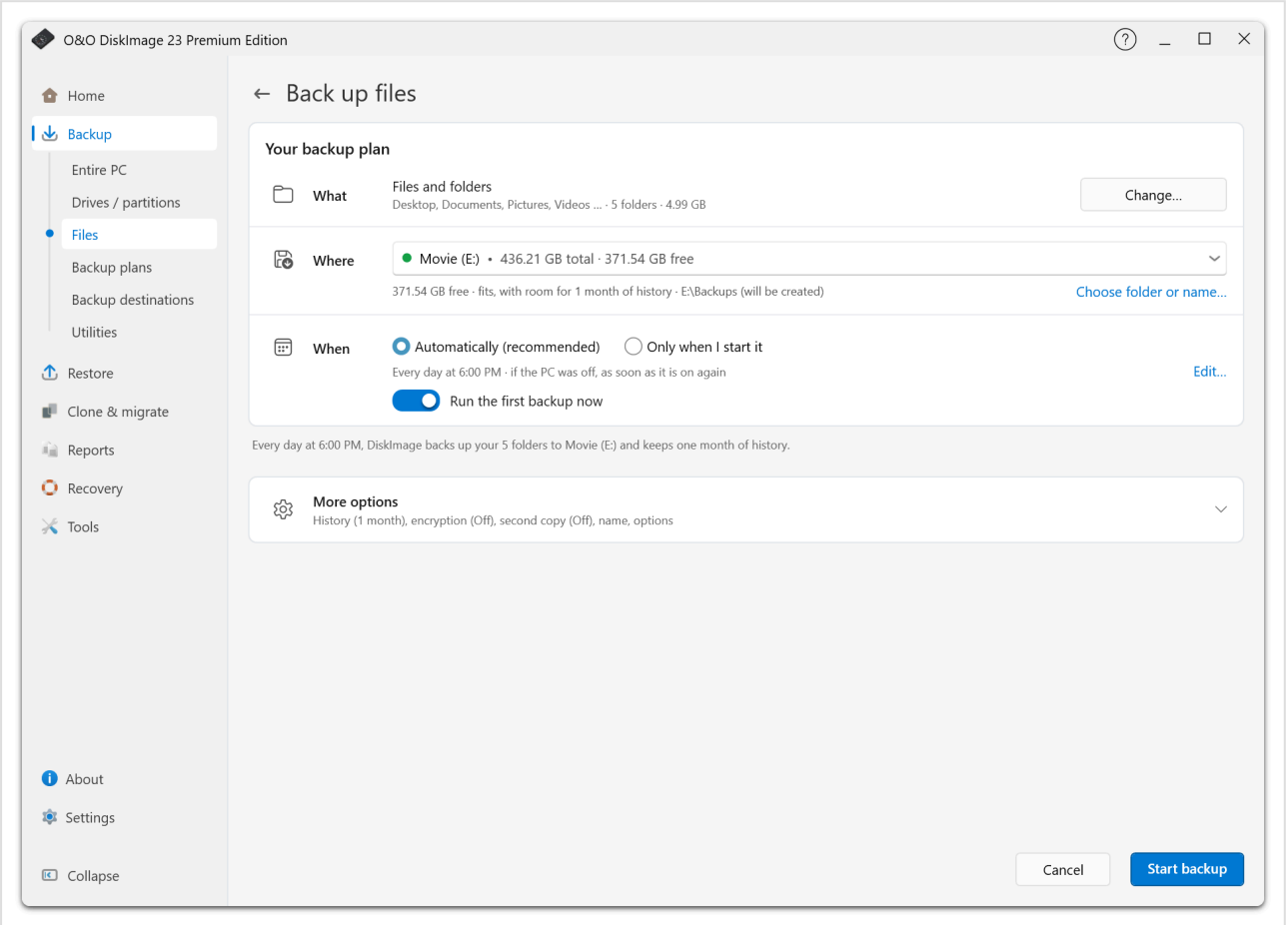
Open **Recovery** to set up the local recovery environment or create bootable startup media. Test that the PC can start from your chosen recovery option and that you can reach the backup.

The status cards on **Home** and **Restore** summarize backup protection, available history, and recovery startup options. Follow their suggestions if a backup is missing or the recovery environment needs to be rebuilt.

See Rescue media and recovery environment.

The first backup

The backup plan page brings together **What**, **Where**, and **When**. Review these rows, adjust **More options** if needed, then start the backup or save the plan.



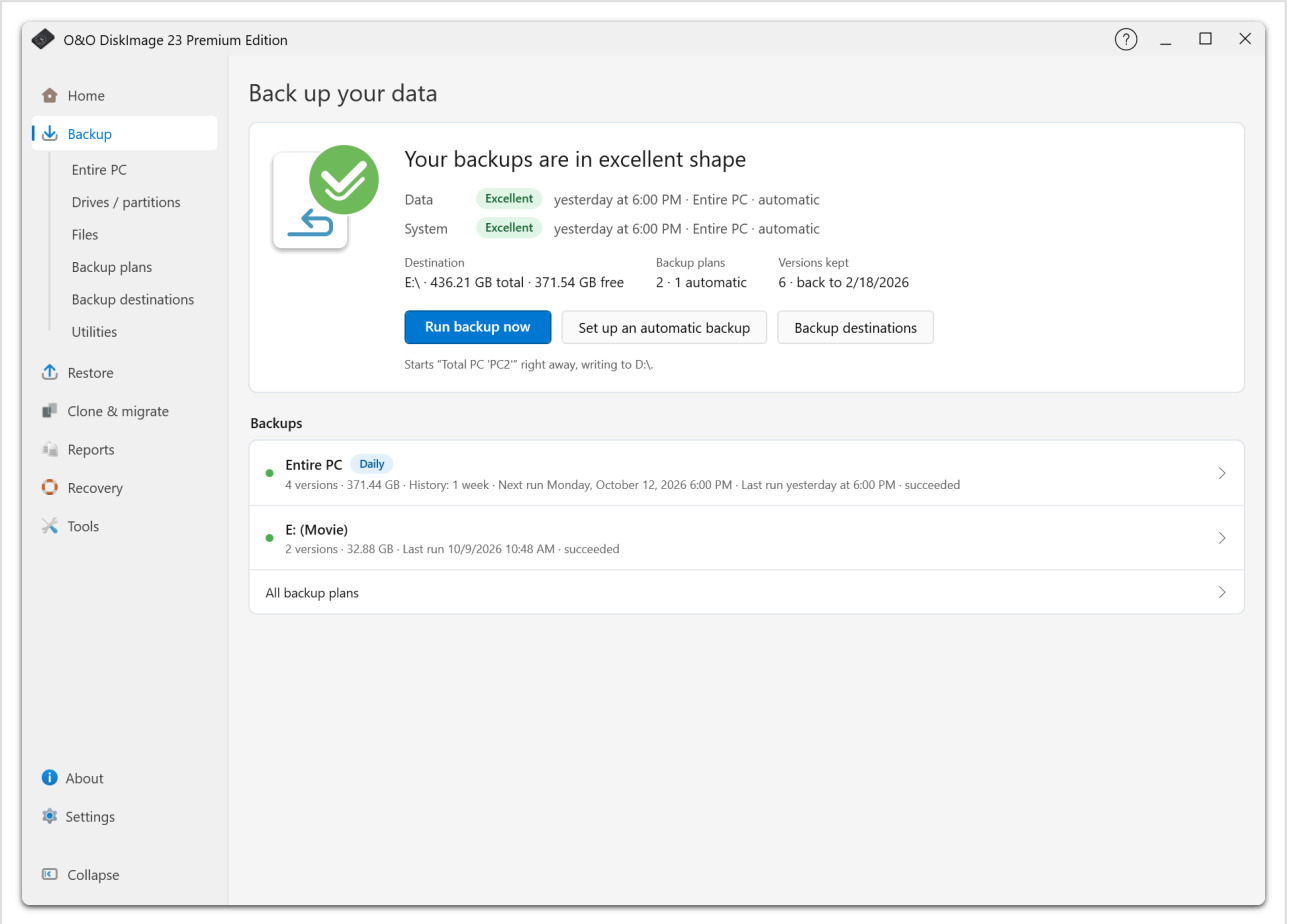
Example file backup: the plan brings together the source, destination, and schedule under What, Where, and When.

Choose what to back up

Under **Backup**, choose one of the source types in the navigation pane:

Choice	Use it for
Entire PC	Windows, applications, settings, and personal data.
Drives / partitions	An image of selected disks or partitions.
Files	Selected files and folders.

For drives or files, select the sources before reviewing the plan. You can return to the selection using **Change…** in the **What** row.



The backup overview shows existing plans and actions for starting or setting up a backup.

Choose where to store it

Choose an external drive or a network share with enough space. For an entire-PC backup, O&O DiskImage suggests external or network storage first and does not suggest the Windows disk.

Enter network credentials when prompted and test the connection. Under **Where**, you can also set up a second copy, including an upload to S3 or WebDAV after the primary backup is created.

Choose when it runs

New plans start with **Automatically (recommended)**. For an external drive, the backup runs when the drive is connected, at most once a day. Otherwise it runs daily at 18:00 and catches up missed runs.

Use **Edit…** to change the schedule, or select **Only when I start it**. Leave **Run the first backup now** selected if you want an immediate backup as well as an automatic plan.

Review more options

- **History**: choose how far back you want to restore and review the storage estimate.
- **Encryption**: set a password before the first backup.
- **Validation**: check the finished backup for integrity and readability.
- **Name**: choose how the plan appears in the plan list.
- **Format and other options**: adjust compression, naming templates, exclusions, backup technology, and reports.

See Backup options for restrictions and details.

Start and check the result

Select **Start backup** to run now, or **Save plan** if the first run should wait for its schedule. The progress window shows the current operation and allows cancellation. Its compact view keeps the status and action buttons visible.

After completion, open **Reports** and review any warnings. If you enabled a second copy, check its result too: a successful primary backup does not mean the copy has finished uploading.

The plan list lets you change the schedule or start another run later.

Backup sources

A source is the data a backup protects. Choose **Entire PC**, **Drives / partitions**, or **Files** under **Backup** in the navigation pane.

Entire PC

An entire-PC backup protects Windows, installed applications, settings, and personal data. Use it as the starting point for system recovery.

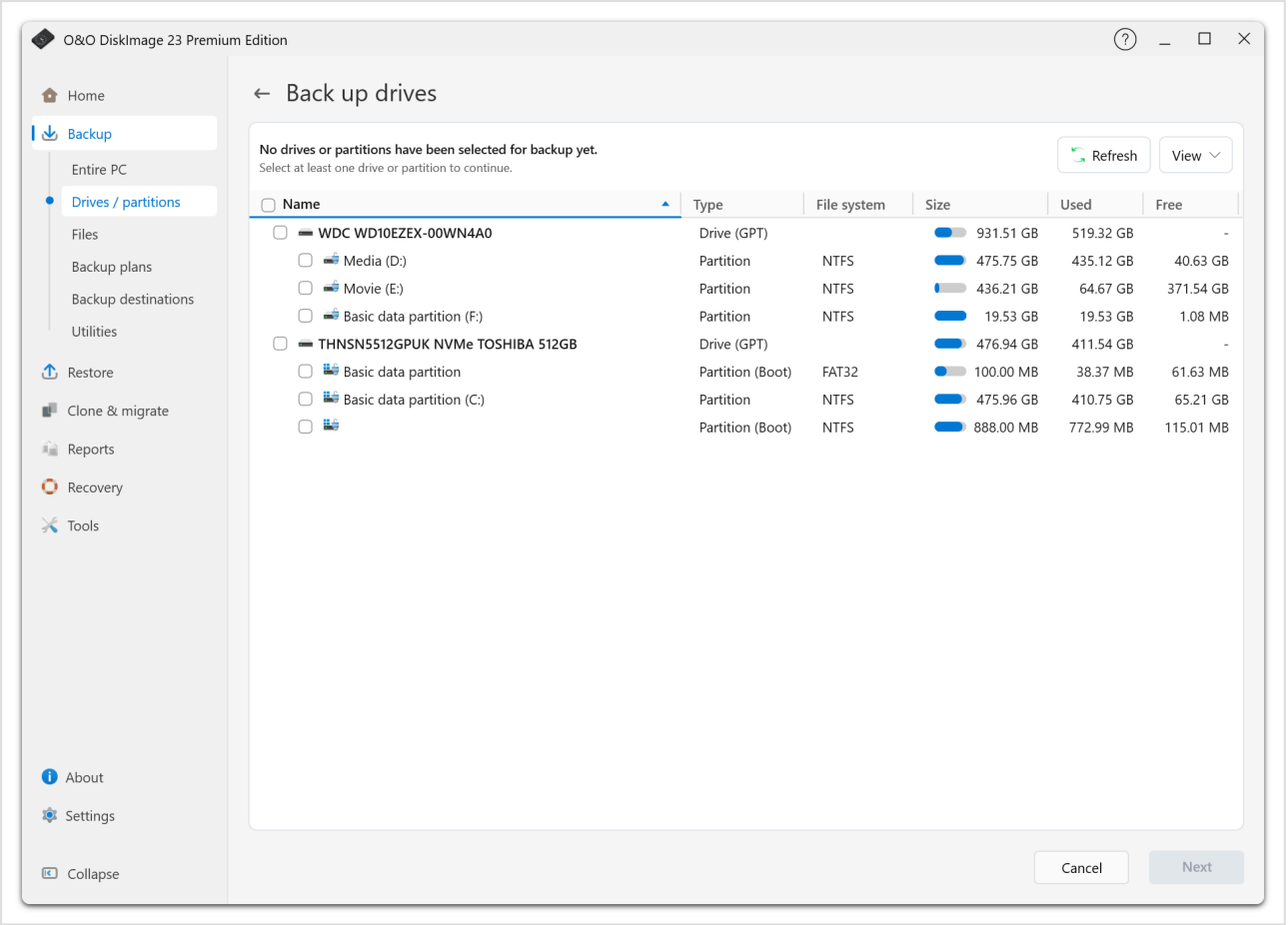
O&O DiskImage avoids imaging a destination disk that contains only backups. A destination disk that also contains other data may remain in the source selection so that data is protected. The report lists disks excluded from an entire-PC backup. Review the sources and destination rather than assuming every attached disk is included.

Drives and partitions

Select whole disks or individual partitions when you need more control. The list identifies whole-disk sources as disks; a disconnected source remains recognizable instead of appearing as an unattached tiny partition.

Use the **View** menu to adjust the display or show the disk map. The **Type** column identifies partition roles.

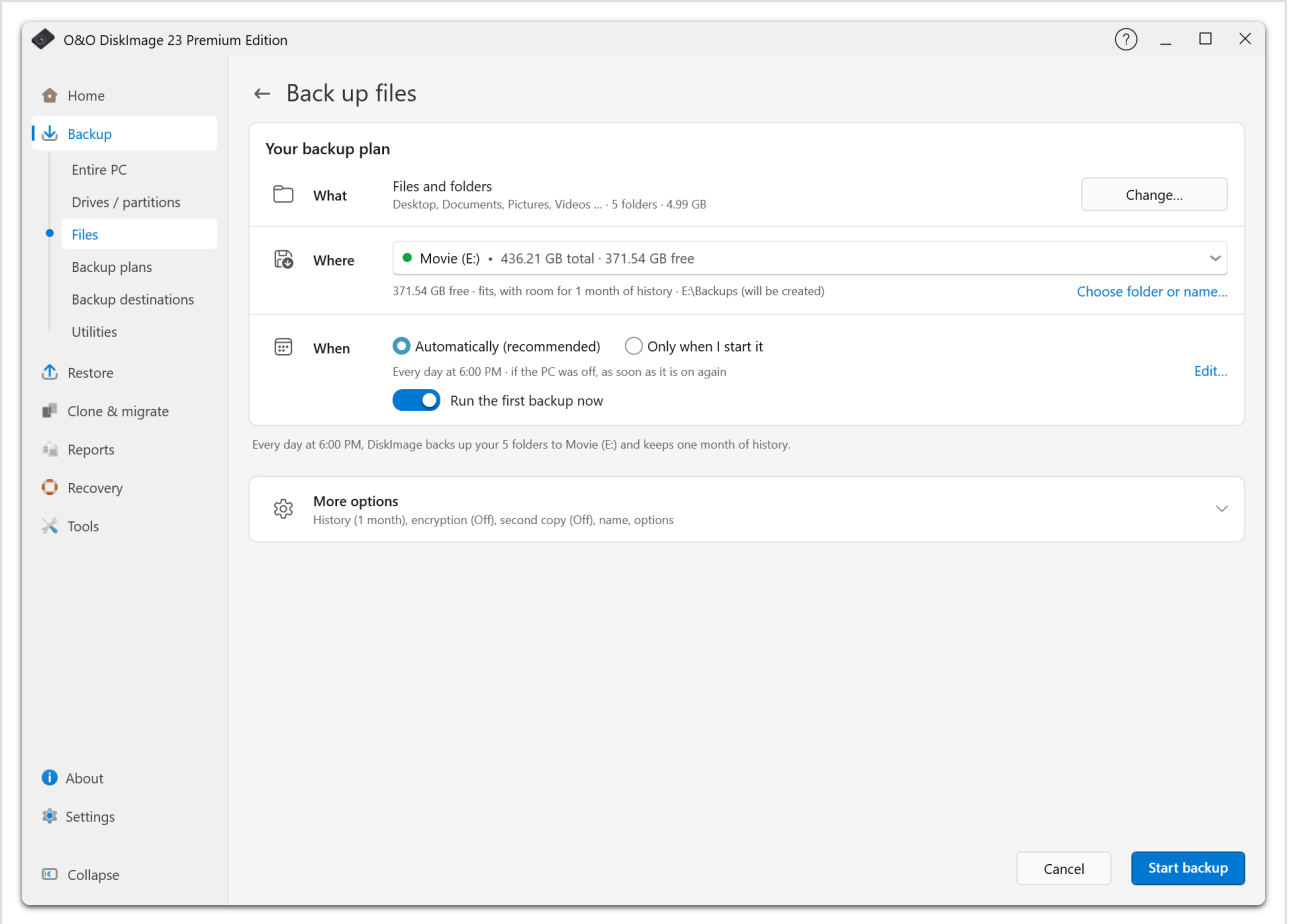
An image normally copies used sectors. Forensic modes copy the full source, including unused sectors. See Backup options for format and technology restrictions.



Select the disks or partitions to back up from the drive list.

Files and folders

Choose individual files or folders for documents, projects, and other data that does not need a complete disk image. File backups do not replace a system image for restoring Windows and installed applications.



Example file backup: the plan brings together the source, destination, and schedule under What, Where, and When.

Change sources

Open an existing drive or file plan and select **Change…** beside **What**. Review and save the new selection. The next backup is a full backup so that later versions can build on the changed sources. Cancelling the plan page discards the changes.

Default exclusions

Temporary files, paging and hibernation files, system volume information, and O&O DiskImage backup containers are excluded where applicable.

Virtual disks such as VHD/VHDX files are included by default. O&O DiskImage's own virtual-disk backups remain excluded to prevent a backup from including itself. A warning appears if an exclusion rule would omit all virtual disks on a drive.

Review exclusions before the first backup; they are locked once the plan has saved versions. See File names and exclusions.

Backup destinations

The destination stores your backup. Choose enough space for the initial full backup, its history, and any temporary space needed during later runs.

Destination types

Destination	Use
Local or external folder	Stores the primary backup on a disk accessible to Windows.
USB drive	Stores the primary backup and can trigger a run when connected.
NAS / network share	Stores backups in a UNC folder such as `\\server\share`.
WebDAV	Receives a second copy after the primary backup is created.
S3-compatible storage	Receives a second copy in a configured bucket and path.

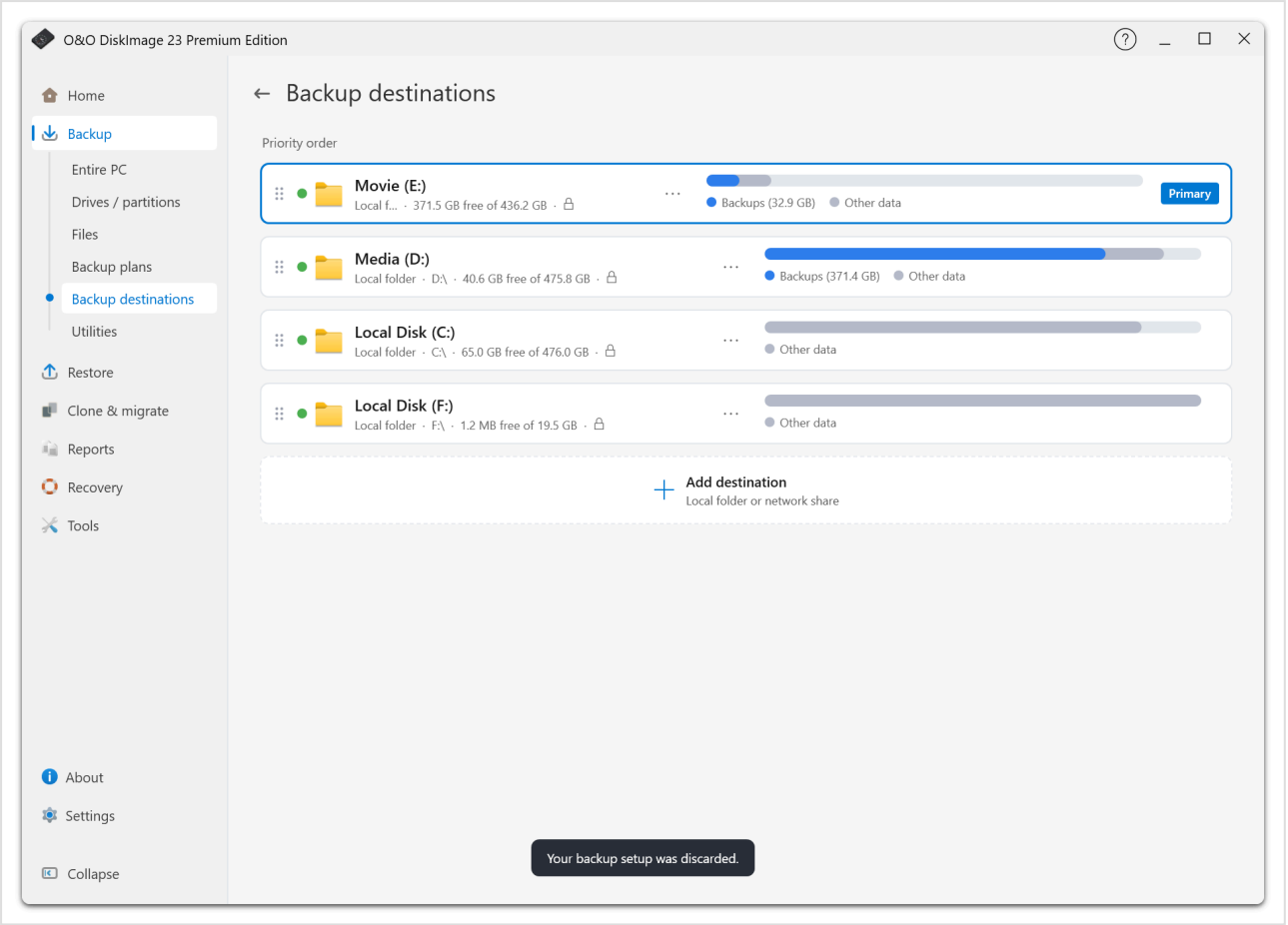
For cloud protection, create the primary backup in a local or network folder and configure a second copy to S3 or WebDAV. Adding a cloud destination does not turn it into a folder that the imaging engine can write to directly.

Choose and organize destinations

Open the backup destinations dialog to add or edit storage and set a primary destination. Availability, free space, total size, and backup usage are shown where the destination provides that information.

Drag destinations by their handles to change their order. For entire-PC backups, automatic suggestions favor external and network storage, then suitable other disks. The Windows disk is not suggested as a destination.

Store backups on a different physical disk from the data they protect. Another partition on the same disk will be lost if that disk fails.



Backup destinations show drive priority, storage usage, and the primary destination.

Network credentials

For a network share, enter its UNC path, username, and password. Credentials are stored through Windows Credential Manager and associated with the intended server.

Use **Test connection** after setup or a password change. Check both access and write permissions. Network paths must contain a valid server and share name.

S3 destinations need the endpoint, bucket, region, access keys, and any path prefix; WebDAV destinations need the server address and credentials. Cloud upload and proxy details are covered under Second copy.

USB drive detection

O&O DiskImage uses available drive identity information, including serial number, volume name, size, and model. This reduces the risk of a different drive with the same letter triggering a backup.

Keep the notification-area application running for drive-triggered backups. You can disconnect an external backup drive after the backup and all copying have finished.

Space and availability

Use the plan's history estimate to check whether the destination has enough room. Retention preserves required backup-chain files, so it may not immediately reclaim every older file.

Reconnect unavailable storage before restoring. If the original destination has failed, use an available second copy.

Backup options

Open **More options** on the backup plan page to choose how much history to keep, set a password, and enable validation. The format and compression options also contain file names, backup technology, exclusions, and report settings.

Backup history

Choose **How much backup history do you want to keep?** to control which versions remain available for restore.

Choice	Versions kept
1 week	Daily versions for seven days with backups.
1 month	Daily versions for seven days, plus weekly versions for four weeks with backups.
3 months	Daily and weekly versions as above, plus monthly versions for three months with backups.
1 year	Daily and weekly versions as above, plus monthly versions for twelve months with backups.
Keep everything	No automatic deletion. You manage the available space yourself.
Custom	Your own daily, weekly, monthly, and yearly history, a fixed number of versions, or no automatic deletion.

History uses periods in which backups actually ran. Time spent with the PC switched off does not by itself erase the history. The presets also keep at least the three newest versions. Older files needed by a retained version remain available, so the number of files on disk can exceed the number of restore points you selected.

The estimated storage requirement helps you choose a history that fits the destination. It is an estimate, not a reservation of space. If space is tight, choose a shorter history or another destination.

Open the backup's history to see why versions are kept and which are due for removal. You can keep individual versions permanently. After successful scheduled backups, the background service removes eligible old versions even when the main application is closed. Existing plans retain their previous retention rules until you change them.

Backup method

Method	What is stored	Files needed for restore
Full	All selected data on every run.	That full backup.
Incremental	Changes since the previous backup, after an initial full backup.	The full backup and every required incremental version up to the selected one.
Differential	Changes since the last full backup.	The full backup and the selected differential version.

The automatic method uses incremental backups between regular full backups. In **Custom**, choose the method yourself if you need differential backups or full backups only.

New full backups

With the automatic method, a one-week history starts a new full backup on the first run of each week. Longer presets start one on the first run of each month. These settings choose the backup method; they do not create extra scheduled runs.

Custom settings can start a new full backup weekly, monthly, after a chosen number of change backups, or only when a usable full backup is needed. A weekday-specific backup method in the schedule applies only when you choose the method yourself.

Make this a full backup starts a new chain for one run without changing the plan's usual method. A full backup may also be required after changing sources or when the previous backup cannot be used. The report explains the reason.

Backup technology

Technology	Meaning
Used sectors	Copies sectors containing data. Suitable for ordinary backups.
Forensic	Copies the entire source, including unused sectors.
Direct forensic	Reads directly from the disk; available in the recovery environment.

Forensic images need space for the full source size, rather than just its used data.

Backup format

The **O&O DiskImage format** supports the normal backup options, including compression, encryption, and change backups. Use it to back up the running Windows system.

VHD and **VHDX** are Microsoft virtual disk formats. O&O DiskImage supports whole-disk backup and restore, mounting, validation, and browsing supported virtual disks, including Hyper-V checkpoints (`.avhd` and `.avhdx`). Keep a checkpoint's parent files available.

VHD/VHDX creation uses full backups and used sectors, without O&O compression or password encryption. Source volumes must be available for exclusive access, the destination must be on another physical disk, and the disk containing the running Windows installation cannot be captured this way. Close applications using the source or use the O&O DiskImage format for a live backup. The plan page explains unsuitable source selections.

Compression

Compression is enabled by default for the O&O DiskImage format. Standard Lempel-Ziv is a good general-purpose choice. Maximum Lempel-Ziv and BZIP options can save more space but take longer. ZIP deflate is available for file backups, not disk images. VHD/VHDX do not use these compression settings.

Encryption

Set the password before creating the first backup. Keep it in a password manager or another safe place: encrypted backups cannot be restored without the original password.

Once a plan has saved versions, its encryption, password, image format, backup technology, and exclusions are locked, including while those versions are offline. Create a new plan to use different settings. History, compression, validation, reports, and naming templates remain editable.

If a stored password is no longer available to the application, re-enter the original password on the plan page. This restores access; it does not change the password. Backups are blocked until the password is available.

Validation

Enable the option to check the backup afterwards to verify its integrity and readability. Validation reads the backup without restoring data or changing the source. It adds time to the operation and does not replace a recovery test.

You can also check an existing backup under **Restore > Utilities**. Recovery partitions are included in validation; the former option to skip them has been removed.

Schedules and automation

Choose when a plan runs in the **When** row of the plan page. **Automatically (recommended)** is selected for new plans: an external backup drive triggers a backup when connected, at most once a day; other destinations use a daily schedule at 18:00 with missed runs caught up. Select **Edit…** to change this.

Choose **Only when I start it** for manual backups. With an automatic plan, **Run the first backup now** lets you create the first backup immediately as well as save the schedule.

Schedule types

Type	Behavior
Once	Runs at the selected date and time.
Daily	Runs every selected number of days at the chosen time.
Weekly	Runs on selected weekdays, with an optional interval of several weeks.
Monthly	Runs on the day of the month given by the start date. In shorter months it runs on the last day.
Hourly	Runs at the chosen interval, starting at the selected time.
Continuous	Starts another backup after the previous run and the configured interval.
When the backup drive is connected	Runs when the configured drive becomes available.

Time-based and drive-triggered schedules are alternatives for the same plan. The start and end dates limit when a schedule is active.

Hourly and continuous backups

Frequent backups suit small datasets that change often. Allow time for the backup and any second copy to finish, and check the storage estimate. Full backups at short intervals can fill a destination quickly.

Drive-triggered backups

The notification-area application detects the configured drive and asks the background service to run the backup. Keep that application running; the plan page warns if it is closed.

Drive matching uses available identity information, such as serial number, volume name, size, and model, rather than only the drive letter. You can set a delay after connection and a minimum interval between runs.

Missed and overlapping runs

Enable **Run the backup as soon as possible after a scheduled start is missed** to catch up after the PC was unavailable. A missed backup to an external drive can run when that drive is reconnected.

Scheduled network backups wait up to three minutes for the destination to become reachable, allowing time for a sleeping NAS or network connection to recover. If it remains unavailable, review the failure report.

Backups that would conflict with another backup, restore, or clone wait until the active operation finishes. A manual start from the notification area can instead be refused with an explanation. The report distinguishes the scheduled time from the actual start.

Wake from sleep

Wake the computer from sleep to run this backup is off by default. Enable it in the schedule if needed, and allow wake timers in the active Windows power plan. This option does not wake a shut-down PC or a PC in hibernation.

The computer is kept awake during backups and transfers. Letting the display turn off is a separate option under **Settings > General**.

Background service and notification area

Time-based schedules run through the background service even when the main window is closed. The notification-area menu shows progress and lets administrators start plans or cancel operations without opening an elevated main window.

If the application and service versions are incompatible, schedules are suspended and the application shows update guidance. Where available, a manual backup can run in the application until the service is updated.

Automatic shutdown is skipped after cancellation and for backups started from the notification-area menu.

File names and exclusions

Use naming templates to keep backups organized and exclusions to leave out data you do not need.

File name templates

Open the plan's format and other options, then **File names**. Templates can include the date, time, user name, computer name, and extension. For example:

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

The storage-folder template can also contain placeholders. Keep folder structures short and predictable, especially on network shares. Changing the application's language does not rename existing plans' files and folders.

Global templates under **Settings > Defaults for new backups > File names** apply to new plans. Adjust an existing plan directly to change its future file names.

Exclusions

Open **Contents** in the backup options to review excluded files and folders. Supported entries include a full file path, a folder path, a wildcard such as `*.tmp`, or a path fragment such as `\System Volume Information\`.

Common temporary files, paging and hibernation files, and DiskImage backup containers are excluded where applicable. Virtual disks such as VHD/VHDX files are included by default, while DiskImage's own virtual-disk backups remain excluded. Review any warning that a rule excludes all virtual disks on a drive.

Folder exclusions also apply to their contents. Excluded files cannot be recovered from that backup and are not offered in its restore browser.

Change exclusions

Choose exclusions before the first backup. Once a plan has saved versions, its exclusion list is locked even if the destination is disconnected. Create a new plan if you need a different list.

Avoid storing backup files inside the source folders. Do not exclude Windows system folders from an entire-PC image unless you understand how that affects recovery.

Second copy

A second copy protects against losing the drive that holds your primary backup. After a successful backup, the background service copies it to another drive, a network share, S3-compatible storage, or a WebDAV server.

Set up a second copy

1. Open the backup plan and find the second-copy option under **Where**.
2. Enable the option and choose a destination.
3. For a network or cloud destination, enter the connection settings and use **Test connection**.
4. Enable checking the copy after writing it if needed.
5. Save the plan or start the backup.

Choose a different physical disk or a remote destination. A second folder on the same disk does not protect against that disk failing. The primary backup folder cannot also be its second-copy folder.

The background service must be available. Update it if the application says its version cannot upload to S3 or WebDAV.

Cloud copies

The primary backup is created in a local or network folder first. The copy then uploads in the background. Progress appears on the backup card and in the Windows notification area. S3 uploads can resume after an interrupted connection, sleep, or a restart.

For S3, supply the endpoint, bucket, region, access keys, and any path prefix. For WebDAV, supply the server address, folder, and credentials. The connection test checks access and write permissions. Uploads use the computer's proxy settings through the service; a successful interactive test may not cover a different service proxy configuration.

Use HTTPS for transfers over the internet. Encrypt the backup before its first run if the remote copy must also be password-protected. Transport encryption alone does not encrypt the stored backup.

History and dependencies

The copy includes earlier versions required to restore the selected backup. When the plan's history removes expired versions, the corresponding versions are removed from the second destination too. Deletions can be caught up when a disconnected destination returns.

The second copy therefore follows the plan's history. Use separate archival storage if you need versions preserved independently of those deletion rules.

If the copy fails

Second copy missing means the primary backup completed but its copy failed or was cancelled. The primary backup can still be restored. Review the reason, reconnect the destination or correct its credentials, and select **Retry copy**.

Do not disconnect a destination while its copy is still in progress.

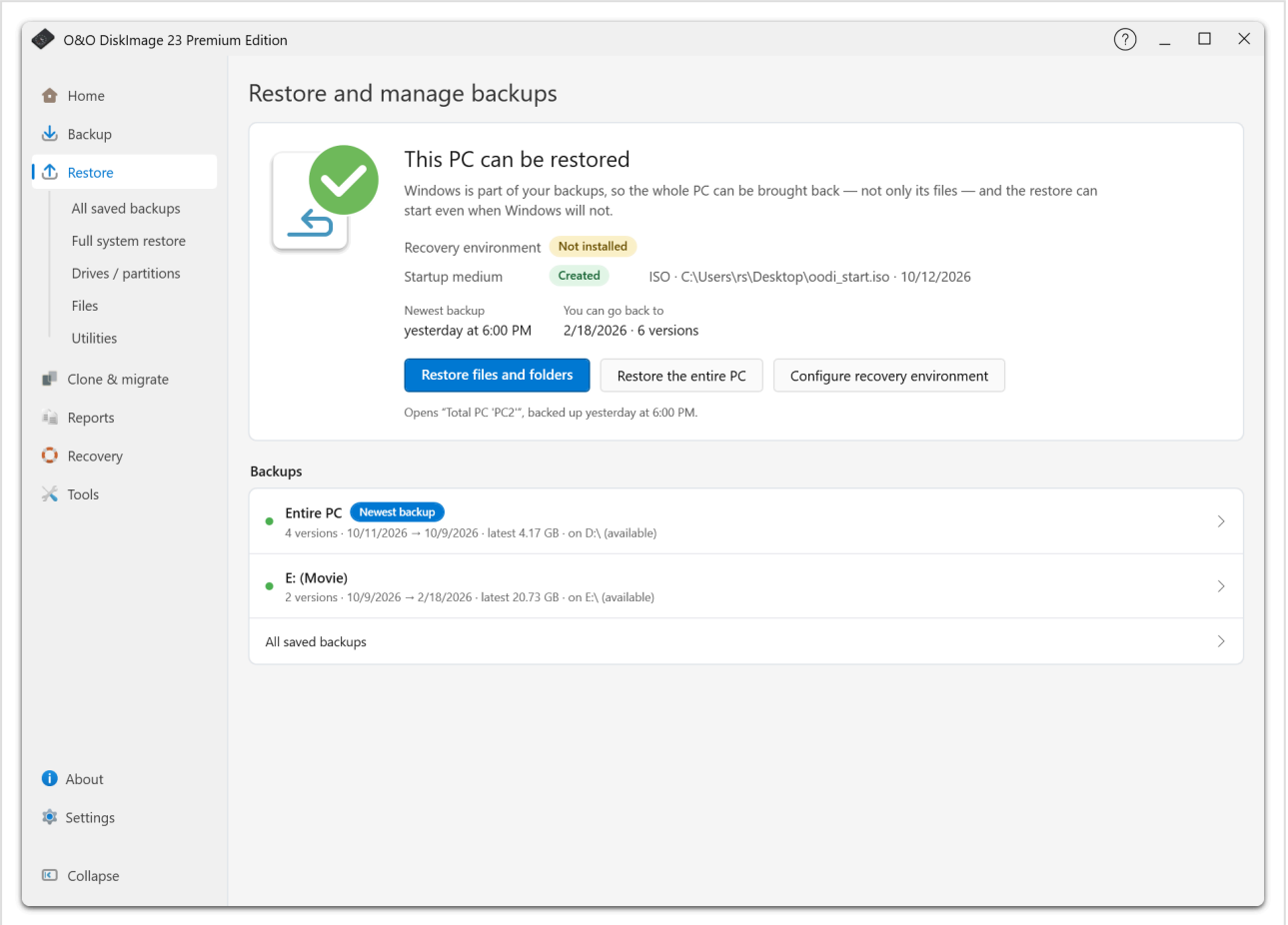
Restore from a second copy

Open the saved backup and select the required version. If the primary file cannot be reached, O&O DiskImage can use the second copy. You can also choose **Restore from the second copy instead**.

Cloud-only versions are downloaded locally before restore, together with any required backup-chain files. Allow time and sufficient local space for the download, and keep the original password available for encrypted backups.

Restore overview

Choose **Restore** to recover files, partitions, or whole disks. The status card shows whether a Windows backup and recovery startup options are available.



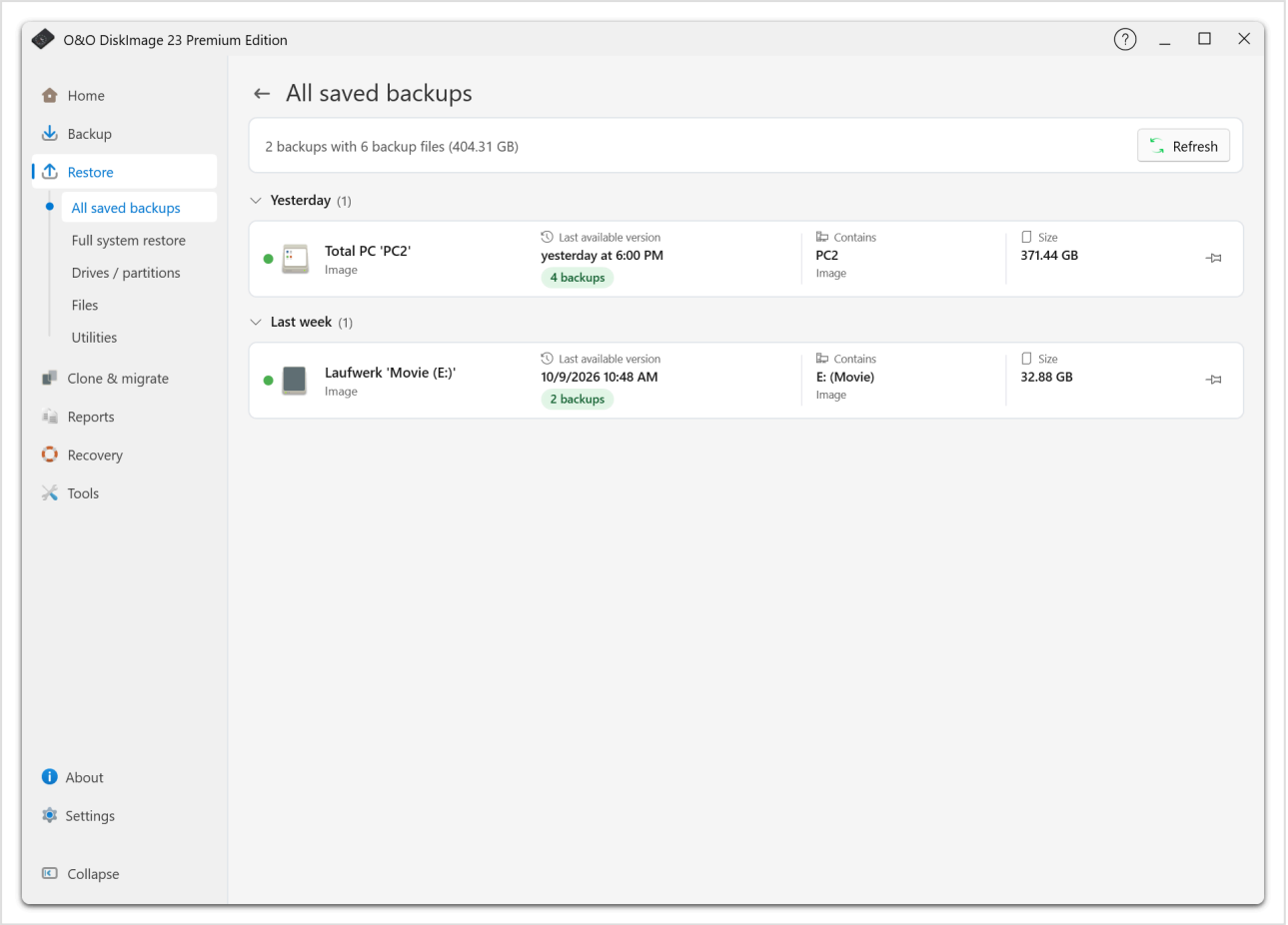
The restore overview shows available backups and the status of recovery startup options.

Find a backup

Restore files and folders on the overview opens the latest available backup directly. To choose an older version or another backup, open **All saved backups** or the relevant source type in the navigation pane.

Backups on disconnected storage remain visible. Reconnect the destination, or use an available second copy. Cloud-only versions must be downloaded before restore.

If the backup is not listed, choose **Add an existing backup** under **Restore > Utilities**. Keep the full backup and any required change backups available.



Saved backups are grouped by date, with the available versions shown for each entry.

Choose a restore type

Type	Purpose
Files	Restore selected files or folders from a file backup or supported image, including VHD backups created by O&O DiskImage.
Drives / partitions	Restore image contents to selected disks or partitions.
Mount a backup	Browse a supported image as a read-only drive and copy files in Explorer.
Full system restore	Restore Windows from the local recovery environment or startup media.

Before you start

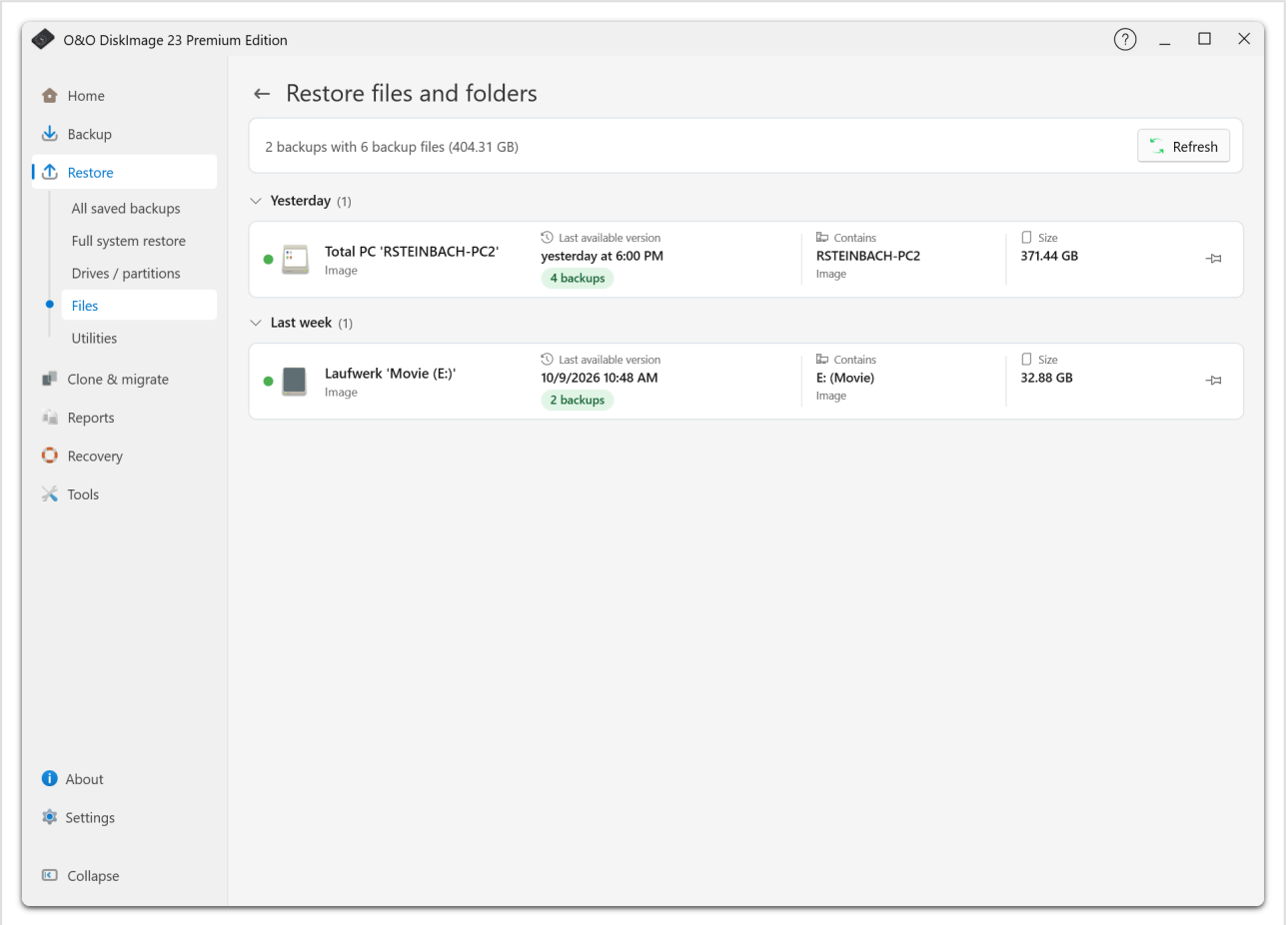
Enter the original password if the backup is encrypted. File restore can overwrite existing files in the chosen folder; drive restore overwrites the selected target disk or partition.

Check the target in the summary and confirmation. A restore cannot overwrite the disk holding its own source file. If that disk cannot be identified, move the file to a known separate disk or a network share and try again.

For the running Windows disk, use the restart offered by **Full system restore** or the target selection dialog. If local recovery is unavailable, use bootable startup media.

Restore files

Restore all files or select individual files and folders from a file backup or supported disk image. File restore is also available for VHD backups created by O&O DiskImage.



Choose one of the listed backups to restore files and folders.

Restore files and folders

1. Open **Restore > Files**, or select a backup under **All saved backups** and choose its file-restore action.
2. Choose the version you need.
3. Enter the original backup password if prompted.
4. Select all available files or choose individual folders and files.
5. Select the destination folder and review the summary.
6. Start the restore and check its result.

The overview's **Restore files and folders** action opens the latest available backup directly. Choose a version from the saved-backup list if you need a different date.

Only files present in the backup are offered. Excluded files and folders cannot be restored from it. Loading a large image's file tree may take time.

Destination folder

Restore to a separate folder when you want to compare files before replacing current data. Restoring to the original location can overwrite existing files. Check the destination and available space first.

Default folder-name templates are under **Settings > Defaults for restores > Folder names**. The file-restore progress window shows the operation and allows cancellation. After completion, review the report and open the restored files you need.

Restore from another copy

If the primary file is unavailable, select an available second copy. A cloud copy is downloaded with its required dependencies before restore. See Second copy.

Mount an image instead

For supported disk images, mounting gives read-only access in Windows Explorer and lets you copy individual files. File-backup containers cannot be mounted.

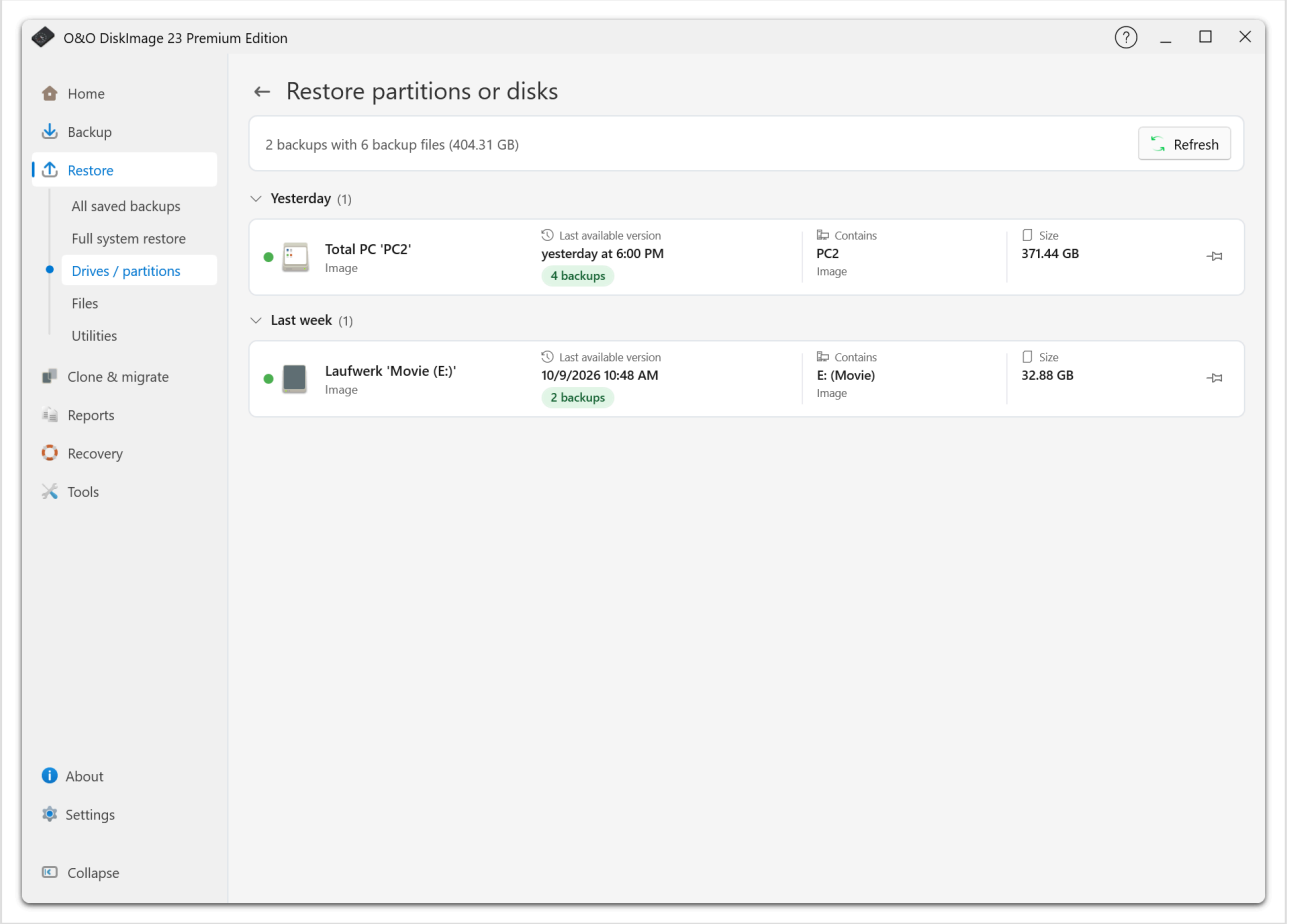
Restore drives

A drive restore writes image data to a disk or partition. Existing data on the selected target is overwritten.

Restore a disk or partition

1. Open **Restore > Drives / partitions**, or choose a saved image and its drive-restore action.
2. Select the backup version and enter its password if needed.
3. Assign each source disk or partition to the intended target.
4. Review the target layout and summary.
5. Confirm the overwrite warning and start the restore.

Keep the full backup and all required change backups available. Supported virtual disks and Hyper-V checkpoints also need their parent files.

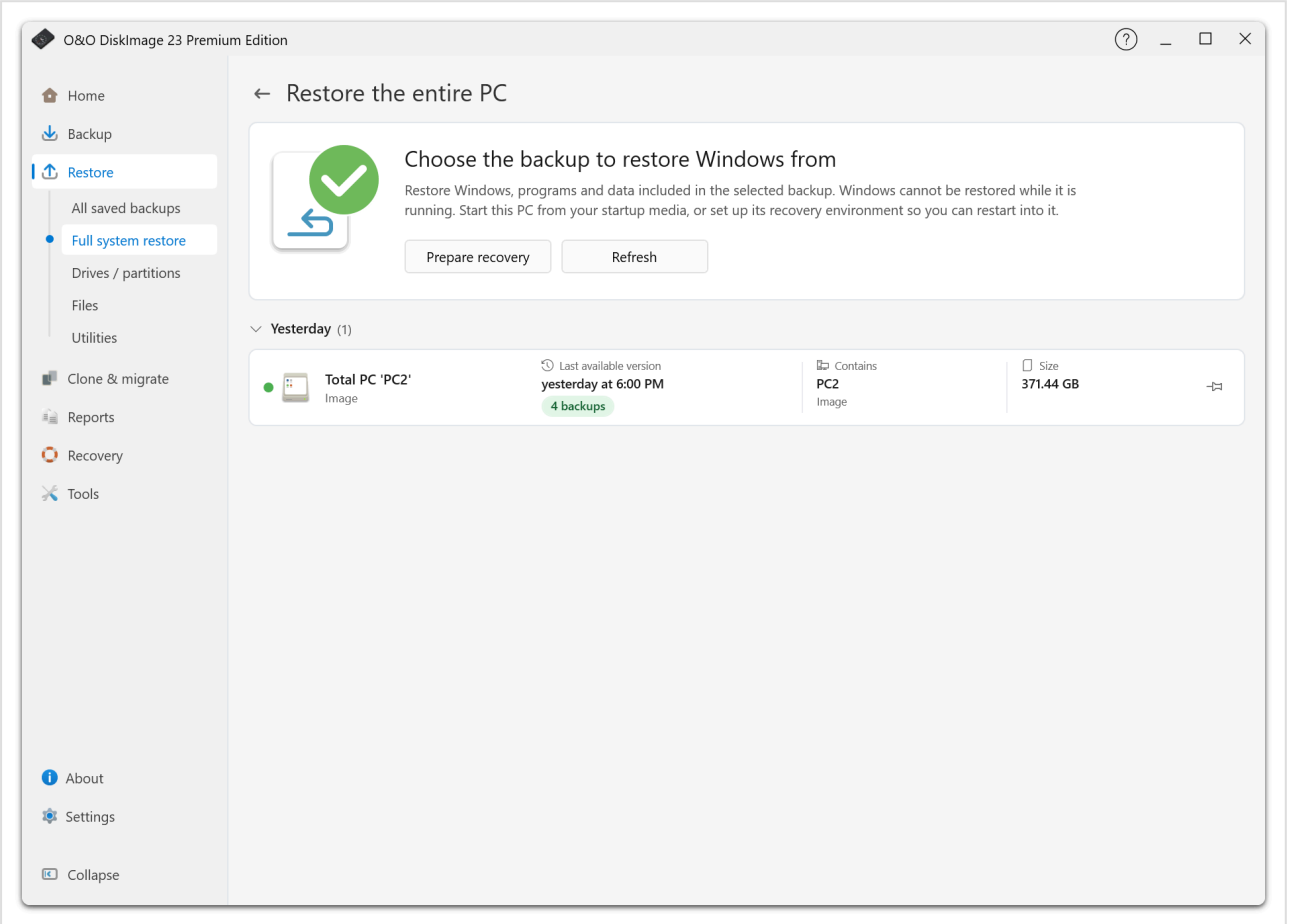


The drives and partitions view lists backups available for restoring disks or partitions.

Restore the Windows disk

The disk containing the running Windows installation cannot be overwritten in normal Windows. Use **Full system restore** or the restart offered when selecting that disk.

If the local recovery environment is ready, O&O DiskImage can carry the chosen backup across the restart. Otherwise use startup media. Review the selected backup and target again in the recovery environment before confirming the restore.



Full system restore shows suitable Windows backups and access to recovery preparation.

Target size checks

The target must meet the minimum size calculated for the image, including used data and file-system overhead. A partition can sometimes be restored to a smaller partition if that minimum fits; this is not guaranteed for every image or format.

VHD/VHDX whole-disk restores must meet the virtual disk's size requirements and use a compatible sector size. The disk storing the source image cannot also be the restore target. If the source location cannot be identified safely, copy it to a separate disk or network share first.

The application checks the target's identity again before writing. If you replace or reconnect disks after selection, review and select the target again.

Mount instead of restore

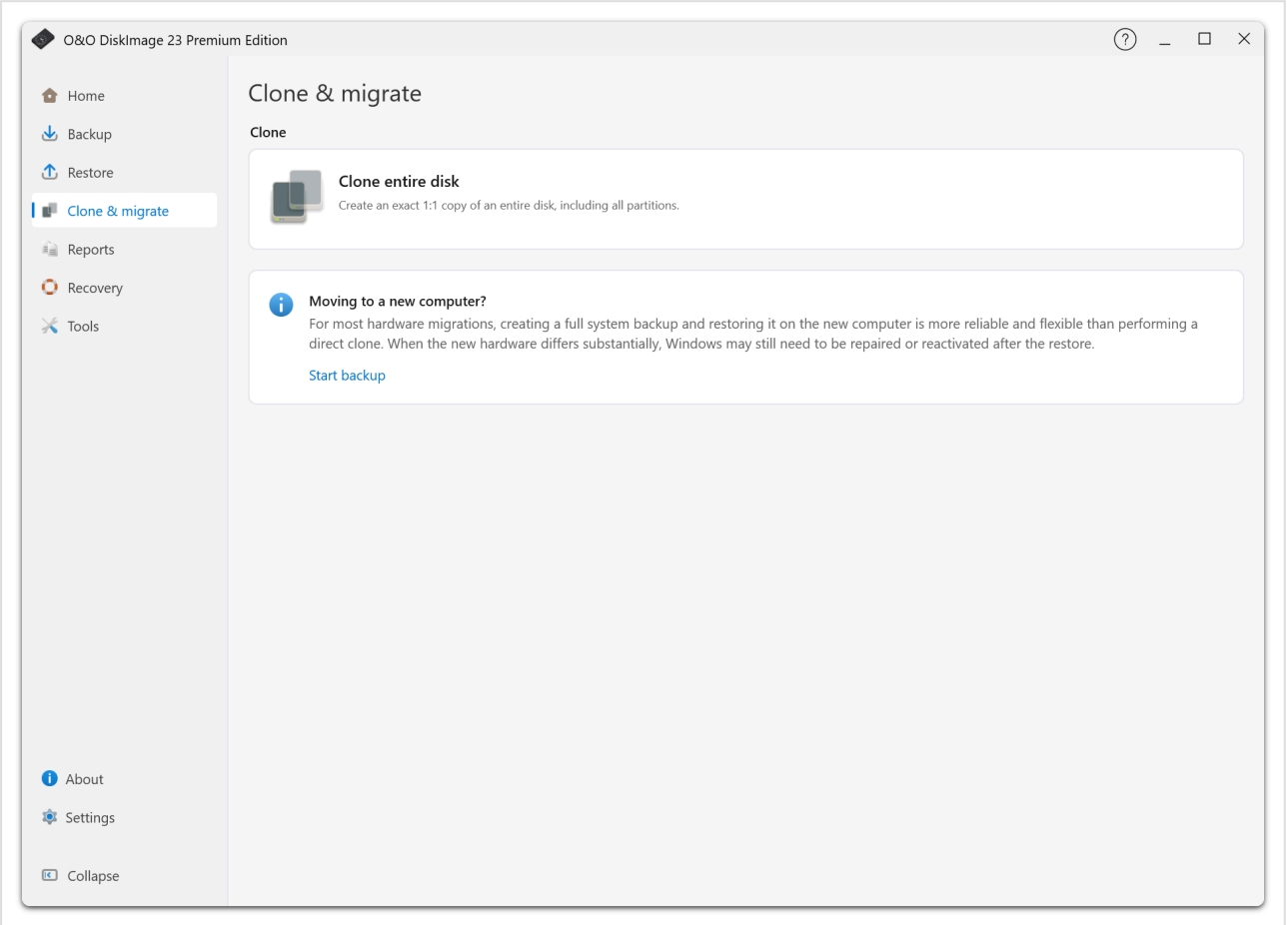
If you only need a few files, use file restore or mount the supported image as a read-only drive. This avoids overwriting an entire target.

After the restore

Check the report and verify the restored data. After restoring Windows, restart the PC and check that it boots. Revisit **Recovery** and rebuild the local recovery environment if the restore overwrote it.

Clone drives

Cloning copies a source disk directly to a target disk. Use it when moving to another drive and you do not need a stored backup history.



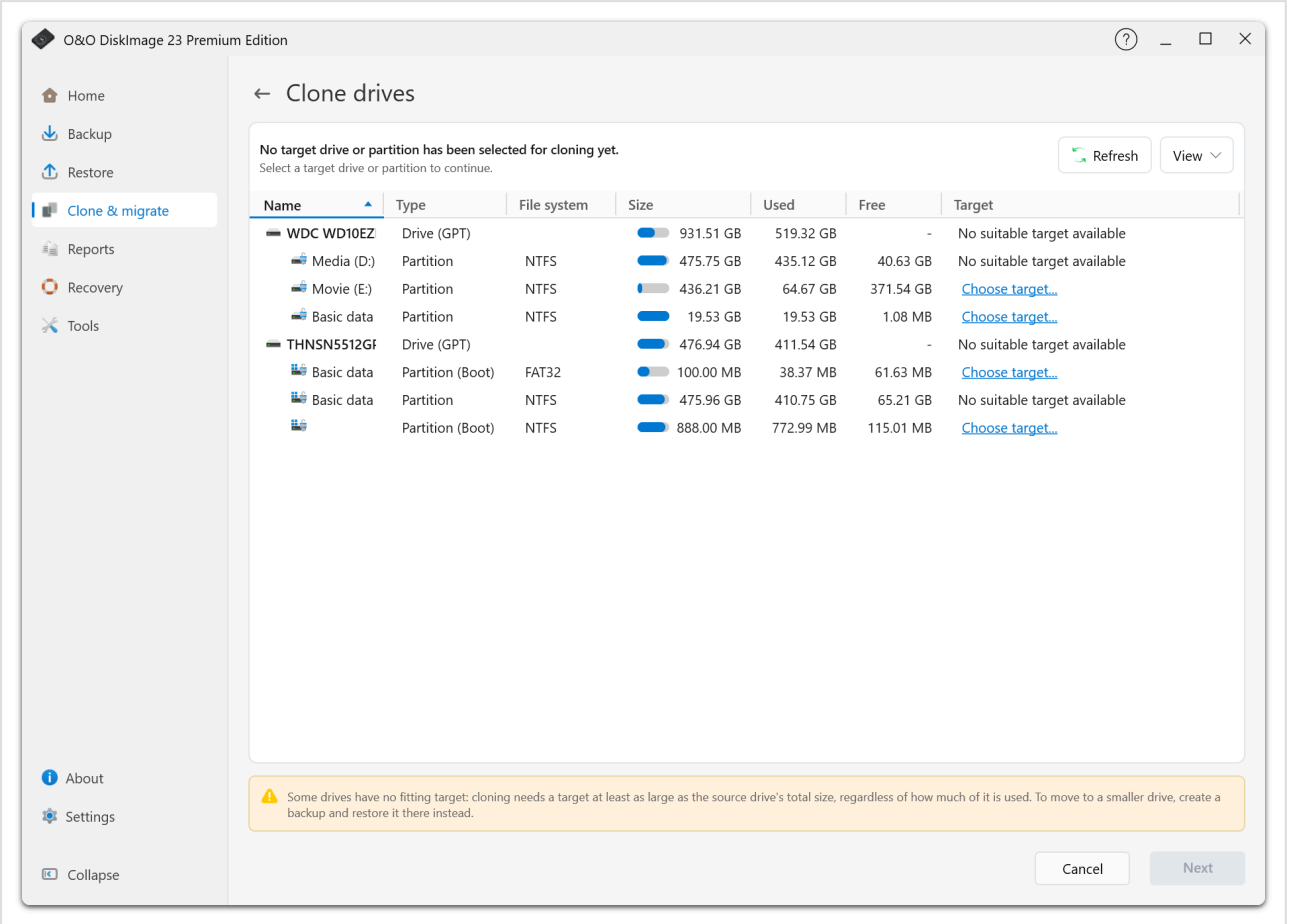
Clone and migrate provides the entry point for copying a disk directly.

Clone a disk

1. Open **Clone & migrate > Clone**.
2. Select the source disk.
3. Select the target disk and review its layout.
4. Check the overwrite warning carefully.
5. Start cloning and review the result when it finishes.

The selected target's existing data is overwritten. The target must be large enough for the data and chosen layout. It cannot be the source disk or the disk containing the currently running Windows installation.

O&O DiskImage checks the target's identity again before writing. If disks have been swapped or reconnected since selection, select and confirm the intended target again.



The disk list shows potential sources and whether suitable cloning targets are available.

Clone technology

Used-sector copying is suitable for ordinary migrations. Forensic modes copy unused sectors too and require enough capacity for the full source size.

After cloning a system disk, shut down before exchanging drives. Keep the original disk until you have confirmed that the new disk starts correctly and contains the expected data.

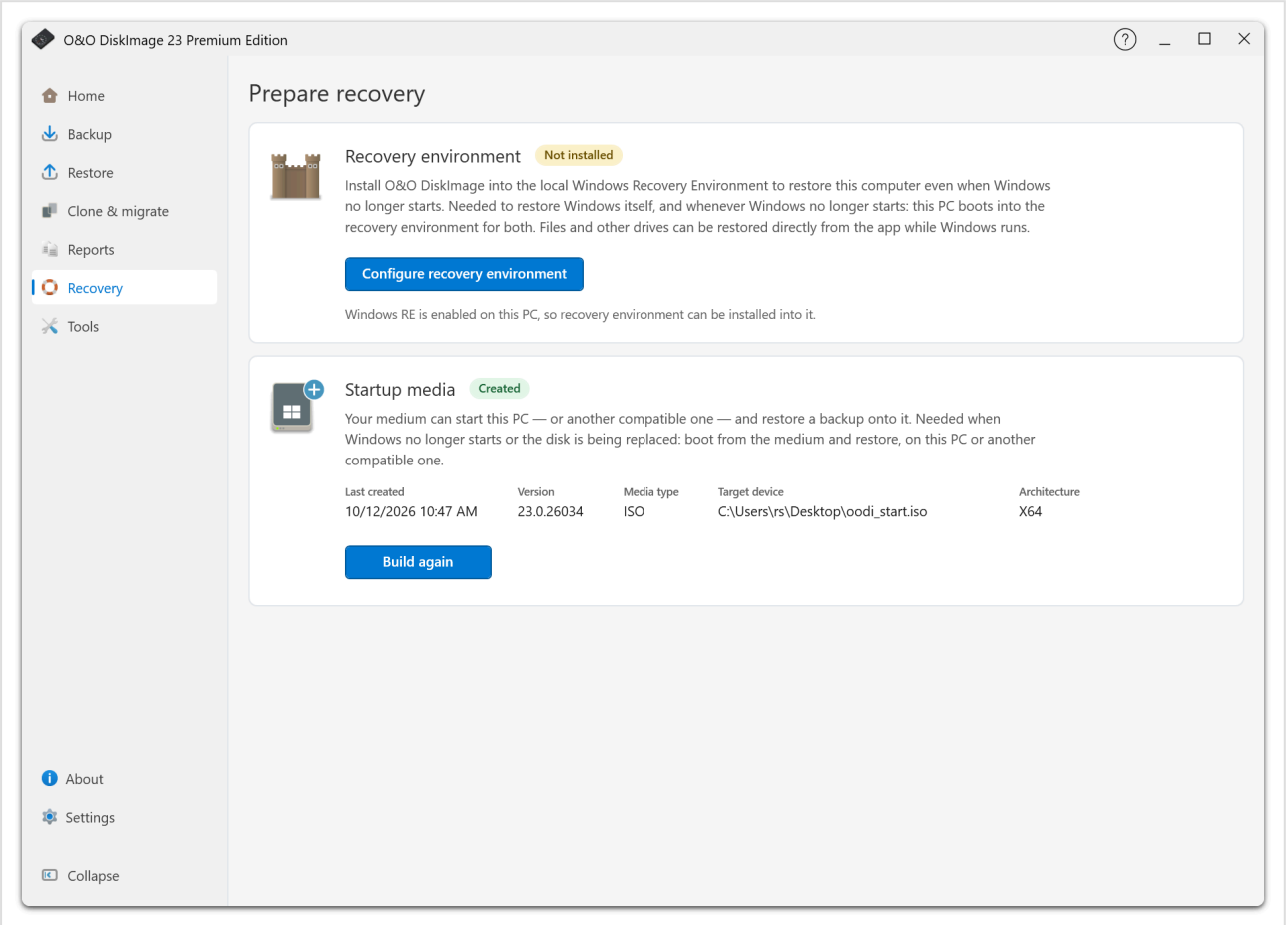
Trial and recovery

Cloning is restricted in the trial; the page explains the restriction and provides purchase and activation links.

Do not restart into the recovery environment while cloning is in progress. Finish or cancel the operation first. If the target is the running Windows disk, perform the operation from an appropriate recovery environment.

Rescue media and recovery environment

Open **Recovery** to prepare a way to start O&O DiskImage outside the installed Windows system. The page shows whether the local environment and startup media are ready or need updating.



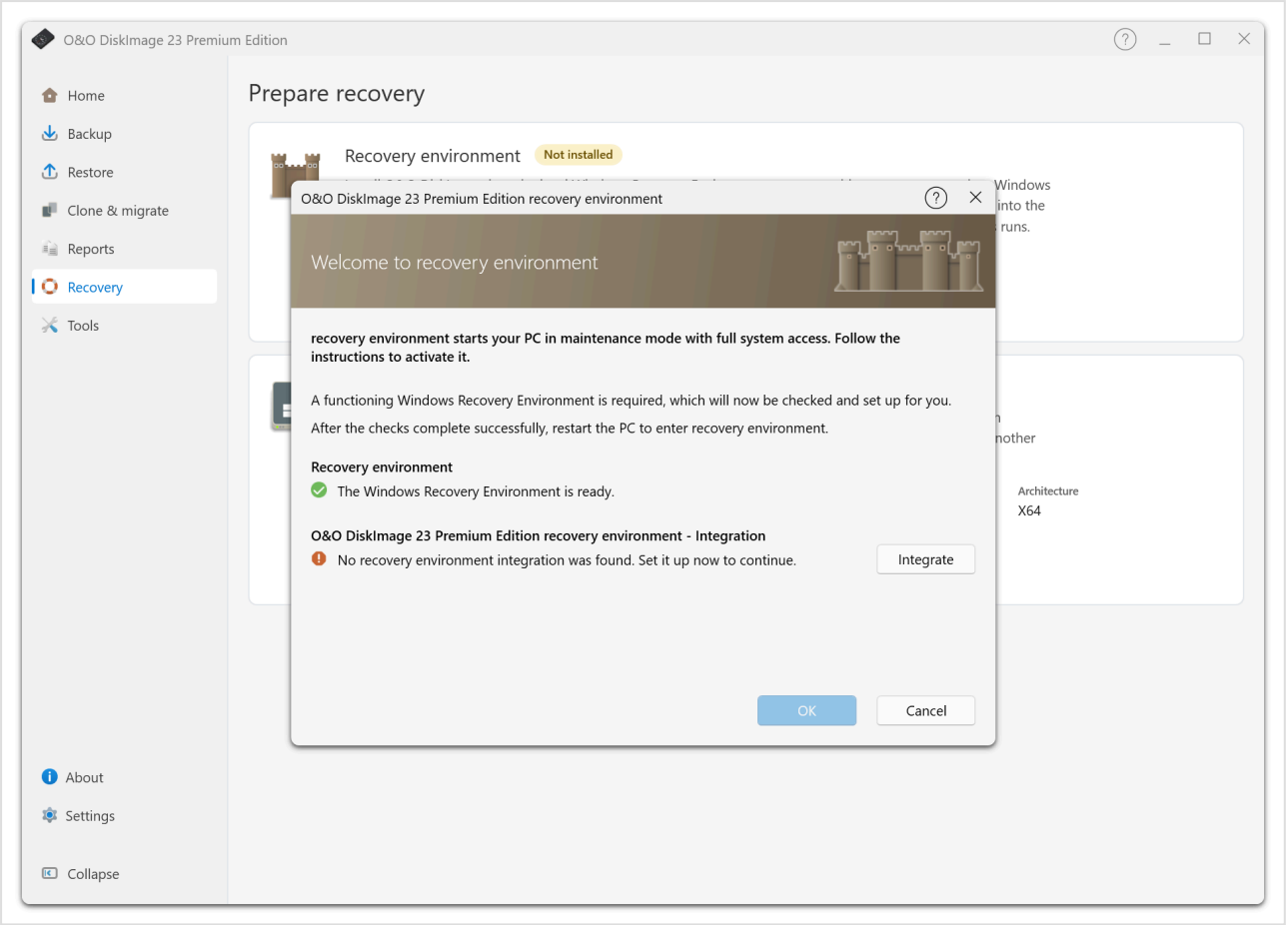
The recovery page shows the status of the local recovery environment and startup media.

Local recovery environment

The feature previously called **Fortress Mode** is now called the **recovery environment**. It adds O&O DiskImage to the local Windows Recovery Environment (WinRE) so you can restore the system without a separate USB stick.

Set it up before a failure. It depends on a working local recovery installation; separate startup media is still useful if the system disk fails.

When the page reports an outdated or unavailable environment, follow its explanation and rebuild it if requested. This may be necessary after an application update or a restore that overwrote the recovery installation.



The setup dialog checks Windows RE and offers to integrate O&O DiskImage.

Restart into recovery

From **Full system restore**, or when selecting a target on the running Windows disk, use the offered restart into the recovery environment if it is ready. O&O DiskImage carries the selected backup into the recovery session where possible.

Save your work before confirming the restart. Restart is blocked while a backup, restore, or clone is active. After restarting, reconnect the backup storage, supply its password if needed, and review the target again before restoring. A restart does not itself authorize overwriting a disk.

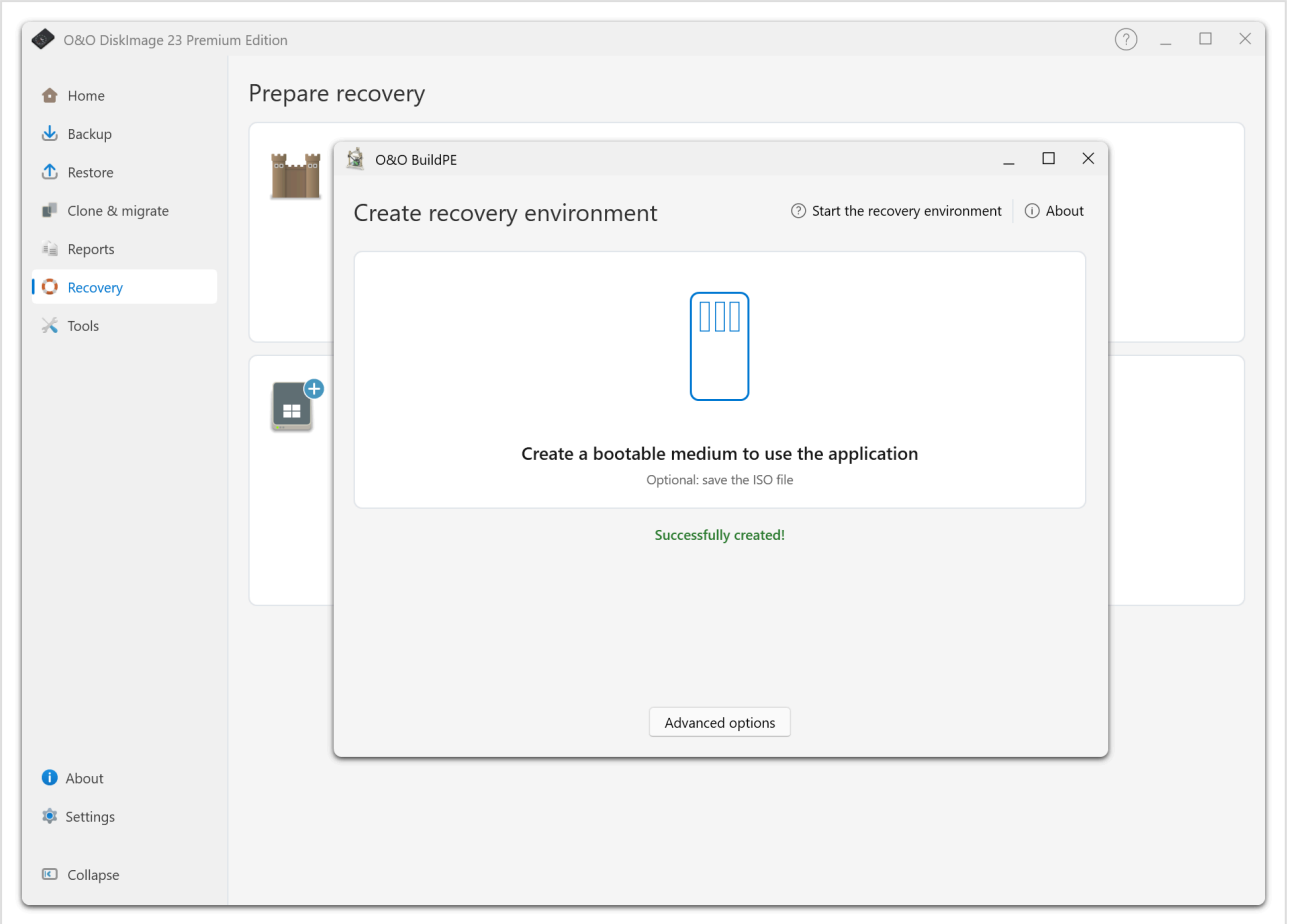
If the local environment cannot be used, follow the startup-media route shown on the restore page.

Bootable rescue media

Create a USB startup medium or an ISO through the startup-media page. Use separate media when the local recovery environment is unavailable or you are replacing the system disk.

The creator excludes the running Windows system disk and shows the detected drive types. Check the selected USB device carefully: the standard media-creation workflow formats it and asks for confirmation. Do not select a drive containing your only backup.

Test that the intended PC can boot from the medium and reach your backup. Check storage and network access as well as the boot itself.



The creator confirms that the bootable recovery medium was created successfully.

Work in the recovery environment

Drive letters may differ from those in normal Windows. Use disk identity, size, and contents to confirm sources and targets.

Keep the original password for encrypted backups available. If license verification needs internet access, use a wired network connection where possible.

After restoring Windows, check the recovery status again. If the local environment was overwritten, rebuild it before relying on it for the next recovery.

Backup plans and saved backups

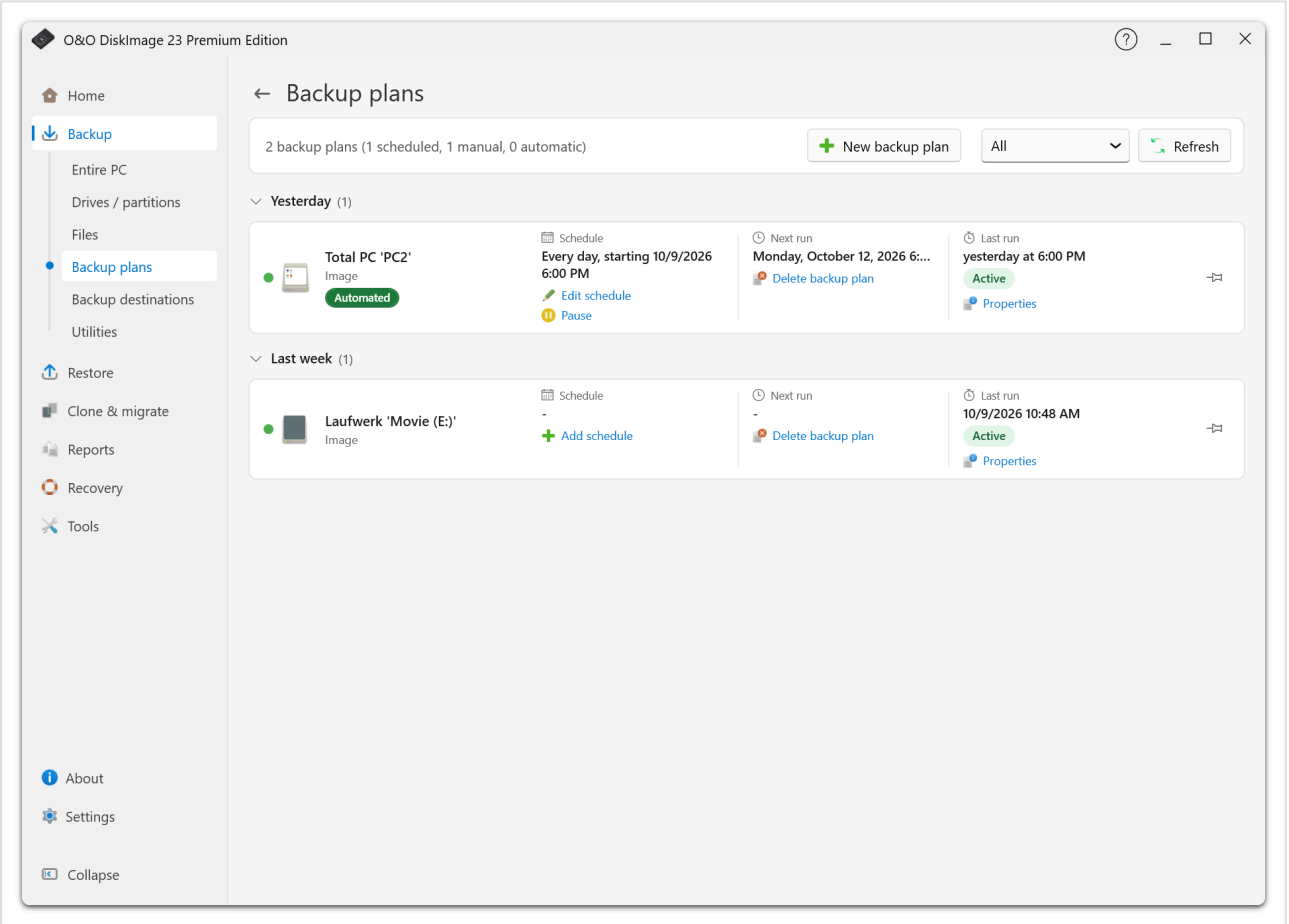
A **plan** stores the source, destination, schedule, and options. A **backup set** groups that configuration with its saved versions. A **run** is one execution; its result and report describe what happened.

Backup plans

Open the plan list under **Backup** to create a plan, start an existing one, or change its settings. A plan can appear before its first run; new plans without backups are listed under **Today**.

The card's **Properties** action opens the plan page. You can rename the plan, edit its schedule and history, or change drive and file sources. Changing sources makes the next run a full backup. Cancelling the page discards your edits.

Format, backup technology, exclusions, and encryption are locked once saved versions exist, even when their storage is offline. Create a new plan to change those options.



The plan list shows schedules, previous and upcoming runs, and actions for editing or starting a backup.

Start a backup

Use **Back up now** to start the existing plan directly. If you need a new independent chain, choose the one-time full-backup action on Home, the plan page, or the notification-area menu. Later runs use the plan's normal method again.

The application shows progress and cancellation for scheduled and drive-triggered backups as well as manual ones.

Saved backups

Open **Restore > All saved backups** to select a version and restore it, inspect its information, or manage its files. The history shows retention reasons and planned removals; individual versions can be kept permanently.

Unavailable storage and missing files are shown differently. Reconnect a disconnected destination. If a file has actually been deleted, remove its obsolete entry only when you no longer need it. An available second copy may still provide the version.

Move or delete backups

Use the application's move and delete actions to keep the plan and file locations in step. Both operations show progress and can be cancelled; after cancellation, inspect the result because some files may already have been processed.

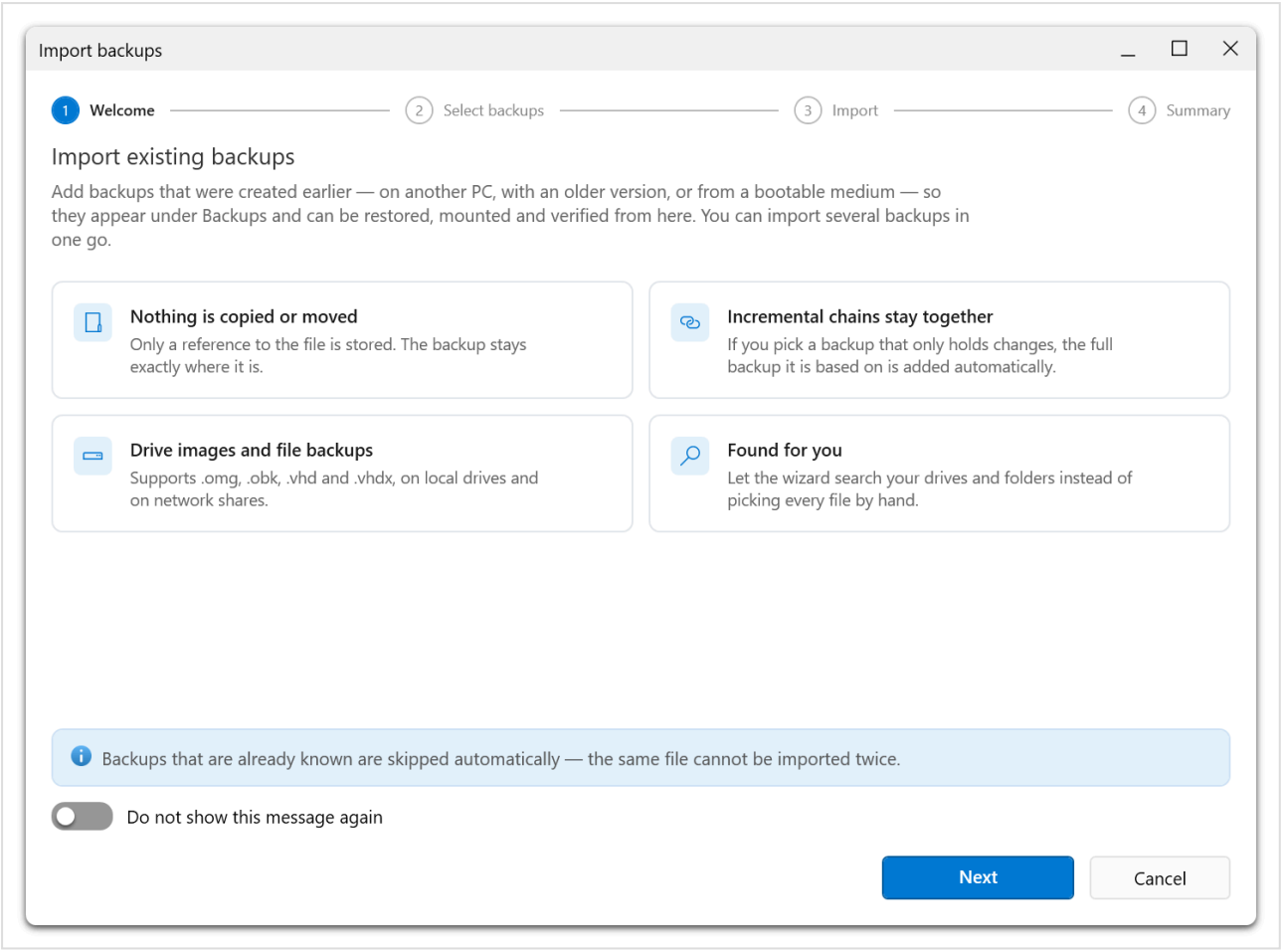
Deleting files is permanent. Removing an earlier backup can also affect later versions that depend on it. Review the confirmation rather than deleting individual chain files in Explorer.

Deleting a plan and deleting its saved files are separate actions. Read the confirmation to see which information and files will remain.

Add an existing backup

The former import action is now **Add an existing backup**. Find it under **Backup > Utilities**, **Restore > Utilities**, or **Tools**.

Choose the backup file and review its information in the wizard. O&O DiskImage adds it to the saved-backup list. Keep any full and incremental files required by that version together and accessible.



The wizard for adding existing backups explains the import and how related backup files are handled.

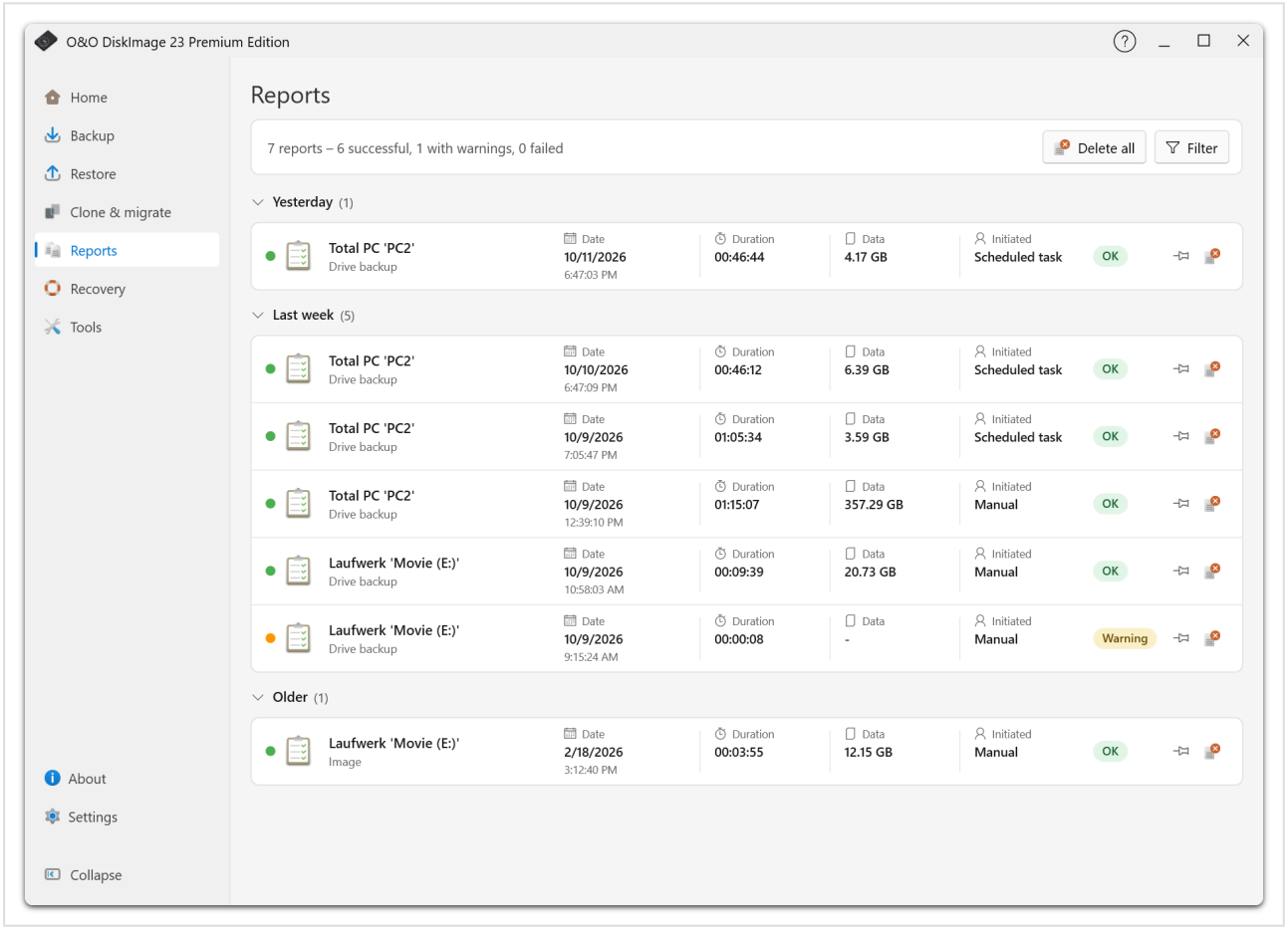
Reports and logs

Reports record individual operations. Logs provide additional detail when troubleshooting.

Reports

When report generation is enabled, O&O DiskImage records the source, destination, method, data volume, duration, result, and any warnings or errors. Scheduled runs also distinguish the planned time from the actual start.

Use **Reports** to open details, view a report in a text editor, save a copy, or delete a report. Deleting a report does not delete its backup.



The reports overview lists completed operations with their date, duration, data volume, and result.

Result statuses

Status	Meaning
Successful	The operation completed without reported issues.
Completed with warnings	The result needs attention; read the warning.
Failed	The operation did not complete successfully, even if no backup version was created.
Cancelled	The operation was stopped before completion.

If an incremental or differential run becomes a full backup, the report explains why. Possible reasons include the history's full-backup interval, changed sources, or an unavailable previous version. Scheduled runs also show this explanation in the notification area.

Second copy missing means the primary backup is usable but its copy failed or was cancelled. Fix the destination problem and use **Retry copy**. An upload may still be running after the primary backup finishes.

Reports show the active history settings and removed versions. Entire-PC backup reports also identify destination disks left out of the sources.

Logs

Application logs record events; engine logs provide lower-level imaging details for support. Configure them under **Settings > Logging**. Some changes require a restart.

In the recovery environment, logs are kept away from a volume being overwritten. After a failed operation, the application attempts to copy the logs beside the backup so they can be inspected after restarting.

Email notifications

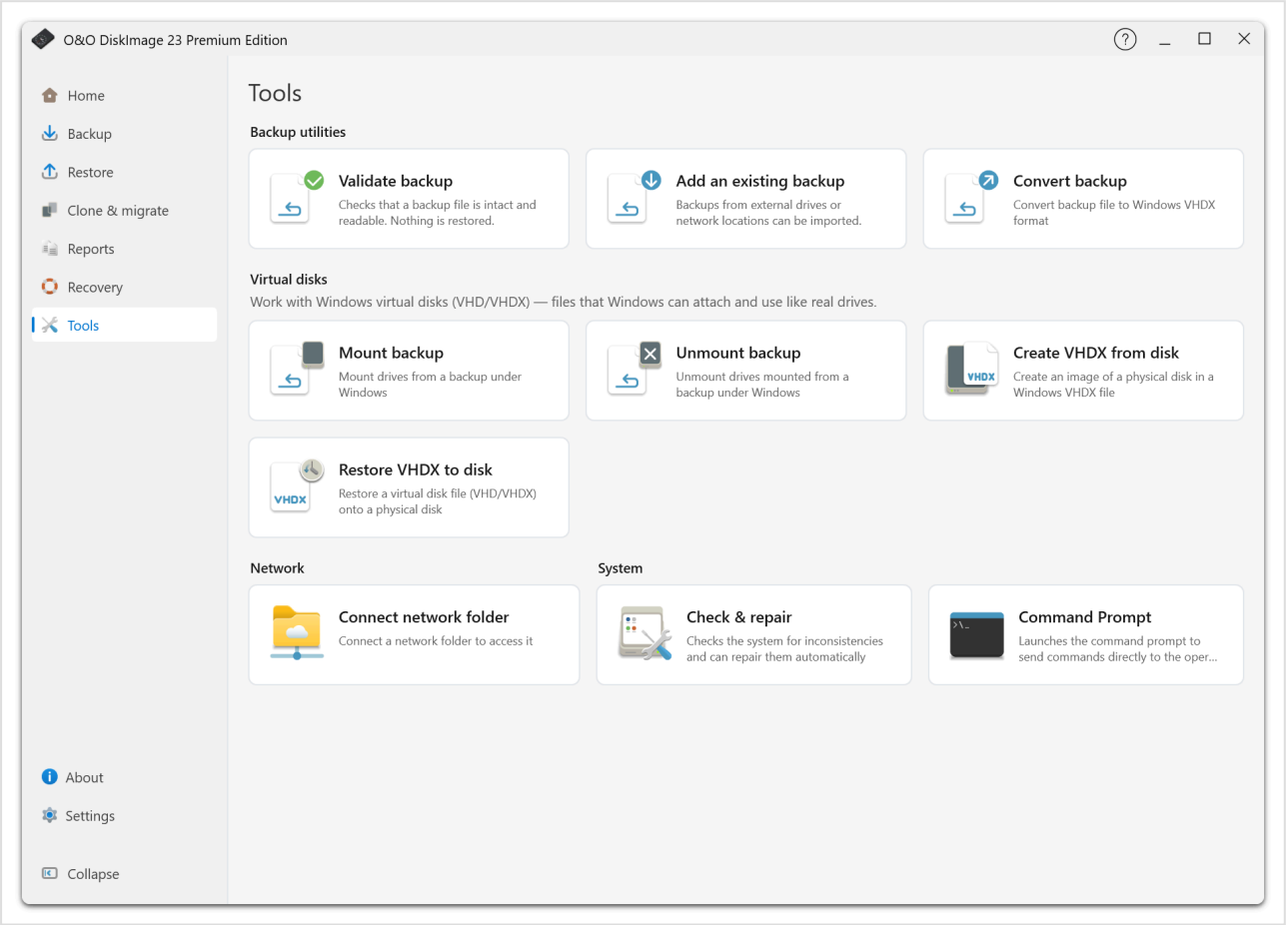
Under **Settings > Notifications**, configure email notifications and send a test message. The background service sends the messages, including failures from unattended runs. Successful-run notifications are optional.

Contact support

Include the product and Windows versions, the failed operation's report, the source and destination types, and whether the run was manual, scheduled, or drive-triggered. Add logs if requested, and say whether the problem occurred in normal Windows or the recovery environment.

Tools

Utilities are available from **Tools** and from the **Utilities** entries under **Backup** and **Restore**.

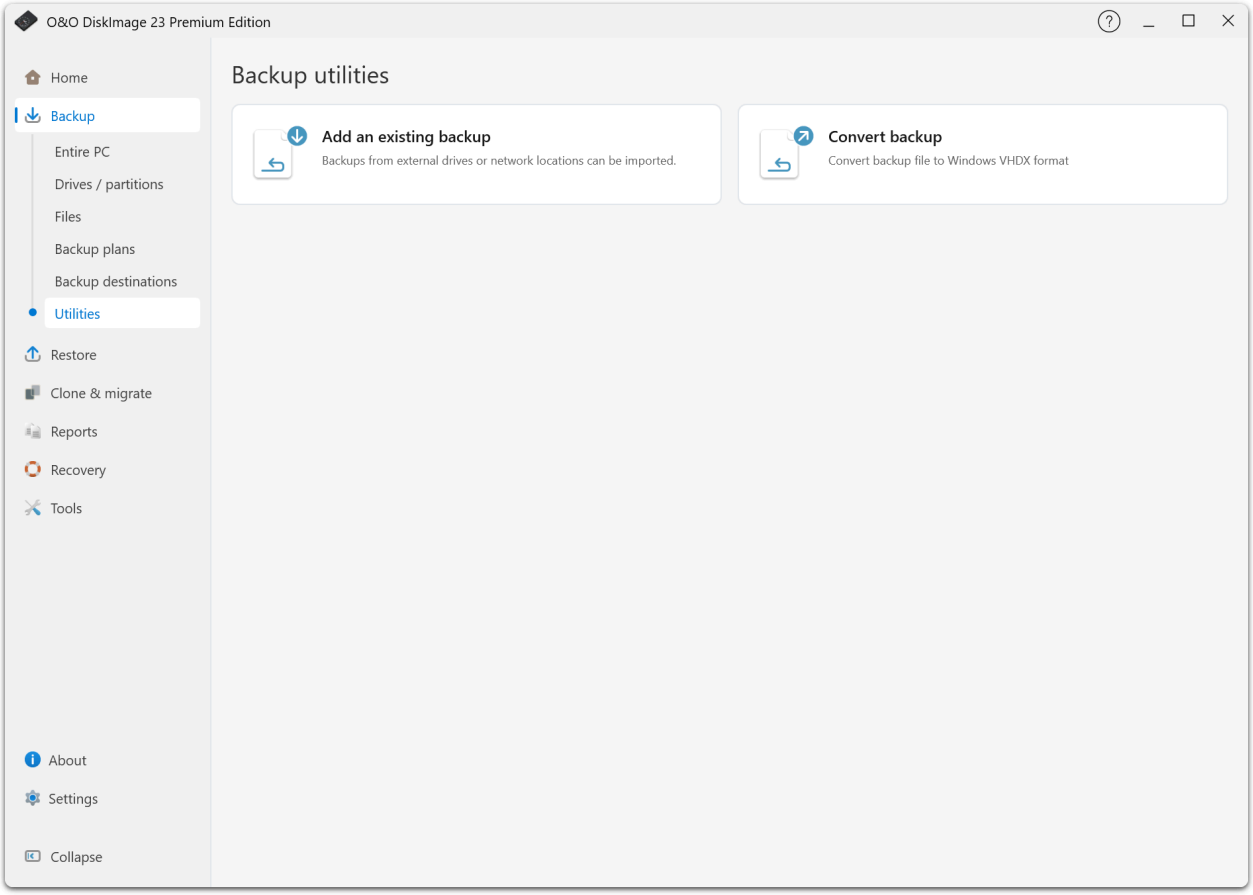


The tools overview groups backup utilities, virtual disk tools, and network and system functions.

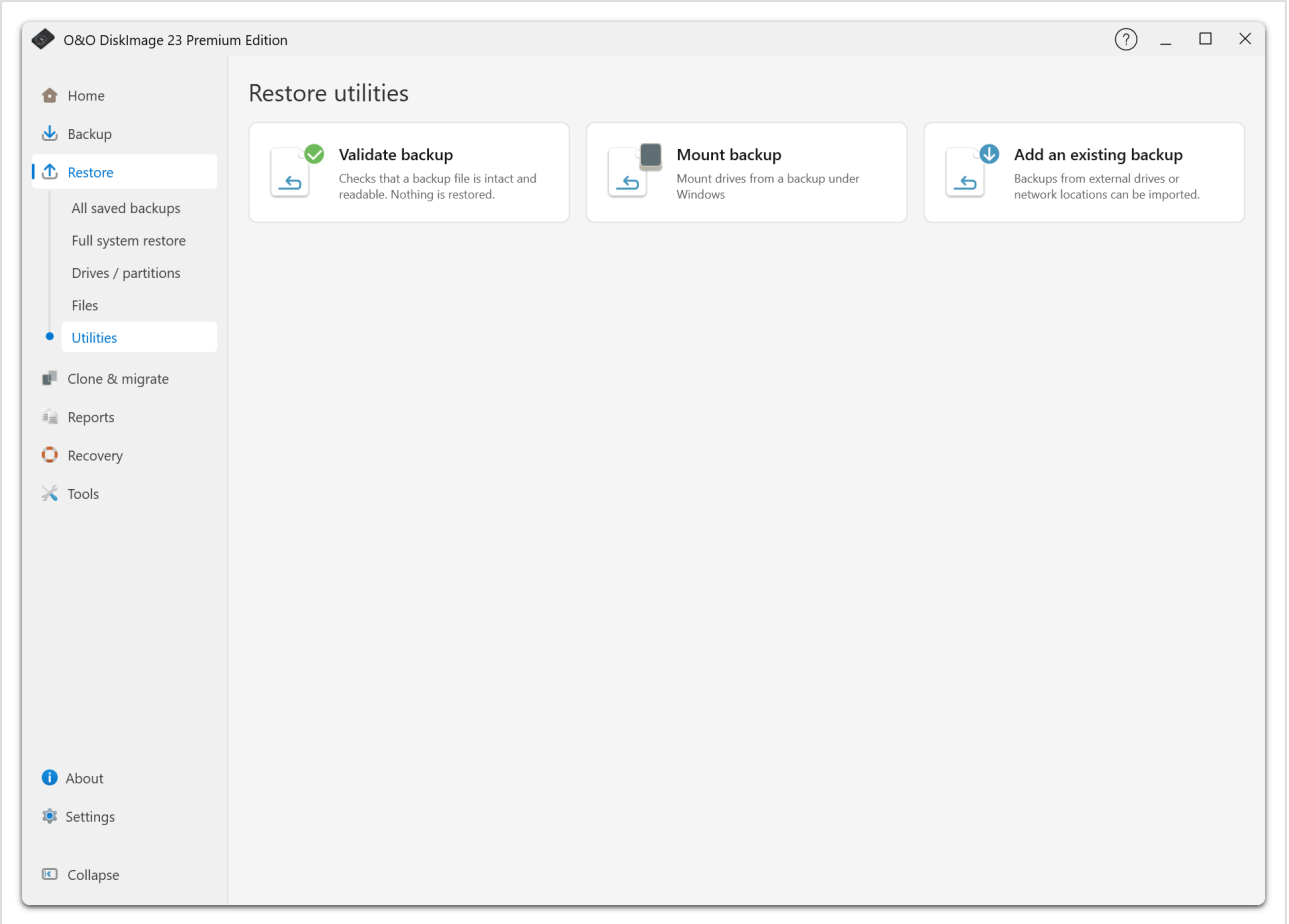
Where to find a tool

Location	Actions
Backup > Utilities	Add an existing backup; convert a backup to VHDX.
Restore > Utilities	Check a backup; mount a backup; add an existing backup.
Tools > Backup Utilities	Validate a backup; add an existing backup; convert a backup.
Tools > Virtual Disks	Mount or unmount a backup; create VHDX from a disk; restore VHDX to a disk.
Tools > Network	Connect a network folder.
Tools > System	Check & repair; Command Prompt.

Some tools are restricted in the trial. The page identifies these tools and offers purchase and license-activation links. Tools unavailable in the recovery environment are hidden.



Backup utilities provide actions for adding existing backups and converting backups to VHDX.

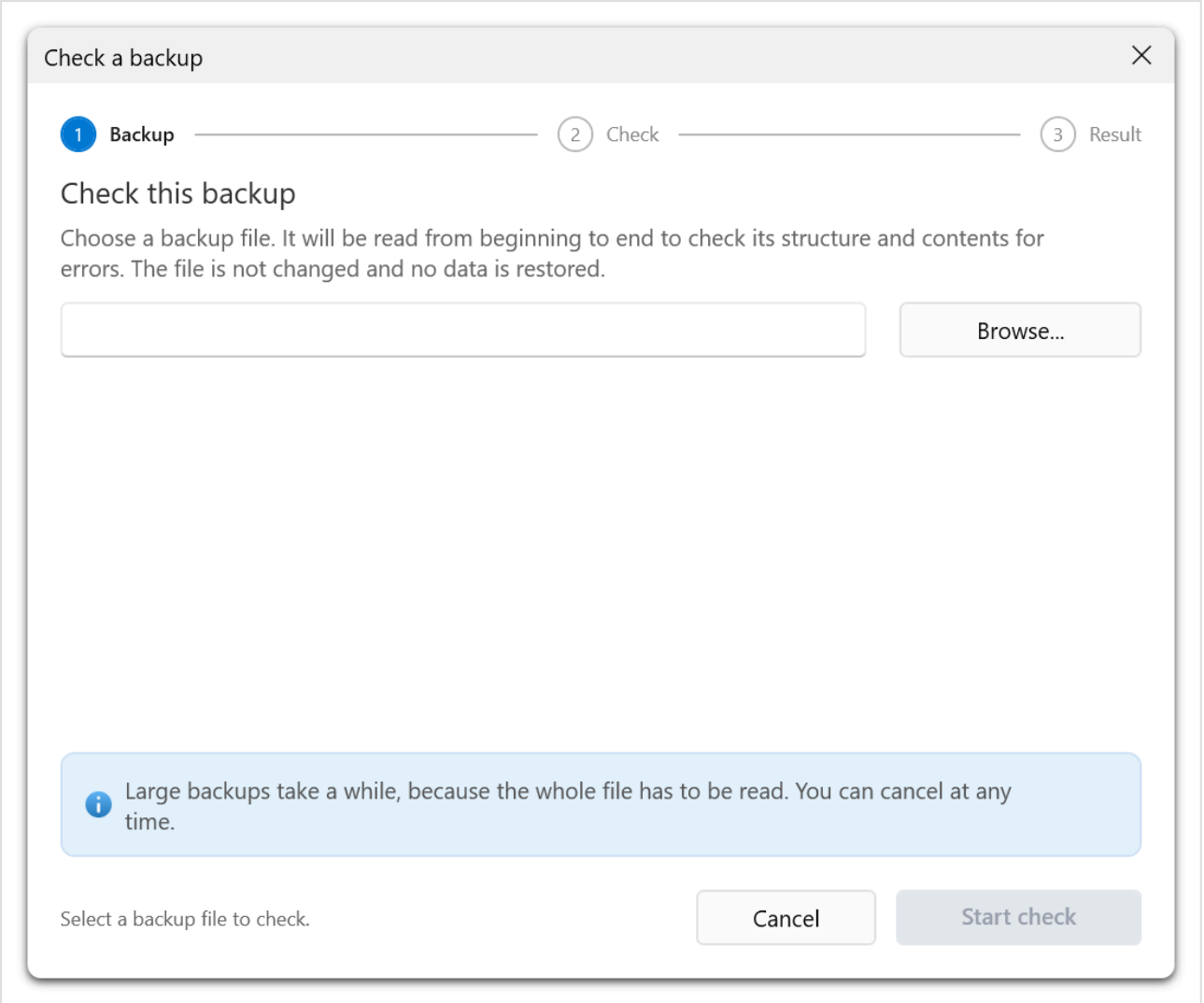


Restore utilities provide actions for validating, mounting, and adding a backup.

Check a backup

The validation wizard reads the backup to check its integrity and readability. The backup file is not changed and no data is restored. Select a file, enter its password if needed, start the check, and review the result.

A cancelled check has not verified the unread portion. If verification fails, keep another usable copy and investigate the storage or file problem before relying on that backup.



Select the backup file whose integrity you want to check in the validation wizard.

Add an existing backup

This replaces the former **Import backups** action. The wizard reads the selected file's information and adds it to the saved-backup list. See Backup plans and saved backups.

Mount and unmount backups

Mounting exposes a supported image as a read-only Windows drive so you can browse or copy its files. File-backup containers cannot be mounted; use Restore files instead.

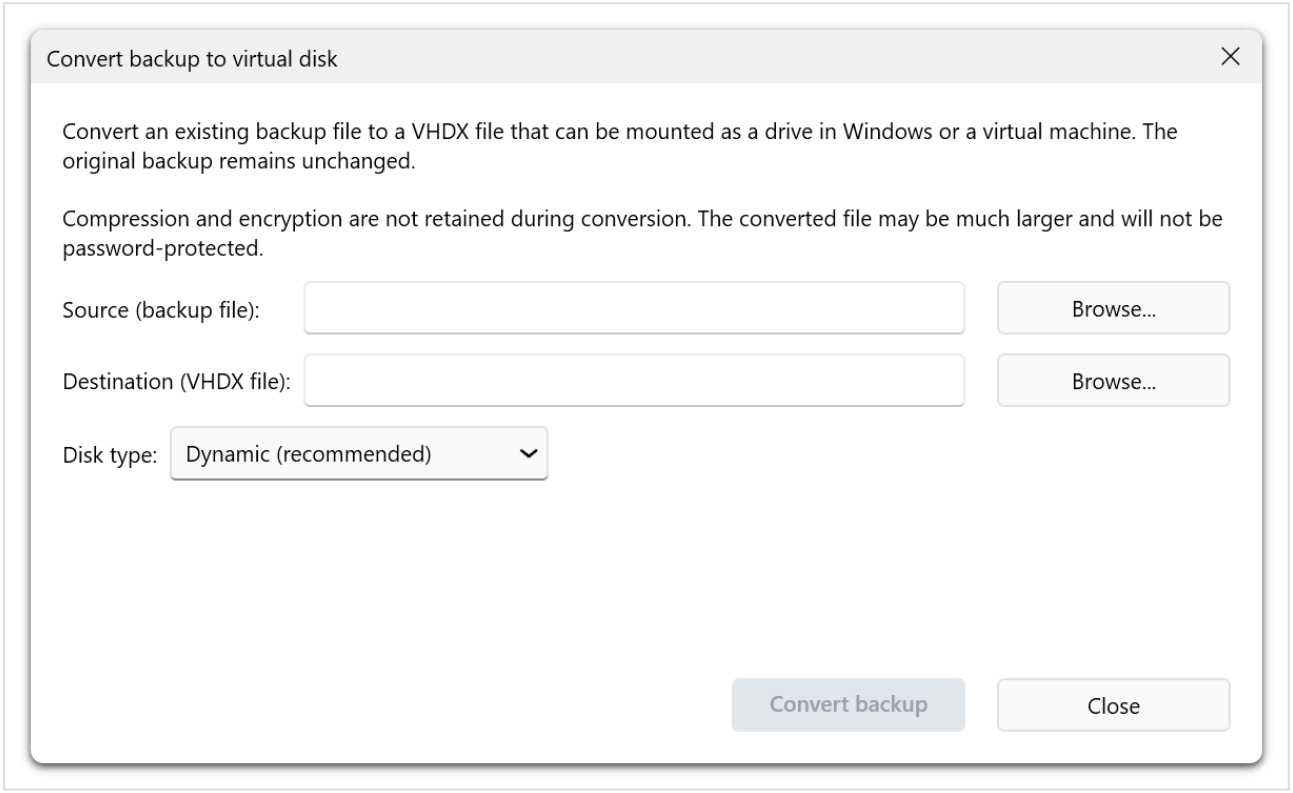
Supported virtual disks include VHD/VHDX and Hyper-V checkpoints. Keep all parent files available for a differencing disk. A VHD/VHDX backup can be mounted on the original PC while the source disk is online.

If the backup is already mounted, use the existing mount or unmount it first. Unmount drives you no longer need to release their drive letters. Unmounting remains available in the trial.

Convert a backup

Convert backup creates a Windows VHDX file from a supported backup; the original remains unchanged. Compression and password encryption are not retained, so allow enough space and protect the resulting file appropriately.

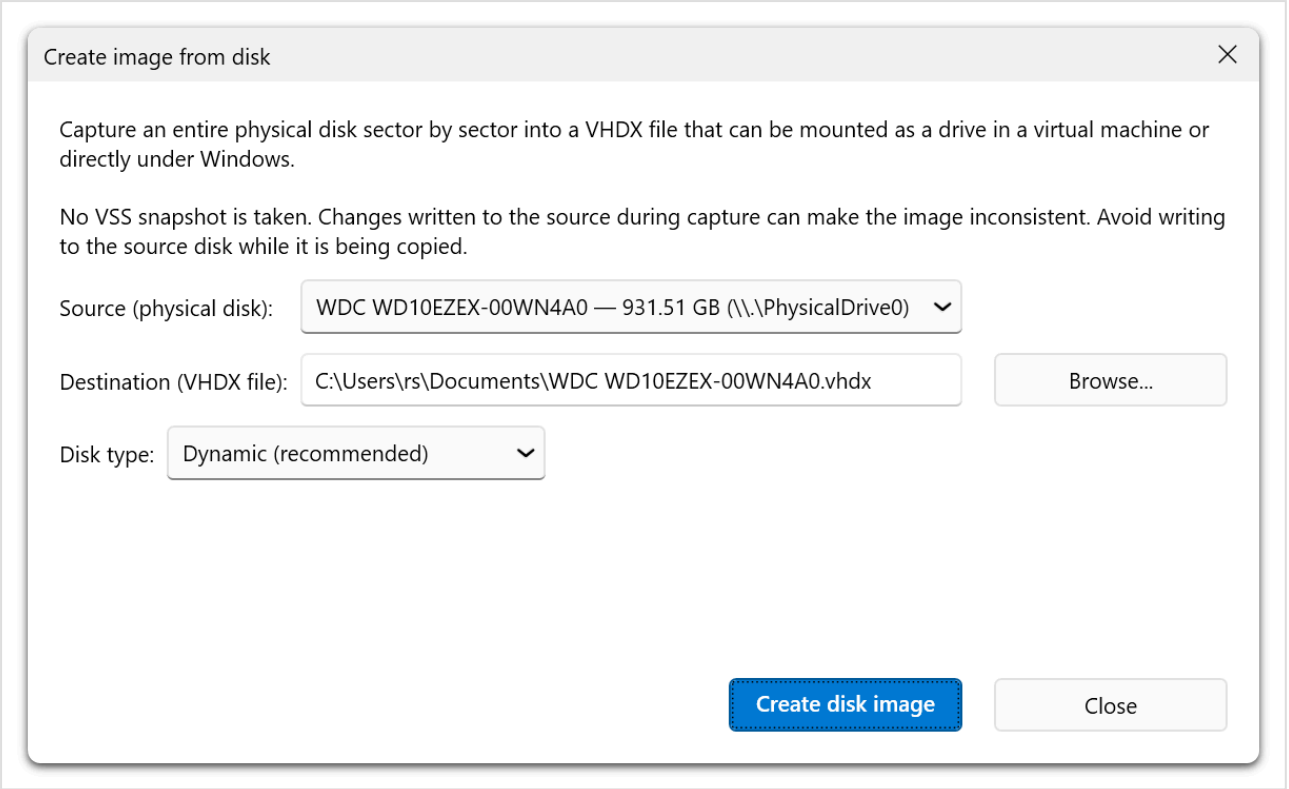
A backup containing only the EFI or System Reserved partition without the rest of its disk cannot be converted. Use an image of the whole disk.



To convert a backup, choose the source backup, destination VHDX file, and disk type.

Create VHDX from disk

This tool captures an entire physical disk into a VHDX file without creating a reusable backup plan. It does not take a VSS snapshot. The source must not be in use, and the destination must be on another physical disk. Use the normal O&O DiskImage backup workflow for a running system.



The dialog creates a VHDX file from the selected physical disk.

Restore VHDX to disk

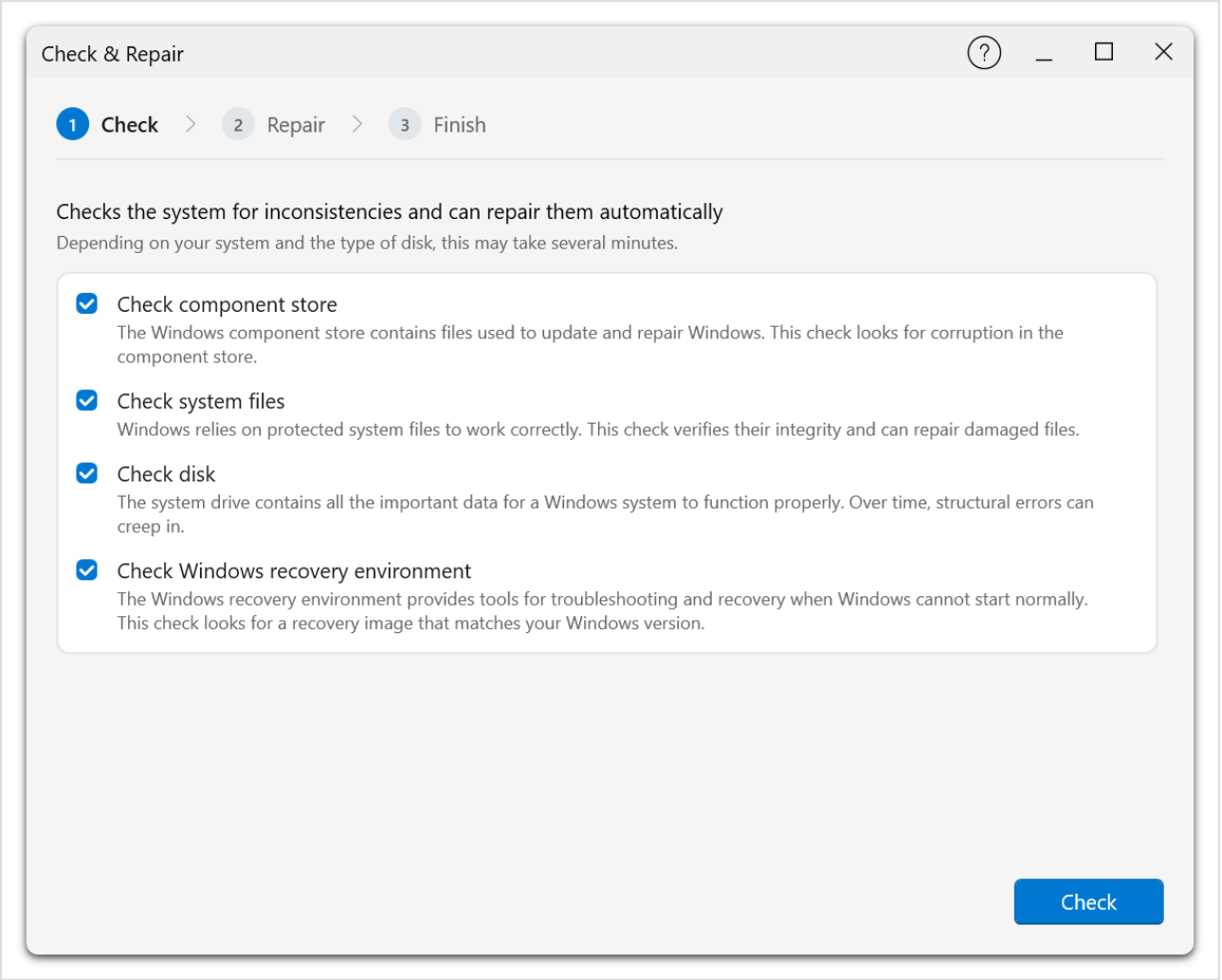
This tool writes a supported VHD/VHDX file to a physical disk and replaces its partition table and data. It cannot target the running Windows disk or the disk holding the source file. Incompatible sector sizes are rejected before writing.

The source disk identifier is preserved by default for bootability. Change the identifier only if the restored disk must coexist with the original on the same computer. For a guided restore from a managed backup, see Restore drives.

Check & Repair

Tools > System > Check & repair checks the Windows system, including system components, system files, the file system, and the recovery environment, and offers repairs where supported. Follow the wizard and review each result.

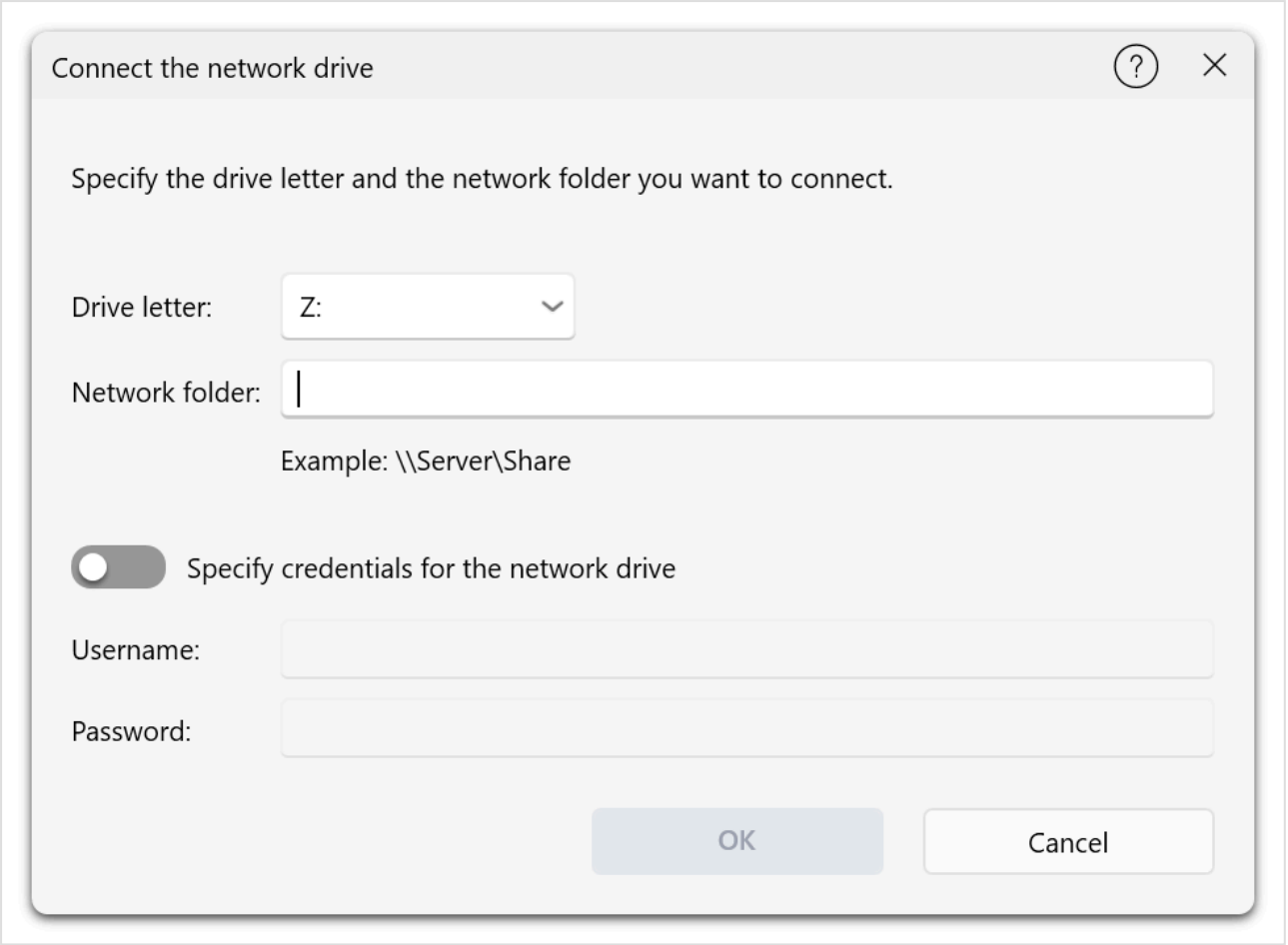
This tool does not repair O&O DiskImage backup containers. To assess a backup file, use the validation wizard. If a backup is damaged, use another verified version or copy.



Check and Repair checks the component store, system files, drives, and the Windows recovery environment.

Connect a network folder

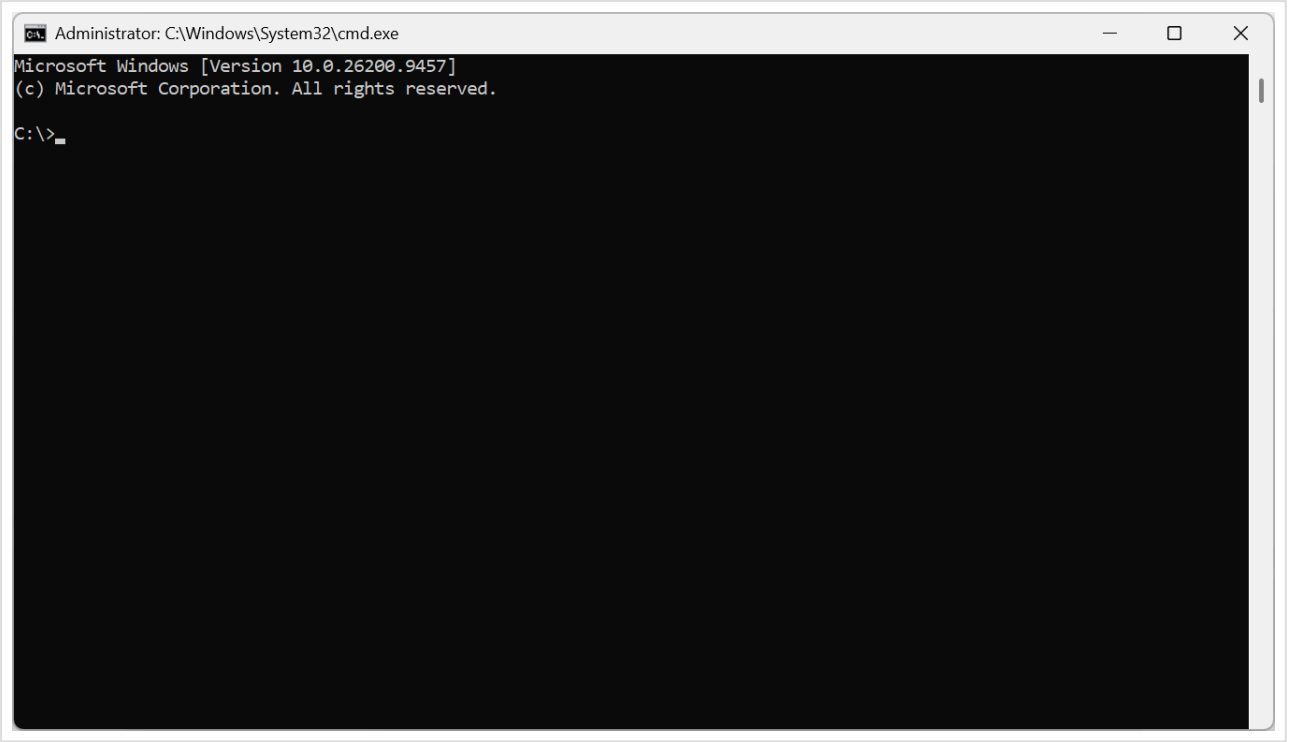
Enter a UNC path and credentials to connect a share to a drive letter. See Backup destinations for stored credentials and connection tests.



Enter a drive letter, network folder, and credentials if required to connect the share.

Command Prompt

Opens the Windows command prompt for diagnostics and support work.



The tool opens the Windows command prompt for diagnostics and support tasks.

Settings

Settings brings application preferences, defaults for new backups, and restore defaults into one dialog. Defaults apply to new plans. To change an existing plan, open its **Properties**.

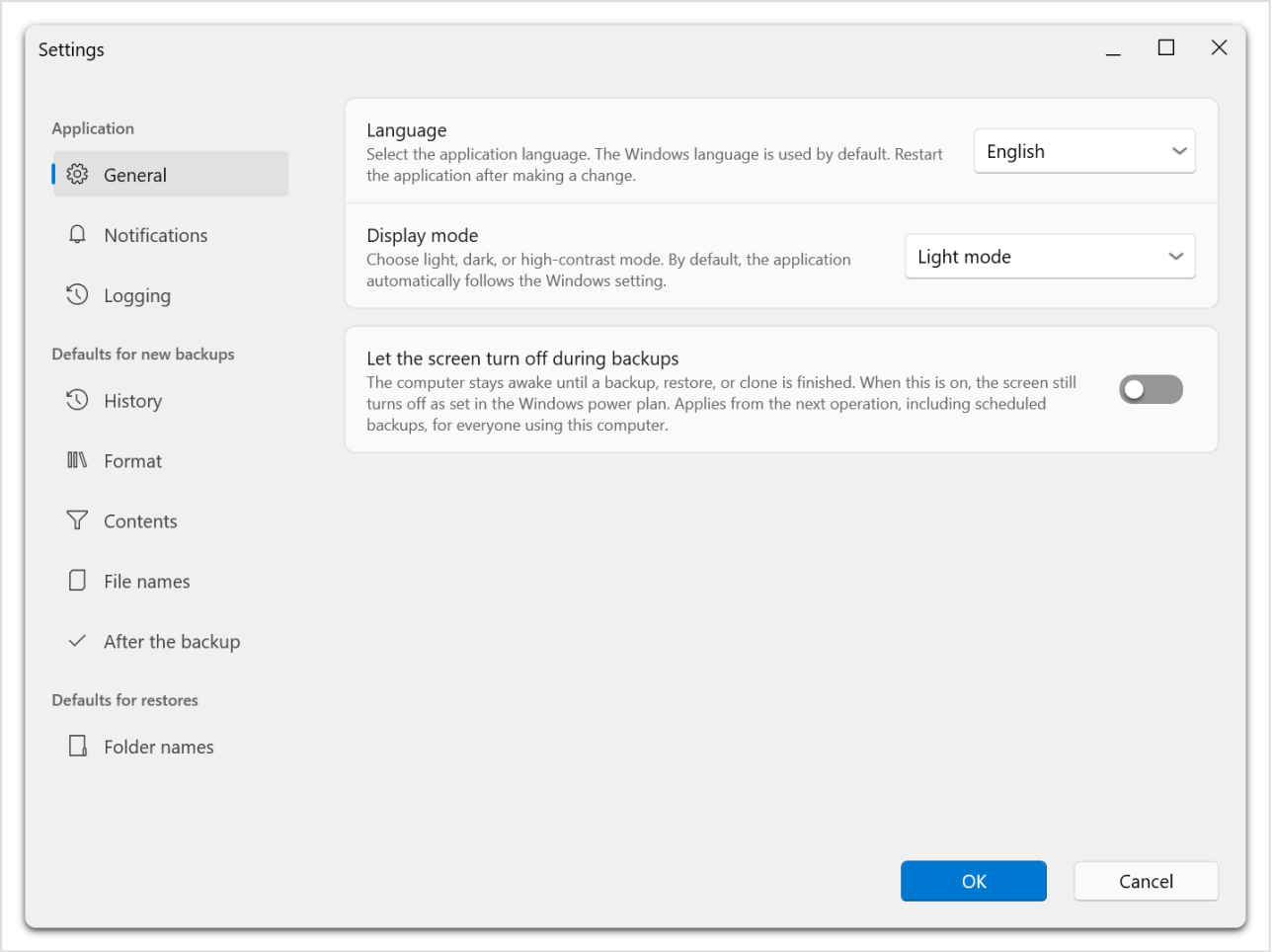
Confirm the dialog to save changes. **Cancel** discards pending edits; actions such as sending a test email or showing dismissed recommendations take effect when selected.

Application settings

Page	Settings
General	Language, appearance, and whether the display may turn off during operations.
Notifications	Desktop result notifications, whether the protection rating includes the system backup, email notifications, and showing dismissed recommendations again.
Logging	Application and engine logging for diagnosis.
Advanced	Support and maintenance options; visible when Settings is opened while holding Shift.

Allowing the display to turn off does not allow the PC to sleep during a backup or transfer. Wake-from-sleep behavior is configured separately in each schedule.

Changing the language can require an application restart. Language changes are unavailable in the recovery environment.



General settings control the language, display mode, and whether the screen may turn off during backups.

Email notifications

Under **Notifications**, enter the SMTP server, port, STARTTLS setting, login details, sender, and recipients. Enable notifications and send a test email. Failures are reported when notifications are enabled; messages after successful runs are optional.

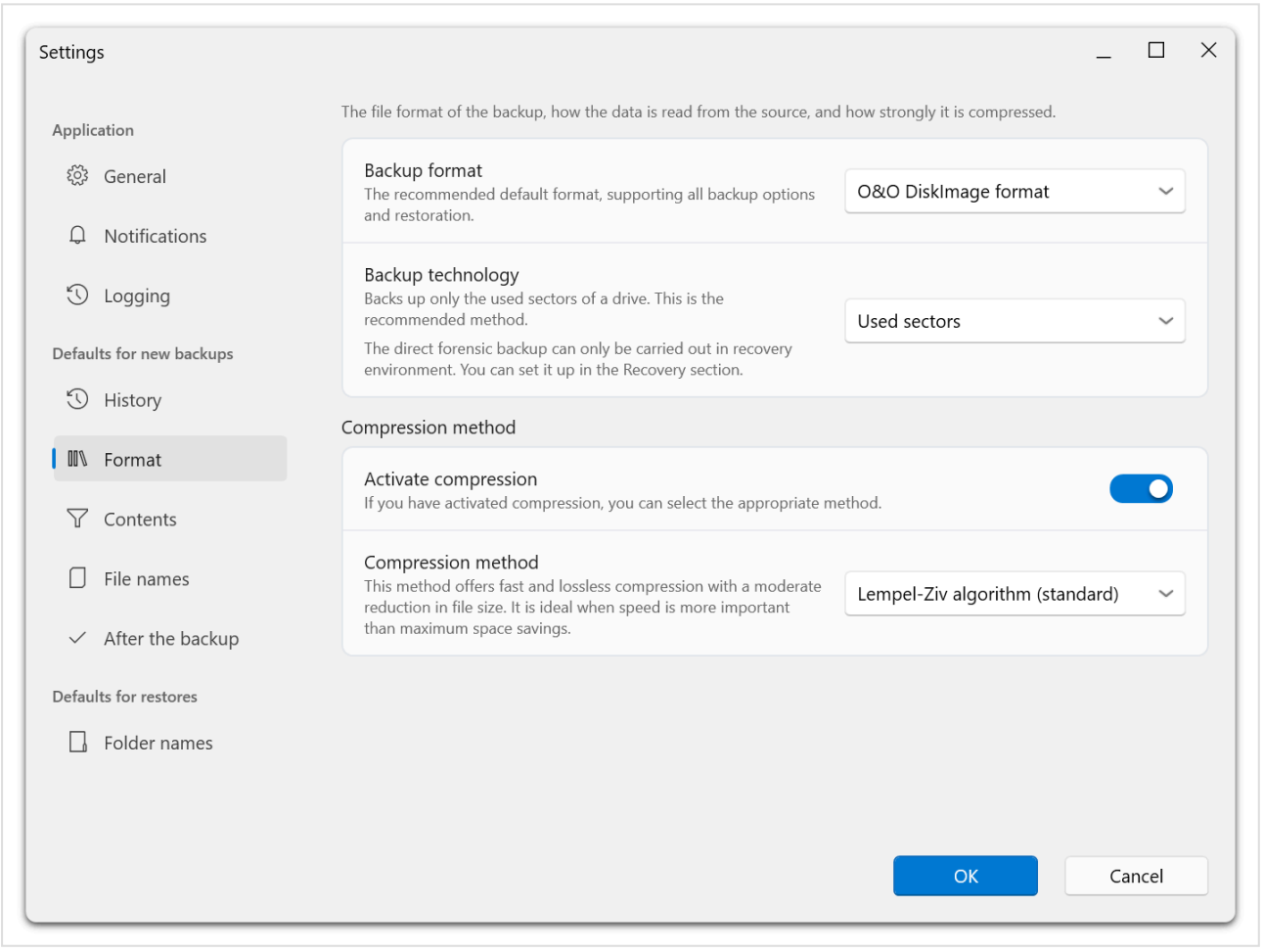
The background service stores the email configuration and sends the messages. If a password is already stored, leaving its field blank keeps it. The settings page indicates when the service is unavailable.

Defaults for new backups

Page	Purpose
History	Retention presets or custom rules, backup method, and full-backup cadence.
Format	O&O DiskImage, VHD, or VHDX; image technology and compression.
Contents	Excluded files and folders.
File names	Templates for backup folders and file names.
After the backup	Validation and report generation.

The same option pages are available for an individual plan, with a note showing which settings you are editing. Image-format and technology controls do not apply to file backups. ZIP deflate is not offered for drive images.

For plans with saved versions, encryption, format, technology, and exclusions are locked even if the backup storage is offline. See Backup options.



Format defaults for new backups include the backup format, backup technology, and compression.

Defaults for restores

Folder names controls the templates for folders used when restoring files. Review the resolved destination in the restore workflow before starting.

Backup destinations

Manage local folders, external drives, network shares, and cloud-copy destinations in the separate backup destinations dialog. Drag the destination handles to reorder the list. See Backup destinations.

Diagnostics and maintenance

Enable logs when investigating a problem or when support requests them. Engine-log changes can require a restart.

Advanced options include re-reading backup information at the next start and resetting user settings. Read the dialog's explanation before applying them. Recovery-partition validation no longer has a separate skip switch.

Glossary

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

Background service: Runs time-based schedules, second copies, the removal of expired versions, and email notifications, even when the main window is closed. See Schedules and automation.

Backup chain: A full backup together with the incremental or differential backups that depend on it. Files of a chain are kept as long as a retained version needs them.

Backup history: The versions a plan keeps for restore, set with a preset or custom retention rules. Expired versions are removed automatically unless they are kept permanently. See Backup options.

Backup plan: Stores the source, destination, schedule, and options of a backup. Each run of the plan can create a new version.

Check & Repair: A tool that checks Windows system components, system files, the file system, and the recovery environment, and offers repairs where supported. It does not repair backup files.

Cloning: Copies a source disk directly to a target disk without storing a backup history. The existing data on the target is overwritten. See Clone drives.

Destination: The location where a backup is stored: a local or external folder, a USB drive, or a network share. S3-compatible storage and WebDAV receive only a second copy. See Backup destinations.

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

Drive-triggered backup: Runs when the configured backup drive is connected. The notification-area application recognizes the drive by its serial number, volume name, size, and model.

Encryption: Protects a backup with a password that is set before the first backup. Encrypted backups cannot be restored without the original password.

File backup: A backup of selected files and folders, stored in a file-backup container. It cannot be mounted; restore its files through the restore workflow.

Forensic backup: Copies the entire source, including unused sectors, and needs space for the full source size. **Direct forensic** reads directly from the disk and is available in the recovery environment.

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

Hyper-V checkpoint: A Hyper-V differencing disk (`.avhd` or `.avhdx`). Mounting or restoring it needs all of its parent files.

Image: A backup of entire disks or partitions. Supported images can be mounted or used to restore individual files.

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

Mount: Makes a supported image available as a read-only Windows drive, so its files can be browsed and copied. See Tools.

Notification-area application: Shows progress in the Windows notification area, starts plans, cancels operations, and detects drives for drive-triggered backups.

Recovery environment: Formerly called Fortress Mode. Adds O&O DiskImage to the local Windows Recovery Environment (WinRE), so the system can be restored without a separate USB stick. See Rescue media and recovery environment.

Run: One execution of a backup plan. It can succeed, fail, or be cancelled; a failed run does not necessarily create a usable version.

S3-compatible storage: Cloud storage addressed by endpoint, bucket, region, and access keys. It can receive a second copy.

Second copy: A copy of a backup on another drive, a network share, S3-compatible storage, or a WebDAV server, created by the background service after the backup. See Second copy.

Shadow copy: A consistent snapshot of the source that Windows provides while a backup reads it. If the shadow copy is lost or overflows, unattended backups stop.

Source: The data a backup protects: the entire PC, drives and partitions, or files and folders. See Backup sources.

Startup media: A bootable USB medium or ISO file with O&O DiskImage. Use it when the local recovery environment is unavailable or the system disk is replaced.

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

Validation: Reads a backup to check its integrity and readability without restoring data or changing the source. It does not replace a recovery test.

Version: A saved backup state that can be restored.

VHD / VHDX: Microsoft virtual disk formats. O&O DiskImage can create, mount, validate, and restore them; VHD/VHDX backups are full backups of used sectors without O&O compression or password encryption.

WebDAV: A protocol for storing files on a web server. A WebDAV server can receive a second copy.

WinRE: The Windows Recovery Environment installed on the local computer. The recovery environment of O&O DiskImage builds on it.

Troubleshooting

A destination is unavailable

Reconnect the drive or check the network share, credentials, and write permissions. Use **Test connection** after changing network settings.

Scheduled network backups allow up to three minutes for a destination to become available. If it remains unreachable, review the report. A missing backup file and disconnected storage are different conditions; reconnect storage before removing an entry.

A scheduled backup did not run

Check that the plan is enabled, its start and end dates include the current date, and the background service is available and compatible with the application. Review the planned and actual run times in the report.

Enable catching up missed runs if needed. For a sleeping PC, enable wake-to-run in the schedule and allow Windows wake timers. This does not start a shut-down PC or wake it from hibernation.

For drive-triggered backups, keep the notification-area application running, connect the expected drive, and wait for the configured delay. A different drive with the same letter may not match the saved identity.

If the plan asks for its encryption password again, enter the original password on its properties page. A scheduled encrypted backup cannot run without the stored password.

A full backup ran instead of an incremental backup

Check the report's explanation. The plan may be starting a new weekly or monthly chain, its sources may have changed, or the previous version may be unavailable or unsuitable. A one-time full-backup request also starts a new chain without changing future plan settings.

The second copy failed

A **Second copy missing** warning does not invalidate a completed primary backup. Reconnect the second destination, check credentials and free space, then select **Retry copy**.

For S3 or WebDAV, also check the endpoint, bucket or folder, region, and permissions. Uploads use the computer's proxy settings, which may differ from those used by the interactive connection test. Keep the computer connected while an upload finishes.

A VHD/VHDX backup cannot start

The source must be exclusively accessible, the destination must be on a different physical disk, and the source cannot contain the running Windows installation. Close programs using the source or choose the O&O DiskImage format for a live backup. Read the specific reason on the plan page.

A backup stops after a snapshot or read error

A lost or overflowing shadow copy means the original consistent snapshot can no longer be read. Unattended backups stop; an interactive run may ask whether to continue. Read the prompt carefully before accepting a backup without that snapshot.

Source read failures also stop the backup. Review the report, check the source disk, and create and validate another backup after resolving the cause.

A backup cannot be mounted

File-backup containers cannot be mounted as drives. Restore their files through the restore workflow.

For supported images, check whether the backup is already mounted, whether a drive letter is available, and whether Windows automount or storage policies prevent mounting. Review the detailed error and logs. Do not change Windows storage policies without understanding their effect.

A restore target is rejected

Check the minimum target size and, for virtual disks, sector-size compatibility. The target cannot be the disk holding the source image or the running Windows installation. Move the backup to a separate disk or network share if its location cannot be identified, or restart into recovery for a system restore.

The backup drive is full or a file cannot be deleted

Review history settings and permanent keeps. Required chain files remain even if they are old. Choose a shorter history or a larger destination, and use the application's deletion workflow.

Unmount a backup before deleting it and close applications using the file. Deletion errors identify the affected file and, where possible, the application holding it open.

A password is not accepted

Use the original password, checking capitalization and keyboard layout. Re-entering a password for an existing plan does not change it. Encrypted backups cannot be restored without the correct password.

Reports are missing

Check report generation in the plan's **After the backup** options or, for new plans, under **Settings > Defaults for new backups > After the backup**. Deleted reports cannot be recreated merely by reconnecting their backup files.

The recovery environment is unavailable

Follow the reason shown under **Recovery** and rebuild the environment if requested. Use startup media if local recovery cannot start. For license checks, try a wired network connection. After a failed recovery operation, look for saved logs beside the backup.

FAQ

Which edition does this guide cover?

This guide covers O&O DiskImage 23 Premium Edition. Trial restrictions are shown on the relevant application pages.

Which backup should I create first?

Start with **Backup > Entire PC** and an external drive or NAS. Then prepare the local recovery environment or startup media. See Quick start.

What is the difference between a plan, a version, and a run?

A plan stores the source, destination, schedule, and options. A version is a saved backup state you can restore. A run is one execution, which may succeed, fail, or be cancelled. A failed run does not necessarily create a usable version.

How do I choose a backup method and history?

Choose a history preset and leave the method automatic for incremental backups between regular full backups. Use **Custom** to choose differential backups, full backups only, or your own retention rules. See Backup options.

Why are more old files kept than I expected?

A retained version may need earlier files in its chain. These dependencies are kept too. History uses periods with actual backups, and the presets keep at least the three newest versions. A permanent keep also prevents automatic removal.

Can backups run while the main window is closed?

Yes. The background service runs time-based schedules. Drive-triggered backups additionally need the notification-area application to detect the drive. Monthly schedules and optional wake-from-sleep are available; wake-to-run is off by default.

Can I store a copy in the cloud?

Yes. Configure a second copy to S3-compatible storage or WebDAV after creating the primary backup in a local or network folder. The second copy follows the plan's retention rules. See Second copy.

Is my backup lost if the second copy fails?

No. A completed primary backup remains usable. Fix the second destination's problem and select **Retry copy**. Check the copy status before relying on it.

Can I change the password or exclusions later?

Those options, along with image format and backup technology, are locked once the plan has saved versions. Create a new plan to use different settings. If the application has lost access to a stored password, re-enter the original password.

Can encrypted backups be restored without the password?

No. Keep the original password available independently of the PC you may need to restore.

Can I restore individual files from an image?

Yes, from supported images, including VHD backups created by O&O DiskImage. Use file restore or mount a supported image read-only and copy files in Explorer. File-backup containers themselves cannot be mounted.

Can I restore to a smaller partition?

Sometimes. The target must meet the minimum size calculated for the image, including used data and file-system overhead. Whole-disk virtual-image restores have additional size and sector requirements.

What happened to Fortress Mode?

It is now called the **recovery environment**. Open **Recovery** to prepare it, check its status, or create separate startup media. See Rescue media and recovery environment.

Does Check & Repair fix damaged backup files?

No. It checks and repairs supported Windows system components and file-system problems. Use backup validation to check a backup file, and restore from another verified version or copy if it is damaged.

Support and more from O&O

O&O Software support helps with questions and problems concerning O&O DiskImage 23.

Contact support

Open O&O Software support. Include:

- The product and Windows versions.
- The report of the failed operation.
- The source and destination types.
- Whether the run was manual, scheduled, or drive-triggered.
- Whether the problem occurred in normal Windows or in the recovery environment.

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

Licensing and updates

The trial, license activation, and what to check after an update 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.