



© O&O **software**

O&O AutoBackup 8

Table of Contents

1 Introduction	3
2 Getting started	6
2.1 Feature overview	6
2.2 O&O AutoBackup, O&O DiskImage, and OneDrive	8
2.3 System requirements	11
2.4 Install and activate	12
2.5 Your first backup	13
3 Back up your files	15
3.1 Create and edit a backup	15
3.2 Sources and destinations	17
3.3 Protect OneDrive with an offline backup	19
3.4 Scheduling and automatic protection	22
3.5 Retention and versions	24
3.6 Encryption and recovery keys	26
3.7 Run and monitor backups	28
4 Synchronization	29
4.1 Understanding synchronization	29
4.2 Every synchronization mode in detail	31
4.3 Deletions, conflicts, and safe use	34
5 Restore	36
5.1 Restore files	36
5.2 Restore an encrypted backup	38
5.3 Search backups	40
5.4 Portable recovery app	41
6 Manage O&O AutoBackup	42
6.1 Backup pairs	42
6.2 Settings	43
6.3 Logs and notifications	44
6.4 Licensing and updates	45
7 Reference	46
7.1 Backup format	46
7.2 Troubleshooting	48

7.3 Privacy and security	49
8 FAQ	50

Welcome to O&O AutoBackup

Thank you for choosing **O&O AutoBackup**. We appreciate your trust in our product and want to help you keep the files that are important to you safe.

Protect what matters

Family photos preserve memories. Personal documents, schoolwork, financial records, and creative projects may represent years of work. Many of these files cannot simply be replaced after they are lost.

O&O AutoBackup protects these files by copying the folders you choose to a separate destination and keeping earlier versions. If an original is deleted, damaged, or overwritten, you can return to a copy from before the problem occurred. Unencrypted backups remain ordinary files and folders, so accessing them does not depend on a proprietary archive format.

Why you need a backup

Data can be lost even when a PC appears to be working normally. The most common risks include:

- **User error** — a file or folder can be deleted accidentally, saved under the wrong name, or replaced with an unwanted version.
- **System or hardware failure** — a defective drive, failed Windows update, file-system error, or damaged PC can make otherwise intact files inaccessible.
- **Malware attacks** — ransomware and other malicious software can encrypt, alter, or delete large numbers of files in a very short time. A backup stored on a disconnected drive provides important separation from the affected PC.
- **Cloud synchronization** — OneDrive and similar services synchronize changes between devices. That is useful, but an accidental deletion, damaged file, or malicious change may also be synchronized.

A cloud drive is not automatically an independent backup. Its data is stored on infrastructure operated by another company, and access depends on the provider, your account, and the recovery options available at that moment. Even when a cloud service offers a recycle bin or version history, it cannot guarantee that every file and every required version can always be recovered. A separate offline copy of your OneDrive folder gives you another recovery path that is under your control.

Protection without backup expertise

O&O AutoBackup is designed so that you do not need previous backup experience. It is particularly well suited to a family PC, where important files are created by several people and backup should not depend on everyone remembering a technical routine.

A practical setup uses an external USB drive and the option to run the backup when that drive is connected:

1. Choose the folders that contain your photos, documents, and other important files.
2. Select the external drive as the destination and enable automatic backup when the drive is connected.

3. Connect the drive regularly. O&O AutoBackup recognizes it, copies new and changed files, and updates the version history automatically.
4. After the backup has completed, disconnect the drive and keep it in a safe place. This also makes it harder for malware on the PC to reach the backup.

Once this is configured, connecting the backup drive is the only regular action required. O&O AutoBackup handles the file comparison, copying, and version management. This simple routine helps ensure that a failed PC, an accidental deletion, or a malware attack does not take irreplaceable family memories and important documents with it.

What O&O AutoBackup does

- **Automatic file protection** — O&O AutoBackup can run continuously, every 15 minutes, hourly, daily, weekly, monthly, or whenever the backup drive is connected.
- **Version history** — earlier copies remain available according to the retention settings, while outdated versions are removed automatically.
- **Destinations you control** — backups can be stored on another internal disk, USB storage, a network share, WebDAV, or S3-compatible storage.
- **Optional encryption** — file contents and, if required, file and folder names can be protected with authenticated encryption and a recovery key.
- **Several recovery paths** — browse a point in time, search across backups, or launch the recovery app stored beside the backup.
- **Backup and synchronization** — create protected backups with version history or keep two folders in step.

The basic idea for first-time users

A backup needs two sides:

- The **source** is where the original files live now.
- The **destination** is independent storage that receives the protected copies.

If source and destination are on the same physical disk, a failure of that disk can destroy both. A USB drive, another physical disk, a NAS, or separately controlled remote storage is therefore a more meaningful destination.

The first backup copies the current data. Later runs detect what is new or changed, so they are usually much faster. Earlier versions remain available according to the retention policy. If a destination is temporarily missing, O&O AutoBackup waits and catches up when it becomes available again.

License and access to backup files

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

The license controls the right to use the software; it does not restrict access to unencrypted backup files. A portable recovery app can also be stored with a backup. See Licensing and updates.

Build protection in layers

O&O AutoBackup protects files; O&O DiskImage protects a complete Windows system; OneDrive synchronizes a current working set. None of those jobs makes the others unnecessary. A practical plan often combines hourly file backup, periodic system images, and cloud synchronization. See [O&O AutoBackup](#), [O&O DiskImage](#), and [OneDrive](#).

Choose your next step

If backup terminology is new, start with [Feature overview](#), then follow [Your first backup](#). If you need a file now, go directly to [Restore files](#).

File Backup Is Not A System Image

O&O AutoBackup protects files and folders. It does not create a bootable image of Windows, installed applications, or disk partitions. For whole-PC recovery, use an imaging product such as [O&O DiskImage](#) in addition to file backup.

Feature overview

The Home page shows at a glance **whether your files are protected and when the backup last ran**. It is both the starting point for common tasks and a status dashboard showing what is protected, where the backup is stored, what comes next, and whether a drive or decision is needed.

For a novice user, the product can be understood as four connected jobs: select, copy, remember, and recover.

1. **Select** the files and folders that matter.
2. **Copy** them to independent storage.
3. **Remember** earlier states instead of keeping only today's copy.
4. **Recover** a whole folder, one file, or one older version when needed.

Backup modes

Back up my files is the quickest path. It offers familiar personal folders, creates version history, and uses an automatic hourly schedule by default. It is the best starting point for most users because it answers the important questions without presenting every advanced setting first.

Custom backup lets you choose any source folders, a destination, retention limits, encryption, and schedule. A backup copies changes in one direction and preserves recoverable versions. Use it for project folders outside the normal Windows locations, several source folders in one backup, or a destination that requires special configuration.

Synchronization keeps locations aligned. Depending on the selected mode, changes can travel in one direction or both directions, and deletions may be propagated. Synchronization is useful for working copies; it is not a replacement for a versioned backup. See Understanding synchronization.

What happens during a backup

O&O AutoBackup first scans the selected sources to discover new, changed, moved, or deleted items. It compares this state with its recorded backup state and creates a plan. Only the required data is transferred, which is why a later backup is normally much faster than the first.

If a file is open exclusively, a destination is unavailable, or an online-only OneDrive file cannot be fetched, O&O AutoBackup reports the condition. It does not silently turn an incomplete run into a reassuring green status. The next suitable run can catch up.

Protection that adapts

Scheduled work runs while you are signed in and O&O AutoBackup is active in the notification area. A missed run is caught up later. If a removable destination is absent, the application waits calmly and continues when the correct drive returns. This is particularly useful for laptops: the backup routine can be “connect the drive when convenient” instead of “remember an exact appointment.”

O&O AutoBackup identifies the destination volume, so another disk that happens to receive the same drive letter is not treated as your backup disk. That protects against an easy-to-miss Windows behavior where removable

drive letters change.

Runs can wait while the PC is on battery, on a metered connection, or actively in use. These behaviors are controlled under **Settings** → **Autostart**. A deferred run is not forgotten; it becomes pending work and starts when the blocking condition clears.

Recovery choices

The restore view presents the files that existed at a selected point in time. You can restore everything or make a precise selection. Search helps locate a file when you no longer remember its folder. The optional recovery app copied to the destination lets you open the backup on another compatible PC without first setting up your original installation.

For unencrypted backups, current files also remain directly accessible through File Explorer. Encrypted backups must first be unlocked with the password or recovery key; see [Restore an encrypted backup](#).

Plain files by design

Unencrypted data is stored as regular files rather than compressed into a single archive. **No compression is a deliberate design decision**, not a missing checkbox. It favors transparency, direct access, and long-term restorability over saving destination space with a proprietary container. Version management and optional encryption add structure where needed; see [Backup format](#).

What O&O AutoBackup does not replace

- It is not a system image and cannot rebuild Windows or installed applications.
- It is not malware protection; it preserves copies but does not judge whether a source file is safe.
- Synchronization is not automatically backup, because it can propagate unwanted changes.
- OneDrive is not an independent offline copy of itself.

See [O&O AutoBackup](#), [O&O DiskImage](#), and [OneDrive](#) for a complete protection strategy.

O&O AutoBackup, O&O DiskImage, and OneDrive

O&O AutoBackup **fills the gap between cloud synchronization and full system imaging** by providing frequent, understandable protection for the documents, photos, and projects that change every day. That does not make system imaging or cloud synchronization unnecessary. The three technologies solve different problems, and the strongest protection uses each for the job it does best.

Three tools, three different questions

Tool	The question it answers	Typical rhythm	Best at
O&O AutoBackup	“Can I get this file—or yesterday's version—back quickly?”	Hourly or continuously	Personal files, version history, simple selective recovery
O&O DiskImage	“Can I rebuild this whole PC after the disk or Windows fails?”	Monthly and before major changes	Windows, installed applications, settings, partitions, complete disks
OneDrive	“Can I reach the current working copy on my other devices?”	Continuously synchronized	Availability, collaboration, sharing, and access from anywhere

The difference is easiest to remember this way:

Image monthly. File-backup hourly. Synchronize continuously.

These intervals are examples, not rigid rules. A PC used for critical work may need more frequent images; a mostly static home PC may need fewer. What matters is that a slowly changing system and rapidly changing personal files do not have to share one recovery schedule.

What O&O AutoBackup protects

O&O AutoBackup concentrates on user data: Documents, Desktop, Pictures, project folders, local archives, and—when selected—OneDrive content. It copies new and changed files, keeps earlier versions, and lets you restore one file without rolling the rest of the computer backwards.

Use O&O AutoBackup when:

- You overwrote a presentation this morning and need yesterday's copy.
- A folder was deleted accidentally.
- You want an offline copy of OneDrive files.
- You want to connect a USB drive and let protection catch up automatically.
- You want unencrypted backups to remain ordinary, directly readable files.

O&O AutoBackup does **not** recreate Windows, installed programs, boot information, or a damaged partition layout. After a total disk failure, you would reinstall Windows and applications first, then restore the files—or use a disk

image.

What O&O DiskImage protects

O&O DiskImage captures complete drives or partitions. A system image contains the elements a file backup deliberately leaves out: Windows itself, installed applications, device configuration, the registry, boot data, and the arrangement of the imaged volumes.

Use O&O DiskImage when:

- The system disk fails and the replacement should become bootable again.
- A Windows update or driver damages the installation.
- You want to return the **entire computer** to a known state.
- Reinstalling and reconfiguring every application would take hours or days.

An image is broad and powerful, but it is usually larger and slower to create than an incremental file backup. Restoring an old image also moves the whole imaged system back in time; that is excessive when only one spreadsheet is missing.

Why both products make sense

Imagine a system image from the first day of the month and hourly file backups from today:

1. The SSD fails on the 24th.
2. Restore the monthly O&O DiskImage image to the replacement SSD. Windows, applications, and settings return together.
3. Restore the newest O&O AutoBackup versions. The documents changed since the image was created return without sacrificing the fast whole-system recovery.

The products complement each other instead of competing. O&O DiskImage shortens the path back to a working **computer**; O&O AutoBackup shortens the path back to current **work**.

Where OneDrive fits

OneDrive is valuable because it keeps a working set available on several devices and in the cloud. But synchronization normally propagates changes—including unwanted changes. A deletion, damaging edit, or encrypted file can be synchronized before you notice it. Provider-side recycle bins and version histories can help, but they remain part of the same account and service.

An O&O AutoBackup copy on storage outside OneDrive creates a separate recovery path under your control. See [Protect OneDrive with an offline backup](#).

A practical protection plan

For a typical home or small-office PC:

1. **OneDrive continuously** for access and collaboration.
2. **O&O AutoBackup hourly** to a separate disk or NAS for recent files and versions.

3. **Disconnect or isolate one backup copy** so a problem on the PC cannot immediately reach it.
4. **O&O DiskImage monthly**, and before major Windows or hardware changes, for complete system recovery.
5. Test one file restore and one image-recovery procedure before an emergency.

Bundle The Recovery Layers

If both lost files and a failed PC would be painful, use both O&O AutoBackup and O&O DiskImage. They protect different layers of the same computer.

System requirements

Supported operating systems

- Windows 10 or Windows 11
- A supported 64-bit Windows PC
- A normal user account; administrator rights are requested only for system-wide actions such as autostart for all users

The application is delivered as a self-contained Windows program. A separate .NET installation is normally not required.

Storage and connectivity

The destination must have enough space for the first copy and the versions retained afterwards. O&O AutoBackup displays the estimated backup size and available capacity during setup.

Supported destination types include:

- Local fixed disks and separate internal disks
- USB hard disks, SSDs, and flash storage
- Windows network paths (UNC)
- WebDAV servers
- S3-compatible object storage

Credentials and network access may be required for remote destinations. For unattended runs, make sure the destination remains accessible in the Windows session that runs O&O AutoBackup.

Practical recommendations

Use a destination on a different physical device from the source. A second folder on the same disk helps with accidental edits, but it does not protect against disk failure, theft, or ransomware affecting that disk.

For laptops, a removable drive plus **run when connected** is often the simplest routine. For always-on PCs, a NAS or another local disk works well with a regular schedule.

Locked Files

Files held exclusively open by another application may have to wait for a later run. Close the application that owns the file and run the backup again. O&O AutoBackup reports skipped or in-use files rather than silently claiming they were protected.

Install and activate

O&O AutoBackup is supplied as a single program file. You can start it directly, then let it move itself to a permanent location before relying on automatic backups.

Put the program in a permanent place

1. Start the downloaded O&O AutoBackup program.
2. Open **Settings** → **General**.
3. Under the program location section, choose **Move to a permanent place** if O&O AutoBackup warns that the current folder may be cleaned up.
4. Choose whether to create Start menu and desktop shortcuts.
5. Restart O&O AutoBackup when prompted.

Downloads and temporary folders are poor locations for scheduled software. If Windows or a cleanup tool removes the executable, automatic backups can no longer run.

Activate your license

During the trial, the title and About page identify the application as an unregistered trial version and show the remaining evaluation time.

1. Open the **About** page from the information button.
2. Select the option to enter or buy a license.
3. Follow the registration wizard and enter the license information supplied with your purchase.
4. Restart if requested, then check the displayed license type and serial number.

Internet access may be needed to validate the license. If validation fails, check the connection and firewall or proxy policy, then retry. O&O Support can help if the license remains unavailable.

Move a license to another PC

Open **About** and select **Release license** before retiring or reinstalling the current PC. Releasing returns the application to trial state and may make it unusable if the trial has expired. License transfers remain subject to your license agreement.

A License Is Required

The trial is for evaluation. A valid license is required to continue using O&O AutoBackup after the trial ends.

Your first backup

The quickest setup protects your personal folders with sensible automatic defaults. You do not need to understand every retention or scheduling option before beginning; the wizard explains the few decisions that affect where the data goes and what is included.

Before you start

Connect the external drive you want to use, or make sure your network destination is reachable. Avoid using the same physical disk that contains the original files.

Before opening the wizard, ask two simple questions:

- **What would be painful or impossible to recreate?** Documents, photos, personal videos, source code, financial records, and creative projects usually belong in the answer.
- **What failure should this copy survive?** If the answer includes failure or theft of the PC, choose storage outside that PC.

The first run may need roughly as much free destination space as the selected sources. Version history requires additional space later, depending on how often those files change.

Create the backup

1. On the Home page, choose **Back up my files**.
2. Select the content to protect. O&O AutoBackup offers familiar locations such as Desktop, Documents, Pictures, Music, Videos, and Downloads, with size and file-count estimates. Start with irreplaceable data; caches and installed programs do not belong in a file backup.
3. Review any detected OneDrive folders. If Desktop, Documents, or Pictures were moved into OneDrive, select either the account or the moved folders—not both. See [Protect OneDrive with an offline backup](#).
4. Choose the destination. Check the capacity bar, connection status, and destination path that O&O AutoBackup will create. Existing unrelated files on the drive are not removed.
5. Review the summary. The default schedule is automatic and the portable recovery app is enabled. Follow **Change** if you need a different schedule or retention policy.
6. Decide whether the destination requires encryption. A USB drive that could be lost is a common reason to enable it. Save the recovery key somewhere else.
7. Choose **Start protecting my files**.

The first run can take longer because every selected file has to be copied. Later runs normally transfer only new and changed content. You may pause or stop a run; O&O AutoBackup catches up when it can continue.

While the first backup runs, the progress page separates scanning from copying. Scanning discovers what needs attention; copying transfers the content. OneDrive online-only files may add a download phase before they can be written to the backup.

Check that protection is active

Return to the Home page. The **My files** card shows the last backup, next planned run, destination, and any item that needs attention. A green or protected state should correspond to a completed run, not merely to a schedule that exists.

If the drive is disconnected, reconnect the same drive; O&O AutoBackup recognizes it and resumes automatically when drive-connect behavior is enabled. If Windows assigns it a new letter, the recorded volume identity helps O&O AutoBackup find the correct device.

Test recovery

A backup is only useful if you know how to restore it. After the first run:

1. Open **Restore**.
2. Select one harmless file.
3. Choose an older restore point if more than one already exists.
4. Restore to a temporary folder rather than over the original.
5. Open the restored file.

For an encrypted backup, perform the test once with the password and make sure the saved recovery key matches the displayed Vault ID. This confirms the destination, credentials, and recovery routine before you depend on them.

What to do next

- Leave O&O AutoBackup configured to start with Windows and remain in the notification area.
- Connect removable destinations regularly.
- Review the Home page after the first few scheduled runs.
- Keep at least one copy offline or otherwise isolated.
- Create periodic O&O DiskImage images for whole-system recovery.

Next: Create and edit backups or Restore files.

Create and edit a backup

A backup pair connects one or more source folders with one destination and stores the schedule, retention, filters, and security choices for that job. Once configured, the same protection rules are applied to every run.

Keeping those decisions together makes automatic operation possible. You do not select everything again for each run; O&O AutoBackup opens the pair, checks what changed, and applies the same protection policy.

Create a custom backup

1. From Home, select **Create custom backup or sync**.
2. Choose **Create Backup** and then **Back up custom folders**.
3. Add the folders you want to protect. Remove overlapping selections so the same file is not copied twice.
4. Choose a local, removable, network, WebDAV, or S3 destination.
5. Review the summary and use **Change** beside schedule or retention if the defaults do not fit.
6. Decide whether to enable encryption and the portable recovery app.
7. Select **Start protecting my files**.

Plan a pair before creating it

Avoid making one enormous pair simply because all data belongs to the same user. Separate pairs can be useful when sources need different destinations, schedules, or security:

- Work documents may run hourly to an encrypted NAS destination.
- A large photo archive may run when an external drive is connected.
- OneDrive may use “download, back up, then free up space.”
- Temporary project exports may need no backup at all.

On the other hand, putting several related personal folders into one pair keeps the Home page simpler and lets them share one restore history. Choose based on recovery needs, not merely folder count.

Edit an existing backup

Select a pair on the Home page and choose **Change**, or double-click the pair. You can update sources, destination behavior, file selection, schedule, and retention. Save the pair when finished.

Changing the source does not delete previously backed-up files immediately; retention rules determine how historical versions are kept. That prevents a configuration mistake from instantly erasing the recovery history.

Changing a removable destination should be done through the application so O&O AutoBackup records the correct volume identity. Copying the destination folder in Explorer and merely editing a drive letter can leave the pair associated with the wrong device.

Encryption and name hiding become fixed once the backup has run. Existing readable files cannot honestly become encrypted after the fact, and encrypted files do not become readable because a switch was turned off.

Create a new pair with an empty destination when changing that design choice.

Delete a pair

Deleting a pair removes its configuration and restore points from the O&O AutoBackup interface. It does **not** delete the files already stored at the destination. Read the confirmation carefully, then clean the destination manually only when you are certain it is no longer needed.

Before deleting a pair, open its destination and perform a test restore. If the pair is being replaced, keep the old destination until the new backup has completed and been tested.

Use Descriptive Names

Names such as “Laptop documents → Office NAS” are easier to diagnose than “Backup 2,” especially once you have several pairs.

Sources and destinations

The source answers **what must be protected**. The destination answers **which failures the backup can survive**. A perfect folder selection on unsuitable storage is still a weak backup, so treat both choices as equally important.

Choosing sources

Select the folders containing irreplaceable work, photos, projects, and other personal data. The content tiles show estimated sizes and file counts before the first run. These estimates help you understand both the first-run duration and the minimum destination capacity.

Good sources are data you created or collected. Windows and installed applications can usually be reinstalled; their program folders are not a substitute for a system image and may contain files that cannot be restored into a working installation by simple copying.

O&O AutoBackup normally excludes operating-system and program folders because they are not useful in a file-only recovery. Custom exclusions and file-type groups can be managed in **Settings** → **Folders** and **Settings** → **Filter**.

Cloud placeholders require special care. When OneDrive integration is enabled, an online-only file may have to be downloaded before it can be backed up. This uses bandwidth and temporary local disk space. O&O AutoBackup can return the file to its placeholder state after processing. See [Protect OneDrive with an offline backup](#).

Choosing a destination

The destination page displays available capacity and how much the backup is expected to use. O&O AutoBackup creates its own folder; other data on the disk remains untouched.

- **USB drive:** portable and easy to disconnect from ransomware, but protect it from loss and damage.
- **Separate internal disk:** always available and fast, but still inside the same PC.
- **Network share:** useful for several PCs; confirm that the signed-in account has persistent access.
- **WebDAV or S3:** suitable for a compatible remote service; performance depends on connection speed and provider behavior.

What each destination protects against

Destination	Survives source-disk failure	Can be isolated from the PC	Available without internet	Main concern
Another folder on the same disk	No	No	Yes	Same hardware and malware boundary
Separate internal disk	Yes	Usually no	Yes	Remains exposed inside the PC
Removable USB drive	Yes	Yes, when disconnected	Yes	Must be connected regularly and stored safely
NAS/network share	Yes	Depends on permissions/snapshots	Usually on local network	Credentials, network, and ransomware reachability
WebDAV/S3	Yes	Depends on account design	No	Provider, credentials, bandwidth, and recovery time

For important data, one destination rarely covers every risk. A regularly connected destination gives frequent recovery points; a disconnected or separately credentialed copy provides isolation.

Removable-drive safety

Windows can assign a different drive letter after reconnecting a device. O&O AutoBackup records the destination volume and can relocate it safely. It refuses to write to an unrelated disk merely because that disk received the old letter.

This is why you should use **Choose another destination** when replacing a drive instead of making a new device imitate the old path. O&O AutoBackup can then record the intentional change.

Destination space

If space runs low, reduce how long old versions are kept or free space on the destination. With managed retention, the oldest eligible versions are removed while the newest version of every file is preserved.

Capacity planning should include change, not only today's source size. A 500 GB photo archive that rarely changes needs little extra version space; a 50 GB project whose large files change daily can create far more history. Check the destination after the first week and again after a typical busy period.

Keep At Least One Offline Copy

A permanently connected backup can be reached by malware or accidental deletion. Periodically disconnect a removable destination or maintain another independent copy.

Protect OneDrive with an offline backup

OneDrive synchronizes files between devices and makes them available for sharing and collaboration. It is not, by itself, an independent backup of your data. A cloud copy can reproduce the very change you wanted protection from, including an accidental deletion or unwanted overwrite.

Synchronization is not independence

When a file changes in a synchronized OneDrive folder, the service's job is to carry that change to the cloud and your other devices. That is normally exactly what you want. It becomes a problem when the change was unwanted:

- You delete a folder and the deletion synchronizes everywhere.
- An application saves a damaged or incomplete file over the good copy.
- Malware encrypts files that OneDrive can see, and those encrypted versions synchronize.
- Someone with access to the account removes or alters data.
- You lose access to the account or need files while the service or internet connection is unavailable.

OneDrive may offer its own versioning and recovery features, but those copies remain inside the same provider, account, and administrative boundary. An offline or separately controlled backup gives you a second route to the data.

What “offline copy” means

An offline copy is stored somewhere that is not simply another synchronized OneDrive folder: for example, a USB drive that is disconnected after backup or storage with access separated from the OneDrive account.

The copy has three important properties:

1. **OneDrive deletions do not automatically remove it.** O&O AutoBackup's version history preserves recoverable points in time.
2. **It remains available without the cloud account.** You can restore from the destination with the recovery app.
3. **It is a separate security boundary.** A disconnected drive cannot be modified through a compromised OneDrive session.

Select OneDrive content in O&O AutoBackup

O&O AutoBackup detects personal and business OneDrive accounts configured for the current Windows user.

1. Start **Back up my files** or create a custom backup.
2. Select the OneDrive account or folders you want to protect.
3. If OneDrive has moved Desktop, Documents, or Pictures into the account, follow the notice in the picker: select the whole account **or** the moved folders, not both.
4. Choose a destination outside that OneDrive account.

5. Review how online-only files will be handled.

OneDrive folders nested inside a broadly selected source are excluded by default so selecting your whole user profile does not unexpectedly download the entire cloud. A OneDrive folder that you select explicitly as a source is backed up.

Files On-Demand and online-only placeholders

An online-only OneDrive file looks like a file in Explorer, but its contents are not currently stored on the PC. O&O AutoBackup cannot copy bytes that are not present, so OneDrive must first deliver them.

O&O AutoBackup offers these strategies:

Choice	What O&O AutoBackup does	When it is useful	Trade-off
Automatic (recommended)	Asks when online-only files are first encountered and remembers the decision for this backup pair	Most users	You make the choice with the actual file count and size in view
Download and back up	Downloads the files, backs them up, and leaves them available locally	PCs with enough disk space that should also hold a local OneDrive copy	Uses local storage after the run
Download, back up, then free up space	Downloads each file, copies it, and asks OneDrive to make it online-only again	Large cloud libraries on PCs with limited free space	Slower and temporarily uses bandwidth and disk space
Skip online-only files	Backs up only content already present on the PC	A deliberately partial local backup	Skipped cloud-only files are not protected by this backup

If there is not enough local space to download every required file, the run protects everything it can and reports the skipped items. Free space and use the catch-up action so those files can be collected later.

Bandwidth, time, and destination size

The first offline copy may download a large amount from OneDrive and then upload or copy it again to the destination. For a remote O&O AutoBackup destination, that means two network transfers. Start the first run on a stable, unmetered connection and leave enough time for completion.

Later runs normally process only new and changed files. The Home page and log distinguish files fetched from the cloud and files that could not be collected.

Recover after an unwanted cloud change

If a bad change has already synchronized:

1. Pause OneDrive synchronization if continuing changes could make the situation worse.
2. Connect the O&O AutoBackup destination.

3. Open **Restore** and choose a restore point from before the deletion or edit.
4. Restore to a separate folder first.
5. Verify the files, then decide what should be copied back into OneDrive.

Restoring to a separate folder avoids immediately feeding partially checked data back into synchronization.

Do Not Back Up OneDrive Into OneDrive

Choose a destination outside the account you are protecting. A backup stored inside the same synchronized tree is exposed to the same synchronization, account, and availability problems.

Scheduling and automatic protection

Open a backup pair and select its automatic-backup settings to choose when it runs. Scheduling is a balance between **recovery freshness** and **resource use**: the more often protection runs, the less recent work can be lost, but the PC, destination, and network are used more frequently.

The maximum amount of recent work you could lose is often called the recovery-point objective. An hourly schedule aims to limit that window to roughly an hour when the PC and destination are available. It does not promise completion at every exact hour if the machine is sleeping or the drive is absent; O&O AutoBackup catches up when it can.

Available schedules

- **Continuously** — watches for file changes and starts after a short quiet period.
- **Every 15 minutes** — frequent protection without continuous monitoring.
- **Hourly** — the default for personal-file protection.
- **Daily, weekly, or monthly** — run at the chosen time and, where applicable, weekday or day of month.
- **Manual only** — runs only when you start it.

Choosing a schedule

- Use **Continuous** for small, frequently edited document sets when the destination is normally reachable.
- Use **Every 15 minutes** for active work where losing an hour would be costly.
- Use **Hourly** as a strong general default for personal files.
- Use **Daily or weekly** for large, slowly changing archives.
- Use **Manual only** only when another routine reliably reminds you; forgotten manual backups are a common failure mode.

Intervals align to the clock rather than drifting from one completion time to the next. A due run is not started back-to-back with one that has just finished.

Continuous mode waits for a short quiet period after a change. This avoids starting a new backup for every temporary write while an application is still saving. If a file keeps changing, a maximum extension count prevents indefinite postponement.

Run when the drive is connected

For removable storage, O&O AutoBackup can begin when the correct destination appears. This is often more reliable than expecting a laptop and its USB drive to be present at one exact time. If a backup was interrupted, reconnecting the drive allows it to continue.

A practical laptop routine is to connect the drive at the desk, let O&O AutoBackup catch up, confirm the protected state, and disconnect it again. The disconnection creates isolation; regular reconnection keeps the recovery point fresh.

Autostart is required

O&O AutoBackup performs scheduled work itself. Under **Settings** → **Autostart**:

1. Enable startup for the current user or all users.
2. Enable **Keep running in the notification area**.
3. Optionally delay the first run after sign-in or run only while the PC is idle.
4. Decide whether automatic work may run on battery and metered networks.

Closing the window can hide it to the notification area. If autostart or tray operation is disabled, schedules only run while O&O AutoBackup is open.

“For all users” requires administrator rights and an application location accessible to all accounts. Most single-user PCs should use the current-user option.

Missed and deferred runs

Sleep, shutdown, battery policy, a metered connection, or a missing destination can defer work. O&O AutoBackup reports the reason and catches up when the condition clears. Use **Run now** when you do not want to wait for the next slot.

Do not interpret “scheduled” as “completed.” The Home page’s last-successful-run state is the evidence that data reached the destination.

Retention and versions

Each successful backup creates another recoverable state. Retention controls how much history remains without allowing old copies to consume the entire destination.

The newest copy answers “what do I have now?” Earlier versions answer different questions: “What did this look like yesterday?”, “What was in the folder before I reorganized it?”, and “Can I recover a file that disappeared last week?” A backup with only the newest state cannot answer those questions.

Managed thinning

The standard policy keeps dense history while changes are fresh and thins it as they age:

- Every version from the most recent hour
- One version per hour for the last 24 hours
- One version per day for the last month
- One version per week for older months

When the destination runs low on space, the oldest eligible backups can be removed automatically. The newest stored version of every protected file is kept.

This graduated policy preserves detail where it is most useful. Recent mistakes are often noticed quickly, so recent versions remain dense. Older recovery points are spaced farther apart, providing long-term history without treating every hour from months ago as equally valuable.

Optional limits

Depending on the selected policy, you can keep all versions, limit retention by age, or let available destination space set the practical boundary. More history improves recovery choices but requires more capacity.

Keep all is appropriate only when destination growth is monitored and storage is intentionally expanded. A time limit is predictable but can remove the only old copy of a rarely noticed deletion. Space-managed retention adapts to actual usage but still requires enough room for current data.

What counts as a version

A new copy is needed when the source file changes. Unchanged data is not rewritten unnecessarily. Deleted source files remain recoverable while a retained restore point still references them.

Retention is not immediate synchronization: deleting a source file from a backup pair does not necessarily remove all historical copies. Use the restore timeline to select the state you need.

Example

Suppose `Budget.xlsx` is edited at 09:00, 10:00, and 15:00. The backup may initially retain all three versions. As they age, the policy can thin the dense history while keeping representative hourly, daily, and weekly points.

Restoring from noon shows the 10:00 version; restoring from the previous day shows the version that existed then.

Retention operates on stored history, not on the live source. Removing an old restore point does not delete the current source file.

Plan For Change Rate

The first backup size is only the baseline. Frequently edited media projects or databases can produce much more history than mostly static documents. Review destination capacity after the first week.

Encryption and recovery keys

Encryption protects a backup if its drive or remote storage is accessed by someone else. O&O AutoBackup encrypts files individually with authenticated AES-256-GCM and derives the key from the password with Argon2id. It can also hide file and folder names.

The technical terms matter less than the practical promise: without the password or recovery key, copied backup data should not be intelligible. Authentication also lets O&O AutoBackup detect encrypted content that has been altered rather than quietly returning corrupted plaintext.

Encryption is most valuable for a portable drive that could be lost, a shared location, or storage you do not physically control. It also adds responsibility: recovery credentials become part of the backup system.

Enable encryption

During backup setup:

1. Enable **Encrypt this backup** on the summary page.
2. Enter a password of at least eight characters. Longer is more valuable than merely substituting a few symbols.
3. Repeat the password exactly.
4. Save, print, or securely copy the generated recovery key.
5. Confirm that the key has been stored somewhere safe before finishing.

Save or print the recovery key and keep it somewhere separate from the backup destination and the protected PC. A password manager and a secured paper copy are good complements. The key is shown during setup; do not assume it can simply be displayed again later.

Permanent design choice

Encryption changes how the destination is written. Treat the choice made during setup as permanent for that backup. If you need a different security configuration, create a new backup pair and destination.

Why? Turning encryption on later would leave earlier files readable, while turning it off would not decrypt data already stored. A label claiming that a mixed destination is encrypted would be dangerously misleading.

Only Backup mode supports encryption. A synchronized destination is a working folder whose files must remain directly editable; encrypting them into backup objects would defeat that purpose.

Hide names as well as contents

Encryption protects file contents, but readable names such as `Tax Return 2026.pdf` can still reveal sensitive information. **Also hide file names and folders** stores data under random names and keeps the directory structure in an encrypted index.

With name hiding enabled, manual recovery through Explorer is intentionally impossible. Keep the portable recovery app with the destination and preserve the encrypted index. O&O AutoBackup can rebuild a missing index from stored objects, but some historical organization details cannot be reconstructed perfectly.

Open an encrypted backup

When browsing or recovering the backup, enter its password. If the password is forgotten, choose the recovery-key option and enter the saved key. Letter case and dashes in the recovery key are not significant.

The unlock dialog can remember access on the current PC so scheduled runs do not prompt each time. Another PC still requires the password or recovery key. See [Restore an encrypted backup](#) for the complete recovery procedure.

Important limits

- O&O Support cannot reconstruct a lost password or recovery key.
- The password should not be stored on the same removable drive as the only backup copy.
- Encryption protects stored backup data, not the unencrypted source files on the PC.
- Losing the destination still loses the backup; encryption does not replace multiple copies.
- Anyone holding the recovery key can read the backup; it is not a harmless receipt.
- Encryption does not compress the files or make the backup smaller.

Keep The Recovery Key

Without the password or recovery key, an encrypted backup cannot be restored. Verify the password with a test restore and confirm that the recovery sheet's Vault ID matches the backup before trusting it.

Run and monitor backups

Start a run

Select **Back up again** on a backup card, use **Back up all now** for all due pairs, or start a run from the notification-area menu. A progress page shows scanning, current file, counts, transferred size, and destination.

You can pause or cancel without invalidating earlier completed work. The next run scans again and catches up with outstanding changes.

Read the Home page

Each pair reports its last and next run and whether attention is needed. Typical states include:

- **Protected** — the latest run completed.
- **Waiting for the backup drive** — reconnect the recorded destination.
- **Paused on battery or metered network** — change policy or wait for the condition to clear.
- **Files in use** — close the owning application and run again.
- **Destination full or unreachable** — restore connectivity or capacity.

Calm waiting states are not failures. They explain why work is pending and what will make it continue.

Notification area

The tray icon keeps schedules active without leaving the main window open. Its menu can open O&O AutoBackup, start work, show backups, or cancel an active operation.

Notifications default to problems only. Routine “started” and “finished” messages stay quiet; the Home page and log retain that history.

Review the log

Open **Log** to inspect completed operations, warnings, and errors. For recurring failures, note the pair, time, source path, destination, and exact message before contacting support.

Understanding synchronization

Synchronization is a controlled way to make two folders agree. It is useful when both locations participate in a workflow—for example, a project folder on a PC and a portable working copy. It is not automatically a backup, because some synchronization modes intentionally overwrite or delete data.

Backup asks “what did this look like before?”

A versioned backup protects history. If today's file is wrong, you can return to yesterday's version. If a source file is deleted, retained restore points can still contain it. The destination is primarily for recovery, not everyday editing.

Synchronization asks “how should these folders agree now?”

A synchronization compares left and right, creates a preview, and applies the selected rules. Depending on the mode, it can:

- Copy in one direction or both directions.
- Replace an older file with a newer one.
- Carry renames and deletions to the other side.
- Combine two sets without deleting anything.
- Resolve a file that changed independently on both sides.

The **same folders can produce completely different outcomes depending on the mode**. Choose the intent first, then create the pair.

A simple decision guide

Your goal	Choose
Recover old and deleted versions	Backup
Add/update files on the right but never remove right-side files	Copy
Combine everything from both folders and never propagate deletions	Merge
Make the right folder an exact replica of the left	Mirror
Work in both folders and carry all changes both ways	Two-way

See Every mode in detail before choosing Mirror or Two-way for valuable data.

Left and right matter

In one-way modes, the **left** folder is the source and the **right** folder is the destination. Reversing them reverses the result. In two-way modes, both sides can provide changes, but conflict policies still refer to left and right.

Use names that preserve the direction, such as `Laptop projects → USB working copy`. Before the first run, confirm both paths in the preview.

The preview is your safety check

Before O&O AutoBackup applies synchronization changes, the preview summarizes files to create, update, move, delete, or skip. Read it as a proposed transaction:

- A high number under **Removed** deserves investigation.
- Unexpected changes in the opposite direction usually mean the wrong mode or reversed folders.
- A conflict means the same logical file changed on both sides since the last comparison.

Canceling the preview changes nothing. When the result is surprising, go back and correct the pair instead of approving it experimentally.

Use Backup And Synchronization Together

Synchronization keeps working folders convenient. A separate Backup pair preserves history when convenience propagates the wrong change.

Every synchronization mode in detail

O&O AutoBackup offers five modes in the pair wizard. **Backup** is included beside the synchronization modes so you can choose the desired outcome in one place.

Backup — keep every version

Idea: Copy new and changed files from left to right while preserving history. Nothing at the destination is deleted merely because it disappeared from the source. A changed file becomes another date-stamped version.

Ideal scenario: Maximum protection for documents, photos, and projects when recovery matters more than keeping the destination visually identical to the source.

Outcome: The destination grows into a versioned history. You can restore deleted files and earlier copies through O&O AutoBackup. Managed retention thins old history and prevents unrestricted growth.

Challenge: It requires the most destination space over time. It is not intended as an everyday working folder because older versions are part of the backup structure.

Copy — add and update, never remove

Idea: Copy new and changed files from left to right. A changed file replaces the older destination copy; the replaced item is sent to the Recycle Bin. Deleting a file on the left does not delete it on the right.

Ideal scenario: Maintaining a convenient secondary collection that should accumulate source files, such as copying exports to a review folder or adding new media to a library.

Outcome: The right side contains current copies of files still present on the left plus older right-side files whose source was deleted. There is no O&O AutoBackup version history.

Challenge: The destination can collect stale files because source deletions never clean it. Replaced files depend on the Recycle Bin rather than managed backup retention.

Merge — combine both folders, never delete

Idea: Copy new and changed files in both directions until each side contains the combined set. Deletions are not propagated.

Ideal scenario: Bringing together two incomplete collections without losing files—for example, merging photo folders from two PCs before organizing them.

Outcome: Both folders contain the union of the two starting sets. A file deleted from one side but still present on the other is copied back.

Challenge: Merge cannot be used to tidy a folder by deletion because the other copy resurrects the file. If the same file changed differently on both sides, the configured conflict policy decides the result.

Mirror — make the right folder an exact replica

Idea: Treat the left folder as authoritative. New files, changes, renames, and deletions are carried from left to right so the right side matches the left.

Ideal scenario: Publishing a prepared folder to a replaceable destination, maintaining a ready replica, or updating a device whose content should be exactly the same as the master folder.

Outcome: After a successful run, the right folder is an exact current copy of the left. Extra right-side items are removed, normally through the Recycle Bin.

Challenge: A mistaken deletion on the left is intentionally propagated. A unique file placed only on the right is considered unwanted and can be removed. Mirror has no version history of its own.

Two-way — keep both folders in step

Idea: Apply new files, edits, renames, and deletions from either side to the other. Both locations are treated as active working folders.

Ideal scenario: Working alternately from two locations, such as a desktop folder and a portable drive, when both sides may legitimately change.

Outcome: Both folders converge to the same current state. If one side deleted a file since the previous run, the deletion is carried to the other. If both sides changed the same file, the conflict policy is applied.

Challenge: This is the most demanding mode to reason about. An unwanted edit or deletion can travel both ways, and clock differences can affect a “newest wins” decision. Always inspect the preview and keep a separate versioned backup.

Comparison at a glance

Mode	Direction	Propagates deletion?	O&O AutoBackup version history?	Final intention
Backup	Left → Right	No	Yes	Recoverable history
Copy	Left → Right	No	No	Add/update collection
Merge	Left ↔ Right	No	No	Union of both folders
Mirror	Left → Right	Yes	No	Right exactly matches left
Two-way	Left ↔ Right	Yes	No	Both current folders match

“No Deletion” Does Not Mean “Backup”

Copy and Merge avoid propagated deletions, but changed files do not receive O&O AutoBackup's managed version history. Use Backup when you need dependable earlier versions.

Deletions, conflicts, and safe use

Most synchronization surprises come from two events: a file was deleted on one side, or the same file was edited independently on both sides. O&O AutoBackup exposes both in the preview so you can decide before data changes.

How deletion propagation works

Mode	If a file is deleted on the left	If a file is deleted on the right
Backup	Destination history remains available	Destination should not be edited manually
Copy	Right-side copy stays	No change is sent back to the left
Merge	The right copy returns to the left	The left copy returns to the right
Mirror	The right copy is removed	A left copy recreates it on the right
Two-way	The deletion is applied to the right	The deletion is applied to the left

Mirror and Two-way normally move removed or replaced files to the Windows Recycle Bin first. That is a helpful safety net, but not a retention policy: Recycle Bin capacity and cleanup are controlled by Windows. Keep a Backup pair when the files matter.

Renames can look like copy plus deletion

O&O AutoBackup detects renames where possible so a moved file does not need to be copied again. If identity cannot be established—for example across some storage types—the preview may show a create at the new path and a removal at the old path. The final folder can still be correct, but review large unexpected operations before continuing.

When the same file changed on both sides

A conflict exists when both copies changed since the previous synchronization. Under **Advanced**, choose the policy that matches your workflow:

- **Keep the newest** — use the modification time. Convenient, but dependent on accurate clocks and timestamps.
- **Keep both** — preserve both variants so you can compare them. This is the safest general choice when edits are valuable.
- **Left wins** — always use the left copy for a conflict.
- **Right wins** — always use the right copy for a conflict.
- **Skip the file** — leave the conflict unresolved for manual attention.

The policy applies to actual conflicts, not every ordinary one-sided change.

A safe first synchronization

1. Make a versioned backup of both folders.
2. Give the pair a directional name.
3. Run manually before enabling a schedule.
4. Read the preview totals and inspect every proposed deletion.
5. Test with a small, non-critical folder if the mode is new to you.
6. Confirm the result on both sides.
7. Only then enable automatic or continuous operation.

Continuous synchronization needs extra care

Continuous mode reacts after a quiet period following changes. It is convenient, but it shortens the time between a mistake and its propagation. For Mirror or Two-way, retain a separate versioned Backup pair and avoid using both sides while a large reorganization is still in progress.

What to do after a wrong synchronization

1. Stop the pair so another run cannot compound the problem.
2. Check the Recycle Bin for files removed or replaced by synchronization.
3. Do not make broad edits on both sides while diagnosing the event.
4. Restore from the independent Backup pair to a separate folder.
5. Compare and verify before putting files back into synchronized locations.

Deletion Is A Feature In Mirror And Two-Way

These modes are doing their job when they propagate a deletion. The protection against a mistaken deletion is a separate versioned backup—not a hope that synchronization will ignore it.

Restore files

O&O AutoBackup provides several ways to restore files. Recovery does not have to depend on the original PC or its original O&O AutoBackup configuration.

Choose the recovery situation

Situation	Best starting point
The original PC and pair still exist	Select the pair on Home and choose Restore
The pair was deleted or this is another PC	Choose Restore from an existing backup
O&O AutoBackup is not installed	Run Recover this backup from the destination
You only need a current unencrypted file	Copy it directly with File Explorer
You do not remember the file's folder	Use Search backups
The backup is encrypted	Unlock it as described in Restore an encrypted backup

Whichever route you choose, restoration reads the backup and writes copies to a target folder. It does not remove the stored backup versions.

Restore from the Home page

1. Select the backup pair and choose **Restore**.
2. If the destination is disconnected, connect it and retry.
3. Choose **Restore entire backup** or **Restore selected files**.
4. For a selective restore, browse the tree or file list and mark the items you need.
5. Use the date controls to **go back in time** and display the state from an earlier restore point.
6. Choose the target folder.
7. Review the selection and start the restore.

Restore everything or select items

Restore entire backup is appropriate after replacing a data drive or rebuilding a user account. Confirm that the target has enough free space and consider restoring one top-level folder first as a test.

Restore selected files is safer for everyday mistakes. The tree view preserves folder context, while the all-files view is useful when names matter more than original locations.

Restoring to a separate folder is safest when you want to compare an earlier file with the current one. If you restore to the original location, review the overwrite choice carefully. A separate folder also prevents a cloud synchronization client from immediately distributing restored data before you have checked it.

Open an existing backup

Choose **Restore from an existing backup** on Home when the pair is not configured on this PC. Select the drive or backup folder, then follow the same file-selection flow.

O&O AutoBackup reads the backup's own metadata; it does not need the original pair settings file. Network destinations may take longer because every folder listing requires communication with the remote system.

Point-in-time view

The displayed date controls which versions appear in the tree. A file deleted yesterday can still appear when you select a restore point from before its deletion. Moving between restore points does not change the backup; it only changes the view.

Think of each restore point as a window into the folder at that time. If a file was renamed, its earlier name may appear in an earlier point. If it was deleted, move to a date before deletion. If it was overwritten, compare several nearby versions rather than assuming the latest stored version is the good one.

Restore with the portable recovery app

When **Keep a copy of the program with the backup** is enabled, the destination contains **Recover this backup**. Launch it on a compatible Windows PC. The restricted recovery mode opens directly on that backup, does not configure scheduled work on the PC, and does not require a product license.

This is the preferred disaster-recovery route because the tool needed to interpret versions travels with the data. See Portable recovery app.

Direct recovery through File Explorer

For an unencrypted backup without hidden names, the current and date-stamped files can be copied directly. This is useful when you need one obvious item and do not need the point-in-time view.

Use O&O AutoBackup for a large restore, for selecting a coherent historical state, or whenever version names are ambiguous. Encrypted backups cannot be recovered by copying their stored objects directly.

After recovery

Verify several restored files by opening documents, previewing photos, and testing archives. Keep the backup until you have checked the recovered data. The restore log records files that could not be written.

If the restore replaced an active working folder, restart the relevant application only after verification. For OneDrive content, resume synchronization after you are confident that the restored set is the one you want propagated.

Restore Is A Copy Operation

Recovery does not erase the backup. However, writing into an existing destination can replace files there. Use a new folder when uncertain.

Restore an encrypted backup

An encrypted backup deliberately cannot be opened as ordinary files. Recovery begins by unlocking the backup with either the password chosen during setup or its recovery key. The encryption does not depend on the original Windows account or original PC.

What you need

You need all three of these:

1. The complete backup destination.
2. O&O AutoBackup or the portable **Recover this backup** application stored with the backup.
3. **Either** the backup password **or** the matching recovery key.

A product license is not required when the recovery copy stored with the backup is launched in its restricted recovery mode. It restores that backup only and does not configure the new PC.

Restore with the password

1. Connect or open the backup destination.
2. Start O&O AutoBackup and choose **Restore from an existing backup**, or double-click **Recover this backup** at the destination.
3. Select the encrypted backup if it is not already selected.
4. In **This backup is encrypted**, enter the password.
5. Optionally select **Remember on this PC**. This allows scheduled backups on this PC to run without prompting; it does not remove the password requirement on another PC.
6. Choose **Unlock**.
7. Select the restore point, files, and destination, then start the restore.

An incorrect password changes nothing at the destination. Check keyboard layout and Caps Lock, then retry.

Restore with the recovery key

If the password is unavailable:

1. Open the unlock dialog.
2. Expand **Password forgotten? Use the recovery key**.
3. Enter or paste the saved recovery key. Upper/lower case and dashes do not matter.
4. Choose **Unlock** and continue with the normal restore selection.

The recovery sheet includes a **Vault ID**. Compare it with the Vault ID shown for the encrypted backup to make sure you are using the correct key.

Anyone who possesses the recovery key can read that backup. Store it as carefully as the password and separately from the backup drive.

If file and folder names are hidden

When **Also hide file names and folders** was enabled, the destination contains random stored names and an encrypted index. This prevents someone from learning even the names and organization of your files.

Do not rename, move, or delete files in the `_ooab-data` folder or the encrypted index. Use O&O AutoBackup to browse and restore. If the list is missing or incomplete, **Repair file list** can rebuild it from stored files after the backup is unlocked, although some historical move/deletion details cannot be reconstructed.

Recover onto a replacement PC

1. Connect the backup drive to the replacement PC.
2. Launch the portable recovery app from that drive. If it is missing, install or download O&O AutoBackup and point it at the backup folder.
3. Unlock with the password or recovery key.
4. Restore to a new folder on the replacement PC.
5. Open representative documents, photos, and archives before deleting any remaining old copy.

If both credentials are lost

There is no back door. O&O Software cannot reset the encryption or derive either credential. This is a security property: a lost or stolen destination is protected—but losing both password and recovery key makes the backup permanently inaccessible.

Test Both Ways In

After creating an encrypted backup, perform a small test restore with the password and verify that the recovery key is readable and stored separately. Do not wait for an emergency to discover that the only copy of the key was on the failed PC.

Search backups

Search is useful when you remember a name but not the original folder or backup pair.

Start a search

Use the search box in the title bar or press **Ctrl+F**. Enter a complete name or a wildcard pattern. Results can span the backups currently reachable from the PC.

For each match, check the backup, path, date, and version before acting. Available actions can open the file, open its folder, or save a copy to another location.

Unavailable destinations

Search names any backup it could not inspect. Connect the missing USB drive or restore access to the network location and repeat the search. An incomplete search is not proof that the file was never backed up.

Search inside restore

When you already know the correct backup, open its restore view and search within the archive. Then select the required restore point and file. This is the best path when you want to compare several versions of the same name.

Search tips

- Search for a distinctive part of the base name.
- Use the extension when looking for a type of file.
- Check older restore points if the current view no longer contains the file.
- Save a recovered copy to a separate folder before replacing the current version.

Portable recovery app

O&O AutoBackup can place a recovery application beside each backup. It is enabled by default in the backup summary.

Why it is useful

The recovery app travels with the data. On another compatible Windows PC, open the backup destination and launch **Recover this backup**. You can then browse the archive and restore files without first recreating the original pair configuration.

This is especially valuable after replacing a failed PC or when the installed program is no longer immediately available.

Encrypted backups

The portable app does not bypass security. You still need the backup password or saved recovery key. Keep the recovery key separately from the destination.

Keep it available

When updating O&O AutoBackup or changing destination settings, allow it to refresh the recovery application. Security software may scrutinize portable executables; if the app is quarantined, verify that the backup came from O&O AutoBackup and restore the signed program through your security product.

Ordinary Files Remain Useful

For an unencrypted backup, regular files can also be copied directly in File Explorer. The recovery app adds version-aware browsing and guided restoration.

Backup pairs

A pair is the saved relationship between sources, one destination, and the rules that operate between them.

The **All pairs** section on Home summarizes backups and synchronizations, protected file counts, last and next activity, and any pair requiring attention. Select a row to expose its actions; double-click it to edit.

Pair actions

- **Back up now / Synchronize now** starts work immediately.
- **Change** opens sources, destination, schedule, filters, and other behavior.
- **Restore** opens recovery for a backup pair.
- **Log** filters operation history to the pair.
- **Delete** removes the configuration but keeps data already written to the destination.

Destination identity

For removable media, a pair records more than a drive letter. This guards against writing to the wrong device after Windows reassigns letters. If the destination has genuinely been replaced, use the destination picker to associate the intended storage.

Repair file list

O&O AutoBackup records destination state to avoid rereading a slow network or cloud target on every run. Use **Repair file list** only when the recorded state needs to be rebuilt, for example after files at the destination were changed outside O&O AutoBackup. The next scan may take longer.

Settings

Open the gear button to configure application-wide behavior. Pair-specific schedules and retention remain in the pair editor.

General and program location

Choose language and appearance, manage the permanent program location, and create Start menu or desktop shortcuts. Changing the interface language restarts the application; it is postponed while an operation is active.

Autostart

Choose startup for the current user or all users, keep O&O AutoBackup in the notification area, delay startup work, wait for idle time, keep the PC awake, and control battery behavior. Scheduled work depends on O&O AutoBackup running.

Notifications

Select everything, runs and problems, problems only, or no routine messages. **Problems only** is recommended. You can optionally announce a scheduled run with a countdown and an opportunity to skip that occurrence.

Folders

System and program folders are skipped by default. Add personal exclusions for caches, temporary exports, or other data that should never enter any backup.

Filter

File groups collect extensions such as office documents, pictures, music, or video. Use them when a selected source folder contains mixed content and only certain types should be copied. Minimum and maximum size rules can exclude unusually small or large files.

Log

Control diagnostic logging and clear stored history. Enable detailed logging when reproducing an issue for Support, then disable it when no longer needed to avoid unnecessary growth.

Logs and notifications

The Home page answers whether protection is current; notifications interrupt you only when a decision or problem deserves attention; the log preserves operational detail.

Notification levels

Under **Settings** → **Notifications**, choose:

- **Everything** — includes routine waiting states.
- **Backups and problems** — reports runs and failures.
- **Only problems** — the recommended quiet default.
- **Nothing** — suppresses routine messages.

You are still told when an action you started cannot run, such as starting a second operation or connecting the wrong destination drive.

The operation log

Open **Log** to filter informational messages, warnings, and errors. A useful support report includes:

- O&O AutoBackup version and Windows version
- Pair name and time of the failed run
- Source and destination type
- Complete error message and affected path
- Whether retrying after reconnecting or closing an application changes the result

Do not publish logs without reviewing them; paths and file names can reveal personal information.

Interrupted runs

If a run pauses for a missing drive, battery policy, or metered network, O&O AutoBackup offers to continue, continue anyway, or postpone. Postponing does not discard completed files. The next valid opportunity catches up.

Licensing and updates

License and trial use

O&O AutoBackup is commercial software. You can try it during the trial period; continued use requires a valid license. The purchase and license terms determine how many PCs and users may run it.

Open **About** to view the license type, licensed version, serial number, and—where applicable—valid-until date. The page also provides the registration and license-release actions.

Release a machine-bound license

Release the license before replacing, reinstalling, or transferring the PC. The application returns to trial state after restart. A transfer is allowed only as described by the O&O end-user license agreement.

Check for updates

O&O AutoBackup can notify you when a newer release is available. Follow the update link, save current work, and allow active backup or restore operations to finish before replacing the application.

After an update, open **About** to verify the installed version. Existing pairs and backups should remain available, but keeping a separate copy of important data is always recommended.

Getting support

Use O&O Support for license validation, activation limits, download access, or reproducible product errors. Never include your full serial number, backup password, or recovery key in a public request.

Backup format

O&O AutoBackup stores readable, versioned files instead of placing the backup in one large compressed container. This is a deliberate design choice: **an unencrypted backup can be restored as ordinary files without depending on a proprietary archive or a particular installation of O&O AutoBackup.**

Backup software often lasts longer than the PC on which it was installed. Years later, the important question is not how elegant the archive looked during backup; it is how many dependencies stand between you and your data. For unencrypted backups, O&O AutoBackup keeps that distance short.

Unencrypted backups

Files are copied to the destination as ordinary files within O&O AutoBackup's managed folder structure. The original application is the easiest way to select a point in time, but individual current files can also be inspected and copied with File Explorer.

This design avoids making decompression, mounting, or a proprietary monolithic archive a prerequisite for basic access. A damaged container cannot make every unrelated file inside it inaccessible because there is no single all-or-nothing container.

Why O&O AutoBackup does not compress

No compression is a **deliberate non-goal**. Compression can save capacity for some data, but it creates costs that conflict with O&O AutoBackup's purpose:

- Recovery depends on software that understands the archive.
- Damage to a container can affect many files at once.
- Opening one file may require reading archive structures first.
- Photos, videos, modern Office files, and many downloads are already compressed and may shrink little.
- Backup and restore need additional CPU work.

The trade-off is straightforward: use enough destination capacity for the actual files and their retained versions in exchange for transparent, durable recovery. Managed retention controls history growth without changing the plain-file model.

Compression is not encryption. A compressed archive may still expose names and contents; an encrypted O&O AutoBackup protects them cryptographically even though it is not designed to save space.

Versions and metadata

O&O AutoBackup records enough state to reconstruct restore points and apply retention. Do not rename, reorganize, or partially delete managed backup folders by hand. External changes can make browsing incomplete until the pair's file list is repaired, and destructive changes may permanently remove versions.

Date-stamped versions remain individual stored files. Use the restore timeline when you need a coherent view of many files from the same moment rather than choosing timestamps manually.

Encrypted backups

Encrypted content is intentionally not directly readable. Use O&O AutoBackup or the portable recovery app with the password or recovery key. Optional name hiding also prevents meaningful file and folder names from being exposed at rest.

Encryption preserves the “each file is protected independently” architecture, but direct Explorer recovery is no longer possible because that would defeat the security promise. Keep the recovery application and recovery key available.

Copying a backup destination

If you migrate the entire destination, preserve its complete folder structure and metadata. Verify the copied backup by opening it through **Restore from an existing backup** before removing the original.

Do not treat a partially copied destination as verified. Complete the copy, unlock it if encrypted, browse more than one restore point, and restore representative files before retiring the source destination.

Troubleshooting

The backup drive is not found

Reconnect the recorded drive, wait for Windows to mount it, and use **Choose another destination** only if the actual storage changed. O&O AutoBackup checks volume identity and will not trust a matching drive letter alone.

Files were skipped because they are in use

Close the program using the files, then run the pair again. Email stores, browser data, databases, and virtual machines are common examples. The next run retries them.

The destination is full

Free space, shorten retention, or move the backup to a larger destination. Managed retention removes eligible old restore points but keeps the newest version of every file.

A scheduled backup did not run

Check **Settings** → **Autostart**. O&O AutoBackup must start with Windows and remain in the notification area. Also check battery, idle, metered-network, startup-delay, and missing-drive states. The Home page usually names the active reason.

A network or cloud destination is unreachable

Confirm the URL or UNC path, internet or LAN connection, credentials, certificate trust, and provider availability. For an unattended network share, verify access under the same Windows account that runs O&O AutoBackup.

An encrypted backup will not open

Retry the password with Caps Lock checked. If it was forgotten, use the saved recovery key. There is no back door; without either credential, the data cannot be decrypted.

The backup view appears out of date

If destination files were changed outside O&O AutoBackup, edit the pair and use **Repair file list**. This forces a slower full read of the destination.

Collect information for support

Record the application version, pair, time, exact message, and steps to reproduce. Enable diagnostic logging only long enough to reproduce the issue, then attach the reviewed log to your private support case.

Privacy and security

O&O AutoBackup works with the storage destinations you choose. It does not require your backup data to be stored in an O&O cloud.

Data paths

Local and network backups travel between your PC and your destination. WebDAV and S3 backups also involve the selected provider and network. Consult that provider's privacy, retention, and data-location policies.

Protect the destination

- Enable O&O AutoBackup encryption for removable or remote storage that could be accessed by others.
- Use a unique password and keep the recovery key separately.
- Restrict share and bucket permissions to the required account.
- Disconnect at least one removable copy when it is not being updated.
- Test recovery regularly.

Logs and support

Operational logs can contain local paths, file names, server addresses, and failure details. Review them before sharing and send them only through an appropriate support channel. O&O Support never needs your backup password or recovery key.

Threat boundaries

Encryption protects backup contents at rest, but it does not clean malware from source files or protect an unlocked Windows session. A connected destination can still be affected by malicious software operating with your permissions. Layered protection combines O&O AutoBackup, offline or immutable copies, Windows security updates, and safe account practices.

Frequently asked questions

Is O&O AutoBackup free?

No. O&O AutoBackup is commercial software. You can try it during the trial period; continued use requires a valid license.

Does O&O AutoBackup create a complete Windows image?

No. It protects selected files and folders. It does not image Windows, installed applications, partitions, or boot information. Use O&O DiskImage for complete system recovery and O&O AutoBackup for frequent versions of changing personal data. See O&O AutoBackup, O&O DiskImage, and OneDrive.

Why should I use O&O AutoBackup and O&O DiskImage together?

They recover different layers. O&O DiskImage can return a failed PC to a bootable system state; O&O AutoBackup can then return the newest personal files created since the last image. A practical rhythm is a system image monthly and file backup hourly, adjusted to how important and changeable the data is.

Is OneDrive already a backup?

OneDrive synchronizes a working set, which means an unwanted deletion or damaging edit can be synchronized too. Provider recovery features can help, but they remain inside the same account and service. O&O AutoBackup creates an independent versioned copy on storage you control. See Protect OneDrive with an offline backup.

Can I open a backup without O&O AutoBackup?

Unencrypted backups contain ordinary files that can be reached with File Explorer. For version-aware recovery, use O&O AutoBackup or the portable recovery app stored with the backup. Encrypted backups require one of those applications plus the password or recovery key.

Why does O&O AutoBackup not compress the backup?

Plain-file recovery is a deliberate design decision. Without a proprietary compressed container, an unencrypted current file can be copied directly and damage to one archive cannot lock away every unrelated file inside it. Many common photos, videos, Office documents, and downloads are already compressed. See Backup format.

Where should I store backups?

On a different physical device or remote system from the source. A USB drive, separate disk, NAS, WebDAV server, or S3-compatible storage can be used. Keep another offline copy for irreplaceable data.

What happens when my USB drive is disconnected?

O&O AutoBackup waits. When the recorded drive returns, drive-connect or catch-up behavior can resume protection automatically. It verifies the device identity instead of relying only on its drive letter.

Can I stop the first backup?

Yes. Pause or cancel the run. Completed files remain useful, and the next run scans and catches up with what remains.

Why was an open file skipped?

Another program may hold it exclusively. Close that program and run the backup again. O&O AutoBackup reports these files so they are not mistaken for protected copies.

How many versions are kept?

The standard policy keeps every recent version, then thins history to hourly, daily, and weekly restore points. Optional limits and available destination space affect the final history.

Does deleting a pair delete my backup files?

No. It removes the pair and its restore information from the interface but leaves files at the destination. Delete destination data separately only after verifying it is no longer needed.

What if I forget an encryption password?

Use the recovery key created during setup. Match its Vault ID to the backup, open **Password forgotten? Use the recovery key**, and unlock it. If both password and recovery key are lost, the backup cannot be decrypted—not even by O&O Support. See [Restore an encrypted backup](#).

Why did my scheduled backup not run?

O&O AutoBackup must start with Windows and stay active in the notification area. It may also be waiting for the drive, mains power, an unmetered connection, or idle time. The Home page shows the reason.

Can I synchronize folders instead of backing them up?

Yes. O&O AutoBackup offers Backup, Copy, Merge, Mirror, and Two-way modes. They differ in direction, version history, and whether deletion is propagated. Synchronization keeps working folders aligned; it does not replace a versioned backup. See [Every synchronization mode in detail](#).

How do I move my license?

Open **About**, release the license on the old PC, then activate it on the new PC according to the license agreement.

Where can I get help?

Use the O&O Support pages. Include the application version, exact error, affected pair, and a reviewed diagnostic log when appropriate. Never send your password or recovery key.