

Unspora User Guide

Version 0.7

November 2026

Contents

Introduction

- What Unspora does for you
- restic underneath
- What Unspora does not involve
- Terms used in this guide

Installing and first launch

- Requirements
- Installing
- Registering
- Full Disk Access (optional)

The main window

- The Overview
- Closing the window

Destinations

- Adding a destination
- Backblaze B2
- S3-compatible storage (S3 / R2)
- SFTP
- Local disk
- Credentials and the Keychain
- The repository password
- Editing and removing a destination

Choosing what to back up

- Folders to back up
- Exploring the proposed backup
- Exclude rules
- Smart Exclude
- Locations excluded automatically

Backing up

- Running a backup
- Backup outcomes

Scheduling

- Turning on automatic backups
- How scheduled backups run

- Approving the agent in Login Items
- Power and network conditions
- What scheduling cannot do

Snapshots and restore

- The snapshot list
- Finding and restoring files
- Restoring a whole snapshot
- How restores protect your files

Retention and storage

- The retention policy
- Automatic retention
- Applying retention now
- Storage and cost estimates

Health and recovery

- Reviewing coverage
- Testing recovery
- Integrity checks
- Monthly checks
- Recovery kits

The menu bar and notifications

- The menu bar icon
- Keeping Unspora out of the Dock
- Notifications

Updates

When settings change outside Unspora

- What happens when the seal breaks
- Reviewing the change
- Settings from another Mac

Settings

- General
- Permissions
- Agents
- Diagnostics

Using Unspora with AI agents

- Installing the command
- Connecting an MCP client

- What needs approval
- The audit log
- How agent backups run
- Things to know

Using the restic command line directly

- Connecting with restic
- Useful commands
- Working alongside Unspora

Troubleshooting

- Backups end incomplete
- Full Disk Access shows Not granted after you turned it on
- “This repository is busy in another Unspora operation”
- A backup or retention run waits a long time before starting
- Scheduled backups are not running
- Registration fails
- Check for Updates says to register
- Unspora says its settings were changed outside the app
- “No repository was found at this address”
- The connection test fails
- macOS warns about opening Unspora
- Getting help

Keyboard shortcuts

Glossary

What’s new

- Version 0.8.0
- Version 0.7.1
- Version 0.7.0
- Version 0.6.0
- Version 0.5.0

Acknowledgements

Introduction

Unspora is a Mac app for encrypted offsite backups. You choose where the backups go (Backblaze B2, any S3-compatible storage, an SFTP server, or a disk attached to your Mac), choose which folders to protect, and Unspora backs them up on demand or on a schedule. When you need something back, you browse a backup by date and restore individual files, folders, or everything.

This guide covers Unspora 0.7.1 (build 14).

What Unspora does for you

- Keeps every backup encrypted with a password only you hold, before anything leaves your Mac.
- Shows, for each destination, when the last complete backup happened and whether the latest attempt had problems.
- Tells you plainly when a backup skipped files it could not read, instead of reporting success.
- Runs scheduled backups in the background, even when the Unspora window is closed.
- Restores into a new folder, never over your existing files, and verifies what it restored.
- Exports a recovery kit so you can reconnect to your backups from a replacement Mac.

restic underneath

Unspora drives restic, a widely used open-source backup program, to do the backup work, and a copy of restic is built into the app. restic handles encryption, deduplication (unchanged data is stored only once), and the storage format.

This has a practical benefit: your backups are ordinary restic repositories. If Unspora were ever unavailable, you could still list, browse, and restore your backups with the free restic command-line tool. Anything Unspora writes, restic can read, and the reverse is also true. See Using the restic command line directly.

What Unspora does not involve

- **No Unspora account.** You register once with a code you were sent. There is no account to create and nothing to sign in to.
- **No hosted service.** Your backups go to storage you own and pay for directly. Your storage provider bills you separately.
- **No tracking.** Unspora never sends anything about your files, folders, destinations, or backups. Only two things go to Unspora's registration server (`api.unspora.com`): registering sends

your code and a random identifier for this Mac, once; checking for updates sends your registration (which carries the name and email your code was issued to), the Unspora version, and the macOS version, about once a day. See Registering and Updates. The diagnostics export described in Settings is a file you save and share only if you choose to.

- **No bootable system images.** Unspora backs up files and folders. It cannot recreate a bootable copy of macOS; to set up a replacement Mac, you install macOS and your apps first, then restore your files.

Terms used in this guide

A **destination** is one place your backups go, together with the settings for it: which folders, which exclusions, which schedule. A **repository** is the restic storage area at that destination. Each backup run creates a **snapshot**, a complete picture of your selected folders at that moment. Because restic stores unchanged data only once, keeping many snapshots costs far less space than keeping many full copies. The Glossary defines these and other terms.

Installing and first launch

Requirements

- A Mac with Apple silicon (M1 or later). Intel Macs are not supported.
- macOS 14 Sonoma or later.
- Storage for your backups: a Backblaze B2 account, an S3-compatible storage account, an SFTP server you can reach with SSH keys, or an external disk.

Installing

Unspora is distributed as a disk image (`.dmg`) outside the Mac App Store. It is signed with an Apple Developer ID and notarized by Apple, so macOS opens it without extra steps. The latest version is always at https://api.unspora.com/download.

To install Unspora:

1. Open the downloaded disk image, for example `Unspora-0.7.1.dmg`.
2. Drag **Unspora** into the **Applications** folder.
3. Eject the disk image.
4. Open Unspora from the Applications folder.

Always run the copy in your Applications folder. Full Disk Access and the scheduled backup agent are tied to that copy, and a copy run from elsewhere does not share them.

Once installed and registered, Unspora updates itself. See Updates.

Registering

Unspora needs a registration code to set up backups and to receive updates. You get the code with your invitation to use Unspora; it looks like `UNSP-XXXX-XXXX-XXXX`, and one code works on several Macs (usually up to five).

To register:

1. Open Unspora. With no destinations set up yet, the window shows **Register Unspora**.
2. Type or paste your code. Letters can be upper or lower case, and the dashes are optional.
3. Click **Register**.

Registering needs an internet connection once. Unspora saves the result on this Mac, so it never needs the connection again for backups or restores. **Settings** > **General** and **About Unspora** then

show **Registered to** with your name.

If Unspora already has destinations, for example after you move to a new Mac, it opens normally and shows a banner on the Overview instead: **This copy of Unspora isn't registered.** Click **Register...** in the banner.

What an unregistered copy can and cannot do:

- **It can** run existing backups, scheduled or on demand, browse snapshots, and restore. Registration never stands between you and your data.
- **It cannot** add a destination, import a recovery kit, or receive updates.

If registration fails, see Registration fails.

Full Disk Access (optional)

macOS protects some of the data in your home folder, such as Mail, Messages, Safari data, and parts of other apps' data. An app can read those locations only if you grant it **Full Disk Access** in System Settings.

Unspora does not need it, and it is off by default. Most protected data can be downloaded again or recreated: mail and messages from their servers or iCloud, browser data from sync. Without Full Disk Access, Unspora backs up everything else and skips the protected locations quietly. Each run lists what it skipped in **Backup history**, but skipped protected data never makes a backup incomplete, and Unspora never asks you for the permission.

Backing up protected app data

If you want protected app data in your backups too:

1. Choose **Unspora** > **Settings...**, click **Permissions**, and turn on **Back up protected app data**. Unspora adds itself to the Full Disk Access list and opens System Settings.
2. In **Privacy & Security** > **Full Disk Access**, find **Unspora** and turn its switch on. macOS may ask for your login password.
3. Quit Unspora and open it again. The permission takes effect for a newly started app.

The permission belongs to the signed Unspora app, and scheduled backups run under that same app identity, so one grant covers both the backups you start and the scheduled ones.

Once you have turned the option on, Unspora holds you to it: while access is still missing, backups are marked **incomplete**, the Overview shows a **Needs Attention** section, and Unspora asks at launch, with **Open System Settings**, **Not Now**, and a **Don't ask again at launch** checkbox. To stop all of that, grant access or turn the option off again.

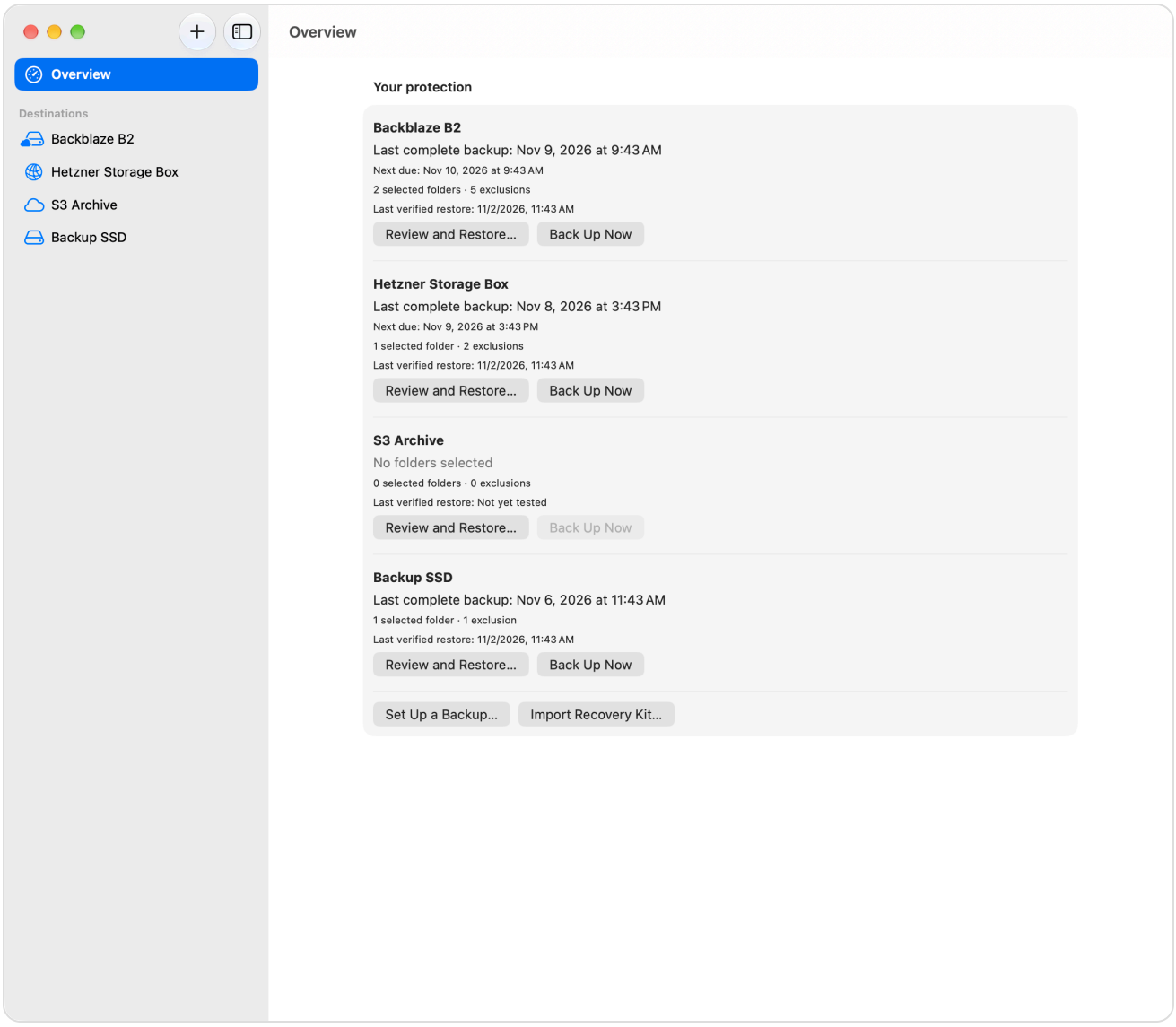
What Full Disk Access does not prove

Full Disk Access is necessary to read protected app data, but it is no guarantee that every important file is recoverable. A backup is only as complete as the folders you select and the exclusions you set. Some files, such as live databases of running apps and cloud-only files that have not been downloaded, can need extra care. Testing a restore is the only way to show that a file comes back. See Health and recovery.

The main window

The Unspora window has a sidebar on the left and a detail area on the right.

- **Overview** at the top of the sidebar shows the protection status of every destination.
- **Destinations** lists each destination by name. Select one to see its details, snapshots, and tools.
- The **Add Destination** button (the plus sign in the toolbar) starts a new destination.



The Overview, showing several destinations and their protection status.

The Overview

The **Your protection** section has one entry per destination. Each entry shows:

- **Last complete backup**, with the date and time. If there has never been a complete backup, it says so, and for a scheduled destination it suggests backing up now or checking that scheduling is approved.
- **Latest attempt**, shown only when the most recent run did not complete, with its outcome (for example, incomplete or failed).
- **Backup is overdue**, when a scheduled destination has gone longer than its interval without a complete backup.
- **Next due**, for scheduled destinations.
- How many folders are selected and how many exclusions are set.
- **Last verified restore**, the last time a restore from this destination finished and was verified.
- **Review and Restore...**, which opens the destination, and **Back Up Now**, which starts a backup immediately.

Below the entries are **Set Up a Backup...** and **Import Recovery Kit...**. Both need a registered copy; see Registering.

Two banners can appear at the top of the Overview:

- **This copy of Unspora isn't registered**, with a **Register...** button.
- **Unspora's settings were changed outside the app**, with a **Review...** button. See When settings change outside Unspora.

A **Needs Attention** section appears when you turned on **Back up protected app data** but Full Disk Access is still off, or when scheduled backups are waiting for your approval in Login Items, each with a button that opens the right place in System Settings.

Closing the window

Unspora keeps running in the menu bar after you close its window, so status stays available. Click the Unspora icon in the Dock or the menu bar to bring the window back. To quit, choose **Unspora** > **Quit Unspora**, or right-click the menu bar icon and choose **Quit Unspora**. See The menu bar and notifications.

Scheduled backups run through a separate background agent, so they continue even after you quit the app.

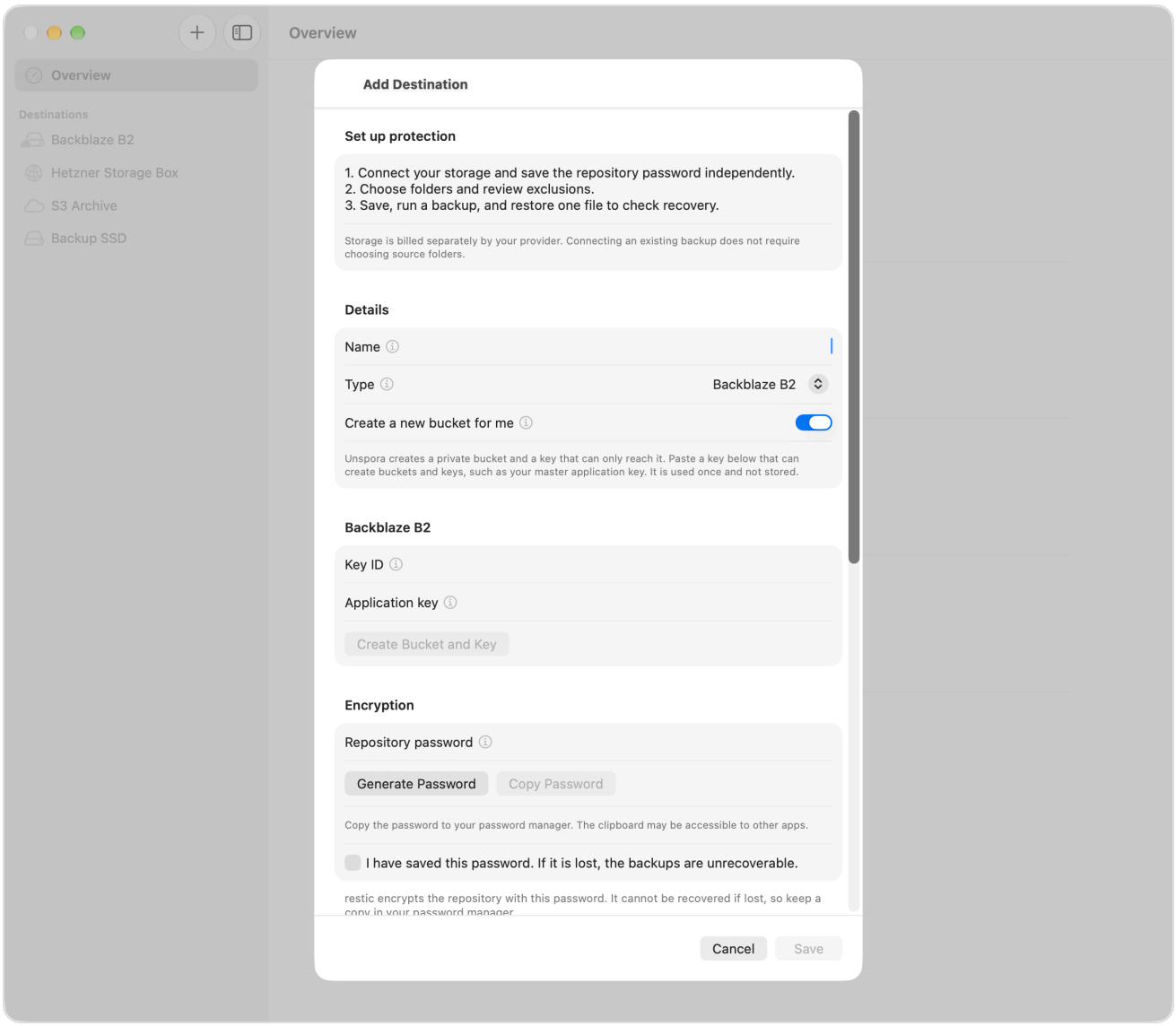
Destinations

A destination ties together a storage location, its credentials, the repository password, the folders to back up, exclusions, a schedule, and a retention policy. You can have several destinations, for example a cloud destination and a local disk.

Adding a destination

To add a destination:

1. Click the **Add Destination** button in the toolbar, choose **File** > **New Destination...** (⌘N), or click **Set Up a Backup...** on the Overview.
2. Enter a **Name**. It is only a label inside Unspora and is never sent to your provider.
3. Choose a **Type**: **Backblaze B2**, **S3 / R2**, **SFTP**, or **Local disk**.
4. Fill in the connection details for that type (see the sections below).
5. Set the **Repository password** (see The repository password).
6. Add the folders to back up and review exclusions (see Choosing what to back up).
7. Choose a schedule, and review **Advanced Options** if you want to change retention, power and network conditions, or cost estimates.
8. Click **Save**.



The Add Destination sheet, set up to create a new Backblaze B2 bucket.

The top of a new destination's editor shows a three-step summary under **Set up protection**: connect storage and save the password independently, choose folders and review exclusions, then save, run a backup, and restore one file to check recovery.

Every setting has a small information button beside its label. Click it for a short explanation of the setting.

What Save does

Save checks the connection before it stores anything. It confirms that the address, keys, and password open the repository. The button reads **Verifying…** while it works.

- If a repository already exists at the address and your password unlocks it, the destination is saved.
- If no repository exists there yet, Unspora asks **Create a new repository?** Click **Create Repository** to create an empty, encrypted repository with your password. If you meant to connect to an existing repository, click **Cancel** and check the address.
- If the connection fails, Unspora shows the reason under **Could not save** and keeps your previous settings.

When **Save** is unavailable, a note at the bottom of the editor says why (for example, **Enter a name for this destination.** or **Check the password acknowledgment box to proceed.**). Hovering over **Save** shows the same reason.

You can also check the connection before saving with **Test Connection** in the **Connection** section. If no repository exists yet, an **Initialize Repository** button appears there.

Existing restic settings

If you already use restic on this Mac, the editor may show an **Existing restic settings** section offering to fill in the fields from settings it found in Unspora's environment variables or in the Keychain items of an existing restic command-line setup. Click **Use These Settings** to fill in the fields. macOS may ask you to allow Unspora to read each Keychain item. Nothing is saved until you click **Save**, and you should test the connection first.

Backblaze B2

Let Unspora create the bucket and key

For a new B2 destination, **Create a new bucket for me** is on by default. Unspora then creates everything it needs in your Backblaze account:

- A new private bucket with a random name that starts with `unspora-` and reveals nothing about you or your Mac.
- A lifecycle rule on the bucket so Backblaze does not keep hidden old versions of files restic has deleted.
- An application key that can reach only that bucket.
- The restic repository inside the bucket, in a folder named `restic`.

To set up B2 automatically:

1. In the Backblaze web console, under **Application Keys**, find your master application key, or create a key with access to all buckets and the **writeBuckets** and **writeKeys** capabilities. Note

its key ID and secret.
2. In Unspora, leave **Create a new bucket for me** on.
3. Paste the **Key ID** and **Application key** into the **Backblaze B2** section.
4. Click **Create Bucket and Key**.

When it finishes, the editor shows the new bucket's name and the message that it created the bucket and a key scoped to it. If you had not already set a repository password, Unspora generates one; save it in your password manager before you continue.

The key you pasted is used for this setup only and is never stored. Unspora keeps only the new, bucket-scoped key in your Keychain. Once setup succeeds, you can delete the broad key in the Backblaze console if you created it just for this.

If Backblaze rejects the key, Unspora says so. A key restricted to a single bucket, or one without the writeBuckets and writeKeys capabilities, cannot create buckets and keys.

Use a bucket you already have

Turn off **Create a new bucket for me** to connect to an existing bucket:

1. Enter the **Bucket name** and the **Folder in bucket** (the default is `restic`). Unspora builds the repository address from these, for example `b2:my-backups:restic`.
2. Enter the **Account ID (keyID)** and **Application key** of a key with access to that bucket.

Turn on **Enter repository address directly** if your repository address does not fit the bucket-and-folder pattern, then type the full address in **Repository**.

Several Macs can share one B2 repository. Each Mac's snapshots stay separate, and restic's deduplication works across them.

S3-compatible storage (S3 / R2)

Choose **S3 / R2** for Amazon S3, Cloudflare R2, Backblaze's S3-compatible endpoint, or other S3-compatible services.

1. Enter the **Repository** address in restic's S3 form, for example `s3:s3.amazonaws.com/my-backups`. For other providers, use the endpoint host your provider documents in place of `s3.amazonaws.com`.
2. Enter the **Access Key ID** and **Secret Access Key**.

SFTP

Choose **SFTP** to back up to a server you reach over SSH.

1. Enter the **Repository** address, for example `sftp:user@backup-server:/srv/restic`.
2. Make sure you can connect to the server with SSH keys. Unspora uses your SSH keys and ssh-agent, and you configure the host in `~/.ssh/config`. There is no password field for SFTP.

Because scheduled backups run without anyone at the keyboard, the SSH key must be usable without typing a passphrase, for example through ssh-agent with the passphrase stored in your Keychain. Test with a manual backup first.

Local disk

Choose **Local disk** to back up to a drive attached to your Mac.

1. Enter the **Repository** path. It must start with `/`, for example `/Volumes/Backup/restic`.

If the repository folder is inside a folder you are backing up, Unspora adds an exclusion for it automatically, so the backup never tries to back up its own repository.

When a scheduled backup is due and the disk is not connected, Unspora waits for the disk to come back and tells you the backup is overdue if notifications are on.

A local disk in the same room as your Mac protects against disk failure and mistakes, but not against fire, theft, or flood. Pair it with an offsite destination for that.

Credentials and the Keychain

Unspora stores the repository password and your storage access keys in your login Keychain. They never appear in Unspora's configuration files or recovery kits.

When you edit a destination, the secret fields start empty and show **Leave blank to keep current**. Leave them blank to keep what is stored, or type a new value to replace it. When you change connection details, Unspora checks the new credentials against the repository before it replaces the saved ones, so a typing mistake cannot leave you with a destination that no longer connects.

The repository password

restic encrypts everything in the repository with the repository password before it leaves your Mac. Neither Unspora nor your storage provider can read your backups, and neither can recover the

password for you.

If you lose the repository password, your backups cannot be read by anyone, including you. This is the cost of real encryption. Keep a copy of the password somewhere other than this Mac, such as a password manager you can reach from another device.

When you add a destination:

1. Type a password, or click **Generate Password** to create a long random one.
2. Click **Copy Password** and save it in your password manager. The clipboard can be read by other apps, so clear it or copy something else afterwards.
3. Check **I have saved this password. If it is lost, the backups are unrecoverable.** Unspora will not save the destination until you do.

Connecting to an existing repository means entering that repository's existing password.

Replacing the stored password

In the destination editor, typing a new password into **Repository password** replaces the copy stored on this Mac. It does not change the repository's encryption password, and the replacement must already unlock the repository. Unspora does not change a repository's encryption password; if you need to, use restic's `key` commands from the command line, then update the password stored in Unspora.

Editing and removing a destination

To edit a destination, select it in the sidebar and click **Edit Destination** in the toolbar, or choose **Destination** > **Edit Destination...** (⌘E).

Unspora never creates a new repository while you edit a destination. If you change the address to one with no repository, Save stops with an explanation, so your backups cannot silently move to an empty repository.

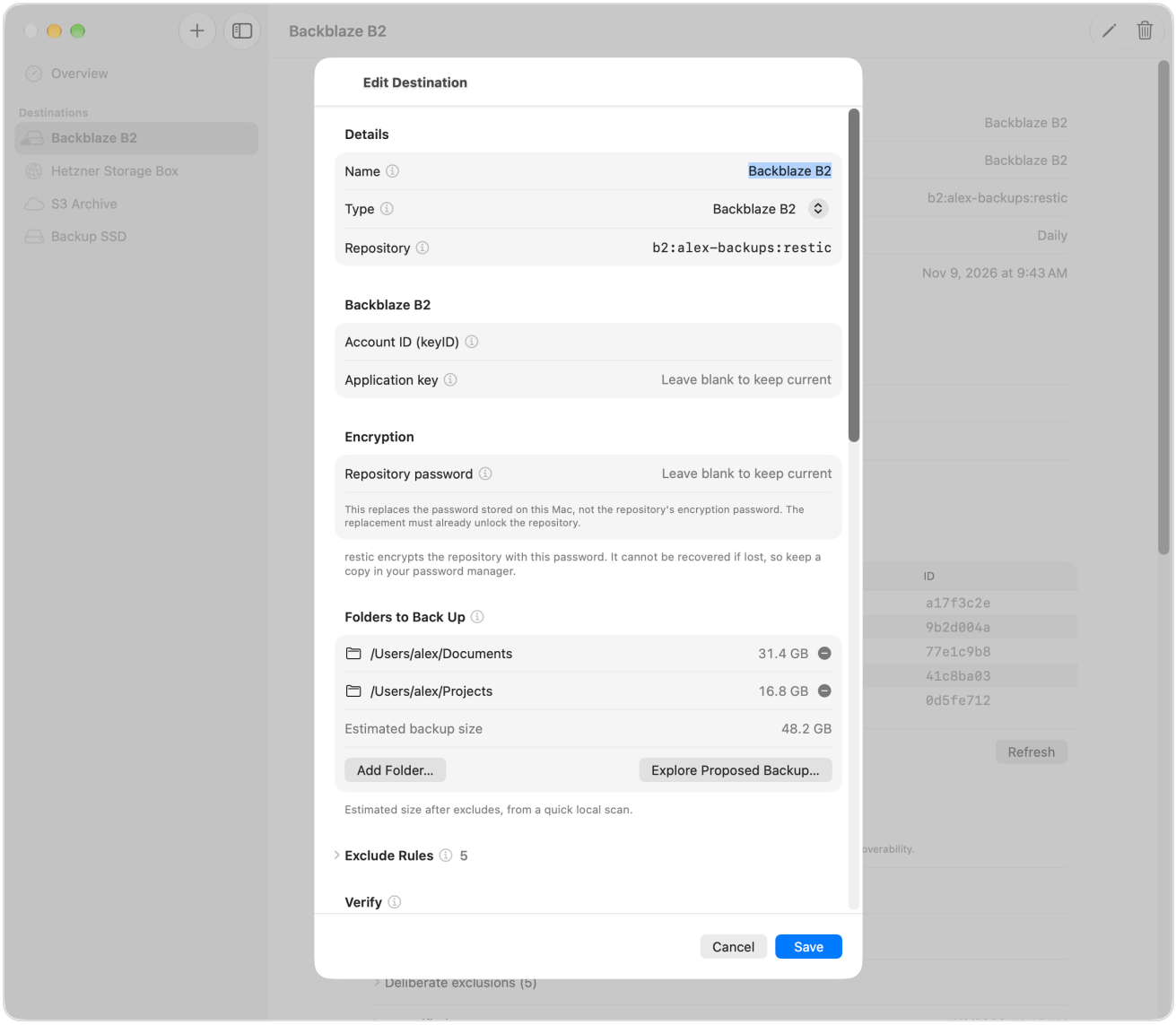
To remove a destination:

1. Select it and click **Remove Destination** in the toolbar, or choose **Destination** > **Remove Destination...** (⌘Delete).
2. Click **Remove Destination** to confirm.

Removing a destination deletes its settings and stored credentials from this Mac. Backups already in the repository are not deleted. If you remove one by mistake, choose **Edit** > **Undo** (⌘Z) to put it back.

Choosing what to back up

You choose what to back up in the destination editor: the folders to include, and exclusion rules for things inside them that you do not need.



The Edit Destination sheet, with credentials, folders and their estimated sizes, and exclude rules.

Folders to back up

To add folders, do one of the following in the **Folders to Back Up** section:

- Click **Add Folder...** and choose one or more folders.
- Drag folders from the Finder onto the editor.

Each folder shows an estimated size, and **Estimated backup size** shows the total after exclusions. To stop backing up a folder, click the minus button beside it.

A common choice is your whole home folder, with exclusions for caches and other data you can recreate. You can also pick specific folders, such as `~/Documents` and `~/Pictures`.

A scheduled destination needs at least one folder. A destination with no folders can still be used to browse and restore from an existing repository, which is how you reconnect on a new Mac.

How accurate the size estimate is

The sizes come from a quick scan of your disk. They are estimates: exclusion matching is approximate, and the numbers are file sizes, not what will be uploaded or what your provider will bill. restic compresses and deduplicates, so the first upload is usually smaller, and later backups upload only changes.

For a more exact count, click **Verify with restic** in the **Verify** section. restic runs in dry-run mode against the repository and reports how many files and bytes the current folders and rules would back up. Nothing is uploaded.

Exploring the proposed backup

Click **Explore Proposed Backup…** to browse what the backup would include, folder by folder, largest first. Excluded items are struck through and move to the bottom. Click the minus button on any item to exclude it, or the plus button to include it again. An item excluded by a broader rule cannot be toggled here; change the rule in **Exclude Rules** instead.

Exclude rules

Open the **Exclude Rules** section to see and edit the patterns that skip files and folders. The number beside the heading is how many rules are set. New destinations start with `.DS_Store` and `.Trash`.

To add a rule, type a pattern and click **Add**. Patterns use restic’s exclude syntax:

Pattern	What it skips
`*.log`	Any file ending in `.log`, in any folder
`node_modules`	Any folder named `node_modules`, wherever it is
`~/Movies/Exports`	That exact folder
`/Volumes/Data/Scratch`	That exact folder
`~/Projects/**/build`	Any `build` folder at any depth inside `~/Projects`

A pattern that is just a name matches by name in any folder. A pattern starting with `/` or `~` matches that exact location. `**` matches any number of folders.

Click **Import...** to add patterns from a text file (one pattern per line, lines starting with `#` ignored), or **Export...** to save the current rules to a text file you can use with restic directly.

Anything you exclude is outside this backup's protection. That includes files that are also synced to a cloud service.

Smart Exclude

Click **Smart Exclude...** in the **Exclude Rules** section to find large folders you probably do not need to back up. Unspora scans your selected folders and lists suggestions, largest first. Each suggestion shows the pattern, why it is suggested, how many matching folders were found, and their total size.

Smart Exclude looks for:

- **Build output and dependency folders** that tools recreate, such as `node_modules`, Xcode `DerivedData`, Python virtual environments, and package-manager caches.
- **App caches** that apps rebuild, such as browser-engine GPU and code caches.
- **Specific `~/Library` folders**, such as `~/Library/Caches`, `~/Library/Logs`, and Xcode build output, in place of excluding all of `~/Library`.
- **Very large app data** (over 2 GB) inside `~/Library/Application Support`, offered for review only.
- **Cloud-synced folders** such as iCloud Drive, Dropbox, OneDrive, and Google Drive, marked **Cloud**.

Suggestions Unspora considers safe start selected; anything that might contain real data starts unselected and says “review” in its reason. Cloud-synced folders always start unselected: a sync service is not an independent backup, because a deletion or corruption syncs everywhere. Exclude a cloud folder only if you have another way to recover it.

Use **Select All Rules** or **Deselect Rules** to change all rule-based selections at once, then click **Add Selected** to add the selected patterns to your exclusions. A bare name, like `node_modules`, matches that folder anywhere under your sources. Smart Exclude only adds exclusion patterns and never deletes files.

Optional Apple Intelligence review

On a Mac with macOS 26 or later and Apple Intelligence turned on, the **Apple Intelligence review** area in Smart Exclude can look deeper, inside nested folders, for more candidates. It is optional, and the rule-based suggestions above work fully without it.

To run it, click **Review Folders**. Unspora scans folder metadata below your sources, then asks the on-device model to assess candidates in small batches. You can click **Stop Review** at any time. If the review is unavailable, a message explains why (for example, unsupported hardware, Apple Intelligence turned off, the model not yet downloaded, or an older macOS); after fixing it, click **Refresh Availability**.

How it protects you:

- **It runs on your Mac.** The model sees relative folder paths, file counts, sizes, and file-type summaries. It never sees the contents of your documents, and nothing is uploaded or saved. The only file content Unspora reads is the short signature line of a cache-tag file.
- **The model cannot decide on its own.** Unspora only allows an AI suggestion when the folder scan was complete, no risky contents were found (documents, source code, configuration, credentials, offline databases, symbolic links, or cloud-only files), and there is concrete evidence the folder can be regenerated, such as a valid cache tag or a matching project file beside build output. A folder’s name and size alone are never enough.
- **You approve each one.** AI results appear in their own section and are never selected by **Select All Rules**. Each row shows the exact folder, file count, size, file types, evidence, how to regenerate it, and a **Reveal in Finder** button. Rows marked **Recommendation: keep backed up** cannot be selected.
- **It rechecks before adding.** When you click **Add Selected**, Unspora checks that each approved folder still matches what was reviewed. If anything changed, nothing is added and you see why.
- **It excludes only that exact folder**, never every folder with the same name.

Limits: the scan stops after 30,000 entries, 24 levels deep, or about 15 seconds, and shows at most 120 candidates. An incomplete scan cannot produce approvals. Suggestions are reviewed once, when you add them; if a folder's purpose changes later, review your exclusions again. Evidence that a folder can be regenerated is a strong hint, not a guarantee that the data can be downloaded or rebuilt in the future.

Locations excluded automatically

macOS denies a few internal locations even to apps with Full Disk Access, such as widget render caches and some private system state. If restic tried to read them, every backup would end incomplete with a permission error. Unspora excludes these locations from every destination automatically when it runs a backup. They do not appear in your exclusion list and contain nothing you would restore.

Backing up

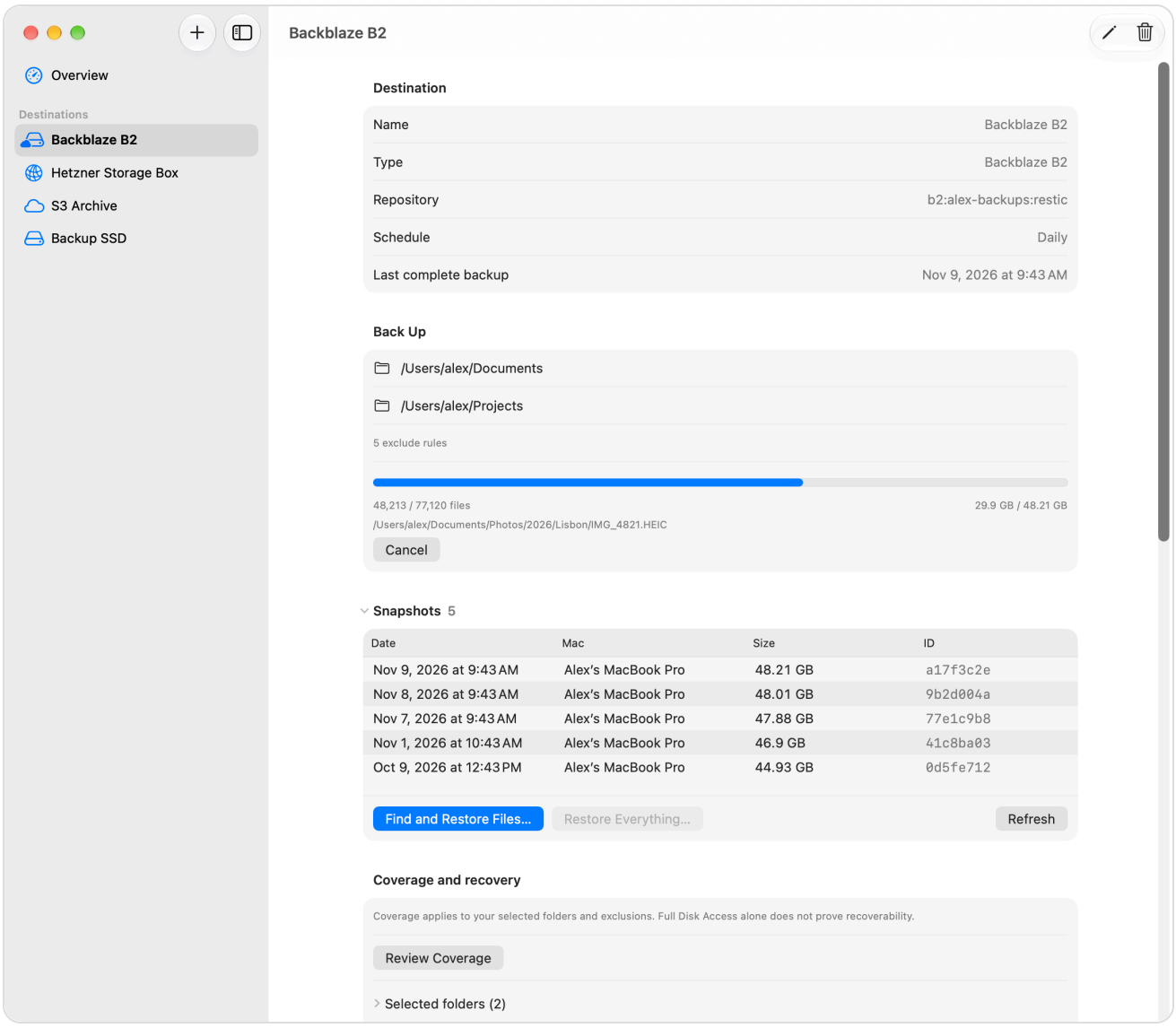
Running a backup

To back up a destination now, do one of the following:

- Select it in the sidebar and click **Back Up Now** in the **Back Up** section.
- Choose **Destination** > **Back Up Now** (⌘B).
- Click **Back Up Now** on its entry in the Overview or in the menu bar window.

The **Back Up** section lists the selected folders and the number of exclude rules. If you chose to back up protected app data and Full Disk Access is still off, it warns that those files will be skipped.

While the backup runs, Unspora shows **Scanning…**, then a progress bar with files and bytes processed and the file currently being read. Click **Cancel** to stop.



A backup in progress, with live progress.

The first backup to a destination uploads everything and can take hours, depending on how much data you have and your upload speed. Later backups are much faster, because restic uploads only new and changed data.

While a backup runs, Unspora asks macOS not to put the Mac to sleep when idle. This does not keep a backup running with the lid closed.

After a backup finishes, the result shows how many files were new or changed, how much data was added, and the new snapshot's short ID. If retention is on, a line reports what retention did.

Backup outcomes

Every run is recorded with one of these outcomes. You can see them in the **Backup history** section of a destination; click an entry to see its issues and maintenance notes.

Outcome	What it means	What to do
complete	A snapshot was created and every selected file was read, apart from protected app data skipped because Full Disk Access is not in use.	Nothing.
incomplete	A snapshot was created, but some files could not be read, or you chose to back up protected app data and Full Disk Access could not be confirmed. The snapshot contains everything else.	Open **Skipped items** to see which files, then fix access or exclude them. See Backups end incomplete.
failed	No verified snapshot was created. The reason is shown in red and in the history entry.	Read the message. Common causes are a connection problem, wrong credentials, or a full disk.
cancelled	You stopped the run.	Run it again when convenient.
running	The run has not recorded a result. It is either still active or was interrupted, for example by a restart.	Do not treat it as complete. Check whether a backup is in progress, or run another.

Unspora counts protection only from complete backups. **Last complete backup** on the Overview and in the destination ignores incomplete, failed, and cancelled runs.

Protection also depends on what you chose to back up. If you change a destination’s folders or exclusions, earlier runs no longer count toward the new plan; the history marks them as using

different settings, and **Last complete backup** waits for a complete backup with the current settings.

Scheduling

Turning on automatic backups

In the destination editor, choose **Automatic backup** in the **Schedule** section:

- **Manual**: Unspora backs up only when you ask.
- **Hourly**: Unspora backs up when at least an hour has passed since the last complete backup.
- **Daily**: Unspora backs up when at least a day has passed since the last complete backup.

Click **Save**. The destination needs at least one folder before you can turn on a schedule.

How scheduled backups run

Scheduled backups run through a small background agent that belongs to the signed Unspora app. macOS starts it once an hour. Each time, it checks which destinations are due, backs them up, and exits. It runs whether or not the Unspora window or app is open, and it uses Unspora's Full Disk Access.

The agent is registered with macOS only while at least one destination has an hourly or daily schedule.

If a backup is incomplete or fails, Unspora retries at the next hourly check, up to three times. After that it waits for the normal interval, so a file that can never be read does not cause a retry every hour forever. A run is never started less than an hour after the previous attempt.

Approving the agent in Login Items

macOS lists Unspora's agent under **System Settings** > **General** > **Login Items & Extensions**, in **Allow in the Background**. On some Macs, macOS asks you to approve it before it can run.

If approval is needed, the Overview shows **Scheduled backups need approval in Login Items before they can run.**, and **Settings** > **Permissions** shows **Background agent** as **Needs approval**. To approve it:

1. Click **Open Login Items Settings...**.
2. Under **Allow in the Background**, turn on **Unspora**.

When everything is working, **Background agent** shows **On**.

Power and network conditions

In the editor's **Advanced Options**, under **Power & Network**:

- **Start scheduled backups only on AC power**: on a laptop running on battery, scheduled backups wait for power. Off by default.
- **Avoid metered and Low Data Mode networks**: scheduled backups wait while you are on a network macOS treats as expensive or in Low Data Mode, such as a phone hotspot. On by default.
- **Upload limit (KiB/s, 0 = unlimited)**: caps upload speed so backups leave room on your connection. This applies to every backup of this destination, including ones you start yourself.

Scheduled backups also wait when there is no network connection, and local-disk destinations wait until the disk is connected.

These conditions are checked when a scheduled backup is about to start. A backup already in progress is not stopped if you unplug the power or switch networks. Backups you start yourself ignore the power and network conditions.

When a due backup waits for one of these reasons and notifications are on, Unspora sends a notification that the backup is overdue, with the reason.

What scheduling cannot do

The agent runs in your user session on your Mac. A scheduled backup cannot run when:

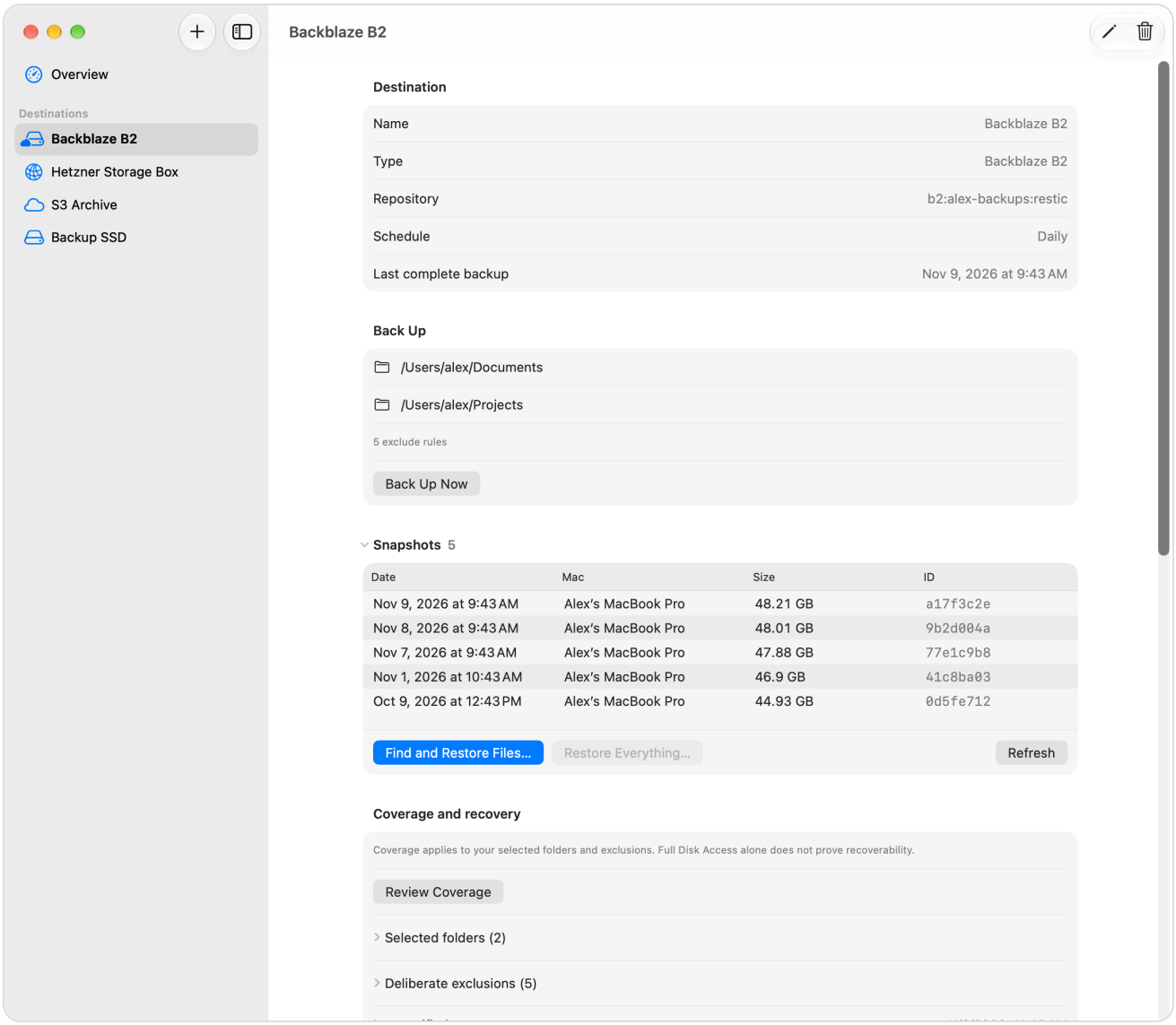
- The Mac is asleep, including a laptop with its lid closed.
- The Mac is shut down.
- You are logged out.

When the Mac wakes or you log back in, the next hourly check catches up on anything that is due. If your Mac is often asleep at the same time each day, an hourly schedule gives more chances to run than a daily one.

Snapshots and restore

The snapshot list

Select a destination to see its **Snapshots** section: every snapshot in the repository, newest first, with its **Date**, the **Mac** that made it, its **Size**, and its short **ID**. The number beside the heading is the snapshot count. If several Macs share the repository, their snapshots all appear here.



A Backblaze B2 destination with its snapshot list and last backup result.

Click **Refresh** or choose **Destination** > **Refresh Snapshots** (⌘R) to reload the list. Right-click a snapshot for **Find and Restore Files...**, **Restore Everything...**, and **Copy Snapshot ID**.

Finding and restoring files

To restore a file or folder:

1. Select a destination, then select a snapshot from around the date you want, or none to start from the newest.
2. Click **Find and Restore Files...**, or double-click the snapshot.
3. In **Find and Restore Files**, use **Backup version** to choose a different date at any time.
4. Navigate to the file:
    - Double-click a folder, or click **Open** beside it, to go inside.
    - Click a folder name in the path bar to jump back to it, click **Root** to return to the top, or press ⌘↑ to go to the parent folder.
    - Or type in **Search filenames and paths in this folder** to search the current folder and everything below it.
5. Select the file or folder. The bar at the bottom shows its name and size and where it will be restored.
6. To restore somewhere other than your Downloads folder, click **Change...** beside **Restore to:**.
7. Click **Restore File**, or **Restore Folder...** for a folder. For a folder, Unspora asks you to confirm, since large folders can take a long time and may cost download fees.
8. When it finishes, click **Show in Finder** to see the restored files.

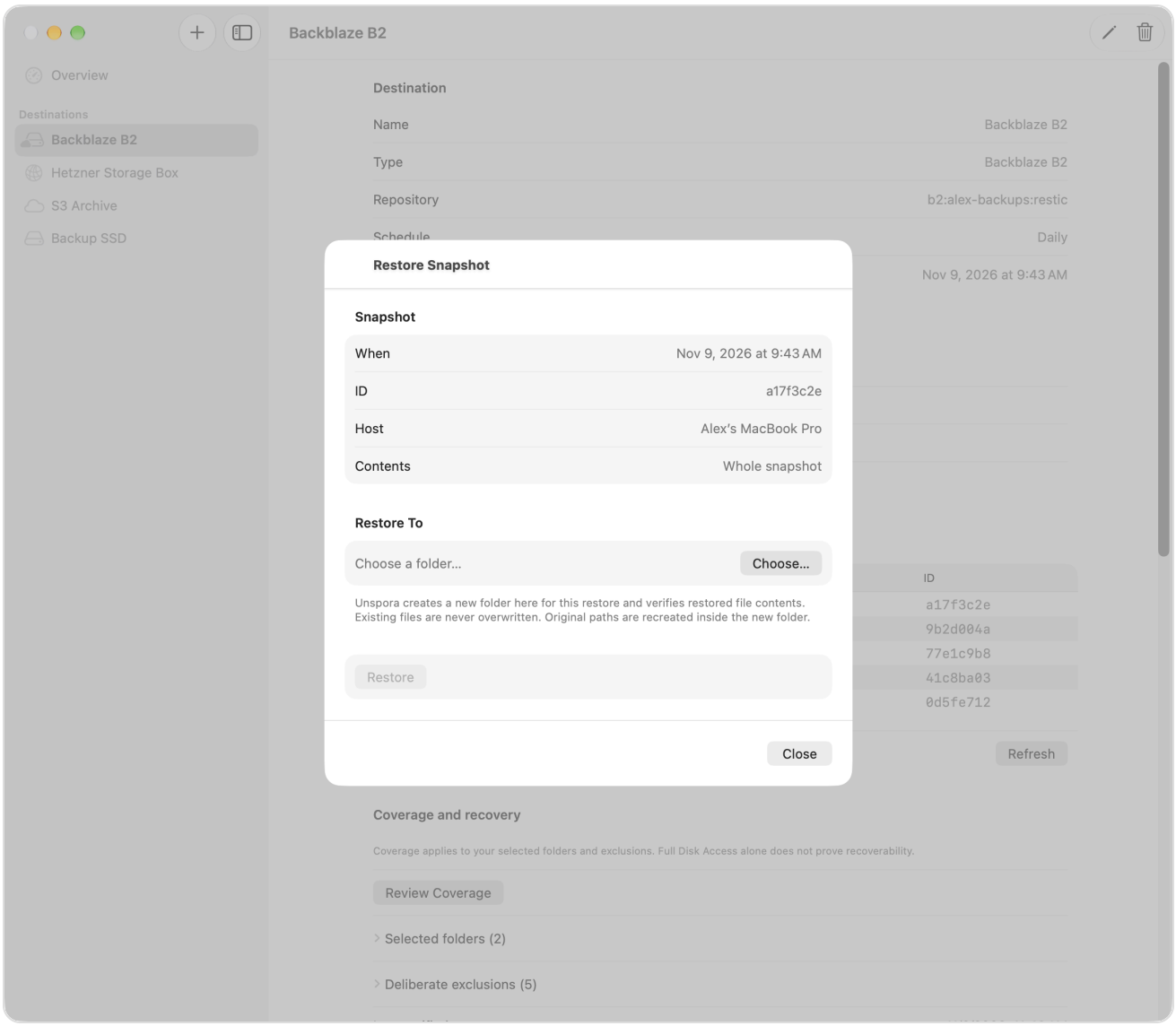
Results show at most 1,000 entries. If you see **Showing the first 1,000 results.**, narrow the search or open a subfolder.

To find an older version of a file, choose an earlier date in **Backup version** and look again. Each snapshot holds the version that existed at its time.

Restoring a whole snapshot

To restore everything in a snapshot:

1. Select the snapshot in the list.
2. Click **Restore Everything...**.
3. In **Restore Snapshot**, click **Choose...** and pick where to restore.
4. Click **Restore**. When it finishes, click **Show Restored Files**.



The Restore Snapshot sheet.

Make sure the target has enough free space for the whole snapshot.

How restores protect your files

Every restore, whether one file or a whole snapshot:

- **Goes into a new folder.** Unspora creates a folder named **Unspora Restore** followed by a unique ID inside the location you choose, and restores into it. The original folder structure is recreated inside it, so a file from `~/Documents/Taxes/2025.pdf` appears under `Users/yourname/Documents/Taxes/2025.pdf` in the new folder.

- **Never overwrites anything.** Your existing files are untouched. To put a restored file back in its original place, move it there yourself in the Finder.
- **Is verified.** restic checks that the restored file contents match the backup.

For a local-disk destination, Unspora refuses to restore into the repository folder itself.

A restore that finishes and verifies updates **Last verified restore** for that destination.

Retention and storage

The retention policy

Without cleanup, a repository keeps every snapshot forever. The retention policy decides which snapshots to keep. You set it in the destination editor under **Advanced Options** > **Retention**:

- **Keep daily**: for each of this many most recent days that have snapshots, keep the last snapshot of that day.
- **Keep weekly**: the same for weeks.
- **Keep monthly**: the same for months.
- **Keep yearly**: the same for years.

The default keeps 7 daily, 4 weekly, 12 monthly, and 3 yearly snapshots. A snapshot that any of these rules covers is kept. The policy must keep at least one snapshot.

Retention applies only to snapshots made by this Mac. In a repository shared by several Macs, each Mac's snapshots are managed by that Mac's own policy.

Automatic retention

Remove expired snapshots after each backup is on by default. When on:

- After each **complete** backup, Unspora removes this Mac's snapshots that the policy no longer covers.
- After an incomplete backup, retention is skipped and existing snapshots are preserved, so a run that missed files never causes older, fuller snapshots to be removed.
- The space that removed snapshots used is freed later by a **prune**, which reads and repacks stored data and is slow, so Unspora prunes at most once a week per destination. To keep this efficient, restic may leave up to 10% of the repository as unused space.

The destination's **Retention** section shows the current policy and whether automatic retention is on.

Applying retention now

To apply the policy immediately:

1. Select the destination and click **Apply Retention Now...** in the **Retention** section, or choose **Destination** > **Apply Retention Now...**.
2. Unspora first counts what the policy would remove. If nothing, it says **Nothing to remove.**

3. Otherwise it asks you to confirm with the exact number, for example **Remove 4 Snapshots**. Click it to proceed.

This removes the snapshots and prunes the data only they used. It cannot be undone.

Storage and cost estimates

The **Storage and cost estimate** section of a destination helps you keep an eye on size and cost.

Click **Measure Repository Data** to measure the data your snapshots refer to. The result shows **Referenced repository data**, when it was measured, and the change since the previous measurement. Unspora keeps the last 30 measurements.

To see a monthly cost estimate:

1. Edit the destination and open **Advanced Options**.
2. Under **Storage estimate assumptions (USD)**, enter **Your provider's USD per TB/month**, the storage price from your provider's current price list.
3. Optionally, enter **Monthly budget warning (USD; 0 = off)**.
4. Save, then measure.

The section then shows **Estimated storage/month**. When a rate is set, scheduled backups also measure the repository after each backup, and if the estimate reaches your budget and notifications are on, Unspora sends a warning.

Know the limits of these numbers:

- **They are estimates, not your bill.** They cover stored data at the rate you entered. They leave out request fees, download fees, taxes, minimum charges, repository overhead, unused data awaiting a prune, and old file versions your provider keeps.
- **The budget is a warning only.** It never stops uploads and does not set a spending cap with your provider. If you need a hard cap, set it in your provider's account, if they offer one.

Health and recovery

A backup is only useful if it can be read back. Unspora has several tools to check this, in the **Coverage and recovery** and **Repository integrity** sections of each destination.

Reviewing coverage

Click **Review Coverage** to scan your selected folders and see what the backup actually covers:

- **Locally readable files**: files Unspora could read.
- **Excluded entries**: items your exclusion rules skip.
- **Cloud-only entries**: files stored only in the cloud, such as iCloud Drive files that are not downloaded to this Mac. They must be downloaded before their contents can be backed up. The scan does not download them.
- Any access problems, listed in orange (up to the first 100).

Selected folders and **Deliberate exclusions** list exactly what this destination includes and skips. If a rule excludes all of `~/Library/Developer`, Unspora warns you, since that also excludes Xcode archives you may not be able to recreate.

The coverage scan reads file information only, and its exclusion matching is approximate.

Testing recovery

The best test is to restore a real file and open it. Use **Find and Restore Files...** (see Finding and restoring files), restore a file you know, and check it.

For a quick automatic test, click **Test Recovery with a Small File**. Unspora picks a small file (up to 1 MiB) from a recent snapshot of this Mac, restores it into a private temporary folder, verifies it, and deletes the sample. On success it shows **Sample file restored, verified, and removed.**

Either way, **Last verified restore** is updated, and **Verified selection** shows which file or snapshot was restored.

A successful restore proves that the data you restored can be recovered. It does not prove that every file in every snapshot can be.

Integrity checks

Click **Check Structure and 5% of Stored Data** to have restic check the repository's structure and read back a random 5% of the stored data. **Last check** and the result appear in the **Repository integrity** section.

This downloads data from your storage, which some providers charge for, and it can take a long time on a large cloud repository. A passing check means no problems were found in the structure and the sample. It does not read every file.

Monthly checks

To run these checks automatically, edit the destination and turn on **Monthly integrity check and small-file recovery test** under **Advanced Options** > **Power & Network**. After a complete scheduled backup, if the last check or last verified restore is more than 30 days old (or the last check failed), Unspora runs an integrity check and a small-file recovery test. If either fails and notifications are on, you get a notification.

Recovery kits

If your Mac is lost, stolen, or broken, you need three things to get your files back: the repository address, the repository password, and your storage credentials. A recovery kit records the first, plus your destination's settings and step-by-step instructions, so you are not reconstructing them from memory.

Exporting a recovery kit

1. Select the destination and click **Export Recovery Kit...** in **Coverage and recovery**.
2. Read the instructions in **Recover on Another Mac**, then click **Export Kit...**.
3. Choose where to save it.

Unspora creates a folder named **Unspora Recovery Kit** followed by a unique ID, containing `recovery-plan.json` (the settings) and `READ-ME.txt` (the instructions, including how to recover with plain restic if Unspora is not available).

The kit contains the repository address, storage type, folder paths, exclusions, and retention policy. It contains **no passwords or access keys**. Store it somewhere independent of this Mac, such as a password manager's secure notes or a cloud drive, and make sure the repository password and storage credentials are in your password manager, reachable from another device. For SFTP, also keep your SSH key, its passphrase, and the host settings.

Recovering on a new Mac

1. Install Unspora on the new Mac and register it with your code (see Registering).
2. Choose **File** > **Import Recovery Kit...**, or click **Import Recovery Kit...** on the Overview.
3. Select `recovery-plan.json` and click **Import Recovery Plan**.
4. The destination editor opens with the settings filled in. Enter the existing repository password and your storage credentials.
5. Click **Test Connection**. It should report the existing snapshots.
6. Click **Save**. Do not create a new repository at this address; if Unspora offers to create one, the address or credentials are wrong.
7. Select the destination, click **Find and Restore Files...**, choose a backup date, and restore your files.

If you moved to the new Mac with Migration Assistant or a restore instead, Unspora's settings come along, and Unspora asks you to confirm them once before backing up. See Settings from another Mac.

For safety, an imported destination starts with no folders selected, a **Manual** schedule, and automatic retention turned off. This prevents the new Mac from immediately backing up or removing snapshots before you have restored what you need. When you are ready to back up the new Mac, edit the destination to choose folders, a schedule, and retention.

The menu bar and notifications

The menu bar icon

Unspora always shows an icon in the menu bar: a small shield divided into panes, the same shape as the app icon.

Click it to open a small window with the same protection summary as the Overview: one entry per destination with its last complete backup, latest attempt, next due time, and last verified restore, plus **Review and Restore...** and **Back Up Now** buttons. At the bottom, **Open Unspora** opens the main window, and the gear menu has **Settings...**, **About Unspora**, and **Quit Unspora**.

Right-click (or Control-click) the icon for a short menu: **Open Unspora**, **About Unspora**, **Check for Updates...**, **Settings...**, **Unspora Help**, and **Quit Unspora**.

If this copy is not registered and has no destinations yet, the small window offers **Register Unspora...** instead.

Keeping Unspora out of the Dock

By default Unspora keeps its Dock icon even when the window is closed. To run it from the menu bar only, turn off **Keep in Dock when the window is closed** in **Settings** > **General**. The Dock icon and the menu bar menus then appear only while an Unspora window is open.

Notifications

Notifications are off until you turn them on. To turn them on:

1. Choose **Unspora** > **Settings...** and click **General**.
2. Click **Enable Backup Notifications** and allow notifications when macOS asks.

If you previously declined, allow Unspora in **System Settings** > **Notifications**.

Unspora then notifies you when:

- A backup ends incomplete, failed, or cancelled, or retention fails after a backup.
- A scheduled backup is due but is waiting for power, a network, or a disconnected disk.
- A monthly integrity check or recovery test fails.
- The storage estimate reaches your budget warning, or could not be refreshed.
- The background agent could not run the schedule at all.

- Unspora's settings were changed outside the app, or came from another Mac and need confirming.

Unspora does not notify you about successful backups.

Updates

A registered copy of Unspora checks for updates about once a day and tells you when a new version is available. To check now, choose **Unspora** > **Check for Updates...**, or right-click the menu bar icon and choose **Check for Updates...**.

When an update is available, Unspora shows what is new, with **Install Update**, **Remind Me Later**, and **Skip This Version**. Installing downloads the new version, checks that it is genuine (signed for Unspora and notarized by Apple), replaces the app, and opens the new version.

- **Running backups are not interrupted.** If a backup, restore, check, or retention run is in progress, Unspora waits for it to finish before restarting, checking every 30 seconds.
- **Your settings carry over,** including Full Disk Access and scheduled backups. The new version re-registers the background agent when it opens.
- **What the check sends:** your registration (the name and email your code was issued to), the Unspora version, and the macOS version. Nothing about your files or backups.

An unregistered copy does not receive updates: **Check for Updates...** says **Register Unspora to receive updates**. Register first, or download the latest version from https://api.unspora.com/download and install it as described in Installing.

To update by hand, quit Unspora, close any AI agent sessions that use Unspora's MCP server, replace the app in Applications with the new version, and open it again.

When settings change outside Unspora

Unspora's settings decide which folders are backed up and where they go, and Unspora may have Full Disk Access. That would make its settings files a target for other software on your Mac: a program that rewrote them could have Unspora back up your protected data to a place that program controls. So Unspora seals its settings.

The seal covers your destinations, the **Allow agents to make changes without asking** setting, and fingerprints of each destination's stored passwords and keys. Its key is kept in a protected part of the Keychain that only Unspora can read or replace. Every change you make in Unspora renews the seal; a change made any other way breaks it.

What happens when the seal breaks

- The Overview shows **Unspora's settings were changed outside the app**, with a **Review...** button, and you are notified.
- Scheduled backups continue, using the settings Unspora last saved. A destination added outside Unspora is ignored, and a destination whose stored password or keys were replaced is skipped.
- **Allow agents to make changes without asking** stays as you last set it in Unspora, whatever the settings files say.
- Unspora saves no further changes until you review this one.

Reviewing the change

Click **Review...**. The list shows each change, such as **Added destination "Name", backing up to address**, **Changed where "Name" backs up to**, or **Replaced the stored password or keys for "Name"**.

- **Undo These Changes** puts back the settings Unspora last saved. A destination whose stored password or keys were replaced cannot be trusted again, so it is removed; its backups are untouched, and you can reconnect to them with **Import Recovery Kit...**.
- **Keep These Changes...** accepts the files as they are, after a confirmation. Choose it only if you made the change yourself, for example by editing Unspora's files by hand.
- **Later** closes the review. The banner stays until you decide.

If you did not make the change, choose **Undo These Changes**, and consider checking your Mac for unwanted software.

Settings from another Mac

The seal's key never leaves the Mac that made it. When Unspora's settings arrive on a new Mac through Migration Assistant, a restore, or a copy, Unspora shows **Confirm settings from another Mac**, listing each destination and where it backs up to.

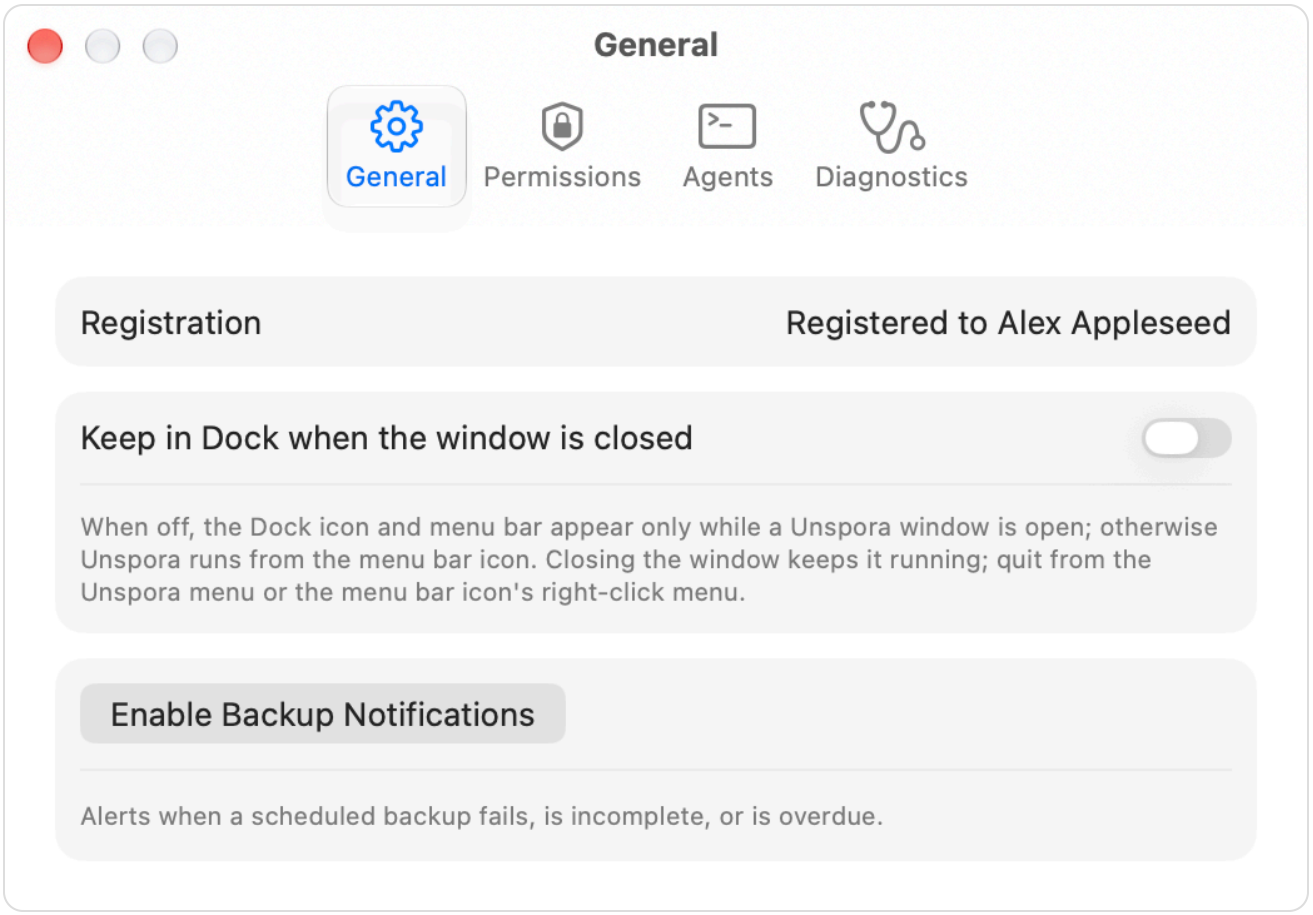
- Click **Use These Settings** if you moved them yourself. Backups on this Mac start once you do.
- Passwords and keys may not move with the settings. If a destination's connection test fails, enter them again in the destination editor.

Setting up the new Mac with **Import Recovery Kit...** instead never needs this confirmation.

Settings

Choose **Unspora** > **Settings...** (⌘,), or choose **Settings...** from the menu bar icon. Settings has four tabs. Settings for a single destination, such as its schedule and retention, are in the destination editor instead.

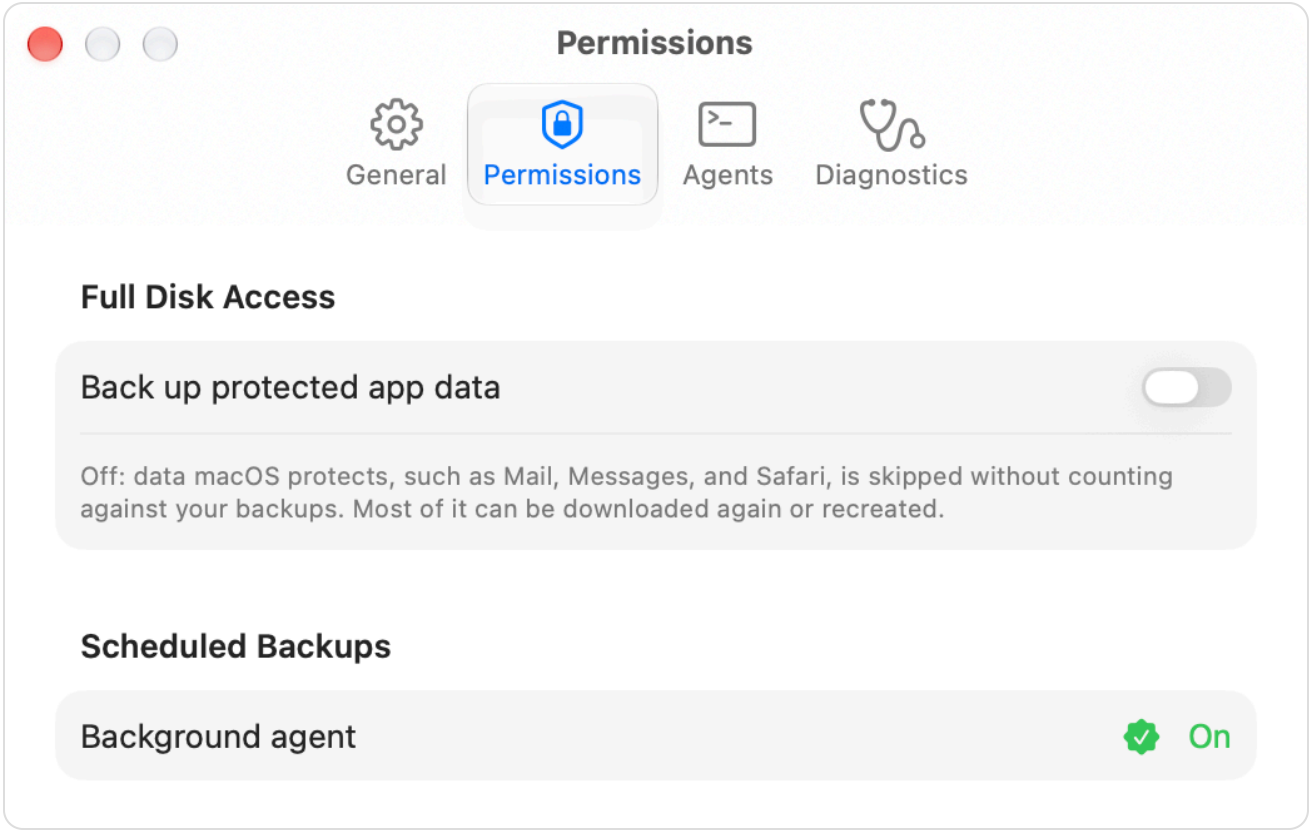
General



The General settings tab.

- **Registration**: **Registered to** and the name your code was issued to, or **Not registered**. See Registering.
- **Keep in Dock when the window is closed**: when off, Unspora runs from the menu bar icon once you close its window. See Keeping Unspora out of the Dock.
- **Enable Backup Notifications**: asks macOS for permission to send backup alerts. See Notifications.

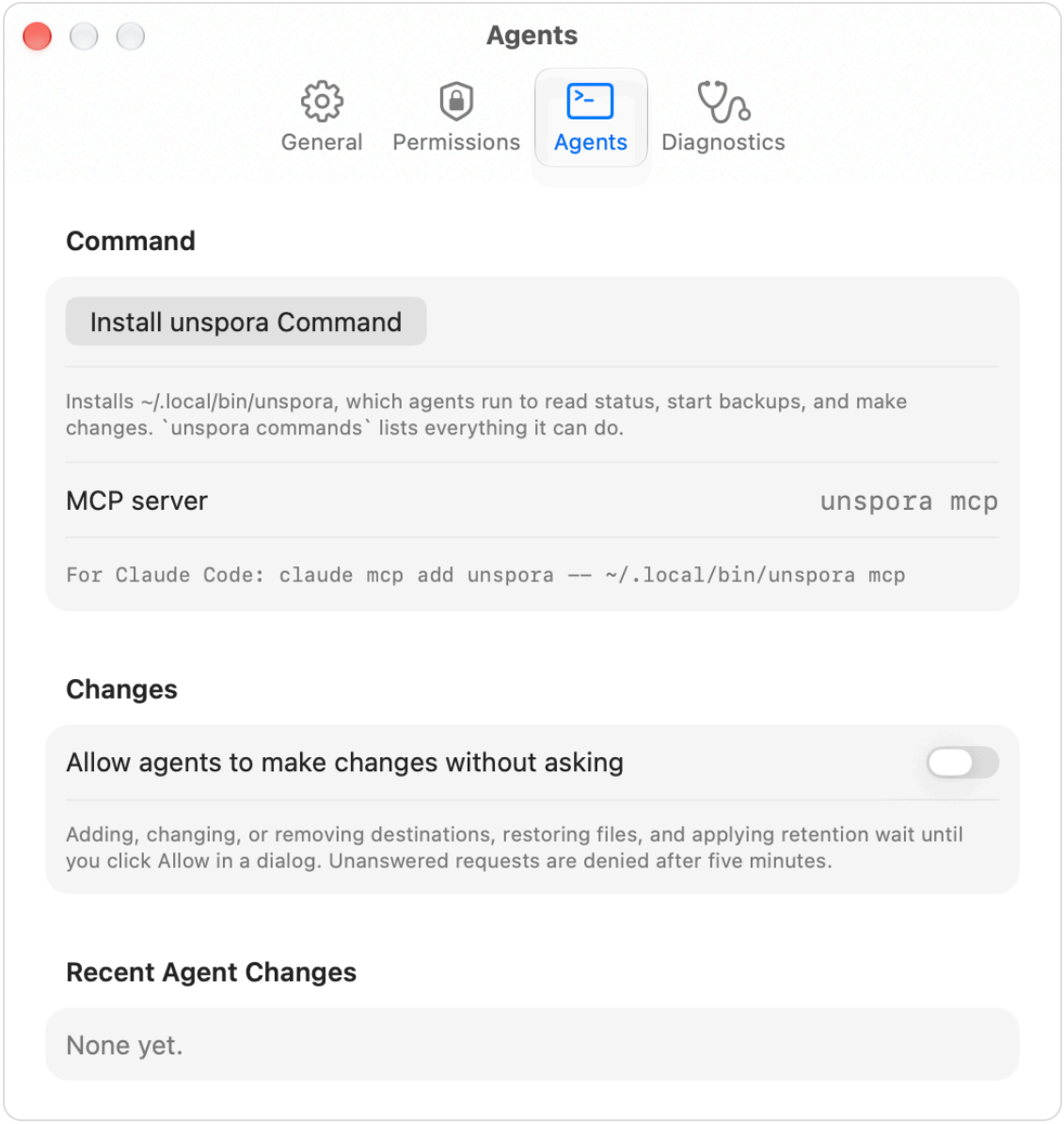
Permissions



The Permissions settings tab.

- **Back up protected app data** turns on backing up data macOS protects, such as Mail, Messages, and Safari. Off by default; see Full Disk Access (optional).
- When it is on, **Full Disk Access** shows **Granted** or **Not granted**. When not granted, **Open Full Disk Access Settings…** takes you to the list in System Settings, and **Ask at launch while access is off** controls the alert at launch (the opposite of the alert's **Don't ask again at launch** checkbox).
- **Scheduled Backups** shows the **Background agent** status: **On** when scheduling works, **Needs approval** when macOS is waiting for your approval in Login Items (with an **Open Login Items Settings…** button), and **Off** when no destination has a schedule.

Agents

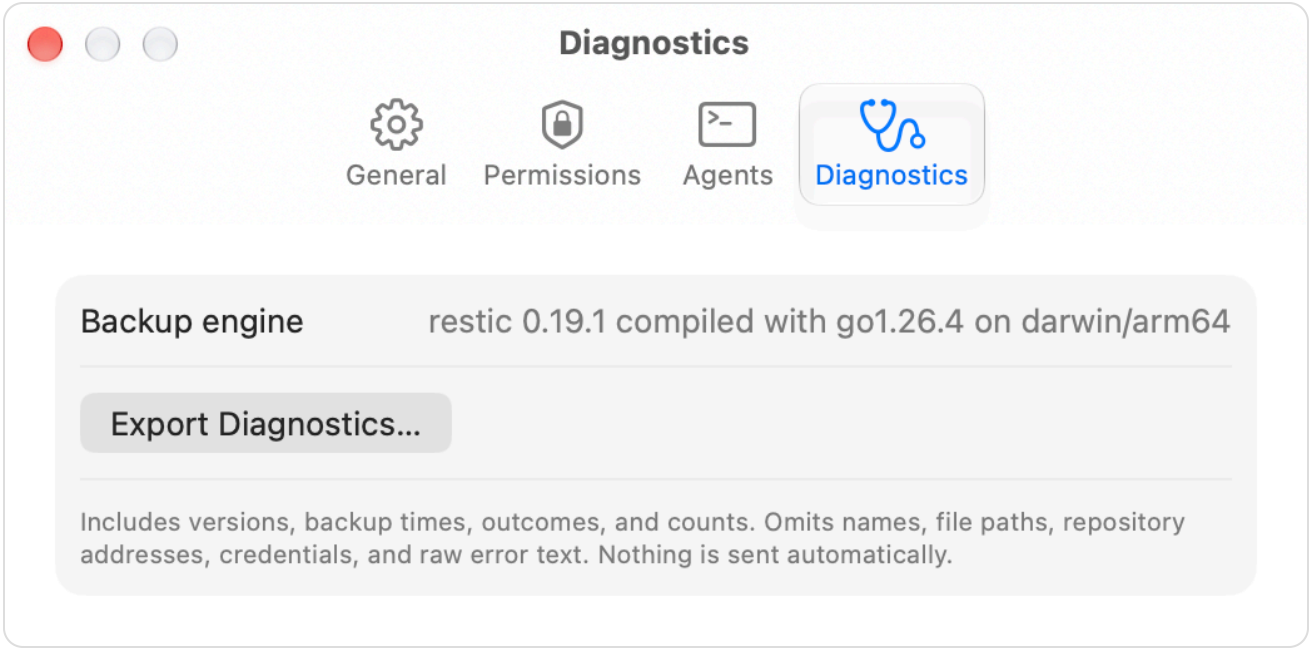


The Agents settings tab.

- **Install unspora Command** installs the `unspora` command for AI agents and scripts.
- **MCP server** shows the command that starts Unspora's MCP server, with the line to add it to Claude Code.
- **Allow agents to make changes without asking** turns off the approval dialog for agent changes. Off by default. It can only be changed here, not by editing Unspora's files; see When settings change outside Unspora.
- **Recent Agent Changes** lists the last ten changes agents asked for and how each was decided.

See Using Unspora with AI agents.

Diagnostics



The Diagnostics settings tab.

- **Backup engine** shows the version of restic built into Unspora.
- **Export Diagnostics...** saves a report file (`Unspora-diagnostics.json`) you can send when asking for help. It includes versions, backup times, outcomes, and counts. It leaves out destination names, file paths, repository addresses, credentials, and raw error text. Nothing is sent automatically.

Using Unspora with AI agents

Unspora can be controlled by AI agents, such as Claude Code, and by your own scripts. An agent can check backup status, browse snapshots, and start backups. Changes, such as adding a destination or restoring files, wait for you to approve them.

Installing the command

1. Choose **Unspora** > **Settings...** and click **Agents**.
2. Click **Install unspora Command**.

This installs a small launcher at `~/.local/bin/unspora`. If `~/.local/bin` is not on your shell's search path, run it by its full path or add the folder to your path. Run `unspora commands` to list every command and its options.

Each command prints its result as JSON. For example:

```
unspora status
unspora snapshots --destination "Offsite"
unspora backup --destination "Offsite"
```

Secrets, such as a repository password for `add-destination`, are passed as JSON on standard input with `--json -`, never as command-line options. Unspora never returns credentials from any command.

Connecting an MCP client

Unspora includes an MCP (Model Context Protocol) server, which lets AI apps use its commands as tools. To add it to Claude Code:

```
claude mcp add unspora -- ~/.local/bin/unspora mcp
```

Other MCP clients can run `~/.local/bin/unspora mcp` as a standard input/output server. Each command becomes a tool with the same name and options.

What needs approval

Commands fall into three groups:

Group	Commands	Approval
Read	`status`, `destination`, `history`, `snapshots`, `browse`, `audit`, `backup-result`	None
Operate	`backup`, `check`, `retention-preview`	None. They act only on existing destinations and change no settings.
Change	`add-destination`, `update-destination`, `remove-destination`, `restore`, `apply-retention`	Your approval in a dialog

`add-destination` also needs a registered copy. On an unregistered copy it fails with the code `unregistered` (exit status 5). `status` reports `registered`, and `configuration` as `sealed` or `changed-outside-unspora`.

When an agent asks for a change, Unspora shows a dialog describing exactly what was requested. **Deny** is the default button, so pressing Return refuses; allowing takes a click on **Allow**. If nobody answers within five minutes, the request is denied, so an agent may wait up to five minutes for an answer.

Agent restores follow the same rules as yours: they go into a new folder and never overwrite existing files. Removing a destination never deletes data from the repository.

To skip the dialog, turn on **Allow agents to make changes without asking** in the **Agents** tab and confirm with **Allow Without Asking**. An agent could then remove destinations, change what is backed up, restore files anywhere you can write, and delete snapshots with no prompt. Leave it off unless you have a specific reason.

The audit log

Every change an agent requests, allowed or not, is recorded. The **Agents** tab shows the last ten under **Recent Agent Changes**, each marked **Allowed**, **Allowed by setting**, **Denied**, or **Not answered**, with “then failed” added if an allowed change did not succeed. Agents can read the log

with the `audit` command. The full log is the file `~/Library/Application Support/Unspora/agent-audit.jsonl`.

How agent backups run

A program started by an agent gets its file access from the agent's terminal or app, not from Unspora. So when an agent runs `backup`, Unspora hands the job to its background agent, which runs with Unspora's Full Disk Access, and returns a request ID. The agent can wait for the result with the `waitSeconds` option or check later with `backup-result`. Results are kept for seven days. Backups requested this way run even if power or network conditions would hold back a scheduled backup.

The background agent exists only while at least one destination has an hourly or daily schedule. If no destination is scheduled, `backup` fails and suggests the `inProcess` option, which runs the backup in the calling process using that process's file access.

Things to know

- **One restic operation per repository at a time.** If an agent asks for an operation on a repository while Unspora, a scheduled backup, or another agent request is already using it, the request fails at once with "This repository is busy in another Unspora operation." Try again after the other operation finishes. Commands that don't touch the repository, such as `status` and `history`, are not affected.
- **Slow commands.** `check` reads 5% of the stored data and can take many minutes on cloud storage. The MCP server runs tool calls side by side, so other calls answer while a long one such as `check` runs.
- **What the approval dialog protects against.** It stops an agent doing something you did not intend. Software that edits Unspora's settings files directly is caught by the seal instead (see When settings change outside Unspora). Neither can stop software that clicks **Allow** for you, or that you allow yourself.

Using the restic command line directly

Unspora's repositories are standard restic repositories. You can use the restic command-line tool on them alongside Unspora, or instead of it.

Connecting with restic

Install restic from restic.net or a package manager. Then point it at your repository and supply credentials through environment variables. For a Backblaze B2 destination:

```
export RESTIC_REPOSITORY="b2:my-backups:restic"
export B2_ACCOUNT_ID="your-key-id"
export B2_ACCOUNT_KEY="your-application-key"
restic snapshots
```

restic asks for the repository password. Avoid putting the password on the command line, where it is saved in your shell history. For S3-compatible storage, use `AWS_ACCESS_KEY_ID` and `AWS_SECRET_ACCESS_KEY`; SFTP uses your SSH configuration; a local disk needs only the path.

The repository address is shown in the destination's **Destination** section as **Repository**.

Useful commands

Task	Command
List snapshots	`restic snapshots`
Browse a snapshot	`restic ls SNAPSHOT_ID`
Restore safely into a new, empty folder	`restic restore SNAPSHOT_ID --target ~/Restored --overwrite never --verify`
Restore one path	add `--include "/Users/yourname/Documents/report.pdf"`
Check the repository	`restic check`

Working alongside Unspora

- Unspora records snapshots under your Mac's short host name (as `hostname -s` prints it). If you back up the same folders with restic from the same Mac, the snapshots appear together in Unspora.
- restic locks a repository during operations. When a backup or retention run finds the repository locked by another Mac or a restic command, Unspora waits up to 30 minutes for the lock to be released.
- Snapshots you create or remove with restic appear in Unspora after **Refresh**.
- Never run `restic init` on an existing repository's address.

Troubleshooting

Backups end incomplete

An incomplete backup created a snapshot, but some files could not be read. Open the destination, find the run in **Backup history** or the **Skipped items** list under the last result, and read the listed files and errors.

- **“Full Disk Access could not be confirmed”**: you turned on **Back up protected app data**. Grant Full Disk Access (see Full Disk Access (optional)) and reopen Unspora, or turn the option off.
- **“Permission denied” or “Operation not permitted” on specific files**: some locations are off-limits even with Full Disk Access. If the files are caches or app data you do not need, add an exclusion for them. Smart Exclude suggests many such folders.
- **“No such file” errors**: files that were deleted while the backup ran, such as temporary files. If they recur, exclude the folder they live in.
- **Files that are always in use**: some apps hold databases open. These are often backed up fine; if one keeps failing, check whether the app offers its own export or backup.

After you fix the cause, run **Back Up Now** and check that the outcome is complete. A scheduled destination also retries on its own, up to three times.

Full Disk Access shows Not granted after you turned it on

- Quit Unspora completely (from the **Unspora** menu or the menu bar icon) and open it again.
- Make sure you are running the copy in your Applications folder, and that the switch you turned on is for that copy. If Unspora appears more than once in the Full Disk Access list, remove the extra entries with the minus button, then click **Open Full Disk Access Settings…** in Unspora again and turn it on.
- Unspora detects access by trying to read a few protected locations, such as Safari and Mail data. On a Mac where none of these exist, it may report access as off even when it is on.

“This repository is busy in another Unspora operation”

Unspora runs one operation at a time on each repository from this Mac: a backup, a restore, a check, retention, or a measurement. Wait for the other operation to finish (it may be a scheduled backup or an agent request running in the background) and try again.

A backup or retention run waits a long time before starting

Another Mac or a restic command may be using the repository. Unspora waits up to 30 minutes for restic's lock. If a lock was left behind by a crashed process on another machine, restic's `unlock` command removes it; use it only when you are sure nothing else is using the repository.

Scheduled backups are not running

1. Open **Settings** > **Permissions** and check **Background agent**.
    - **Needs approval**: click **Open Login Items Settings...** and turn on Unspora under **Allow in the Background**.
    - **Off**: no destination has a schedule. Edit a destination and choose **Hourly** or **Daily**.
2. Check the destination's **Backup history**. Runs that started but did not complete show their reasons there.
3. Check the conditions in **Advanced Options** > **Power & Network**. A laptop on battery with **Start scheduled backups only on AC power** turned on, or a hotspot connection with **Avoid metered and Low Data Mode networks** turned on, holds backups back. Turn on notifications to be told when this happens.
4. Remember that scheduled backups cannot run while the Mac is asleep, off, or logged out.
5. After updating Unspora by hand, open the new version once. Opening it re-registers the background agent for the new version. Updates installed through **Check for Updates...** do this for you.
6. If the Overview says **Unspora's settings were changed outside the app**, backups run only for the destinations Unspora last saved. Review the change; see When settings change outside Unspora.

If saving a destination shows "automatic backups could not be registered", check **Login Items** in System Settings as described above.

Registration fails

- **"Could not reach the registration server"**: check your internet connection and try again. Only registering needs it.
- **"That registration code was not found"** or **"That is not a valid registration code"**: check the code against the one you were sent. The letter O is read as the digit 0, and I and L as 1, so either works.
- **"This code is already registered on 5 Macs"**: the code has reached its limit. Ask whoever sent it for another code or for a Mac to be freed.
- **"That registration code has been revoked"**: ask whoever sent it.

Check for Updates says to register

Updates come to registered copies only. Register (see Registering), or download the latest version from https://api.unspora.com/download.

Unspora says its settings were changed outside the app

Something other than Unspora edited its settings files or the stored passwords and keys. Click **Review…** on the Overview to see exactly what changed, then undo or keep it. See When settings change outside Unspora.

“No repository was found at this address”

The address, bucket name, or folder does not point at an existing repository, or the credentials do not reach it. Check each part carefully. When editing a destination, Unspora never creates a new repository, to avoid silently moving your backups to an empty one. When adding a destination, create a new repository only if you meant to start fresh.

The connection test fails

The error message comes from restic or your provider. Common causes:

- Wrong key ID or secret, or a key without access to the bucket.
- Wrong repository password: the message says the password does not unlock the repository. You need the original password; it cannot be recovered.
- For SFTP: the host is not reachable, or your SSH key is not loaded into ssh-agent. Try `ssh user@backup-server` in Terminal.
- For a local disk: the disk is not connected or the path is wrong.

macOS warns about opening Unspora

Unspora is signed and notarized by Apple, so a copy downloaded from the official source opens normally. If macOS says it cannot verify the app or that the app is damaged, delete it, download the disk image again, and drag a fresh copy into Applications. Do not bypass the warning for a copy whose origin you are unsure of.

Getting help

This guide is built into Unspora. Choose **Help** > **Unspora Help** (⌘?), or type a question into the search field at the top of the **Help** menu to find a topic. **Help** > **What's New in Unspora**, **Troubleshooting**, and **Keyboard Shortcuts** open those sections directly, and **Download User Guide (PDF)** gets a printable copy of this guide for your version. In menu-bar-only mode, right-click the menu bar icon and choose **Unspora Help**.

To ask a question or report a problem, choose **Help** > **Contact Support...**, which opens the support form on unspora.com.

When you report a problem, include a diagnostics report from **Settings** > **Diagnostics** > **Export Diagnostics...**. It contains no names, paths, addresses, or credentials, and you choose whether to share it.

Keyboard shortcuts

Shortcut	Action	Where
⌘N	**New Destination…**	File menu
⌘B	**Back Up Now**	Destination menu, with a destination selected
⌘E	**Edit Destination…**	Destination menu, with a destination selected
⌘R	**Refresh Snapshots**	Destination menu, with a destination selected
⌘Delete	**Remove Destination…**	Destination menu, with a destination selected
⌘Z	**Undo** (restores a removed destination)	Edit menu
⌘,	**Settings…**	Unspora menu, and the menu bar icon’s right-click menu
⌘?	**Unspora Help**	Help menu
⌘↑	Go to the parent folder	**Find and Restore Files**
Return or double-click	Browse the selected snapshot	Snapshot list
⌘Q	**Quit Unspora**	Unspora menu, and the menu bar icon’s right-click menu

Import Recovery Kit… (File menu), **Test Connection**, **Apply Retention Now…** (Destination menu), and **Check for Updates…** (Unspora menu) have no shortcuts.

Glossary

Allow in the Background
: The list in **System Settings** > **General** > **Login Items & Extensions** where you approve background agents such as Unspora's scheduler.

Background agent
: The part of Unspora that macOS starts once an hour to run scheduled backups, even when the app is closed.

Complete backup
: A backup that created a snapshot and read every selected file, apart from protected app data skipped because Full Disk Access is not in use.

Configuration seal
: Unspora's tamper check on its own settings, keyed from a protected part of the Keychain. See When settings change outside Unspora.

Deduplication
: restic's technique of storing each piece of unchanged data only once, across all snapshots and Macs sharing a repository.

Destination
: One place your backups go, together with its credentials, folders, exclusions, schedule, and retention policy.

Exclusion (exclude rule)
: A pattern that tells restic to skip matching files or folders.

Full Disk Access
: A macOS permission that lets an app read protected data such as Mail, Messages, and Safari data.

Incomplete backup
: A backup that created a snapshot but could not read some files, or could not confirm Full Disk Access you chose to use.

Integrity check
: A restic check of the repository's structure and a random sample of its stored data.

MCP (Model Context Protocol)
: A standard way for AI apps to use external tools. Unspora's MCP server exposes its commands to AI agents.

Prune
: The restic operation that deletes stored data no remaining snapshot uses, freeing space after snapshots are removed.

Recovery kit
: A folder with a destination's settings and recovery instructions, without passwords or keys, for reconnecting from another Mac.

Registration code

The code, in the form `UNSP-XXXX-XXXX-XXXX`, that unlocks setting up backups and receiving updates on a few Macs.

Repository

The encrypted restic storage area at a destination that holds your snapshots.

Repository password

The password restic uses to encrypt the repository. If lost, the backups cannot be read.

restic

The open-source backup program Unspora uses to create, store, and restore backups.

Retention policy

Rules deciding which snapshots to keep (daily, weekly, monthly, yearly) and which to remove.

Snapshot

A record of your selected folders at the moment a backup ran. You restore from snapshots.

Verified restore

A restore whose contents restic checked against the backup.

What’s new

Each version’s changes, newest first. The same notes appear in the update window when Unspora offers a new version.

Version 0.8.0

- **Full Disk Access is now optional and off by default.** Unspora backs up your files without it and skips the data macOS protects, such as Mail, Messages, and Safari, without marking backups incomplete, retrying, or asking you for the permission. To include that data, turn on **Back up protected app data** in **Settings** > **Permissions**. Macs that already granted Full Disk Access keep it on. See Full Disk Access (optional).
- **Help is built in. Help** > **Unspora Help** (⌘?) opens the user guide, and the search field in the **Help** menu finds topics in it. The **Help** menu also opens **What’s New in Unspora**, **Troubleshooting**, and **Keyboard Shortcuts** directly, downloads the guide as a PDF for your version, and has **Contact Support…** and **Acknowledgements**.
- **Unspora Help** is also in the menu bar icon’s right-click menu.
- The licenses of the open-source software inside Unspora now ship with the app. See Acknowledgements.

Version 0.7.1

- A new app icon: the capital U of the Major Mono Display typeface, a shield, filled with a grid after Mondrian’s *Composition with Large Red Plane* (1921).
- The menu bar icon is now the same shield as a one-colour outline that follows light and dark menu bars.

Version 0.7.0

- **Unspora seals its settings.** If another program changes your destinations, the stored passwords and keys, or the agent approval setting, Unspora notices, keeps backing up with the settings it last saved, and asks you to review the change. See When settings change outside Unspora.
- Settings brought over from another Mac, for example by Migration Assistant, are recognised and need one confirmation.

Version 0.6.0

- **Registration.** Setting up backups and receiving updates need a registration code; backups and restores never do. See Registering.
- **Automatic updates.** Unspora checks for updates once a day and installs them on request, waiting for any running backup to finish first. See Updates.

Version 0.5.0

- **Control from AI agents and scripts.** The `unspora` command and its MCP server let agents check status, browse snapshots, and start backups; changes wait for your approval. See Using Unspora with AI agents.

Acknowledgements

Unspora is built on open-source software. Their licenses are inside the app, in `Unspora.app/Contents/Resources/Licenses` (in Finder, Control-click Unspora and choose **Show Package Contents**).

- **restic** does the backup work. Copyright Alexander Neumann and the restic contributors; BSD 2-Clause License. restic includes Go libraries under their own open-source licenses, listed in its source repository.
- **Sparkle** installs updates. Copyright Andy Matuschak and the Sparkle contributors; MIT License. It includes bsdiff, sais-lite, and an Ed25519 implementation, whose licenses are in Sparkle's license file.
- **Major Mono Display** provides the capital U the icon is drawn from. Copyright 2018 The Major Mono Project Authors; SIL Open Font License 1.1.
- **The icon's grid** follows Rachel's homage to Piet Mondrian's *Composition with Large Red Plane, Yellow, Black, Gray and Blue* (1921).