



HARBOR PROTECT

Harbor Protect Manual

Setup, features, cloud destinations, and a quick-reference appendix

User guide for Harbor Protect 3.0 • Build 1

At a glance Harbor Protect protects whole drives, individual project folders, and multi-folder Collections. Backups can go to a local folder or Amazon S3, and Pro adds automatic scheduling, a second destination, and version history. Chapters 1–12 walk through every feature; the Quick Reference appendix at the back is for fast lookup.

Contents

- 1. Start here
- 2. Choose your plan: Free, Standard, and Pro
- 3. Set up protection
- 4. Understand Collections and DAW sessions
- 5. Analyze and run backups
- 6. Read the dashboard
- 7. Restore files safely
- 8. Amazon S3 setup
- 9. Use Dropbox or Google Drive as a destination
- 10. Backup behavior and previous versions
- 11. Troubleshooting
- 12. Recommended routine and glossary
- Appendix: Quick Reference

1. Start here

Harbor Protect is a macOS backup manager designed for studio projects. It lets you choose what to protect, control the order in which items run, preview changes before copying, and restore from a local or cloud backup.

What you need

- The source drive or project folder connected and available in Finder.
- A separate local destination with enough free space, or an Amazon S3 account and bucket.
- Permission for Harbor Protect to access the selected folders and external drives when macOS asks.

Important A backup destination should not be inside the source folder. For whole-drive protection, choose a different physical drive whenever possible.

First launch

1. Open Harbor Protect. The welcome screen appears when nothing is configured.
2. Select Get Started.
3. Choose a default destination, then add at least one whole drive, project folder, or Collection.
4. Confirm every selected item has a valid destination, then select Save.
5. Run Analyze before your first backup, review the preview, then select Protect All.

© 2026 Veit Renn / RennMusic. All rights reserved.

Harbor Protect and the Harbor Protect logo are trademarks of Veit Renn / RennMusic.

2. Choose your plan: Free, Standard, and Pro

Harbor Protect is one app with three protection levels. The plan name in the toolbar (or the gear menu) opens the License window, where a Standard or Pro key is activated. Upgrading never touches existing configurations, backups, or Restore access.

Plan	Best for	Includes
Free	Trying Harbor Protect	Protects one local backup item, with full Analyze, Protect, and Restore for it.
Standard	Everyday studio backup	Unlimited protection items, Amazon S3 off-site destinations, Collections and DAW session guidance, Archive Protection, and Protection History.
Pro	Hands-off, redundant protection	Everything in Standard, plus Version History, Automatic Backups, and Dual-destination backup.

Pro at a glance Version History keeps dated, restorable snapshots instead of just the latest copy. Automatic Backups runs Protect All on a schedule you set, with no clicking required. Dual-destination backup keeps a second copy of everything — a second drive or Amazon S3 — for simple 3-2-1 protection.

Upgrading from Standard to Pro

Standard customers can upgrade to Pro from the same License window, without buying a whole new setup from scratch.

- Open the License window (the plan name in the toolbar, or the gear menu).
- A Harbor Pro card appears with an Upgrade to Pro button, priced as the difference from Standard rather than Pro's full price.
- Activating a Pro key upgrades the plan immediately. Deactivating the old Standard license first is not required.

Availability The upgrade card only appears once Pro is available for purchase. Until then, Standard remains the top available plan.

3. Set up protection

Open the gear menu and choose Choose Drives & Projects. The Protect Your Work window contains the default destination, backup order, and the three ways to add sources.

Choose a default destination

The default is applied to newly added items. Each item can be changed afterward.

Destination	Best for	What to select
Local Folder	Fast backups and restores to another disk	Choose a folder on a separate drive
Amazon S3	Off-site protection	Connect S3, choose Standard or Glacier

Plan requirement Amazon S3 (Standard or Glacier storage class) requires a Standard or Pro license. Free is limited to a Local Folder destination and one active protection item.

Add a whole drive

1. Connect the external drive and select Refresh Drives if it does not appear.
2. In Whole Drives, turn on the drive.
3. Confirm or change its destination.

Add one project folder

1. Under Specific Projects, select Add Project Folder...
2. Choose the project folder.
3. Confirm or change its destination.

Set backup order

The numbered Backup Order list determines the order used by Protect All. Use the up and down arrows to move items. A Collection runs its source folders one by one.

Save requirement Save becomes available only when at least one source is selected and every selected item has a ready local or S3 destination.

Dual-destination backup (Pro)

Pro can keep a second, independent copy of everything in the plan at the same time as the primary backup — a second hard drive, or Amazon S3, in any combination with the primary destination. This is a plan-wide setting, not a per-item one.

1. In Protect Your Work, turn on Also back up to a second destination.
2. Choose where the second copy goes: another Local Folder or an Amazon S3 bucket.
3. Select Save. The setting applies to every whole drive, project folder, and Collection already in the plan.

Dashboard cards for dual-protected items show a small “2×” badge. A mounted Dropbox or Google Drive folder can be chosen as either destination the same way any other Local Folder is chosen — Harbor Protect just sees it as a regular folder, and the sync app handles the upload afterward.

What stays primary Protected status, Last verified, and Restore all read from the primary destination only. The second copy is extra insurance, not an alternate source for Restore.

4. Understand Collections and DAW sessions

A Collection groups several source folders into one dashboard item. Use one when a project depends on files stored across multiple drives. Harbor Protect warns when a required source is missing and protects the Collection’s folders together.

Create a Collection

1. Select Add Folder as Collection... for a general multi-folder project, or Add DAW Session... for a supported session type.
2. Choose the Collection root or session and add every source folder the project depends on.
3. Choose one destination for the Collection.
4. Review the source list and select Save.

Prepare DAW projects

DAW	Before adding it to Harbor Protect
Pro Tools	Use Save Copy In... with Audio Files included.
Ableton Live	Use Collect All and Save.

DAW	Before adding it to Harbor Protect
Logic Pro	Use Consolidate Project Assets or Save a Copy As... with assets included.
Studio One / Fender	Use the app's copy/save-to-new-folder workflow.

Why this matters A session can reference audio or samples outside its visible project folder. Collecting assets first reduces the chance of an incomplete backup.

5. Analyze and run backups

Preview with Analyze

Analyze performs a dry run. It compares each source and destination but does not copy or delete anything. The Analysis window summarizes new, modified, and removed items, folder changes, and estimated transfer size when available.

1. Connect all required source and local destination drives.
2. Select Analyze in the bottom action bar.
3. Review the Analysis preview. Look for missing sources, unexpected deletions, or unusually large transfers.
4. Select Done when the preview looks correct.

Run protection

- Protect All runs every configured item in Backup Order.
- Protect on an individual card runs only that drive, folder, or Collection.
- Only new and modified files are copied; unchanged files are not recopied.
- The activity panel shows the current item, status, and progress.
- Stop ends the active Analyze, backup, or restore process. A stopped run is not considered verified.

Good practice Keep the Mac awake and leave required drives connected until the run finishes. Open Log afterward if any item does not show as protected.

Automatic Backups (Pro)

Automatic Backups runs Protect All on its own, on a schedule, without anyone clicking Protect. Open it from the gear menu.

Setting	What it does
Run backups automatically	Turns the schedule on or off.
Frequency	Every 6 hours, every 12 hours, daily, or weekly.
Day	For Weekly, the day of the week the backup runs.
Time	For Daily and Weekly, the specific time of day the backup runs.
Launch Harbor Protect at login	Keeps Harbor Protect open in the background so a scheduled backup is not missed.

It has to be running Automatic Backups only fires while Harbor Protect is open. Turn on Launch Harbor Protect at login so a scheduled run isn't skipped because the app wasn't open at the scheduled time.

6. Read the dashboard

Indicator	Meaning	What to do
Ready	Configured but not yet verified	Run Analyze, then protect it
Protected	Most recent run completed successfully	Continue your regular schedule
Syncing	A backup is currently running	Leave sources and destinations connected
Attention	A source or destination is missing, or a run was interrupted	Reconnect it and review Log

Protection Confidence

Protection Confidence is the percentage of dashboard entries currently marked Protected. A Collection counts as protected only when its required source jobs are protected. It is a quick status summary, not a substitute for periodic restore testing.

Last verified and Log

Last verified shows when Harbor Protect last completed a successful backup. Select Log to view the current session's activity and error messages. The log is the first place to look when a run was skipped or failed.

Archive Protection (Standard)

Archive Protection retires a finished project or drive from the active dashboard and Protect All without deleting its backup history. Select the archive icon on a protection card, then confirm Archive Protection.

- Archived items no longer appear in Analyze or Protect All, so they stop crowding the active list.
- Existing backup files are not deleted, and the item can be restored or reactivated at any time.
- Select Archived Protection from the gear menu to view, restore, or permanently remove archived items.

Plan requirement Archive Protection requires a Standard or Pro license. On Free, the gear menu shows a locked upsell instead of the archive list.

Protection History (Standard)

Protection History is a searchable, plain-English record of every protection run — separate from the current session's Log. Select Protection History from the gear menu.

Field	What it shows
Outcome	Protected, Needs Attention, or Stopped for that run.
Destination	Local Folder, Amazon S3, or both, for that run.
Keep	How long records are retained: 90 Days, One Year, or Forever.

Plan requirement Protection History requires a Standard or Pro license. On Free, the gear menu shows a locked upsell instead of the history list.

7. Restore files safely

Recommended Use Restore to New Location... for routine testing and recovery whenever possible. It copies the backup to a folder you choose without overwriting the original project.

Restore to a new location

1. Select Restore in the bottom action bar.
2. Find the Collection or individual backup.
3. Select Restore All to New Location... for a Collection, or Restore to New Location... for one backup.
4. Choose an empty or clearly named recovery folder.
5. Confirm Restore Copy, wait for completion, then open and verify the recovered files.

Restore to the original location

Select Restore or Restore All only when you intentionally want to recover into the original source location. Matching local files may be overwritten. Harbor Protect displays a destructive confirmation before starting.

Before restoring in place If the original folder still exists, make a separate copy or rename it first. Confirm that the correct backup source and destination drives are connected.

Version History (Pro)

Standard's _PreviousVersions is a safety net for the latest replaced files. Pro's Version History goes further: it keeps dated, restorable snapshots from before each protection run, so an older version can be recovered even after several more backups have run.

1. Select Previous Versions from the gear menu.
2. Choose the protected item and a dated snapshot from its list.

3. Restore that snapshot to its original location or to a new folder, the same way any other restore works.

Local snapshots save space by sharing unchanged files between versions; Amazon S3 snapshots are kept safely separated in the bucket.

8. Amazon S3 setup

Harbor Protect's Amazon S3 destination requires an AWS account. S3 and Glacier do not need separate signups: both are storage options inside the same AWS account.

Create an AWS account

1. Open aws.amazon.com/resources/create-account and choose Create an AWS Account.
2. Enter and verify the root user email address, choose an account name, and create the root password.
3. Choose Personal or Business and enter the requested contact information.
4. Add a valid payment method. AWS requires one even when a free-plan option is available.
5. Complete phone or identity verification.
6. Choose a support plan. Basic support is sufficient for many individual users.
7. Wait for the account activation confirmation. AWS says activation usually takes minutes but can take up to 24 hours.

Protect the account Enable multi-factor authentication for the root user, do not share root credentials, and use an IAM identity for Harbor Protect's access keys.

Create the S3 bucket

1. Sign in to the AWS Management Console and open Amazon S3.
2. Choose the AWS Region you want to use, then choose Create bucket.
3. Enter a globally unique bucket name and keep Block Public Access enabled.
4. Create the bucket. AWS charges for storage and data operations, not for creating the empty bucket itself.

Create credentials for Harbor Protect

1. In AWS Identity and Access Management (IAM), create or select a dedicated identity for Harbor Protect and grant it only the S3 permissions needed for the chosen bucket.
2. Open that IAM user's Security credentials tab and choose Create access key.

3. Review AWS's alternatives and security warning. If a long-term key is still appropriate, create it and save the Access Key ID and Secret Access Key securely.
4. Enter those two values, the bucket Region, and bucket name in Harbor Protect's Connect to Amazon S3 window, then use Test Connection.

Access-key safety Never create or use a root-user access key for Harbor Protect. The secret access key is shown only when it is created; if lost, delete that key and create a new one.

Connect Amazon S3 in Harbor Protect

Choose Amazon S3 as a destination, then select Connect Amazon S3... Harbor Protect asks for an Access Key ID, Secret Access Key, region, and bucket name. Credentials are stored in macOS Keychain and are not written to a plain-text file.

1. Enter the Access Key ID and Secret Access Key for the AWS account.
2. Enter the AWS region. The interface suggests us-west-1 for Las Vegas.
3. Enter an existing bucket name, or enter a new globally unique name and select Create New Bucket.
4. Select Test Connection and wait for Connected successfully.
5. Select Done, then choose a storage class for each S3 destination.

Bucket names Use 3–63 characters: lowercase letters, numbers, dots, and hyphens. Start and end with a letter or number. Names are globally unique; avoiding dots is recommended.

Choose Standard or Glacier

Harbor Protect option	Use it for	Access behavior
Standard (fast access)	Active projects and backups that may need quick recovery	Immediate online access
Glacier (cheap archive)	Long-term copies that are rarely restored	Deep Archive; restore request required, typically 9–48 hours

There is no separate Glacier account. Harbor Protect places uploaded objects into the S3 Glacier Deep Archive storage class when Glacier is selected. AWS applies minimum-storage-duration and retrieval charges, so review current AWS pricing before using it.

Example: 1 TB stored for six months

The example below uses public AWS rates for US West (N. California), checked July 16, 2026. It assumes 1 TB = 1,024 GB and no changes to the stored data during the six months. Storage is shown separately from the optional cost of downloading the entire backup to a Mac.

Cost component	S3 Standard	Glacier Deep Archive
Storage for six months	\$159.74	\$12.29
Cost if stored but not downloaded	\$159.74	\$12.29
Archive retrieval for full 1 TB	\$0.00	\$22.53 Standard or \$3.58 Bulk
One-day temporary restored copy	Not needed	About \$0.89
Full 1 TB internet download	\$83.16	\$83.16
Six months plus full download	\$242.90	\$118.86 Standard or \$99.92 Bulk

Why a normal bill may be much lower If the backup remains stored and is never fully downloaded, there is no \$83.16 internet-transfer charge. That charge appears only in this worst-case example because all 1,024 GB are restored to a Mac in one month. Harbor Protect's incremental backups may also store less than a full new terabyte each month.

Glacier restore sequence Deep Archive data must first be restored to a temporary online copy in AWS. Standard retrieval usually completes within 12 hours; Bulk can take up to 48 hours. After AWS marks the objects available, Harbor Protect can copy them back to the Mac.

Calculation details: S3 Standard storage = $1,024 \times \$0.026 \times 6$. Deep Archive storage = $1,024 \times \$0.002 \times 6$. Deep Archive Standard retrieval = $1,024 \times \$0.022$; Bulk retrieval = $1,024 \times \$0.0035$. Download = $(1,024 - 100 \text{ free GB}) \times \0.09 . The temporary copy estimate assumes one day at the S3 Standard rate: $1,024 \times \$0.026 \div 30$.

Actual bills vary with the AWS Region, number and size of files, PUT/GET/restore requests, temporary-copy duration, other monthly AWS data transfer, taxes, pricing changes, and the 40 KB metadata overhead per archived object. Deep Archive has a 180-day minimum storage duration. Use the AWS Pricing Calculator before committing large archives.

9. Use Dropbox or Google Drive as a destination

Harbor Protect does not connect to Dropbox or Google Drive directly. Each desktop app creates a folder that macOS can access. Harbor Protect treats a folder inside it as a Local Folder destination, and the sync app then uploads the copied files to the account.

Create and install Dropbox

1. Create an account at dropbox.com. Enter an email address, name, and password, accept the terms, and choose a suitable plan.
2. Download the Dropbox desktop app from dropbox.com/downloading and run the installer.
3. Sign in to the desktop app. Dropbox creates its synced location in Finder.
4. In the Dropbox folder, create a dedicated folder such as Harbor Protect Backups.

Select Dropbox in Harbor Protect

1. Open Harbor Protect's protection setup and choose Local Folder for the destination.
2. Select the dedicated Harbor Protect Backups folder inside Dropbox.
3. Save the Harbor Protect setup and run Analyze before the first protection run.
4. After the backup finishes, wait until Dropbox reports Up to date before disconnecting drives or shutting down the Mac.

How this works Harbor Protect first writes a normal local copy into the Dropbox folder. The Dropbox app performs the separate upload. Harbor Protect's Protected status confirms Harbor Protect's copy operation, not Dropbox's cloud upload status.

Capacity and availability The Mac needs enough local space for the files Harbor Protect writes. Keep the destination folder available in Finder and avoid selecting the same Dropbox folder as both source and destination.

Google Drive works the same way Google Drive for desktop also creates a synced folder that macOS can access. Point a Local Folder destination at a dedicated folder inside it and the same steps and notes above apply. This also works for the Pro secondary destination.

10. Backup behavior and previous versions

- Backups are incremental: new and modified files are copied; unchanged files are skipped.
- For local backups, files removed or replaced from the current source are retained under `_PreviousVersions` rather than immediately erased.
- For S3 backups, Harbor Protect uses a corresponding `_PreviousVersions` location.
- Common macOS metadata is excluded, including `.Spotlight-V100`, `.Trashes`, `.fsevents`, `.TemporaryItems`, `.DocumentRevisions-V100`, `.DS_Store`, and AppleDouble files.

Version history `_PreviousVersions` is a safety area, not a full cataloged version-control system. Check storage use periodically and keep an independent retention policy for critical work.

11. Troubleshooting

Problem	Likely cause	Action
Drive does not appear	It is not mounted or the list is stale	Confirm it appears in Finder, then select Refresh Drives
Save is disabled	A source or destination is incomplete	Assign a valid destination to every selected item
Attention status	Source/destination missing or run interrupted	Reconnect drives, run Analyze, and inspect Log
Source missing	Drive name/path changed or drive is disconnected	Reconnect the correct drive and verify the source path
S3 connection fails	Credentials, region, bucket, permissions, or network	Recheck fields and AWS access, then Test Connection
Bucket name rejected	Name is invalid or already owned	Use a more specific lowercase globally unique name
Backup stopped	Stop was selected or the process ended	Review Log and rerun; successful prior files remain
Restore could overwrite files	Original-location mode selected	Cancel and use Restore to New Location...

Problem	Likely cause	Action
Automatic Backups didn't run	Harbor Protect wasn't open at the scheduled time	Turn on Launch Harbor Protect at login in Automatic Backups
Automatic Backups / dual-destination greyed out	The active plan is Free or Standard	These are Pro features; open the plan name to upgrade
Archived Protection / Protection History locked	The active plan is Free	These are Standard features; open the plan name to upgrade
Amazon S3 option disabled	The active plan is Free	Amazon S3 requires Standard or Pro; open the plan name to upgrade
No Upgrade to Pro button	Pro isn't available for purchase yet	Standard remains the top available plan until Pro launches

Reset Harbor Protect

From the gear menu or setup window, select Reset Harbor Protect... Reset clears setup, Collections, backup order, and last-verified memory. It does not delete original files or backup files.

12. Recommended routine and glossary

A simple protection routine

1. Before a session, confirm required drives are connected and the dashboard has no Attention warnings.
2. After important work, run Analyze and review the preview.
3. Run Protect All and wait until the activity completes.
4. Confirm entries show Protected and check Log for skipped or failed items.
5. Regularly restore a representative project to a new location and open it in the DAW.

Glossary

Term	Meaning
Analyze	A dry-run comparison that does not copy or delete files.
Collection	Several related source folders protected and displayed as one project.

Term	Meaning
Destination	The local folder or S3 location that receives the backup.
Protect	Run a backup for one dashboard item.
Protect All	Run every configured item in the saved order.
Restore	Copy backup content into the original location, potentially overwriting matches.
Restore to New Location	Copy backup content to a separate recovery folder.
Verified	Harbor Protect's record that a backup job completed successfully.
Automatic Backups	Pro: runs Protect All on a set schedule without user action.
Dual-destination backup	Pro: keeps a second, independent copy of the whole plan at a second destination.
Version History	Pro: dated, restorable snapshots kept before each protection run.
Archive Protection	Standard: retires an item from the active list and Protect All without deleting its backup history.
Protection History	Standard: a searchable, plain-English record of past protection runs.

Appendix: Quick Reference

Fast lookup tables for every function, grouped the same way as the dashboard and setup windows. See the numbered chapters above for full explanations.

Dashboard functions

Function	What it is for
Get Started	Opens protection setup when Harbor Protect has no configured backup items.
Plan name (toolbar)	Shows the active plan — Free, Standard, or Pro — and opens the License window.
Gear menu	Opens drive and project setup, Automatic Backups, Previous Versions, Archived Protection, Protection History, License, or resets Harbor Protect's saved configuration.
Protection card	Represents one whole drive, project folder, or Collection and shows its current state.
Protect	Runs a backup for only the item shown on that card.
Analyze	Previews differences between sources and destinations without copying or deleting files.
Protect All	Runs all configured backup items in the saved backup order.
Restore	Opens the recovery window for Collections and individual backups.
Archived Protection (Standard)	Retires an item from the active list without deleting its backup history; view, restore, or remove it here.
Protection History (Standard)	Opens a searchable, plain-English record of every past protection run.
Previous Versions (Pro)	Opens dated, restorable snapshots for a protected item, not just its latest backup.
Automatic Backups... (Pro)	Opens the schedule for backups that run on their own, without user action.
Log	Shows activity, skipped items, completed operations, and error details for the current app session.
Stop	Ends the active analysis, backup, or restore operation.

Status and progress

Indicator	What it means
Ready	The item is configured but Harbor Protect has not recorded a successful backup yet.
Protected	The item's latest attempted backup completed successfully.
Syncing	Harbor Protect is currently processing the item.
Attention	A required source or destination is unavailable, or a previous run was interrupted.
Last verified	The time Harbor Protect last recorded a successful backup for the item.
Protection Confidence	The percentage of dashboard entries currently marked Protected.
Activity progress	Shows the current item, operation status, and overall run progress.

Protection setup functions

Function	What it is for
Default Destination	Sets the destination automatically assigned to new backup items.
Backup Order	Controls the sequence used when Protect All runs.
Whole Drives	Protects the contents of a selected external drive.
Specific Projects	Protects one selected project folder instead of an entire drive.
Collections	Groups related folders from one or more drives into a single dashboard item.
Add Folder as Collection	Creates a general Collection from a project and its related source folders.
Add DAW Session	Creates a Collection around a supported Pro Tools, Ableton Live, Logic Pro, or Studio One/Fender session.
Add Source Folder	Adds another required folder to an existing Collection.
Local Folder	Uses a folder that macOS can access as the backup destination.

Function	What it is for
Amazon S3	Uses an AWS S3 bucket as the off-site backup destination.
Secondary destination (Pro)	An optional second Local Folder or Amazon S3 destination applied plan-wide, for simple 3-2-1 protection.
Refresh Drives	Scans again for currently mounted external drives.
Save	Stores the selected sources, destinations, Collections, and backup order.
Reset Harbor Protect	Clears Harbor Protect's setup and verification memory without deleting source or backup files.

Restore functions

Function	What it is for
Restore	Copies one backup into its original source location. Matching files may be overwritten.
Restore All	Restores every source folder belonging to a Collection into its original locations.
Restore to New Location	Copies one backup into a separate folder without overwriting the original project.
Restore All to New Location	Copies all parts of a Collection into a separate recovery location.
Previous Versions (Pro)	Opens dated, restorable snapshots kept before each protection run, instead of only the latest backup.

Backup behavior

Behavior	Purpose
Incremental copying	Copies new and modified files without recopying unchanged files.
Dry-run analysis	Shows expected changes without modifying either side.
Previous versions	Moves replaced or source-deleted items into _PreviousVersions.

Behavior	Purpose
Metadata exclusions	Skips common macOS housekeeping items such as .DS_Store, .Trashes, and .Spotlight-V100.

Official setup references

- **Create an AWS account:** <https://aws.amazon.com/resources/create-account/>
- **Get started with Amazon S3:**
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/GetStartedWithS3.html>
- **AWS IAM access keys:** https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html
- **S3 Glacier storage classes:** <https://docs.aws.amazon.com/AmazonS3/latest/userguide/glacier-storage-classes.html>
- **Create a Dropbox account:** <https://help.dropbox.com/account-access/create-account>
- **Install the Dropbox desktop app:** <https://help.dropbox.com/installs/download-dropbox>